

Setup

Attack Machine: Kali Linux

Target Machine: Windows

Kali Linux IPaddress	192.168.37.130
Windows IPaddress	192.168.37.129
Default Gateway	192.168.37.2

Both machines are virtualized and connected within the same network.

Steps Executed

1. Network Configuration Verification

On Kali Linux: Terminal

```
ifconfig
```

Output displayed the IP address and network configuration of the attacking machine.

On Windows: CMD

```
ipconfig
```

Output displayed the IP address and network configuration of the target machine.

2. ARP Table Check (Windows)

Command executed:

```
arp -a
```

Verified the initial ARP table entries, ensuring normal gateway configurations.

3. Enable IP Forwarding (Kali Linux)

Verified IP forwarding status:

```
cat /proc/sys/net/ipv4/ip_forward
```

If the result was not "1", enabled IP forwarding:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

4. Launching Ettercap

Opened Ettercap on Kali Linux.

Clicked the Search button to list available hosts in the network.

5. Target Selection in Ettercap

Selected the gateway address from the host list and set it as Target 1.

Selected the Windows machine IP address and set it as Target 2.

6. ARP Poisoning Attack

Enabled ARP Poisoning in Ettercap.

Started the attack.

Observed that the victims were successfully added to groups (Group 1 and Group 2).

7. ARP Table Check (Windows)

Rechecked the ARP table on the Windows machine:

```
arp -a
```

Verified that the physical address of the gateway had changed to match the physical address of the Kali Linux machine.

8. Packet Capture using Wireshark

Started Wireshark on Kali Linux, listening on the "eth0" interface.

9. HTTP Traffic Monitoring

Opened a browser on the Windows machine and accessed an HTTP website.

Observed HTTP data captured on Wireshark in real-time.

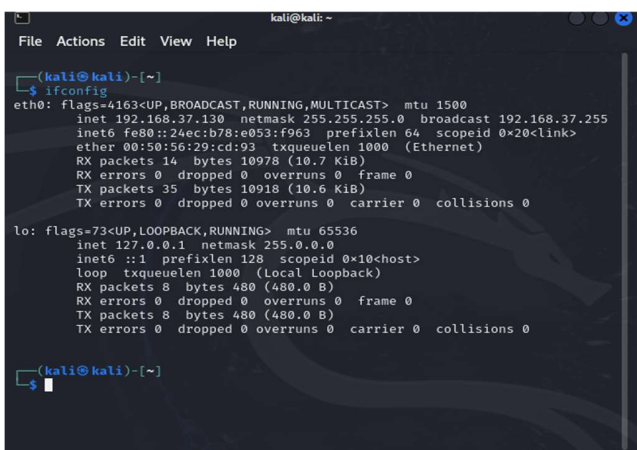
Result

The ARP Spoofing attack was successful. The target machine's ARP table was manipulated to redirect traffic through the attack machine. HTTP data from the target machine was intercepted and analyzed using Wireshark.

Screenshots

(Included the following screenshots for reference):

Ifconfig & Ipconfig



```
kali@kali: ~  
File Actions Edit View Help  
$ ifconfig  
eth0: flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500  
    inet 192.168.37.130 netmask 255.255.255.0 broadcast 192.168.37.255  
    inet6 fe80::24ec:b78:e053:f963 prefixlen 64 scopeid 0x20<link>  
    ether 00:50:56:29:cd:93 txqueuelen 1000 (Ethernet)  
    RX packets 14 bytes 10978 (10.7 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 35 bytes 10918 (10.6 KiB)  
    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 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
$
```

ASSIGNMENT REPORT: ARP SPOOFING BY- SRIDHAR S

```
Administrator: Command Prompt

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\admin>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::2921:c230:3005:703a%3
    IPv4 Address. . . . . : 192.168.37.129
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.37.2

Tunnel adapter isatap.localdomain:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : localdomain

C:\Users\admin>
```

- Initial ARP table (`arp -a`) from Windows.

```
Select Administrator: Command Prompt

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\admin>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::2921:c230:3005:703a%3
    IPv4 Address. . . . . : 192.168.37.129
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.37.2

Tunnel adapter isatap.localdomain:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : localdomain

C:\Users\admin>arp -a

Interface: 192.168.37.129 --- 0x3
    Internet Address      Physical Address         Type
    192.168.37.1          00-50-56-c0-00-08       dynamic
    192.168.37.2          00-50-56-f7-98-84       dynamic
    192.168.37.130        00-50-56-29-cd-93       dynamic
    192.168.37.254        00-50-56-fb-e4-d7       dynamic
    192.168.37.255        ff-ff-ff-ff-ff-ff       static
    224.0.0.9             01-00-5e-00-00-09       static
    224.0.0.22            01-00-5e-00-00-16       static
    224.0.0.252           01-00-5e-00-00-fc       static
    239.255.255.250       01-00-5e-7f-ff-fa       static
    255.255.255.255       ff-ff-ff-ff-ff-ff       static

C:\Users\admin>
```

- IP forwarding command and its result in Kali Linux.

ASSIGNMENT REPORT: ARP SPOOFING BY- SRIDHAR S

```
root@kali: /home/kali
File Actions Edit View Help

(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
# cat /proc/sys/net/ipv4/ip_forward
0

(root㉿kali)-[/home/kali]
# echo 1 > /proc/sys/net/ipv4/ip_forward

(root㉿kali)-[/home/kali]
# cat /proc/sys/net/ipv4/ip_forward
1

(root㉿kali)-[/home/kali]
#
```

- Ettercap host list and target selection.

```
Ettercap
0.8.3.1 (EB)

Host List x

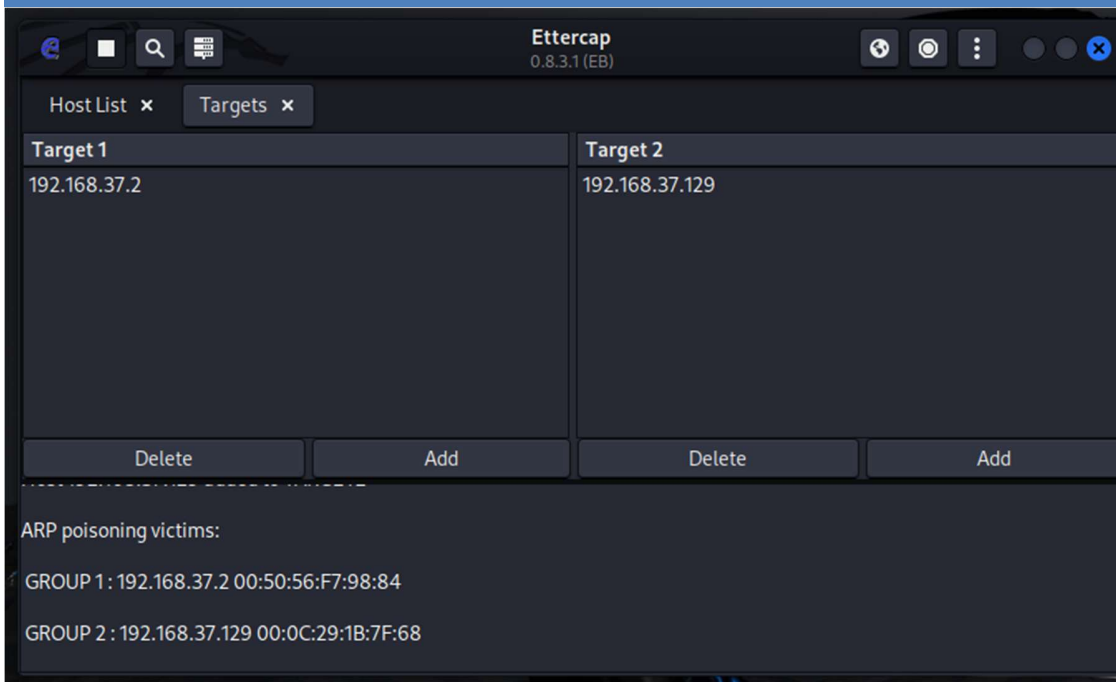
IP Address  MAC Address  Description
192.168.37.1  00:50:56:C0:00:08
192.168.37.2  00:50:56:F7:98:84
192.168.37.129  00:0C:29:1B:7F:68
192.168.37.254  00:50:56:FB:E4:D7

Delete Host  Add to Target 1  Add to Target 2

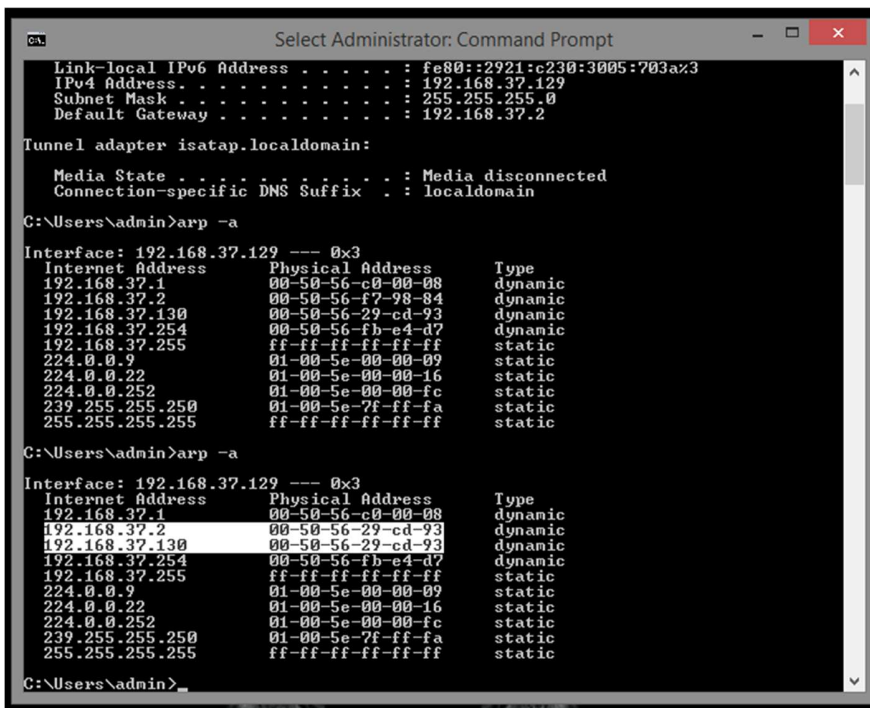
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Host 192.168.37.2 added to TARGET1
Host 192.168.37.129 added to TARGET2
```

- Ettercap showing ARP Poisoning groups.

ASSIGNMENT REPORT: ARP SPOOFING BY- SRIDHAR S

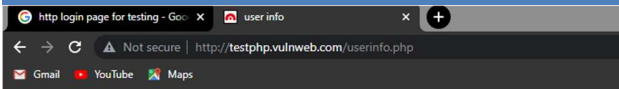


- Modified ARP table from Windows.



- Captured HTTP traffic in Wireshark.

ASSIGNMENT REPORT: ARP SPOOFING BY- SRIDHAR S



acunetix **acuart**

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo | Logout test

search art

John Smith (test)

On this page you can visualize or edit you user information.

Name:

Credit card number:

E-Mail:

Phone number:

Address:

You have 0 items in your cart. You visualize you cart here.

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip. Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

No.	Time	Source	Destination	Protocol	Length	Info
21409	591.087079179	44.228.249.3	192.168.37.129	HTTP	338	HTTP/1.1 302 Found (text/html)
21411	591.092513581	192.168.37.129	44.228.249.3	HTTP	370	GET /login.php HTTP/1.1
21416	591.393660095	44.228.249.3	192.168.37.129	HTTP	1342	HTTP/1.1 200 OK (text/html)
21454	618.302179609	192.168.37.129	44.228.249.3	HTTP	699	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
21480	618.734131211	44.228.249.3	192.168.37.129	HTTP	1514	HTTP/1.1 200 OK (text/html)
21647	645.426351214	192.168.37.129	44.228.249.3	HTTP	824	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
21661	645.834297922	44.228.249.3	192.168.37.129	HTTP	1498	HTTP/1.1 200 OK (text/html)
21876	713.705059613	192.168.37.129	163.182.194.25	HTTP	526	GET /login/login.asp HTTP/1.1
21886	714.041698267	163.182.194.25	192.168.37.129	HTTP	799	HTTP/1.1 200 OK (text/html)
21892	714.085095584	192.168.37.129	163.182.194.25	HTTP	484	GET /favicon.ico HTTP/1.1
21948	714.421111695	163.182.194.25	192.168.37.129	HTTP	1337	HTTP/1.1 404 Object Not Found (text/html)
21968	727.602341199	192.168.37.129	163.182.194.25	HTTP	757	POST /login/login_results.asp HTTP/1.1 (application/x-www-form-urlencoded)
21972	727.959744946	163.182.194.25	192.168.37.129	HTTP	143	HTTP/1.1 100 Continue
21977	728.460871745	163.182.194.25	192.168.37.129	HTTP	376	HTTP/1.1 200 OK (text/html)
22022	738.933053723	192.168.37.129	44.228.249.3	HTTP	558	GET /login.php HTTP/1.1
22035	739.226980124	44.228.249.3	192.168.37.129	HTTP	1375	HTTP/1.1 200 OK (text/html)
22109	748.539873331	192.168.37.129	44.228.249.3	HTTP	726	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
22115	748.828710332	44.228.249.3	192.168.37.129	HTTP	65	HTTP/1.1 200 OK (text/html)
22123	750.975148088	192.168.37.129	44.228.249.3	HTTP	827	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
22136	751.168977742	44.228.249.3	192.168.37.129	HTTP	1494	HTTP/1.1 200 OK (text/html)

Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
Origin: http://testphp.vulnweb.com\r\n
Content-Type: application/x-www-form-urlencoded\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Referer: http://testphp.vulnweb.com/userinfo.php\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
Cookie: login=test%2Ftest\r\n\r\n

[Response in frame: 22136]
[Full request URI: http://testphp.vulnweb.com/userinfo.php]

File Data: 117 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "username" = "John Smith123"
Form item: "ucc" = "1234-5678-2300-9000"
Form item: "uemail" = "email@email.com"
Form item: "uphone" = "2323345"
Form item: "uaddress" = "21 street"
Form item: "update" = "update"

The full requested URI (including host name) (http.request.full_uri) | Packets: 22332 - Displayed: 433 (1.9%) | Profile: Default

ASSIGNMENT REPORT: ARP SPOOFING BY- SRIDHAR S

http login page for testing - Google Chrome x login page x +

Not secure | http://testphp.vulnweb.com/login.php

Gmail YouTube Maps

acunetix **acuart**

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)


Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)



[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

Windows taskbar: Start, File Explorer, Google Chrome, Terminal

Ettercap 0.8.3.1 (EB)

Host List x Targets x

Target 1	Target 2
192.168.37.2	192.168.37.129
<input type="button" value="Delete"/>	<input type="button" value="Add"/>

ARP poisoning victims:

GROUP 1: 192.168.37.2 00:50:56:F7:98:84

GROUP 2: 192.168.37.129 00:0C:29:1B:7F:68

HTTP: 44.228.249.3:80 -> USER: kali PASS: arptestng INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=kali&pass=arptestng

HTTP: 44.228.249.3:80 -> USER: test PASS: test INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=test&pass=test

HTTP: 44.228.249.3:80 -> USER: test PASS: test INFO: http://testphp.vulnweb.com/login.php
CONTENT: uname=test&pass=test

ARP poisoner deactivated.
RE-ARPing the victims...