Abertay University

Penetration Test Final Report

Jack Sime – 1801476@uad.ac.uk

CMP210: Ethical Hacking 1

2020/21

.

Abstract

This paper is a final report detailing the outcomes and findings from a penetration test carried out on a network for Abertay University. The aim of the test was to identify any vulnerabilities to the network, evaluate the risk the potential vulnerabilities cause, test the vulnerabilities on the network and advise on any relevant solutions there may be to fix the discovered vulnerabilities.

The network was first scanned to locate the servers in question and gather information on them to aid the further testing. There were 2 tools were used to scan the networks which were advanced IP scanner and NMAP. An NMAP script was used to scan both server's TCP and UDP ports to provide useful information that will be relevant during further testing such as port information for both servers and information on operating systems that were currently in use on both systems.
Enumeration was then attempted on both systems with server 2 providing more information than on server 1. Multiple tools that were used were both Linux and Windows-based and included rpcclient, nbtstat, Nbtnum3.3, and Enum4linux. Attempted DNS zone transfers failed on both servers and rpcclient and Enum4linux both returned useful information from server 2. NBTNUM3.3 was successful on server 2 also when using the provided test login. NBTSTAT returned the NetBIOS table for both servers which revealed the registered hosts for both servers. Both servers were then scanned for vulnerabilities using both NMAP and Nessus. The initial NMAP vulnerability scan revealed a small number of vulnerabilities within both systems. They were both then scanned using the tool NESSUS which is designed for scanning and revealing exploitable issues and it revealed several critical and high-level issues within both servers that could be exploited to gain access to them, therefore, breaching the network. Armitage, which is a graphical front end used to manipulate both the abilities of Metasploit and NMAP, was then used to hack into both servers using an exploit in the operating system, that they both used, using a reverse connection to allow us to gain access. A meterpreter shell was then opened on both servers using another exploit known as shell_to and from the meterpreter shell system privileges were then able to be escalated and so passwords for both servers were able to be dumped while files and processes were visible along with allowing us to open a windows command prompt. Fgdump was also used to dump the account hashes from both servers and the hash cracking tool Cain was used to crack the dumped hashes using a dictionary attack with its Cain.txt file. Active directory explorer was then used with the cracked hashes to explore the active directories of accounts on the servers.

From the vulnerability scanning, a large number of potential exploits were found that were major security risks. Both servers were vulnerable in multiple ways and both were able to be exploited in a way that would seriously impact the network they were connected to. Server 2 was easier to exploit and gather information on compared to server 1. From our findings, it was concluded that a large amount of these vulnerabilities that were found have simple solutions that would improve the security of the network and could be solved by updating the operating system and programs on both systems.

.

+Contents

.

1 INTRODUCTION

1.1 BACKGROUND

Penetration testing is a method that is used to gain an idea of the level of security that an IT system has and to develop an idea of the level of vulnerability assessment and management that the client has through the use of tools that would generally available to anyone who was to attempt to exploit the IT system. A penetration test is a chance for you to evaluate the quality of you or your team's ability to find vulnerabilities in your systems and manage them to make your system secure from these external attacks. (National Cyber Security Centre, 2017)
The area of penetration testing is becoming more and more essential as the modern world progresses further with its use of technology. Most devices these days come with internet capabilities and operating systems and with those capabilities comes the problem of the security of those devices. From May 2019-2020 up to around 88% of all businesses within the UK have suffered data breaches and these breaches can end up costing companies millions of pounds and can affect customer relations as they may not feel safe using that service or product. (Swinhoe, 2020). One example of this was Adobe back in 2013 when it was breached and as a result of that, over 38 million user logins and passwords were stolen from their databases. (BBC News, 2013). Without penetration testers, there would be no benchmark to test your organisation's vulnerability identification and management methodology and no way to effectively evaluate if your methods are working until it's eventually too late and you suffer a breach. This work allows an independent company to come and perform tests into your systems and provides the client with useful information on any potential breaches along with potentially better methodologies to identify and sort these problems in the future. Penetration testing focuses on the aspects of hardware and software of a system along with the people that have access to such systems. Testers will use a mix of testing the physical Hardware and software in use but will also test staff to identify any social engineering opportunities. Social engineering is a method that the testers may use that aims to gain information by tricking someone into releasing certain info that would benefit them in their test. (Symanovich, 2018). Testing can safeguard clients against breaches that would otherwise result in big financial losses and can identify where staff training may be required to reaffirm security protocols (Krebs, 2016). There are 3 different methods of testing that are carried out, White-Box which is when the testers are given all the information on their target system, Black-Box which is when the testers are given no information on their target system and then Grey-Box which is a middle ground and testers are given some information on the target system but not all the information. (Shebli and Beheshti, 2018). Different testing companies will all have different testing methodology's, that have been planned out and tested using select tools, that they will follow but in general should meet similar conclusions if they all test the same base factors. The testing and evaluation of these factors are vital to be able to keep systems secure and to provide customers with the satisfaction that their data is safe and that the device or software that they may be using is also safe.

1.2 AIM

The aim of this project was to test and evaluate the network provided by the client, Abertay University, and produce a report detailing the errors found along with solutions to them.

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

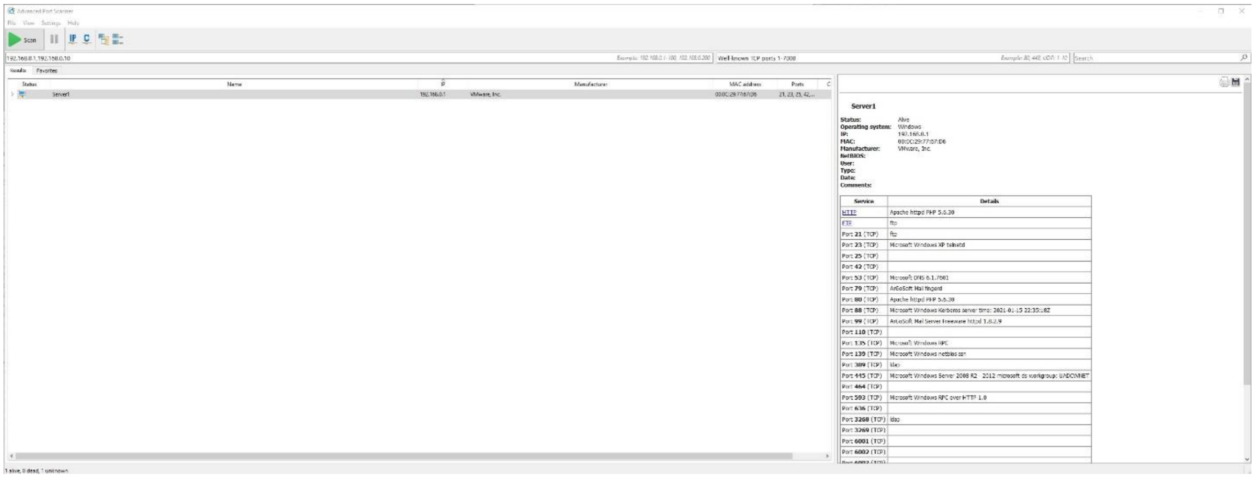
From the start to the finish of the test followed in this report a plan was followed which involved both systems being scanned followed by then both being enumerated using several tools to achieve this. After the first two steps, both systems were then scanned again for vulnerabilities based on the information gathered in the initial scanning phase. From the vulnerability scanning phase, the info gathered was then used in the next phase which is system hacking. In this stage, more tools were used to exploit the different vulnerabilities found in both systems.

The scanning section was started by using the advanced IP Scanner tool, shown in figure 1, to ensure both of the target servers were on and running along with providing information on the ports from both servers. Following on from there, NMAP was then used to again scan the 2 servers for both TCP and UDP ports along with each of the servers operating systems. The NMAP scan was run using a script, shown in figure 2, to allow for all tests to be run consecutively and results were outputted to text documents after each test. TCP ports 1-6000 were scanned for both servers while ports 1-500 were scanned for UDP on both of the servers.

After scanning was the enumeration phase, all tests were run individually on each system, using the test account where login details were required, and started with an attempt to transfer DNS zones which can reveal DNS records when misconfigured (Nidecki, 2019). After the attempted DNS transfers the tool rpcclient was then used from a Linux system to enumerate with the testing account we had been given. Enum4linux was used following on from rpcclient using the -a switch which runs all the simple enumerations such as getting the user-list and group and member lists. The information gathered was again printed in a text document for further use. NBTenum3.3 was then used on the target servers to return a formatted webpage detailing Group and User info along with administrator account names.

Now that both the systems had been enumerated as far as they could the next step was to once again scan both systems but for vulnerabilities. NMAP was used again to scan for vulnerabilities using a different script that was provided with NMAP and these results were once again outputted to a text file to be examined. A more in-depth and comprehensive vulnerability scan was then performed using the tool Nessus along with the test account details that were provided. Using Nessus, a basic network scan was selected, and the IP's of both systems were input as targets. The testing credentials were then added along with the domain that was being worked in. After the scan, a pdf report was made detailing the vulnerabilities found.

The Final process was system hacking where the exploits are now exploited. Armitage was used at first to exploit both systems. An exploit known as ms17_010_eternalblue using a reverse connection was used against both systems to gain a command prompt on the systems. Another exploit known as shell_to_meterpreter was used to gain access to a meterpreter shell on the systems. From there the system processes were accessed and used to escalate privileges on the system to allow for hashes to be dumped using the meterpreter interface using the wdigest method and registry through the access menu. Files on both systems were also available to be explored through meterpreter. The hashes for both systems were then dumped again using fgdump which dumped both systems hashes into text files ready for them to be cracked. Two programs were used to crack the hashes that were dumped. Cain was used first, and a dictionary attack was used with the dictionary being the cain.txt file that's included with the software. This was attempted on both servers dumped hashes. The dumped hashes were then used with rcrack_mt in an attempt to use rainbow tables instead of the already tried dictionary attack to crack some of the hashes. The rainbow table that was chosen was ntlmmixalphanumericspace1-7 available from https://freerainbowtables.com/. Active directory explorer was used against the servers along with the test account details given in order to search through the directories on the systems. After connecting to the systems, a search using AD explorer was done that would search for any descriptions on the systems that were not empty. This was the final step of the process and now the results found from each step along with details that were discovered will be further explored in the subsections below.



192.168.0.1,192.168.0.10

Well-known TCP ports 1-7000

Status	Name	IP	Manufacturer	MAC address	Ports
	Server1	192.168.0.1	VMware, Inc.	00:0C:29:77:67:D6	21, 23, 25, 42,...

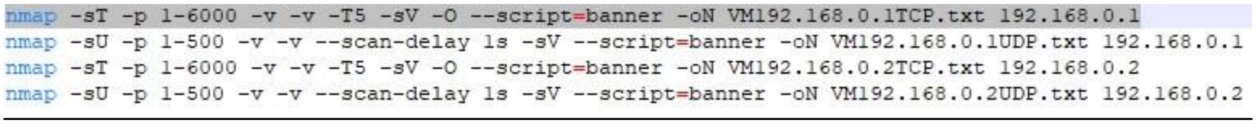
Server1

Status: Alive
Operating system: Windows
IP: 192.168.0.1
MAC: 00:0C:29:77:67:D6
Manufacturer: VMware, Inc.
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
HTTP	Apache httpd PHP 5.6.30
FTP	ftp
Port **21** (TCP)	ftp
Port **23** (TCP)	Microsoft Windows XP telnetd
Port **25** (TCP)	
Port **42** (TCP)	
Port **53** (TCP)	Microsoft DNS 6.1.7601
Port **79** (TCP)	ArGoSoft Mail fingerd
Port **80** (TCP)	Apache httpd PHP 5.6.30
Port **88** (TCP)	Microsoft Windows Kerberos server time: 2021-01-15 22:35:18Z
Port **99** (TCP)	ArGoSoft Mail Server Freeware httpd 1.8.2.9
Port **110** (TCP)	
Port **135** (TCP)	Microsoft Windows RPC
Port **139** (TCP)	Microsoft Windows netbios ssn
Port **389** (TCP)	ldap
Port **445** (TCP)	Microsoft Windows Server 2008 R2 - 2012 microsoft ds workgroup: UADCWNET
Port **464** (TCP)	
Port **593** (TCP)	Microsoft Windows RPC over HTTP 1.0
Port **636** (TCP)	
Port **3268** (TCP)	ldap
Port **3269** (TCP)	
Port **6001** (TCP)	
Port **6002** (TCP)	

1 alive, 0 dead, 1 unknown

Figure 1: Interface from Advanced Port Scanner



```
nmap -sT -p 1-6000 -v -v -T5 -sV -O --script=banner -oN VM192.168.0.1TCP.txt 192.168.0.1
nmap -sU -p 1-500 -v -v --scan-delay 1s -sV --script=banner -oN VM192.168.0.1UDP.txt 192.168.0.1
nmap -sT -p 1-6000 -v -v -T5 -sV -O --script=banner -oN VM192.168.0.2TCP.txt 192.168.0.2
nmap -sU -p 1-500 -v -v --scan-delay 1s -sV --script=banner -oN VM192.168.0.2UDP.txt 192.168.0.2
```

Figure 2: Script used to run NMAP scan

2.2 SCANNING RESULTS

From the scanning phase, we found that both servers had apache servers running and server 1 is an email server due to both TCP ports 25 and 110 were open. These systems are both DNS servers also due to port 53 being open on them both in both TCP and UDP. The operating system of both systems was revealed, and they were both running Windows Server 2008 R2 Sp1. The complete scan finding will be included in Appendices A and B.

2.3 ENUMERATION RESULTS

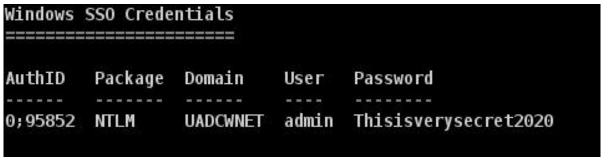
After the enumeration stage, we found the testing details provided were only valid on server 2 and so any test that required login details for the server simply failed on server 1. From the scanning, it was known that both servers were DNS and so a zone transfer was attempted on both systems which failed on both systems. Rpcclient was then used and returned information on both built-in and domain groups and was used to query the user 500 which returned the admin account name which was Administrator. Enum4linux was then used to further enumerate both servers but as the login details required do not work with server 1 information gathered for that server was limited. A script was used to run enum4linux on both servers with the -a switch used. The script returned basic information for server 1 such as the domain and the NBTstat info. This information was also returned for server 2 but with added information including domain and built-in groups and the memberships belonging to these groups relating to the users on server 2. Shares on server 2 were also enumerated through enum4linux along with the suspected password policy for the domain. NBTnum3.3 was used to enumerate both servers but without valid logins for server 1 information gathered for that system was minimal. Server 2 returned much of the data previously returned through other tools but thanks to nbtnum3.3 its returned in a formatted HTML page revealing all the domain admins, computers, and users among other details. The information gathered from these tools set up a firm base to proceed onto the next step of testing. Copies of enumeration documents will be available in appendices C-E.

2.4 VULNERABILITY SCANNING RESULTS

During the Vulnerability scanning phase, NMAP was used again to scan both servers but they were scanned for vulnerabilities during this scan. This scan revealed that both servers were vulnerable to a slowloris DOS attack which affects HTTP servers. This was the only major vulnerability that NMAP was able to find during its scans. This initial scan was followed up using the tool Nessus which returned a much more comprehensive report on the vulnerabilities on both systems. As both systems used the same OS, both servers had similar vulnerabilities that related to that operating system. The vulnerabilities of MS11-030 (Microsoft Security Bulletin MS11-030 - Critical, 2011) and MS11-058 (Microsoft Security Bulletin MS11-058 - Critical, 2011) both relate to DNS and could both be exploited on the servers to allow for remote code execution to occur. Both servers were also running unsupported versions on Windows and PHP and both servers were affected by a further DNS exploit that would once again allow for remote code to be executed. Both the NMAP report and the Nessus report detailing only the critical and high vulnerabilities will be available in the Appendices F &G.

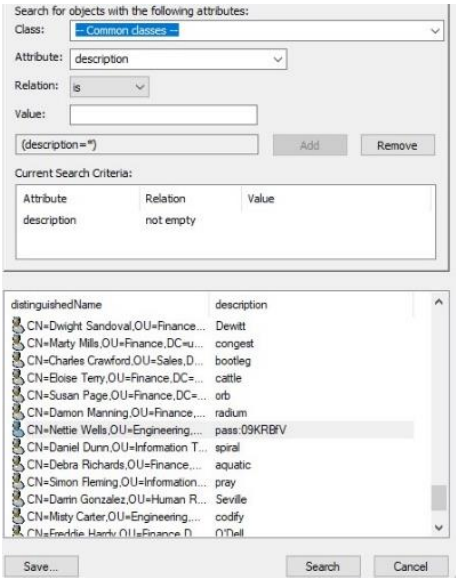
2.5 SYSTEM HACKING RESULTS

Using the information gathered in the last stage the vulnerabilities were then exploited. An exploit known as ms17_010_eternalblue that exploited vulnerability MS17-010 (Microsoft Security Bulletin MS17-010 - Critical, 2017) was used against both systems along with a meterpreter shell through the program known as Armitage, from there we were able to escalate our privileges. The escalated privileges were then used to dump hashes from both systems in an attempt to crack them. When the hashes were dumped using the wdigest method from a meterpreter shell, an admin password was revealed in plain text shown in figure 3. Fgdump was then used to further dump all the passwords from both systems using the admin details that had been discovered from the use of Armitage. The dumped lists were cracked using Cain with its included cain.txt document as the dictionary and 10 passwords were successfully cracked from Server2 as seen in figure 4 while none of the Server1 users were cracked. Rainbow table cracking through rcrack_mt using the ntlmmixalphanumericspace1-7 table resulted in zero cracked hashes. Active directory explorer was used on both servers and from the search of the descriptions in the directories a password was found stored in a directory for the user Nettie Wells. The password was in the description in plain text as you can see in figure 5.



```
Windows SSO Credentials
=======================

AuthID   Package  Domain    User   Password
------   -------  ------    ----   --------
0;95852  NTLM     UADCWNET  admin  Thisisverysecret2020
```

Figure 3: Admin password in plain text dumped from meterpreter



Search for objects with the following attributes:

Class: -- Common classes --

Attribute: description

Relation: is

Value:

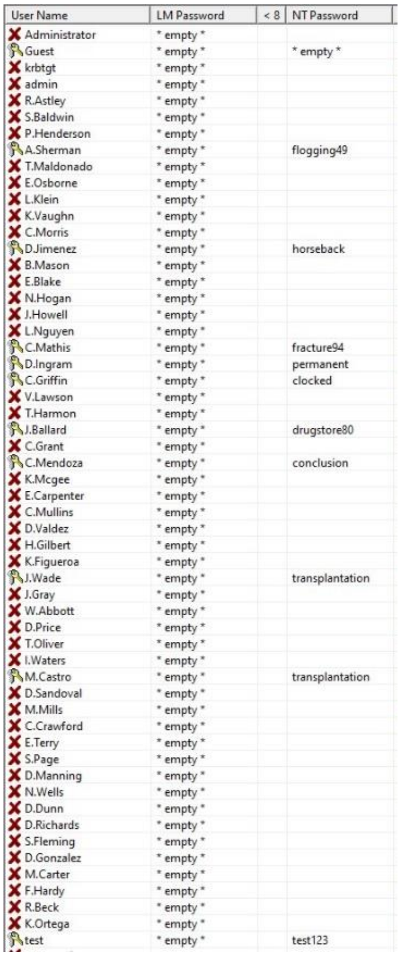
(description=*)

Current Search Criteria:

Attribute	Relation	Value
description	not empty	

distinguishedName	description
CN=Dwight Sandoval,OU=Finance...	Dewitt
CN=Marty Mills,OU=Finance,DC=u...	congest
CN=Charles Crawford,OU=Sales,D...	bootleg
CN=Eloise Terry,OU=Finance,DC=...	cattle
CN=Susan Page,OU=Finance,DC=...	orb
CN=Damon Manning,OU=Finance,...	radium
CN=Nettie Wells,OU=Engineering,...	pass:09KRBfV
CN=Daniel Dunn,OU=Information T...	spiral
CN=Debra Richards,OU=Finance,...	aquatic
CN=Simon Fleming,OU=Information...	pray
CN=Darrin Gonzalez,OU=Human R...	Seville
CN=Misty Carter,OU=Engineering,...	codify
CN=Freddie Hardy,OU=Finance,D...	O'Dell

Figure 5: Password for user N.Wells found in account description



User Name	LM Password	< 8	NT Password
Administrator	* empty *		
Guest	* empty *		* empty *
krbtgt	* empty *		
admin	* empty *		
R.Astley	* empty *		
S.Baldwin	* empty *		
P.Henderson	* empty *		
A.Sherman	* empty *		flogging49
T.Maldonado	* empty *		
E.Osborne	* empty *		
L.Klein	* empty *		
K.Vaughn	* empty *		
C.Morris	* empty *		
D.Jimenez	* empty *		horseback
B.Mason	* empty *		
E.Blake	* empty *		
N.Hogan	* empty *		
J.Howell	* empty *		
L.Nguyen	* empty *		
C.Mathis	* empty *		fracture94
D.Ingram	* empty *		permanent
C.Griffin	* empty *		clocked
V.Lawson	* empty *		
T.Harmon	* empty *		
J.Ballard	* empty *		drugstore80
C.Grant	* empty *		
C.Mendoza	* empty *		conclusion
K.Mcgee	* empty *		
E.Carpenter	* empty *		
C.Mullins	* empty *		
D.Valdez	* empty *		
H.Gilbert	* empty *		
K.Figueroa	* empty *		
J.Wade	* empty *		transplantation
J.Gray	* empty *		
W.Abbott	* empty *		
D.Price	* empty *		
T.Oliver	* empty *		
I.Waters	* empty *		
M.Castro	* empty *		transplantation
D.Sandoval	* empty *		
M.Mills	* empty *		
C.Crawford	* empty *		
E.Terry	* empty *		
S.Page	* empty *		
D.Manning	* empty *		
N.Wells	* empty *		
D.Dunn	* empty *		
D.Richards	* empty *		
S.Fleming	* empty *		
D.Gonzalez	* empty *		
M.Carter	* empty *		
F.Hardy	* empty *		
R.Beck	* empty *		
K.Ortega	* empty *		
test	* empty *		test123

Figure 4: Cain cracked password list from server2

3 DISCUSSION

3.1 GENERAL DISCUSSION

From the testing and results above it's clear to see that both systems suffer from extreme security risks that could jeopardise the network. Several issues are related to the operating system of the machines, both systems are running out of date and unsupported versions of the operating system that have had updates to fix issues, along with the actual software installed and running on them with some of that software also being out of date and unsupported. Unsupported software is dangerous as it does not receive any relevant security updates if and when the developers find them. These issues created extreme risks as they allowed the tester to gain access to both of the systems and allowed them to be hijacked and then potentially used to disrupt the network or those that use it. Both systems had their DNS configured and set up correctly and so a DNS zone transfer couldn’t be done. Server 2 was the more vulnerable of the two as the login details given worked on only that server and so enumeration on the system was much more thorough and revealed information that wouldn’t have been available on server 1. From the active directory, a password was able to be found on server 2, information as sensitive as passwords shouldn’t be stored in the description on accounts and provided a very simple access point into another system account. From the use of the Armitage program and a meterpreter shell, an admin account password was obtained and would’ve provided access to the most sensitive areas of the network and would result in major problems for the network. The aim of this report was met as the network was tested and evaluated in terms of its security and a report was created detailing the problems within the network. The testing was completed within the client's timeline and returned a complied report on issues that the client's security evaluation team can act on and use as a training and evaluation tool. The tests carried out were done with tools that most competent computer users would have access to and provides a real test to the network to simulate a member of the public trying to break in. This is useful as it shows how dangerous these vulnerabilities can be too widely available exploits and displays to clients the importance of the network security.

3.2 Countermeasures

The vulnerabilities found in this report can mostly be solved by updating the software and operating systems not only to modern versions but too supported versions that will receive relevant security updates as problems are found by the manufacturer or developer. This is most important when the vulnerabilities are from the operating system and having security flaws within an OS can allow the system in question to be extremely vulnerable (Davis, 2017). Having network admins keeping systems up to date ensures that systems are protected once again by manufacturer's updates and are usually the safest way to protect against any exploits. Ensuring that sensitive data such as passwords aren't stored in easily accessed places is essential to avoid giving an attacker an easy access route in the system and ensuring that systems are configured correctly can slow down an attacker and limit their avenues of approach. Good password policies could help slow down an attacker if they are able to dump some hashes from the system as more complex passwords take longer to crack and using several words relating more to a password sentence than a word can increase the chance that the passwords are unable to be cracked (Password policy: updating your approach, 2018).

3.3 Future Work

Given more time on these systems, further exploits could have been exploited using some of the lower-tiered threats, and server 1 could have been further enumerated using the extra account details that were found during the system hacking stage on server 2 and could have resulted in more opportunities to exploit server 1 as more information would have been available and may have resulted in more threats to the system being found. In future work the same mythology would be followed and moving through each process individually and building a good database of information and problems allows for further information gathering later in the test and avoids wasted time.

REFERENCES

Ncsc.gov.uk. 2017. *Penetration Testing*. [online] Available at: <https://www.ncsc.gov.uk/guidance/penetration-testing> [Accessed 15 January 2021].

Swinhoe, D., 2020. *UK Cybersecurity Statistics You Need To Know*. [online] CSO Online. Available at: <https://www.csoonline.com/article/3440069/uk-cybersecurity-statistics-you-need-to-know.html> [Accessed 15 January 2021].

BBC News. 2013. *Adobe Hack: At Least 38 Million Accounts Breached*. [online] Available at: <https://www.bbc.co.uk/news/technology-24740873> [Accessed 15 January 2021].

Symanovich, S., 2018. *What Is Social Engineering? Tips To Help Avoid Becoming A Victim*. [online] Us.norton.com. Available at: <https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html#:~:text=Social%20engineering%20is%20the%20act,natural%20tendencies%20and%20emotional%20reactions.> [Accessed 15 January 2021].

Krebs, B., 2016. *Adobe Fined $1M In Multistate Suit Over 2013 Breach; No Jail For Spamhaus Attacker — Krebs On Security*. [online] Krebsonsecurity.com. Available at: <https://krebsonsecurity.com/2016/11/adobe-fined-1m-in-multistate-suit-over-2013-breach-no-jail-for-spamhaus-attacker/> [Accessed 15 January 2021].

Shebli, H. and Beheshti, B., 2018. *A Study On Penetration Testing Process And Tools - IEEE Conference Publication*. [online] Ieeexplore.ieee.org. Available at: <https://ieeexplore.ieee.org/abstract/document/8378035/authors#authors> [Accessed 15 January 2021].

Nidecki, T., 2019. What Are DNS Zone Transfers. [Blog] *acunetix*, Available at: <https://www.acunetix.com/blog/articles/dns-zone-transfers-axfr/#:~:text=A%20DNS%20zone%20is%20a,also%20be%20a%20separate%20zone.> [Accessed 17 January 2021].

Docs.microsoft.com. 2011. *Microsoft Security Bulletin MS11-030 - Critical*. [online] Available at: <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-030> [Accessed 17 January 2021].

Docs.microsoft.com. 2011. *Microsoft Security Bulletin MS11-058 - Critical*. [online] Available at: <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-058> [Accessed 17 January 2021].

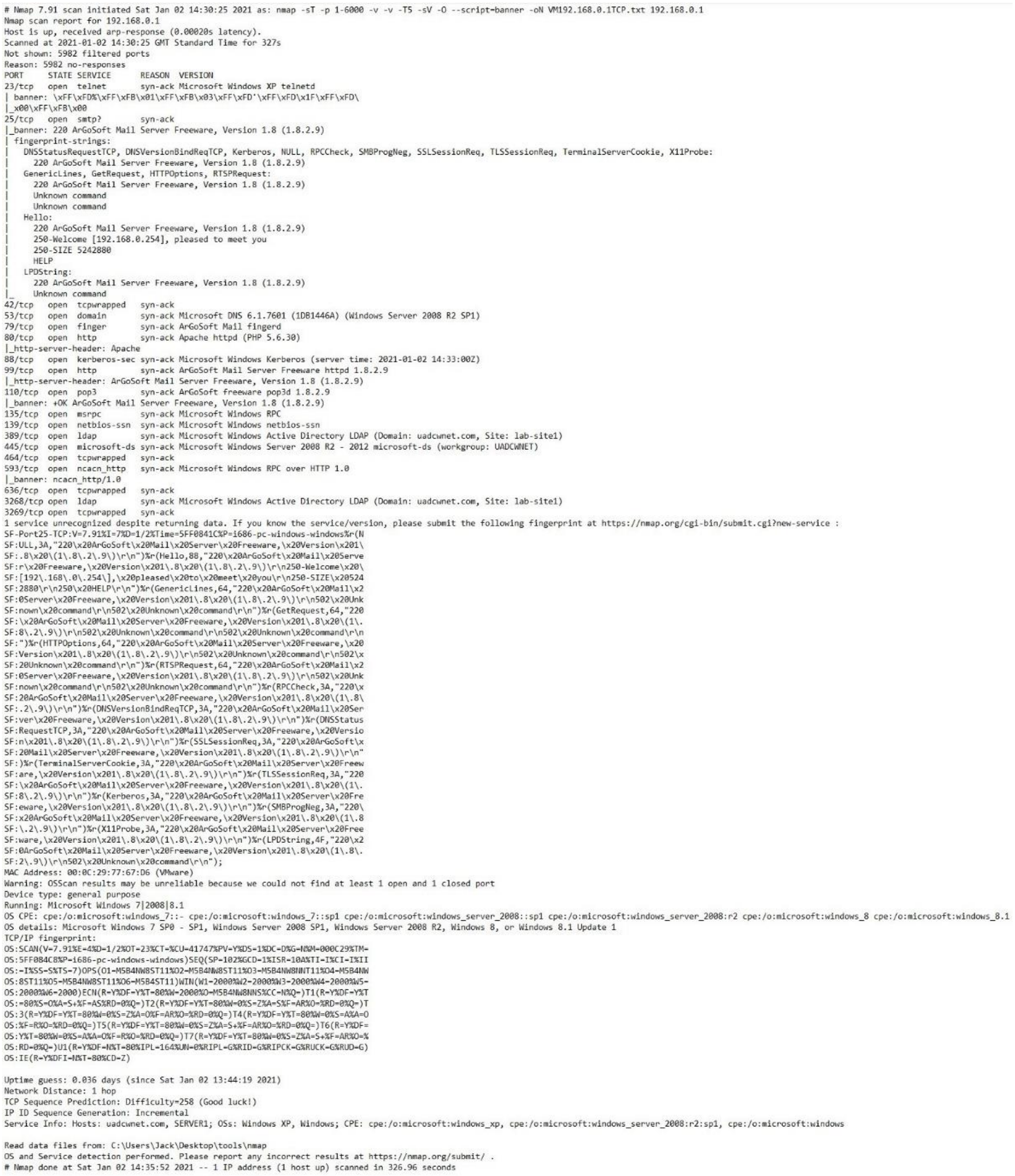
Docs.microsoft.com. 2017. *Microsoft Security Bulletin MS17-010 - Critical*. [online] Available at: <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010> [Accessed 17 January 2021].

Davis, G., 2017. Why Software Updates Are So Important. [Blog] *McAfee Consumer Threat Notices*, Available at: <https://www.mcafee.com/blogs/consumer/consumer-threat-notices/software-updates-important/> [Accessed 17 January 2021].

Ncsc.gov.uk. 2018. *Password Policy: Updating Your Approach*. [online] Available at: <https://www.ncsc.gov.uk/collection/passwords/updating-your-approach> [Accessed 17 January 2021].

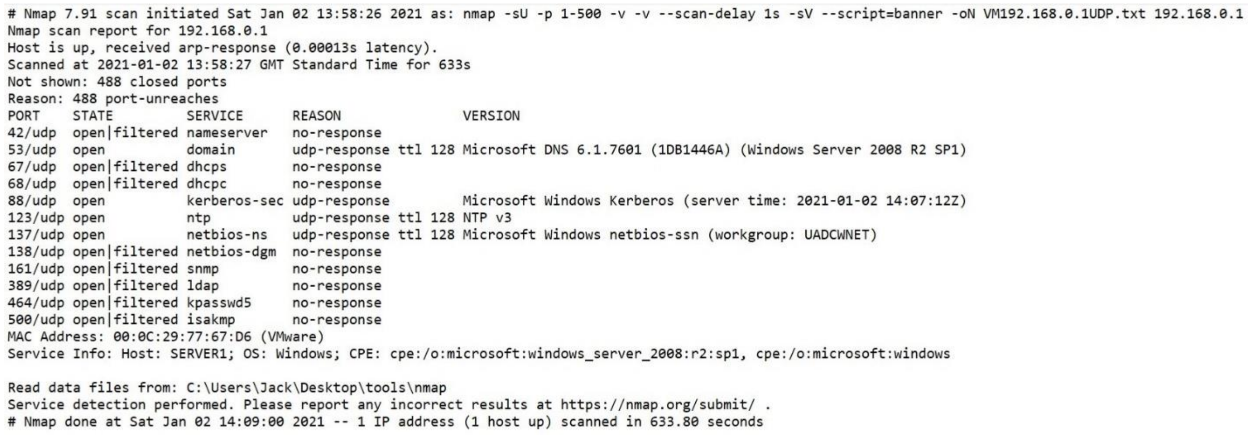
APPENDICES

APPENDIX A



```
# Nmap 7.91 scan initiated Sat Jan 02 14:30:25 2021 as: nmap -sT -p 1-6000 -v -v -T5 -sV -O --script-banner -oN VM192.168.0.1TCP.txt 192.168.0.1
Nmap scan report for 192.168.0.1
Host is up, received arp-response (0.00020s latency).
Scanned at 2021-01-02 14:30:25 GMT Standard Time for 327s
Not shown: 5982 filtered ports
Reason: 5982 no-responses
PORT     STATE SERVICE      REASON  VERSION
23/tcp   open  telnet       syn-ack Microsoft Windows XP telnetd
| banner: \xFF\xFD%\xFF\xFB\x01\xFF\xFB\x03\xFF\xFD'\xFF\xFD\x1F\xFF\xFD\
|_x00\xFF\xFB\x00
25/tcp   open  smtp?        syn-ack
|_banner: 220 ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Kerberos, NULL, RPCCheck, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie, X11Probe:
|     220 ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
|   GenericLines, GetRequest, HTTPOptions, RTSPRequest:
|     220 ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
|     Unknown command
|     Unknown command
|   Hello:
|     220 ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
|     250-Welcome [192.168.0.254], pleased to meet you
|     250-SIZE 5242880
|     HELP
|   LPDString:
|     220 ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
|_    Unknown command
42/tcp   open  tcpwrapped   syn-ack
53/tcp   open  domain       syn-ack Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
79/tcp   open  finger       syn-ack ArGoSoft Mail fingerd
80/tcp   open  http         syn-ack Apache httpd (PHP 5.6.30)
|_http-server-header: Apache
88/tcp   open  kerberos-sec syn-ack Microsoft Windows Kerberos (server time: 2021-01-02 14:33:00Z)
99/tcp   open  http         syn-ack ArGoSoft Mail Server Freeware httpd 1.8.2.9
|_http-server-header: ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
110/tcp  open  pop3         syn-ack ArGoSoft freeware pop3d 1.8.2.9
|_banner: +OK ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
135/tcp  open  msrpc        syn-ack Microsoft Windows RPC
139/tcp  open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
389/tcp  open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)
445/tcp  open  microsoft-ds syn-ack Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: UADCWNET)
464/tcp  open  tcpwrapped   syn-ack
593/tcp  open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
|_banner: ncacn_http/1.0
636/tcp  open  tcpwrapped   syn-ack
3268/tcp open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)
3269/tcp open  tcpwrapped   syn-ack
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-Port25-TCP:V=7.91%I=7%D=1/2%Time=5FF0841C%P=i686-pc-windows-windows%r(N
SF:ULL,3A,"220\x20ArGoSoft\x20Mail\x20Server\x20Freeware,\x20Version\x201\
SF:.8\x20\(1\.8\.2\.9\)\r\n")%r(Hello,88,"220\x20ArGoSoft\x20Mail\x20Serve
SF:r\x20Freeware,\x20Version\x201\.8\x20\(1\.8\.2\.9\)\r\n250-Welcome\x20\
SF:[192\.168\.0\.254\],\x20pleased\x20to\x20meet\x20you\r\n250-SIZE\x20524
SF:2880\r\n250\x20HELP\r\n")%r(GenericLines,64,"220\x20ArGoSoft\x20Mail\x2
SF:0Server\x20Freeware,\x20Version\x201\.8\x20\(1\.8\.2\.9\)\r\n502\x20Unk
SF:nown\x20command\r\n502\x20Unknown\x20command\r\n")%r(GetRequest,64,"220
SF:\x20ArGoSoft\x20Mail\x20Server\x20Freeware,\x20Version\x201\.8\x20\(1\.
SF:8\.2\.9\)\r\n502\x20Unknown\x20command\r\n502\x20Unknown\x20command\r\n
SF:")%r(HTTPOptions,64,"220\x20ArGoSoft\x20Mail\x20Server\x20Freeware,\x20
SF:Version\x201\.8\x20\(1\.8\.2\.9\)\r\n502\x20Unknown\x20command\r\n502\x
SF:20Unknown\x20command\r\n")%r(RTSPRequest,64,"220\x20ArGoSoft\x20Mail\x2
SF:0Server\x20Freeware,\x20Version\x201\.8\x20\(1\.8\.2\.9\)\r\n502\x20Unk
SF:nown\x20command\r\n502\x20Unknown\x20command\r\n")%r(RPCCheck,3A,"220\x
SF:20ArGoSoft\x20Mail\x20Server\x20Freeware,\x20Version\x201\.8\x20\(1\.8\
SF:.2\.9\)\r\n")%r(DNSVersionBindReqTCP,3A,"220\x20ArGoSoft\x20Mail\x20Ser
SF:ver\x20Freeware,\x20Version\x201\.8\x20\(1\.8\.2\.9\)\r\n")%r(DNSStatus
SF:RequestTCP,3A,"220\x20ArGoSoft\x20Mail\x20Server\x20Freeware,\x20Versio
SF:n\x201\.8\x20\(1\.8\.2\.9\)\r\n")%r(SSLSessionReq,3A,"220\x20ArGoSoft\x
SF:20Mail\x20Server\x20Freeware,\x20Version\x201\.8\x20\(1\.8\.2\.9\)\r\n"
SF:)%r(TerminalServerCookie,3A,"220\x20ArGoSoft\x20Mail\x20Server\x20Freew
SF:are,\x20Version\x201\.8\x20\(1\.8\.2\.9\)\r\n")%r(TLSSessionReq,3A,"220
SF:\x20ArGoSoft\x20Mail\x20Server\x20Freeware,\x20Version\x201\.8\x20\(1\.
SF:8\.2\.9\)\r\n")%r(Kerberos,3A,"220\x20ArGoSoft\x20Mail\x20Server\x20Fre
SF:eware,\x20Version\x201\.8\x20\(1\.8\.2\.9\)\r\n")%r(SMBProgNeg,3A,"220\
SF:x20ArGoSoft\x20Mail\x20Server\x20Freeware,\x20Version\x201\.8\x20\(1\.8
SF:\.2\.9\)\r\n")%r(X11Probe,3A,"220\x20ArGoSoft\x20Mail\x20Server\x20Free
SF:ware,\x20Version\x201\.8\x20\(1\.8\.2\.9\)\r\n")%r(LPDString,4F,"220\x2
SF:0ArGoSoft\x20Mail\x20Server\x20Freeware,\x20Version\x201\.8\x20\(1\.8\.
SF:2\.9\)\r\n502\x20Unknown\x20command\r\n");
MAC Address: 00:0C:29:77:67:D6 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=1/2%OT=23%CT=%CU=41747%PV=Y%DS=1%DC=D%G=N%M=000C29%TM=
OS:5FF084C8%P=i686-pc-windows-windows)SEQ(SP=102%GCD=1%ISR=10A%TI=I%CI=I%II
OS:=I%SS=S%TS=7)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW
OS:8ST11%O5=M5B4NW8ST11%O6=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=
OS:2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T
OS:=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T
OS:3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O
OS:%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=
OS:Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%
OS:RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
OS:IE(R=Y%DFI=N%T=80%CD=Z)

Uptime guess: 0.036 days (since Sat Jan 02 13:44:19 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Hosts: uadcwnet.com, SERVER1; OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Read data files from: C:\Users\Jack\Desktop\tools\nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jan 02 14:35:52 2021 -- 1 IP address (1 host up) scanned in 326.96 seconds
```

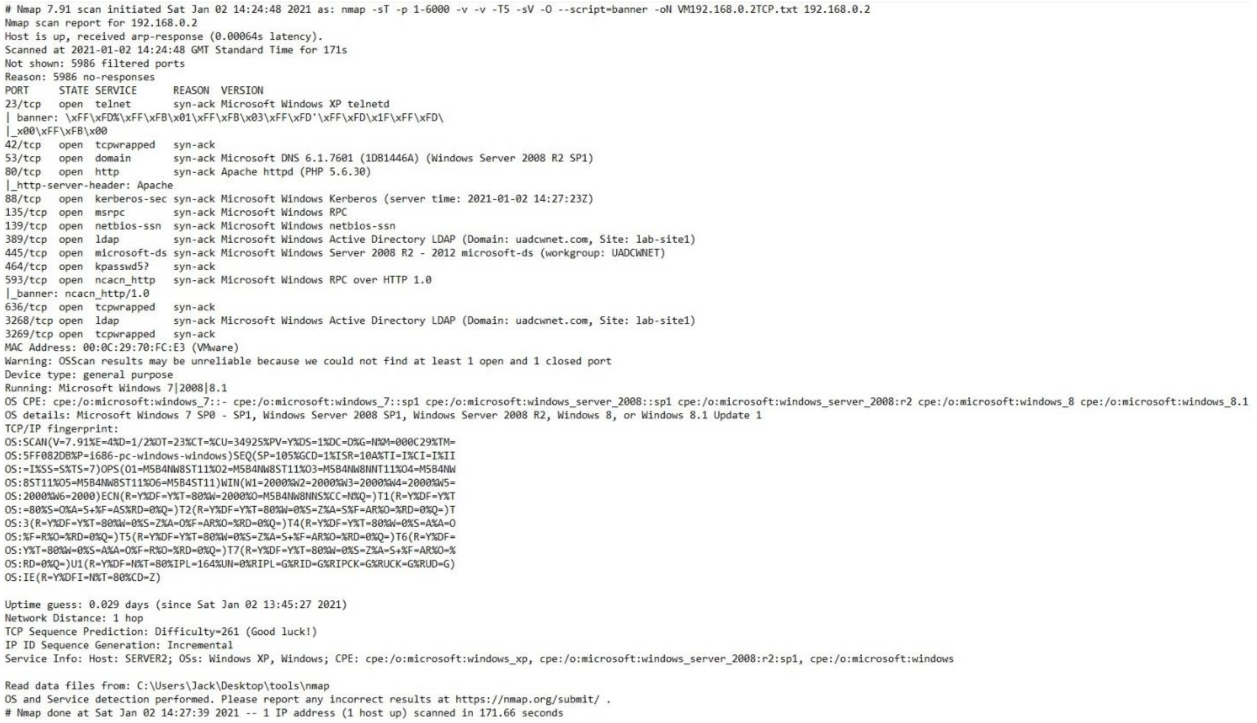
Appendix A1: NMAP Scan from server 1 TCP Ports



```
# Nmap 7.91 scan initiated Sat Jan 02 13:58:26 2021 as: nmap -sU -p 1-500 -v -v --scan-delay 1s -sV --script=banner -oN VM192.168.0.1UDP.txt 192.168.0.1
Nmap scan report for 192.168.0.1
Host is up, received arp-response (0.00013s latency).
Scanned at 2021-01-02 13:58:27 GMT Standard Time for 633s
Not shown: 488 closed ports
Reason: 488 port-unreaches
PORT    STATE         SERVICE      REASON              VERSION
42/udp  open|filtered nameserver   no-response
53/udp  open          domain       udp-response ttl 128 Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
67/udp  open|filtered dhcps        no-response
68/udp  open|filtered dhcpc        no-response
88/udp  open          kerberos-sec udp-response         Microsoft Windows Kerberos (server time: 2021-01-02 14:07:12Z)
123/udp open          ntp          udp-response ttl 128 NTP v3
137/udp open          netbios-ns   udp-response ttl 128 Microsoft Windows netbios-ssn (workgroup: UADCWNET)
138/udp open|filtered netbios-dgm  no-response
161/udp open|filtered snmp         no-response
389/udp open|filtered ldap         no-response
464/udp open|filtered kpasswd5     no-response
500/udp open|filtered isakmp       no-response
MAC Address: 00:0C:29:77:67:D6 (VMware)
Service Info: Host: SERVER1; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Read data files from: C:\Users\Jack\Desktop\tools\nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jan 02 14:09:00 2021 -- 1 IP address (1 host up) scanned in 633.80 seconds
```

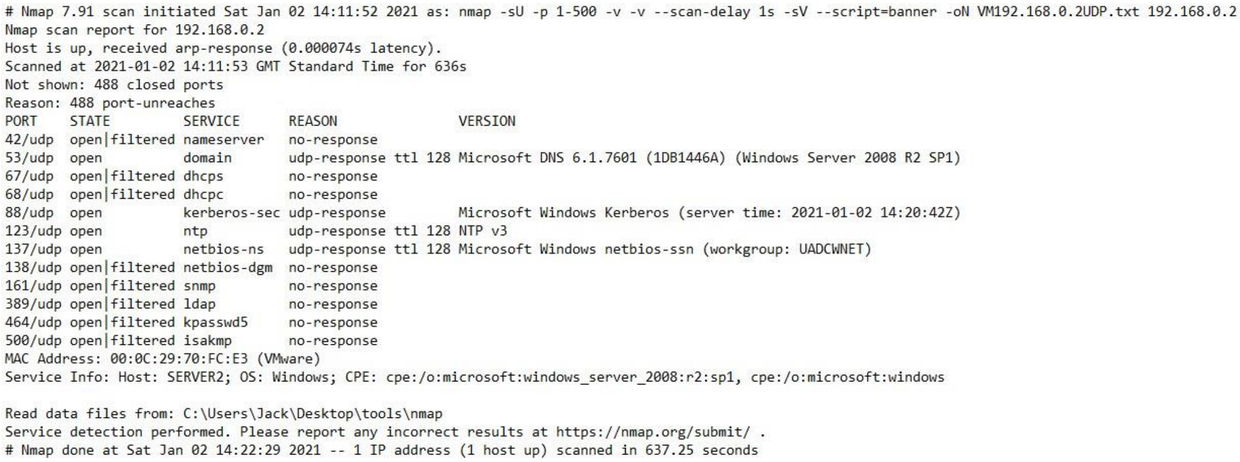
Appendix A2: NMAP Scan from server 1 UDP Ports

APPENDIX B



```
# Nmap 7.91 scan initiated Sat Jan 02 14:24:48 2021 as: nmap -sT -p 1-6000 -v -v -T5 -sV -O --script=banner -oN VM192.168.0.2TCP.txt 192.168.0.2
Nmap scan report for 192.168.0.2
Host is up, received arp-response (0.00064s latency).
Scanned at 2021-01-02 14:24:48 GMT Standard Time for 171s
Not shown: 5986 filtered ports
Reason: 5986 no-responses
PORT     STATE SERVICE      REASON  VERSION
23/tcp   open  telnet       syn-ack Microsoft Windows XP telnetd
| banner: \xFF\xFD%\xFF\xFB\x01\xFF\xFB\x03\xFF\xFD'\xFF\xFD\x1F\xFF\xFD\
|_x00\xFF\xFB\x00
42/tcp   open  tcpwrapped   syn-ack
53/tcp   open  domain       syn-ack Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
80/tcp   open  http         syn-ack Apache httpd (PHP 5.6.30)
|_http-server-header: Apache
88/tcp   open  kerberos-sec syn-ack Microsoft Windows Kerberos (server time: 2021-01-02 14:27:23Z)
135/tcp  open  msrpc        syn-ack Microsoft Windows RPC
139/tcp  open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
389/tcp  open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)
445/tcp  open  microsoft-ds syn-ack Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: UADCWNET)
464/tcp  open  kpasswd5?    syn-ack
593/tcp  open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
|_banner: ncacn_http/1.0
636/tcp  open  tcpwrapped   syn-ack
3268/tcp open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)
3269/tcp open  tcpwrapped   syn-ack
MAC Address: 00:0C:29:70:FC:E3 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=1/2%OT=23%CT=%CU=34925%PV=Y%DS=1%DC=D%G=N%M=000C29%TM=
OS:5FF082DB%P=i686-pc-windows-windows)SEQ(SP=105%GCD=1%ISR=10A%TI=I%CI=I%II
OS:=I%SS=S%TS=7)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW
OS:8ST11%O5=M5B4NW8ST11%O6=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=
OS:2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T
OS:=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T
OS:3(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O
OS:%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=
OS:Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%
OS:RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
OS:IE(R=Y%DFI=N%T=80%CD=Z)

Uptime guess: 0.029 days (since Sat Jan 02 13:45:27 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: SERVER2; OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Read data files from: C:\Users\Jack\Desktop\tools\nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jan 02 14:27:39 2021 -- 1 IP address (1 host up) scanned in 171.66 seconds
```

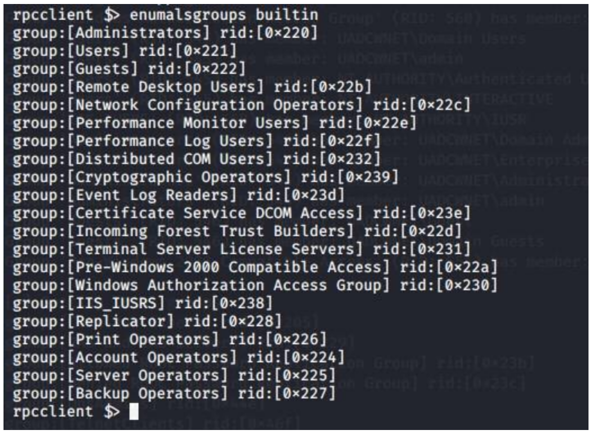
Appendix B1: NMAP Scan from server 2 TCP Ports



```
# Nmap 7.91 scan initiated Sat Jan 02 14:11:52 2021 as: nmap -sU -p 1-500 -v -v --scan-delay 1s -sV --script=banner -oN VM192.168.0.2UDP.txt 192.168.0.2
Nmap scan report for 192.168.0.2
Host is up, received arp-response (0.000074s latency).
Scanned at 2021-01-02 14:11:53 GMT Standard Time for 636s
Not shown: 488 closed ports
Reason: 488 port-unreaches
PORT    STATE         SERVICE      REASON               VERSION
42/udp  open|filtered nameserver   no-response
53/udp  open          domain       udp-response ttl 128 Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
67/udp  open|filtered dhcps        no-response
68/udp  open|filtered dhcpc        no-response
88/udp  open          kerberos-sec udp-response         Microsoft Windows Kerberos (server time: 2021-01-02 14:20:42Z)
123/udp open          ntp          udp-response ttl 128 NTP v3
137/udp open          netbios-ns   udp-response ttl 128 Microsoft Windows netbios-ssn (workgroup: UADCWNET)
138/udp open|filtered netbios-dgm  no-response
161/udp open|filtered snmp         no-response
389/udp open|filtered ldap         no-response
464/udp open|filtered kpasswd5     no-response
500/udp open|filtered isakmp       no-response
MAC Address: 00:0C:29:70:FC:E3 (VMware)
Service Info: Host: SERVER2; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Read data files from: C:\Users\Jack\Desktop\tools\nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jan 02 14:22:29 2021 -- 1 IP address (1 host up) scanned in 637.25 seconds
```

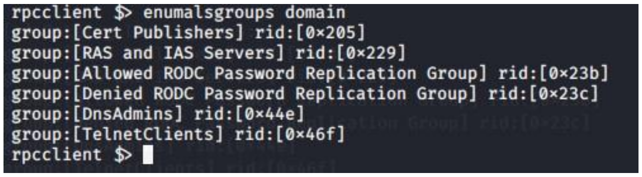
Appendix B2: NMAP Scan from server 2 UDP Ports

APPENDIX C



```
rpcclient $> enumalsgroups builtin
group:[Administrators] rid:[0×220]
group:[Users] rid:[0×221]
group:[Guests] rid:[0×222]
group:[Remote Desktop Users] rid:[0×22b]
group:[Network Configuration Operators] rid:[0×22c]
group:[Performance Monitor Users] rid:[0×22e]
group:[Performance Log Users] rid:[0×22f]
group:[Distributed COM Users] rid:[0×232]
group:[Cryptographic Operators] rid:[0×239]
group:[Event Log Readers] rid:[0×23d]
group:[Certificate Service DCOM Access] rid:[0×23e]
group:[Incoming Forest Trust Builders] rid:[0×22d]
group:[Terminal Server License Servers] rid:[0×231]
group:[Pre-Windows 2000 Compatible Access] rid:[0×22a]
group:[Windows Authorization Access Group] rid:[0×230]
group:[IIS_IUSRS] rid:[0×238]
group:[Replicator] rid:[0×228]
group:[Print Operators] rid:[0×226]
group:[Account Operators] rid:[0×224]
group:[Server Operators] rid:[0×225]
group:[Backup Operators] rid:[0×227]
rpcclient $> 
```

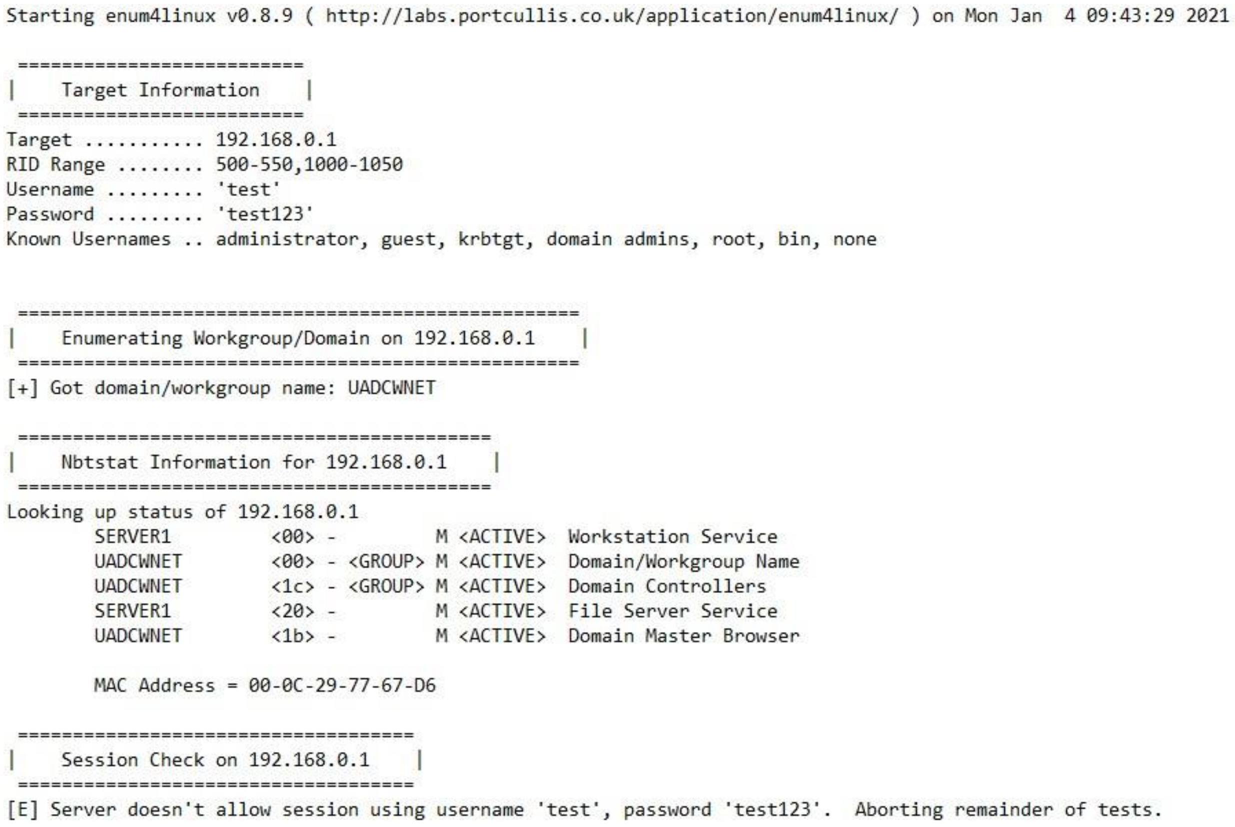
Appendix C1: Rpcclient result from built-in groups



```
rpcclient $> enumalsgroups domain
group:[Cert Publishers] rid:[0×205]
group:[RAS and IAS Servers] rid:[0×229]
group:[Allowed RODC Password Replication Group] rid:[0×23b]
group:[Denied RODC Password Replication Group] rid:[0×23c]
group:[DnsAdmins] rid:[0×44e]
group:[TelnetClients] rid:[0×46f]
rpcclient $> 
```

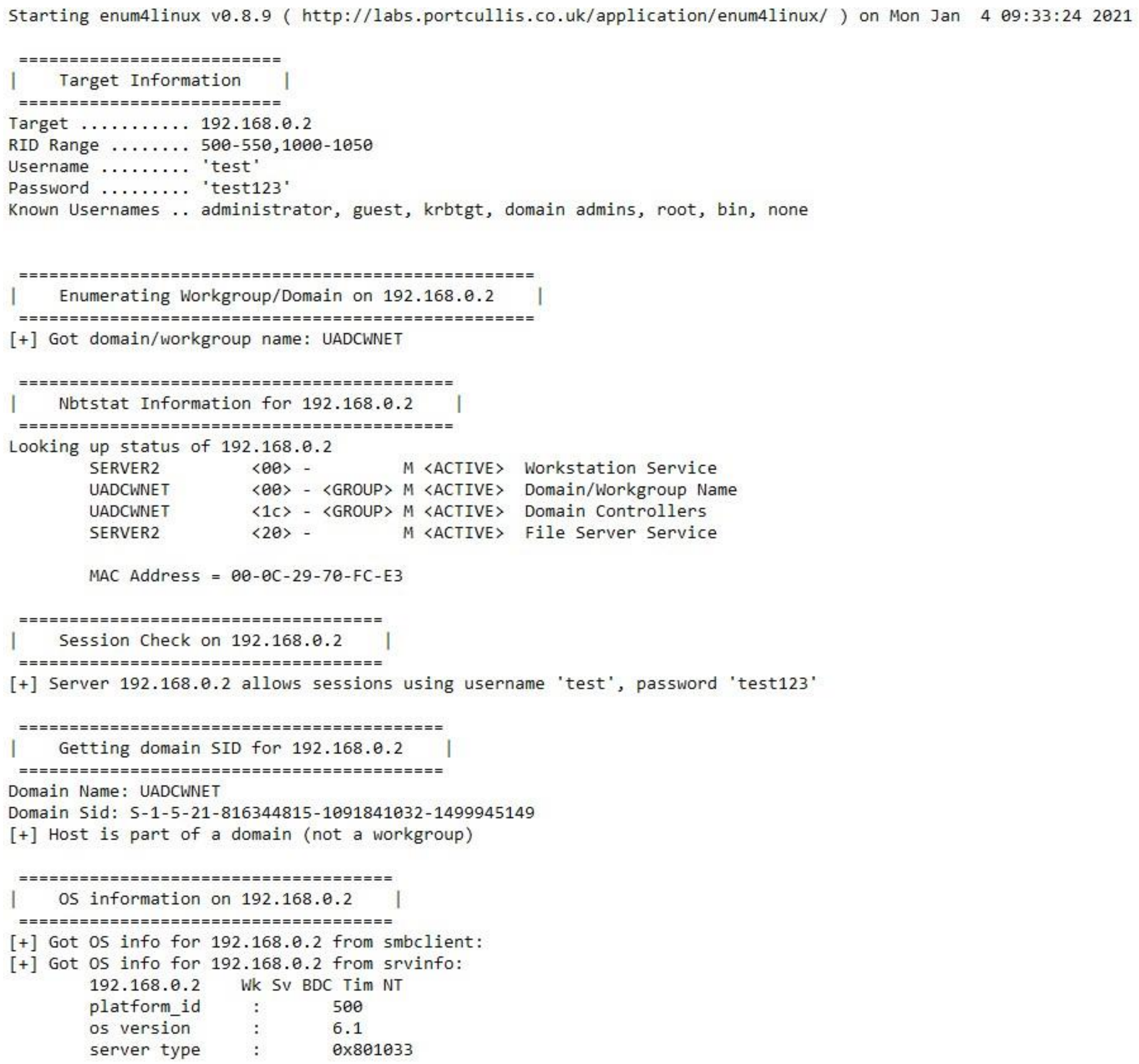
Appendix C2: Rpcclient result from domain groups

APPENDIX D

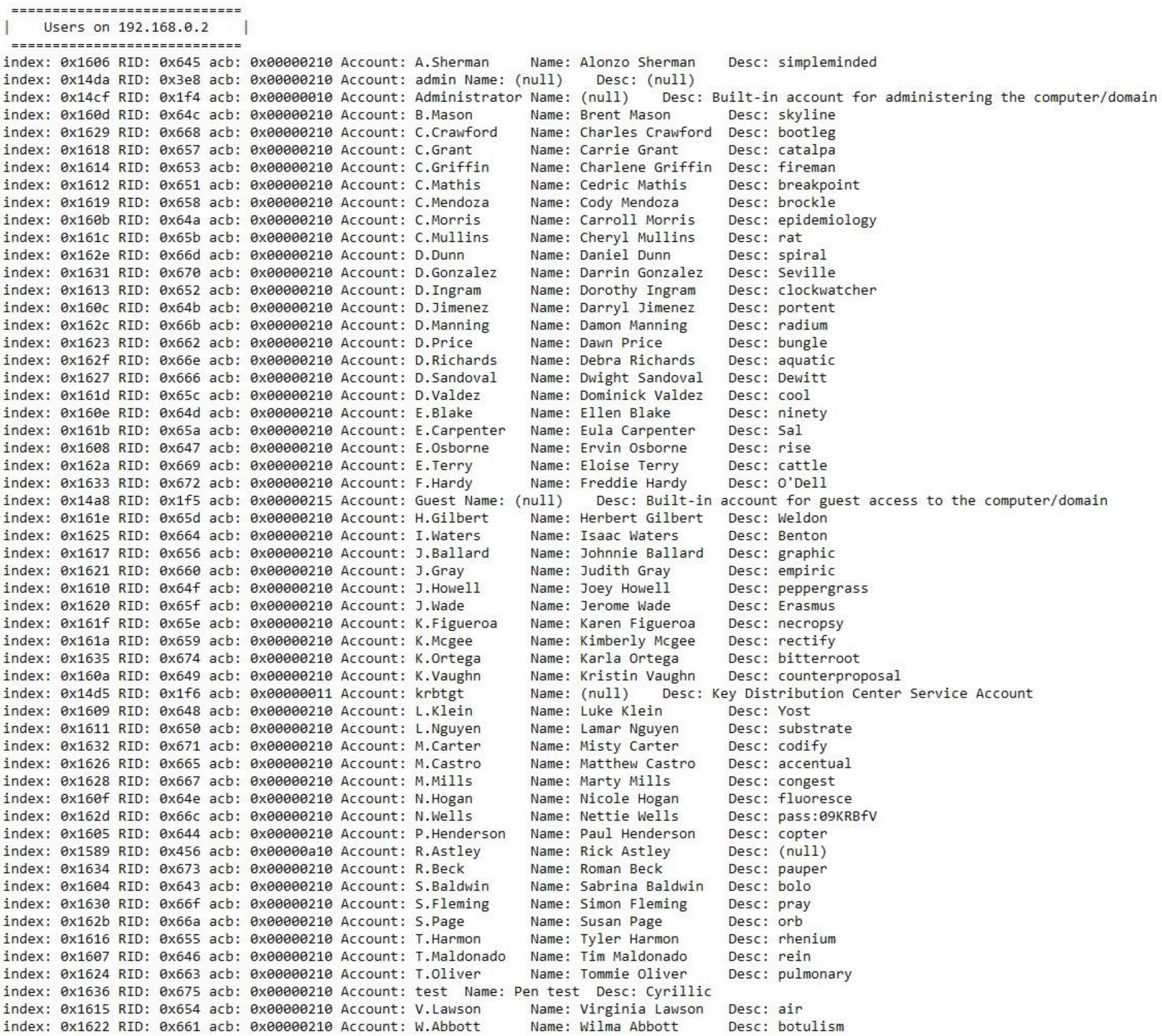


```
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Jan  4 09:43:29 2021

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.0.1
RID Range ........ 500-550,1000-1050
Username ......... 'test'
Password ......... 'test123'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===================================================
|    Enumerating Workgroup/Domain on 192.168.0.1    |
 ===================================================
[+] Got domain/workgroup name: UADCWNET

 ===========================================
|    Nbtstat Information for 192.168.0.1    |
 ===========================================
Looking up status of 192.168.0.1
        SERVER1         <00> -         M <ACTIVE>  Workstation Service
        UADCWNET        <00> - <GROUP> M <ACTIVE>  Domain/Workgroup Name
        UADCWNET        <1c> - <GROUP> M <ACTIVE>  Domain Controllers
        SERVER1         <20> -         M <ACTIVE>  File Server Service
        UADCWNET        <1b> -         M <ACTIVE>  Domain Master Browser

        MAC Address = 00-0C-29-77-67-D6

 ====================================
|    Session Check on 192.168.0.1    |
 ====================================
[E] Server doesn't allow session using username 'test', password 'test123'.  Aborting remainder of tests.
```

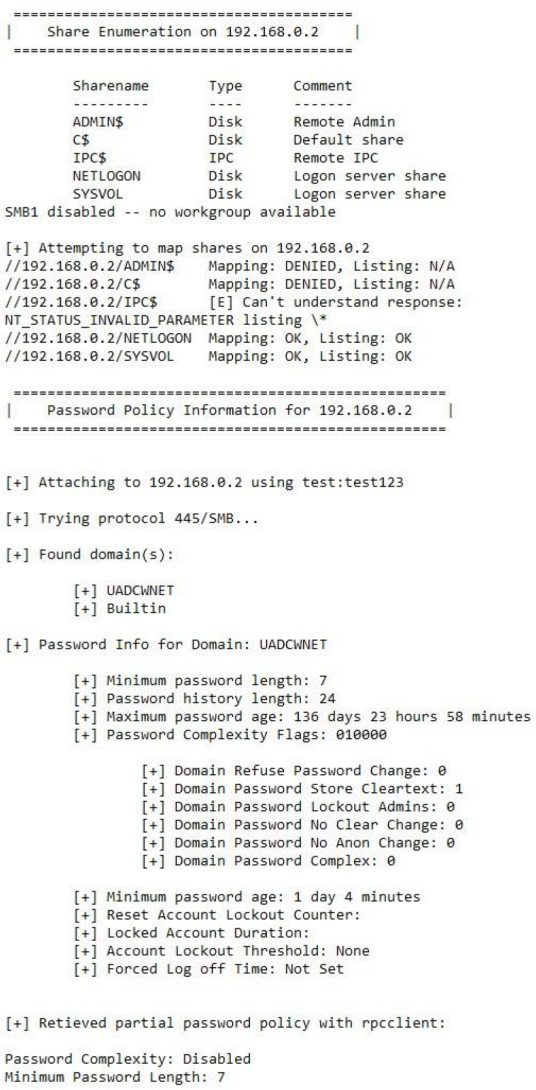
Appendix D1: Enum4linux output from server 1



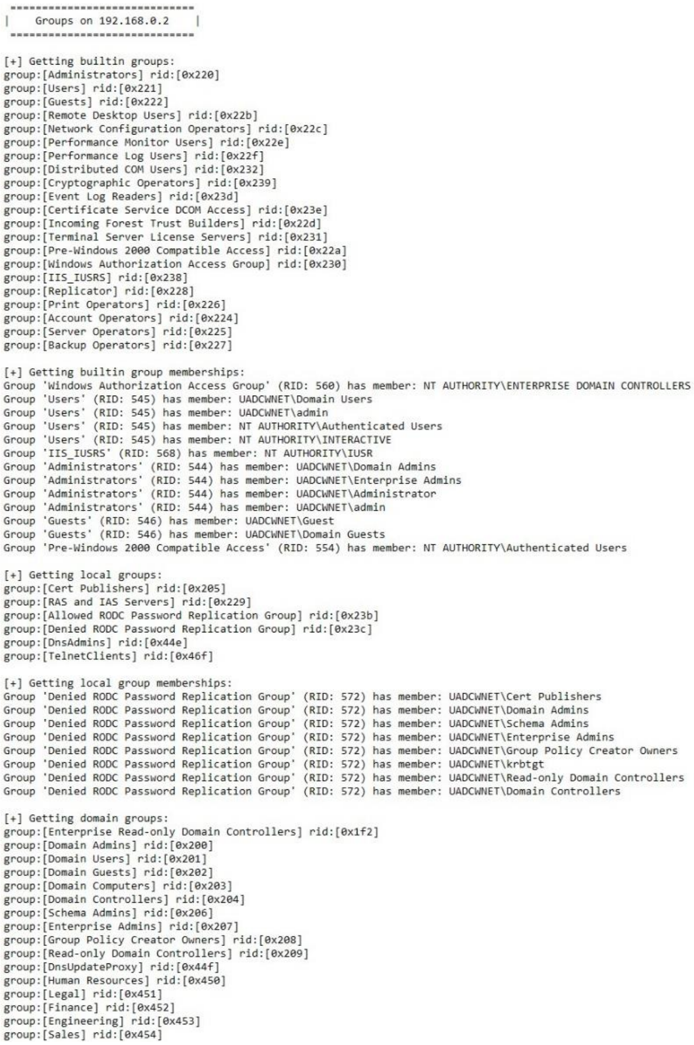
```
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Jan  4 09:33:24 2021

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.0.2
RID Range ........ 500-550,1000-1050
Username ......... 'test'
Password ......... 'test123'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===================================================
|    Enumerating Workgroup/Domain on 192.168.0.2    |
 ===================================================
[+] Got domain/workgroup name: UADCWNET

 ===========================================
|    Nbtstat Information for 192.168.0.2    |
 ===========================================
Looking up status of 192.168.0.2
        SERVER2         <00> -         M <ACTIVE>  Workstation Service
        UADCWNET        <00> - <GROUP> M <ACTIVE>  Domain/Workgroup Name
        UADCWNET        <1c> - <GROUP> M <ACTIVE>  Domain Controllers
        SERVER2         <20> -         M <ACTIVE>  File Server Service

        MAC Address = 00-0C-29-70-FC-E3

 ====================================
|    Session Check on 192.168.0.2    |
 ====================================
[+] Server 192.168.0.2 allows sessions using username 'test', password 'test123'

 ==========================================
|    Getting domain SID for 192.168.0.2    |
 ==========================================
Domain Name: UADCWNET
Domain Sid: S-1-5-21-816344815-1091841032-1499945149
[+] Host is part of a domain (not a workgroup)

 =====================================
|    OS information on 192.168.0.2    |
 =====================================
[+] Got OS info for 192.168.0.2 from smbclient:
[+] Got OS info for 192.168.0.2 from srvinfo:
        192.168.0.2    Wk Sv BDC Tim NT
        platform_id     :       500
        os version      :       6.1
        server type     :       0x801033
```



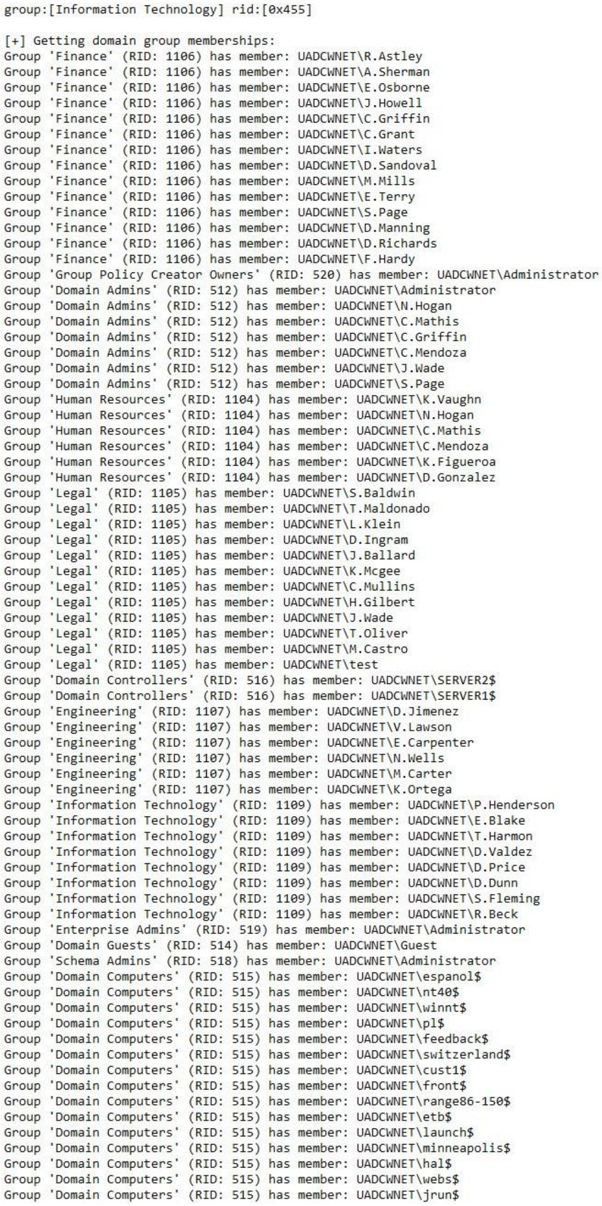
```
 ============================
|    Users on 192.168.0.2    |
 ============================
index: 0x1606 RID: 0x645 acb: 0x00000210 Account: A.Sherman     Name: Alonzo Sherman   Desc: simpleminded
index: 0x14da RID: 0x3e8 acb: 0x00000210 Account: admin Name: (null)    Desc: (null)
index: 0x14cf RID: 0x1f4 acb: 0x00000010 Account: Administrator Name: (null)    Desc: Built-in account for administering the computer/domain
index: 0x160d RID: 0x64c acb: 0x00000210 Account: B.Mason       Name: Brent Mason      Desc: skyline
index: 0x1629 RID: 0x668 acb: 0x00000210 Account: C.Crawford    Name: Charles Crawford Desc: bootleg
index: 0x1618 RID: 0x657 acb: 0x00000210 Account: C.Grant       Name: Carrie Grant     Desc: catalpa
index: 0x1614 RID: 0x653 acb: 0x00000210 Account: C.Griffin     Name: Charlene Griffin Desc: fireman
index: 0x1612 RID: 0x651 acb: 0x00000210 Account: C.Mathis      Name: Cedric Mathis    Desc: breakpoint
index: 0x1619 RID: 0x658 acb: 0x00000210 Account: C.Mendoza     Name: Cody Mendoza     Desc: brockle
index: 0x160b RID: 0x64a acb: 0x00000210 Account: C.Morris      Name: Carroll Morris   Desc: epidemiology
index: 0x161c RID: 0x65b acb: 0x00000210 Account: C.Mullins     Name: Cheryl Mullins   Desc: rat
index: 0x162e RID: 0x66d acb: 0x00000210 Account: D.Dunn        Name: Daniel Dunn      Desc: spiral
index: 0x1631 RID: 0x670 acb: 0x00000210 Account: D.Gonzalez    Name: Darrin Gonzalez  Desc: Seville
index: 0x1613 RID: 0x652 acb: 0x00000210 Account: D.Ingram      Name: Dorothy Ingram   Desc: clockwatcher
index: 0x160c RID: 0x64b acb: 0x00000210 Account: D.Jimenez     Name: Darryl Jimenez   Desc: portent
index: 0x162c RID: 0x66b acb: 0x00000210 Account: D.Manning     Name: Damon Manning    Desc: radium
index: 0x1623 RID: 0x662 acb: 0x00000210 Account: D.Price       Name: Dawn Price       Desc: bungle
index: 0x162f RID: 0x66e acb: 0x00000210 Account: D.Richards    Name: Debra Richards   Desc: aquatic
index: 0x1627 RID: 0x666 acb: 0x00000210 Account: D.Sandoval    Name: Dwight Sandoval  Desc: Dewitt
index: 0x161d RID: 0x65c acb: 0x00000210 Account: D.Valdez      Name: Dominick Valdez  Desc: cool
index: 0x160e RID: 0x64d acb: 0x00000210 Account: E.Blake       Name: Ellen Blake      Desc: ninety
index: 0x161b RID: 0x65a acb: 0x00000210 Account: E.Carpenter   Name: Eula Carpenter   Desc: Sal
index: 0x1608 RID: 0x647 acb: 0x00000210 Account: E.Osborne     Name: Ervin Osborne    Desc: rise
index: 0x162a RID: 0x669 acb: 0x00000210 Account: E.Terry       Name: Eloise Terry     Desc: cattle
index: 0x1633 RID: 0x672 acb: 0x00000210 Account: F.Hardy       Name: Freddie Hardy    Desc: O'Dell
index: 0x14a8 RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0x161e RID: 0x65d acb: 0x00000210 Account: H.Gilbert     Name: Herbert Gilbert  Desc: Weldon
index: 0x1625 RID: 0x664 acb: 0x00000210 Account: I.Waters      Name: Isaac Waters     Desc: Benton
index: 0x1617 RID: 0x656 acb: 0x00000210 Account: J.Ballard     Name: Johnnie Ballard  Desc: graphic
index: 0x1621 RID: 0x660 acb: 0x00000210 Account: J.Gray        Name: Judith Gray      Desc: empiric
index: 0x1610 RID: 0x64f acb: 0x00000210 Account: J.Howell      Name: Joey Howell      Desc: peppergrass
index: 0x1620 RID: 0x65f acb: 0x00000210 Account: J.Wade        Name: Jerome Wade      Desc: Erasmus
index: 0x161f RID: 0x65e acb: 0x00000210 Account: K.Figueroa    Name: Karen Figueroa   Desc: necropsy
index: 0x161a RID: 0x659 acb: 0x00000210 Account: K.Mcgee       Name: Kimberly Mcgee   Desc: rectify
index: 0x1635 RID: 0x674 acb: 0x00000210 Account: K.Ortega      Name: Karla Ortega     Desc: bitterroot
index: 0x160a RID: 0x649 acb: 0x00000210 Account: K.Vaughn      Name: Kristin Vaughn   Desc: counterproposal
index: 0x14d5 RID: 0x1f6 acb: 0x00000011 Account: krbtgt        Name: (null)    Desc: Key Distribution Center Service Account
index: 0x1609 RID: 0x648 acb: 0x00000210 Account: L.Klein       Name: Luke Klein       Desc: Yost
index: 0x1611 RID: 0x650 acb: 0x00000210 Account: L.Nguyen      Name: Lamar Nguyen     Desc: substrate
index: 0x1632 RID: 0x671 acb: 0x00000210 Account: M.Carter      Name: Misty Carter     Desc: codify
index: 0x1626 RID: 0x665 acb: 0x00000210 Account: M.Castro      Name: Matthew Castro   Desc: accentual
index: 0x1628 RID: 0x667 acb: 0x00000210 Account: M.Mills       Name: Marty Mills      Desc: congest
index: 0x160f RID: 0x64e acb: 0x00000210 Account: N.Hogan       Name: Nicole Hogan     Desc: fluoresce
index: 0x162d RID: 0x66c acb: 0x00000210 Account: N.Wells       Name: Nettie Wells     Desc: pass:09KRBfV
index: 0x1605 RID: 0x644 acb: 0x00000210 Account: P.Henderson   Name: Paul Henderson   Desc: copter
index: 0x1589 RID: 0x456 acb: 0x00000a10 Account: R.Astley      Name: Rick Astley      Desc: (null)
index: 0x1634 RID: 0x673 acb: 0x00000210 Account: R.Beck        Name: Roman Beck       Desc: pauper
index: 0x1604 RID: 0x643 acb: 0x00000210 Account: S.Baldwin     Name: Sabrina Baldwin  Desc: bolo
index: 0x1630 RID: 0x66f acb: 0x00000210 Account: S.Fleming     Name: Simon Fleming    Desc: pray
index: 0x162b RID: 0x66a acb: 0x00000210 Account: S.Page        Name: Susan Page       Desc: orb
index: 0x1616 RID: 0x655 acb: 0x00000210 Account: T.Harmon      Name: Tyler Harmon     Desc: rhenium
index: 0x1607 RID: 0x646 acb: 0x00000210 Account: T.Maldonado   Name: Tim Maldonado    Desc: rein
index: 0x1624 RID: 0x663 acb: 0x00000210 Account: T.Oliver      Name: Tommie Oliver    Desc: pulmonary
index: 0x1636 RID: 0x675 acb: 0x00000210 Account: test  Name: Pen test  Desc: Cyrillic
index: 0x1615 RID: 0x654 acb: 0x00000210 Account: V.Lawson      Name: Virginia Lawson  Desc: air
index: 0x1622 RID: 0x661 acb: 0x00000210 Account: W.Abbott      Name: Wilma Abbott     Desc: botulism
```



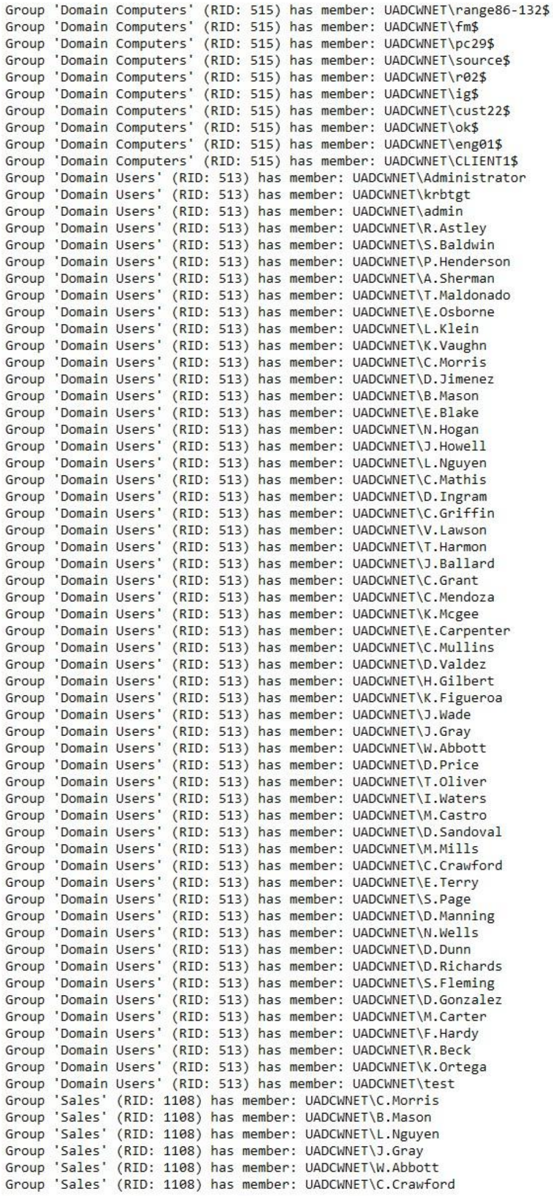
```
 ========================================
|    Share Enumeration on 192.168.0.2    |
 ========================================

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

[+] Attempting to map shares on 192.168.0.2
//192.168.0.2/ADMIN$    Mapping: DENIED, Listing: N/A
//192.168.0.2/C$        Mapping: DENIED, Listing: N/A
//192.168.0.2/IPC$      [E] Can't understand response:
NT_STATUS_INVALID_PARAMETER listing \*
//192.168.0.2/NETLOGON  Mapping: OK, Listing: OK
//192.168.0.2/SYSVOL    Mapping: OK, Listing: OK

 ===================================================
|    Password Policy Information for 192.168.0.2    |
 ===================================================


[+] Attaching to 192.168.0.2 using test:test123

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] UADCWNET
        [+] Builtin

[+] Password Info for Domain: UADCWNET

        [+] 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:
        [+] Locked Account Duration:
        [+] 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 192.168.0.2    |
 ============================

[+] Getting builtin groups:
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Terminal Server License Servers] rid:[0x231]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Windows Authorization Access Group] rid:[0x230]
group:[IIS_IUSRS] rid:[0x238]
group:[Replicator] rid:[0x228]
group:[Print Operators] rid:[0x226]
group:[Account Operators] rid:[0x224]
group:[Server Operators] rid:[0x225]
group:[Backup Operators] rid:[0x227]

[+] Getting builtin group memberships:
Group 'Windows Authorization Access Group' (RID: 560) has member: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
Group 'Users' (RID: 545) has member: UADCWNET\Domain Users
Group 'Users' (RID: 545) has member: UADCWNET\admin
Group 'Users' (RID: 545) has member: NT AUTHORITY\Authenticated Users
Group 'Users' (RID: 545) has member: NT AUTHORITY\INTERACTIVE
Group 'IIS_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR
Group 'Administrators' (RID: 544) has member: UADCWNET\Domain Admins
Group 'Administrators' (RID: 544) has member: UADCWNET\Enterprise Admins
Group 'Administrators' (RID: 544) has member: UADCWNET\Administrator
Group 'Administrators' (RID: 544) has member: UADCWNET\admin
Group 'Guests' (RID: 546) has member: UADCWNET\Guest
Group 'Guests' (RID: 546) has member: UADCWNET\Domain Guests
Group 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: NT AUTHORITY\Authenticated Users

[+] Getting local groups:
group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44e]
group:[TelnetClients] rid:[0x46f]

[+] Getting local group memberships:
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Cert Publishers
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Schema Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Enterprise Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Group Policy Creator Owners
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\krbtgt
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Read-only Domain Controllers
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Controllers

[+] Getting domain groups:
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[DnsUpdateProxy] rid:[0x44f]
group:[Human Resources] rid:[0x450]
group:[Legal] rid:[0x451]
group:[Finance] rid:[0x452]
group:[Engineering] rid:[0x453]
group:[Sales] rid:[0x454]
```



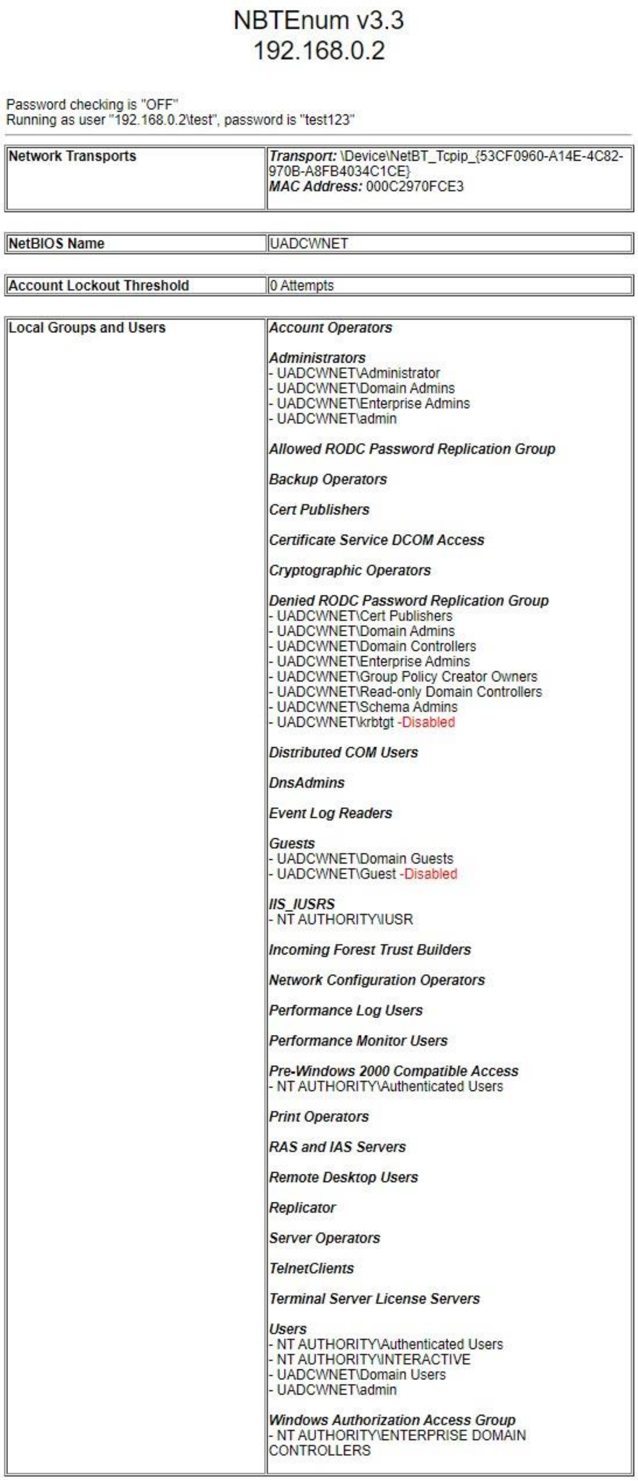
```
group:[Information Technology] rid:[0x455]

[+] Getting domain group memberships:
Group 'Finance' (RID: 1106) has member: UADCWNET\R.Astley
Group 'Finance' (RID: 1106) has member: UADCWNET\A.Sherman
Group 'Finance' (RID: 1106) has member: UADCWNET\E.Osborne
Group 'Finance' (RID: 1106) has member: UADCWNET\J.Howell
Group 'Finance' (RID: 1106) has member: UADCWNET\C.Griffin
Group 'Finance' (RID: 1106) has member: UADCWNET\C.Grant
Group 'Finance' (RID: 1106) has member: UADCWNET\I.Waters
Group 'Finance' (RID: 1106) has member: UADCWNET\D.Sandoval
Group 'Finance' (RID: 1106) has member: UADCWNET\M.Mills
Group 'Finance' (RID: 1106) has member: UADCWNET\E.Terry
Group 'Finance' (RID: 1106) has member: UADCWNET\S.Page
Group 'Finance' (RID: 1106) has member: UADCWNET\D.Manning
Group 'Finance' (RID: 1106) has member: UADCWNET\D.Richards
Group 'Finance' (RID: 1106) has member: UADCWNET\F.Hardy
Group 'Group Policy Creator Owners' (RID: 520) has member: UADCWNET\Administrator
Group 'Domain Admins' (RID: 512) has member: UADCWNET\Administrator
Group 'Domain Admins' (RID: 512) has member: UADCWNET\N.Hogan
Group 'Domain Admins' (RID: 512) has member: UADCWNET\C.Mathis
Group 'Domain Admins' (RID: 512) has member: UADCWNET\C.Griffin
Group 'Domain Admins' (RID: 512) has member: UADCWNET\C.Mendoza
Group 'Domain Admins' (RID: 512) has member: UADCWNET\J.Wade
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Page
Group 'Human Resources' (RID: 1104) has member: UADCWNET\K.Vaughn
Group 'Human Resources' (RID: 1104) has member: UADCWNET\N.Hogan
Group 'Human Resources' (RID: 1104) has member: UADCWNET\C.Mathis
Group 'Human Resources' (RID: 1104) has member: UADCWNET\C.Mendoza
Group 'Human Resources' (RID: 1104) has member: UADCWNET\K.Figueroa
Group 'Human Resources' (RID: 1104) has member: UADCWNET\D.Gonzalez
Group 'Legal' (RID: 1105) has member: UADCWNET\S.Baldwin
Group 'Legal' (RID: 1105) has member: UADCWNET\T.Maldonado
Group 'Legal' (RID: 1105) has member: UADCWNET\L.Klein
Group 'Legal' (RID: 1105) has member: UADCWNET\D.Ingram
Group 'Legal' (RID: 1105) has member: UADCWNET\J.Ballard
Group 'Legal' (RID: 1105) has member: UADCWNET\K.Mcgee
Group 'Legal' (RID: 1105) has member: UADCWNET\C.Mullins
Group 'Legal' (RID: 1105) has member: UADCWNET\H.Gilbert
Group 'Legal' (RID: 1105) has member: UADCWNET\J.Wade
Group 'Legal' (RID: 1105) has member: UADCWNET\T.Oliver
Group 'Legal' (RID: 1105) has member: UADCWNET\M.Castro
Group 'Legal' (RID: 1105) has member: UADCWNET\test
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER2$
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER1$
Group 'Engineering' (RID: 1107) has member: UADCWNET\D.Jimenez
Group 'Engineering' (RID: 1107) has member: UADCWNET\V.Lawson
Group 'Engineering' (RID: 1107) has member: UADCWNET\E.Carpenter
Group 'Engineering' (RID: 1107) has member: UADCWNET\N.Wells
Group 'Engineering' (RID: 1107) has member: UADCWNET\M.Carter
Group 'Engineering' (RID: 1107) has member: UADCWNET\K.Ortega
Group 'Information Technology' (RID: 1109) has member: UADCWNET\P.Henderson
Group 'Information Technology' (RID: 1109) has member: UADCWNET\E.Blake
Group 'Information Technology' (RID: 1109) has member: UADCWNET\T.Harmon
Group 'Information Technology' (RID: 1109) has member: UADCWNET\D.Valdez
Group 'Information Technology' (RID: 1109) has member: UADCWNET\D.Price
Group 'Information Technology' (RID: 1109) has member: UADCWNET\D.Dunn
Group 'Information Technology' (RID: 1109) has member: UADCWNET\S.Fleming
Group 'Information Technology' (RID: 1109) has member: UADCWNET\R.Beck
Group 'Enterprise Admins' (RID: 519) has member: UADCWNET\Administrator
Group 'Domain Guests' (RID: 514) has member: UADCWNET\Guest
Group 'Schema Admins' (RID: 518) has member: UADCWNET\Administrator
Group 'Domain Computers' (RID: 515) has member: UADCWNET\espanol$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\nt40$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\winnt$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\pl$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\feedback$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\switzerland$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cust1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\front$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\range86-150$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\etb$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\launch$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\minneapolis$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\hal$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\webs$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\jrun$
```



```
Group 'Domain Computers' (RID: 515) has member: UADCWNET\range86-132$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\fm$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\pc29$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\source$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\r02$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ig$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cust22$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ok$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\eng01$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT1$
Group 'Domain Users' (RID: 513) has member: UADCWNET\Administrator
Group 'Domain Users' (RID: 513) has member: UADCWNET\krbtgt
Group 'Domain Users' (RID: 513) has member: UADCWNET\admin
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Astley
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Baldwin
Group 'Domain Users' (RID: 513) has member: UADCWNET\P.Henderson
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Sherman
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Maldonado
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Osborne
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Klein
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Vaughn
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Morris
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Jimenez
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Mason
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Blake
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Hogan
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Howell
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Nguyen
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Mathis
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Ingram
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Griffin
Group 'Domain Users' (RID: 513) has member: UADCWNET\V.Lawson
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Harmon
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Ballard
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Grant
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Mendoza
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Mcgee
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Carpenter
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Mullins
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Valdez
Group 'Domain Users' (RID: 513) has member: UADCWNET\H.Gilbert
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Figueroa
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Wade
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Gray
Group 'Domain Users' (RID: 513) has member: UADCWNET\W.Abbott
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Price
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Oliver
Group 'Domain Users' (RID: 513) has member: UADCWNET\I.Waters
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Castro
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Sandoval
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Mills
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Crawford
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Terry
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Page
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Manning
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Wells
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Dunn
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Richards
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Fleming
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Gonzalez
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Carter
Group 'Domain Users' (RID: 513) has member: UADCWNET\F.Hardy
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Beck
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Ortega
Group 'Domain Users' (RID: 513) has member: UADCWNET\test
Group 'Sales' (RID: 1108) has member: UADCWNET\C.Morris
Group 'Sales' (RID: 1108) has member: UADCWNET\B.Mason
Group 'Sales' (RID: 1108) has member: UADCWNET\L.Nguyen
Group 'Sales' (RID: 1108) has member: UADCWNET\J.Gray
Group 'Sales' (RID: 1108) has member: UADCWNET\W.Abbott
Group 'Sales' (RID: 1108) has member: UADCWNET\C.Crawford
```

Appendix D2: Enum4linux output from server 2, not the complete file due to size but parts mentioned in the results and processes is included.

APPENDIX E



NBTEnum v3.3
192.168.0.2

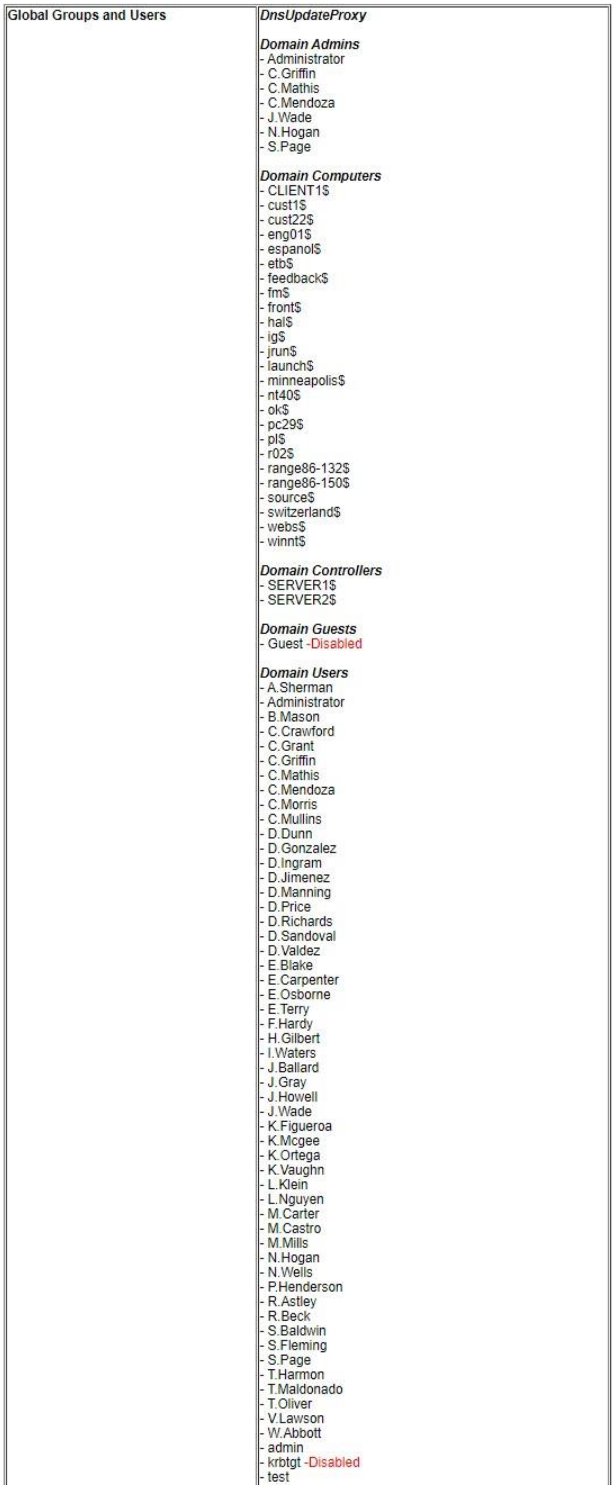
Password checking is "OFF"
Running as user "192.168.0.2\test", password is "test123"

Network Transports	***Transport:*** \Device\NetBT_Tcpip_{53CF0960-A14E-4C82-970B-A8FB4034C1CE} ***MAC Address:*** 000C2970FCE3

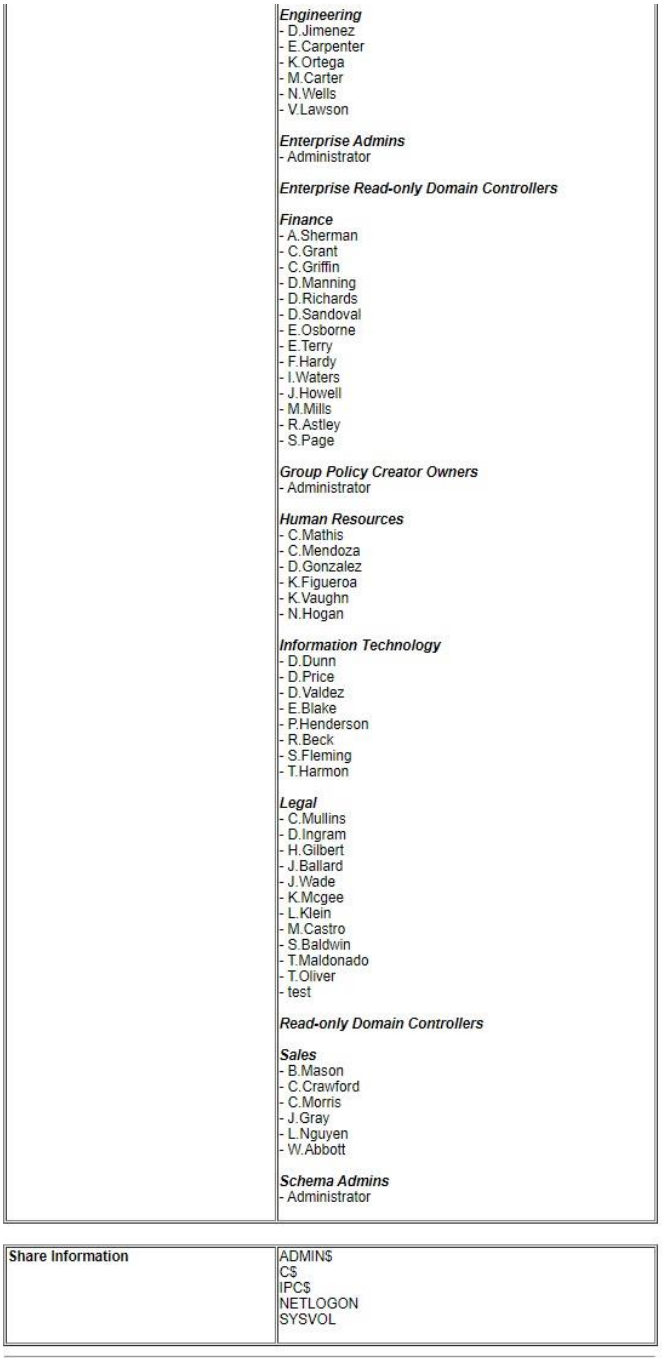
NetBIOS Name	UADCWNET

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

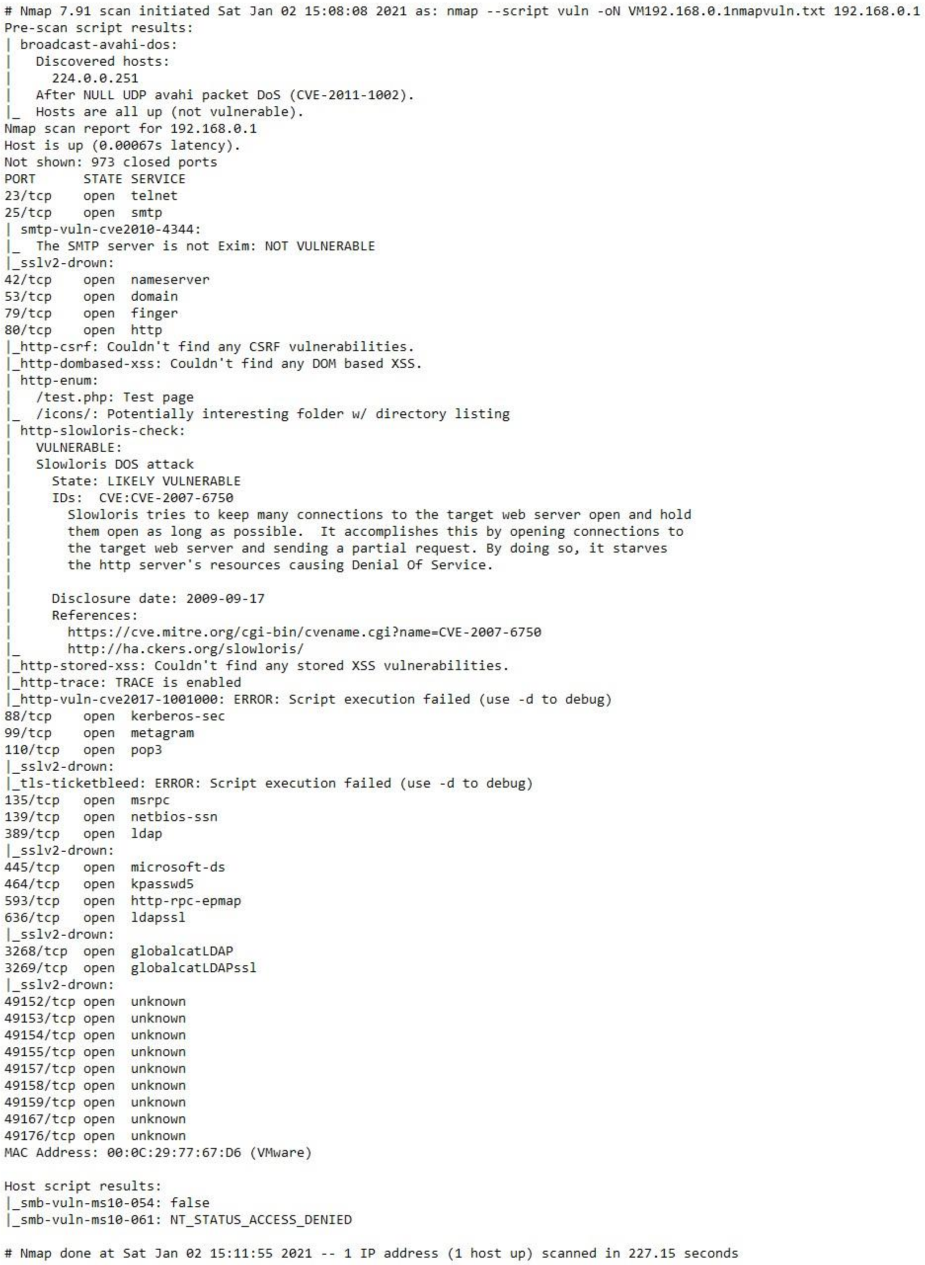


	Engineering - D.Jimenez - E.Carpenter - K.Ortega - M.Carter - N.Wells - V.Lawson ***Enterprise Admins*** - Administrator ***Enterprise Read-only Domain Controllers*** ***Finance*** - A.Sherman - C.Grant - C.Griffin - D.Manning - D.Richards - D.Sandoval - E.Osborne - E.Terry - F.Hardy - I.Waters - J.Howell - M.Mills - R.Astley - S.Page ***Group Policy Creator Owners*** - Administrator ***Human Resources*** - C.Mathis - C.Mendoza - D.Gonzalez - K.Figueroa - K.Vaughn - N.Hogan ***Information Technology*** - D.Dunn - D.Price - D.Valdez - E.Blake - P.Henderson - R.Beck - S.Fleming - T.Harmon ***Legal*** - C.Mullins - D.Ingram - H.Gilbert - J.Ballard - J.Wade - K.Mcgee - L.Klein - M.Castro - S.Baldwin - T.Maldonado - T.Oliver - test ***Read-only Domain Controllers*** ***Sales*** - B.Mason - C.Crawford - C.Morris - J.Gray - L.Nguyen - W.Abbott ***Schema Admins*** - Administrator

Share Information	ADMIN$ C$ IPC$ NETLOGON SYSVOL

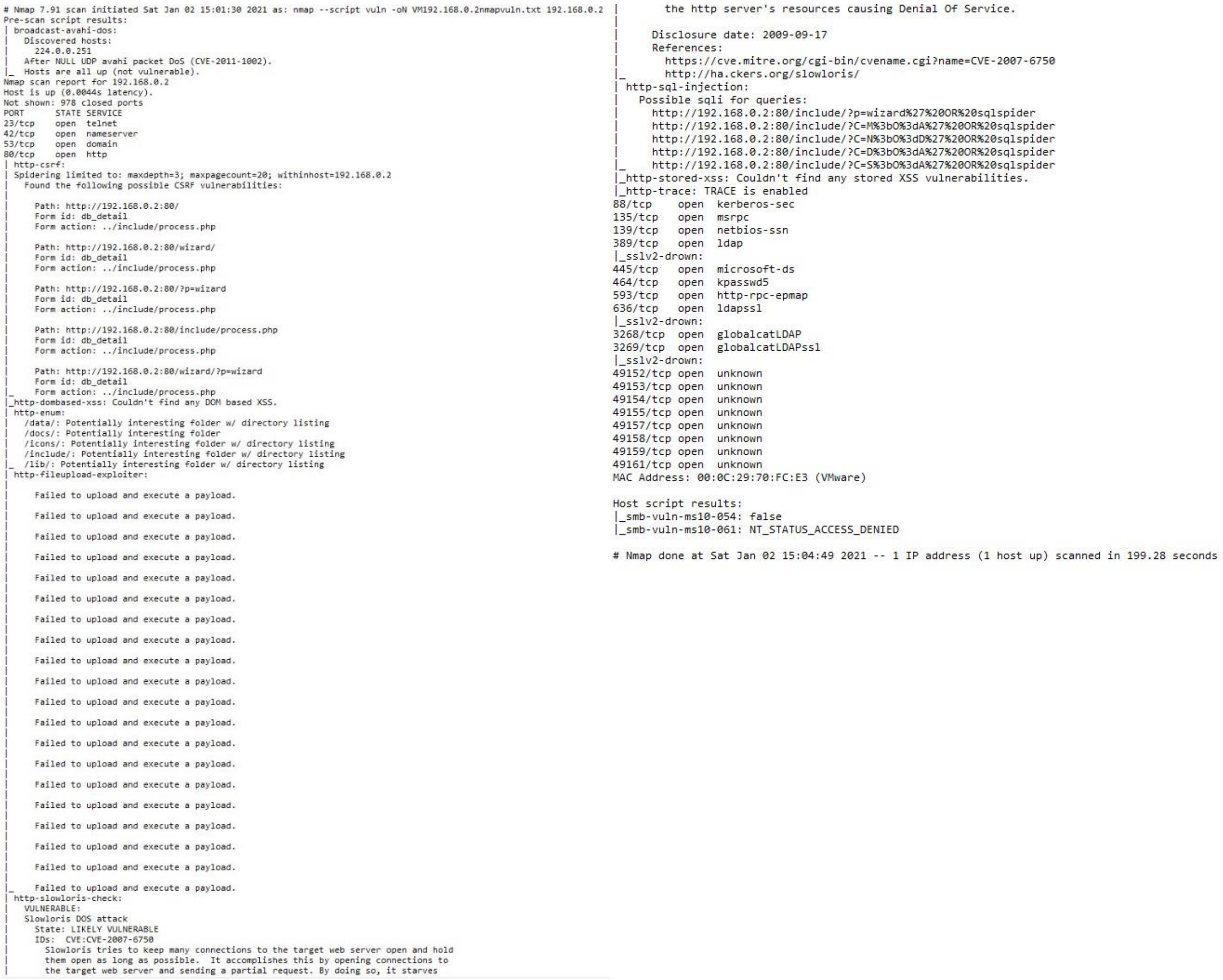
Appendix E1: NBTnum3.3 server 2 documents

APPENDIX F



```
# Nmap 7.91 scan initiated Sat Jan 02 15:08:08 2021 as: nmap --script vuln -oN VM192.168.0.1nmapvuln.txt 192.168.0.1
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.1
Host is up (0.00067s latency).
Not shown: 973 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
25/tcp    open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
|_sslv2-drown:
42/tcp    open  nameserver
53/tcp    open  domain
79/tcp    open  finger
80/tcp    open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /test.php: Test page
|_  /icons/: Potentially interesting folder w/ directory listing
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
88/tcp    open  kerberos-sec
99/tcp    open  metagram
110/tcp   open  pop3
|_sslv2-drown:
|_tls-ticketbleed: ERROR: Script execution failed (use -d to debug)
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
|_sslv2-drown:
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
|_sslv2-drown:
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
|_sslv2-drown:
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
49176/tcp open  unknown
MAC Address: 00:0C:29:77:67:D6 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

# Nmap done at Sat Jan 02 15:11:55 2021 -- 1 IP address (1 host up) scanned in 227.15 seconds
```

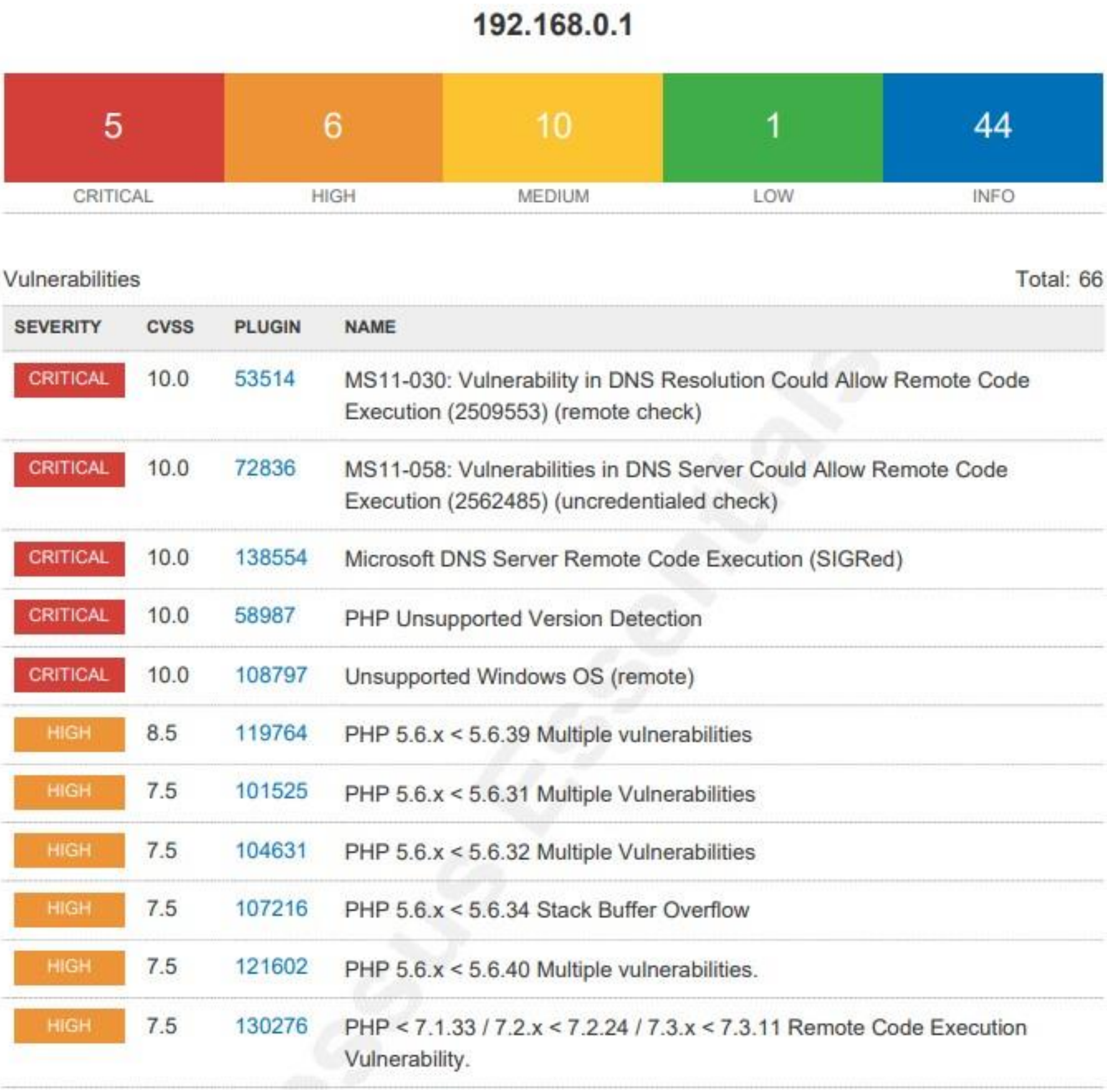
Appendix F1: NMAP Vulnerability report from server 1



```
# Nmap 7.91 scan initiated Sat Jan 02 15:01:30 2021 as: nmap --script vuln -oN VM192.168.0.2nmapvuln.txt 192.168.0.2
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.0.2
Host is up (0.0044s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.0.2
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.0.2:80/
|     Form id: db_detail
|     Form action: ../include/process.php
|
|     Path: http://192.168.0.2:80/wizard/
|     Form id: db_detail
|     Form action: ../include/process.php
|
|     Path: http://192.168.0.2:80/?p=wizard
|     Form id: db_detail
|     Form action: ../include/process.php
|
|     Path: http://192.168.0.2:80/include/process.php
|     Form id: db_detail
|     Form action: ../include/process.php
|
|     Path: http://192.168.0.2:80/wizard/?p=wizard
|     Form id: db_detail
|_    Form action: ../include/process.php
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /data/: Potentially interesting folder w/ directory listing
|   /docs/: Potentially interesting folder
|   /icons/: Potentially interesting folder w/ directory listing
|   /include/: Potentially interesting folder w/ directory listing
|_  /lib/: Potentially interesting folder w/ directory listing
| http-fileupload-exploiter:
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|     Failed to upload and execute a payload.
|
|_    Failed to upload and execute a payload.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.0.2:80/include/?p=wizard%27%20OR%20sqlspider
|     http://192.168.0.2:80/include/?C=M%3bO%3dA%27%20OR%20sqlspider
|     http://192.168.0.2:80/include/?C=N%3bO%3dD%27%20OR%20sqlspider
|     http://192.168.0.2:80/include/?C=D%3bO%3dA%27%20OR%20sqlspider
|_    http://192.168.0.2:80/include/?C=S%3bO%3dA%27%20OR%20sqlspider
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
|_sslv2-drown:
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
|_sslv2-drown:
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
|_sslv2-drown:
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
49161/tcp open  unknown
MAC Address: 00:0C:29:70:FC:E3 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

# Nmap done at Sat Jan 02 15:04:49 2021 -- 1 IP address (1 host up) scanned in 199.28 seconds
```

Appendix F2: NMAP Vulnerability report from server 2

APPENDIX G



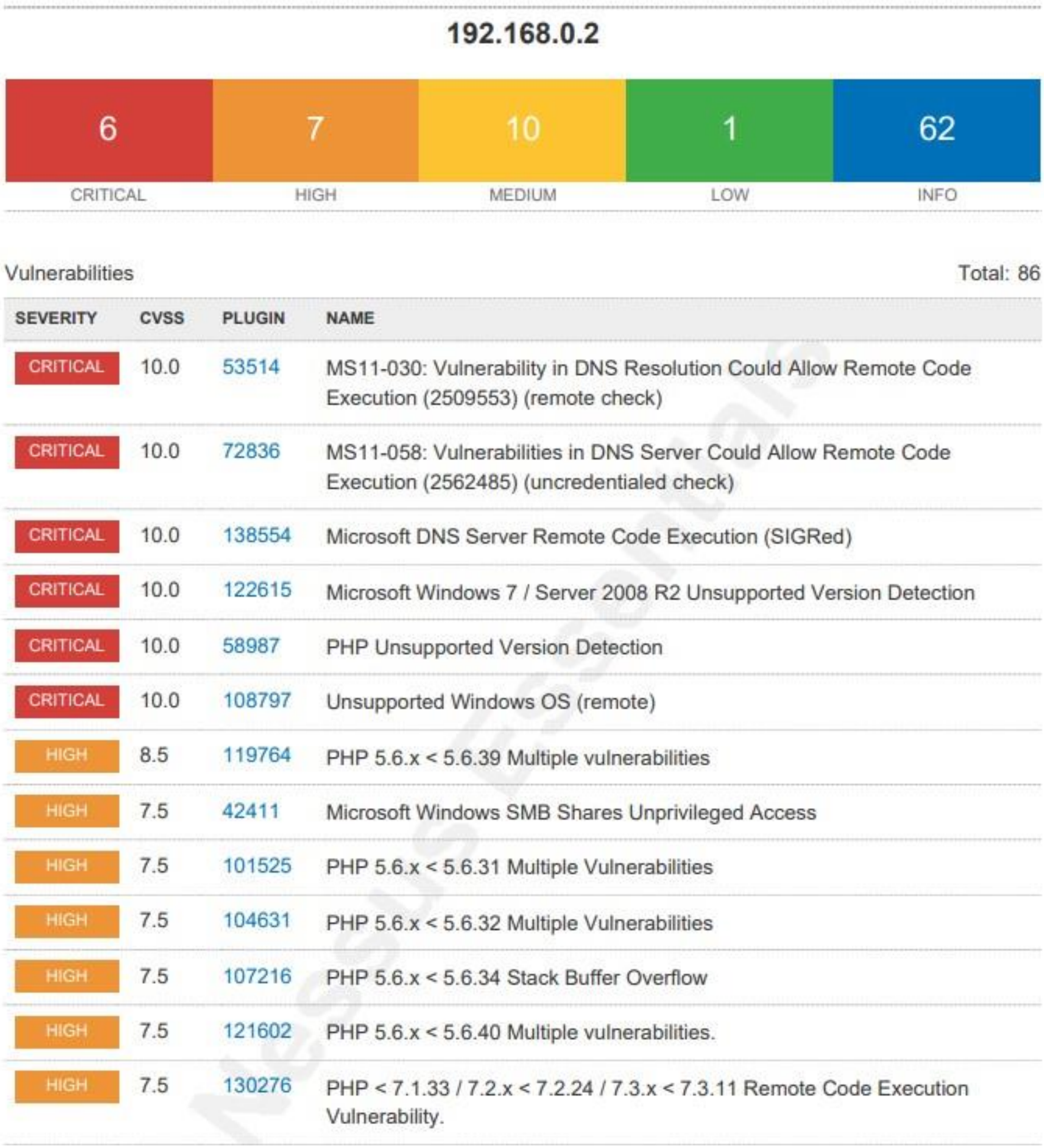
192.168.0.1

5	6	10	1	44
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 66

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)
CRITICAL	10.0	138554	Microsoft DNS Server Remote Code Execution (SIGRed)
CRITICAL	10.0	58987	PHP Unsupported Version Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	8.5	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	7.5	101525	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities
HIGH	7.5	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
HIGH	7.5	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
HIGH	7.5	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
HIGH	7.5	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.

Appendix G1: Nessus report only including critical and high reports for server 1



192.168.0.2

CRITICAL	HIGH	MEDIUM	LOW	INFO
6	7	10	1	62

Vulnerabilities Total: 86

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)
CRITICAL	10.0	138554	Microsoft DNS Server Remote Code Execution (SIGRed)
CRITICAL	10.0	122615	Microsoft Windows 7 / Server 2008 R2 Unsupported Version Detection
CRITICAL	10.0	58987	PHP Unsupported Version Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	8.5	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	7.5	42411	Microsoft Windows SMB Shares Unprivileged Access
HIGH	7.5	101525	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities
HIGH	7.5	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
HIGH	7.5	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
HIGH	7.5	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
HIGH	7.5	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.

Appendix G2: Nessus report only including critical and high reports for server 2