



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



Internet Security (IS)

Lab – Hacking Data Packets

Faculty of Architecture, Computing & Engineering

School of Applied Computing

Mount Pleasant Campus

Swansea

SA1 6ED

Data packet sniffing in computer networks

Computers communicate using networks. These networks could be on a local area network (LAN) or exposed to the Internet. **Network sniffers are programs that capture low-level package data that is been transmitted over a network.** An attacker can analyze this sniffed data to discover valuable information such as user ids and passwords.

In this lab exercise, we will introduce you to common network sniffing techniques and tools used to sniff data from computer networks. We will also look at counter measures that you can put in place to protect sensitive information transmitted over a computer network.

Topics covered in this tutorial

- What is IP & MAC Address?
- What is network sniffing?
- Active and passive sniffing.
- What is Address Resolution Protocol (ARP) Poisoning?
- Hacking Activity: Configure Static ARP in Windows.
- What is Media Access Control (MAC) Flooding?
- Hacking Activity: Sniff Network.

What is IP and MAC Address?

IP Address is the acronym for Internet Protocol address. An internet protocol address is used to uniquely identify a computer or device such as printers, storage disks on a computer network. There are currently two versions of IP addresses. IPv4 uses 32 bit numbers. Due to the massive growth of the internet, IPv6 has been developed and it uses 128 bit numbers.

IPv4 addresses are formatted in four groups of numbers separated by dots. The minimum number is 0 and the maximum number is 255. An example of an IPv4 address looks like this;

127.0.0.1

IPv6 addresses are formatted in groups of six numbers separated by full colons. The group numbers are written as 4 hexadecimal digits. An example of an IPv6 address looks like this;

2001:0db8:85a3:0000:0000:8a2e:0370:7334

In order to simplify the representation of the IP addresses in text format, leading zeros are omitted and group of zeros are completely omitted. The above address in a simplified format is displayed as;

2001:db8:85a3::8a2e:370:7334

MAC Address is the acronym for media access control address. MAC addresses are used to

uniquely identify network interfaces for communication at the physical layer of the network. MAC addresses are usually embedded into the network card.

A MAC address is like a serial number of a phone while the IP address is like the phone number.

Exercise

Remove any in your CD drive and boot the computer in Windows operating system. Open the command prompt and type the following command: **ipconfig /all**

You will get detailed information about all the network connections available on your computer. The results shown below are for a broadband modem. It shows the MAC address and IPv4 address. It also shows IP ver 6 address.

```
Mobile Broadband adapter Mobile Broadband Connection 3:
Connection-specific DNS Suffix . : 
Description . . . . . : HUAWEI Mobile Connect - Network Adapter #
3
Physical Address. . . . . : 58-2C-80-13-92-63 ← MAC Address
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 10.131.70.186 (Preferred)
Subnet Mask . . . . . : 255.255.255.252
Default Gateway . . . . . : 10.131.70.185 ← IPv4 Address
DNS Servers . . . . . : 41.223.4.97
                        41.223.5.33
NetBIOS over Tcpip. . . . . : Enabled
```

Figure 1: MAC address and ver 4 IP address.

```
Tunnel adapter Teredo Tunneling Pseudo-Interface:
Connection-specific DNS Suffix . : 
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:0:9d38:6ab8:28fc:13be:3a05:bf3b (Preferred)
Link-local IPv6 Address . . . . . : fe80::28fc:13be:3a05:bf3b%16 (Preferred)
Default Gateway . . . . . : ::
NetBIOS over Tcpip. . . . . : Disabled
```

Figure 2: IP ver 6 address.

What is network sniffing?

Computers communicate by broadcasting messages on a network using IP addresses. Once a message has been sent on a network, the recipient computer with the matching IP address responds with its MAC address.

Network sniffing is the process of intercepting data packets sent over a network. This can be done by specialized software program or hardware equipment. Sniffing can be used to;

- Capture sensitive data such as login credentials.

- Eavesdrop on chat messages.
- Capture files been transmitted over a network.

The following are protocols that are vulnerable to packet sniffing:

- Telnet
- Rlogin
- HTTP
- SMTP
- NNTP
- POP
- FTP
- IMAP

The above protocols are vulnerable if login details are sent in plain text.

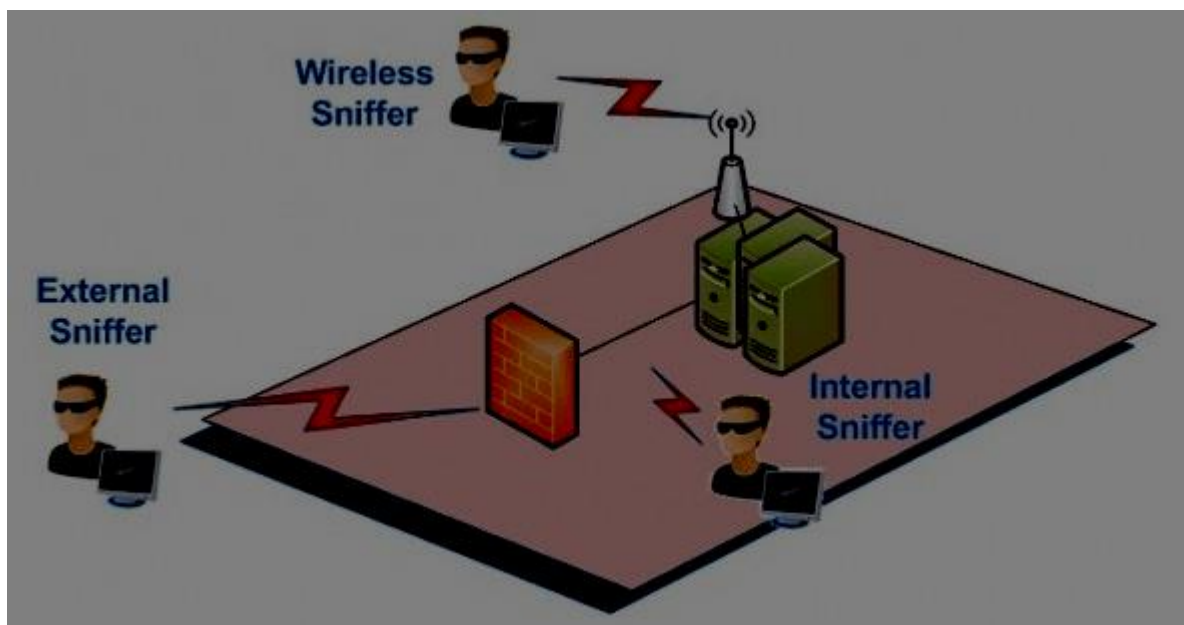


Figure 3: Data packet sniffing.

Passive and Active Sniffing

Before we look at passive and active sniffing, let's look at two major devices used in networking computers. These are hubs and switches.

A hub works by sending broadcast messages to all output ports on it except the one that has sent the broadcast. The recipient computer responds to the broadcast message if the IP address matches. This means when using a hub, all the computers on a network can see the broadcast message. It operates at the physical layer (layer 1) of the OSI Model.

Figure 4 below illustrates how the hub works.

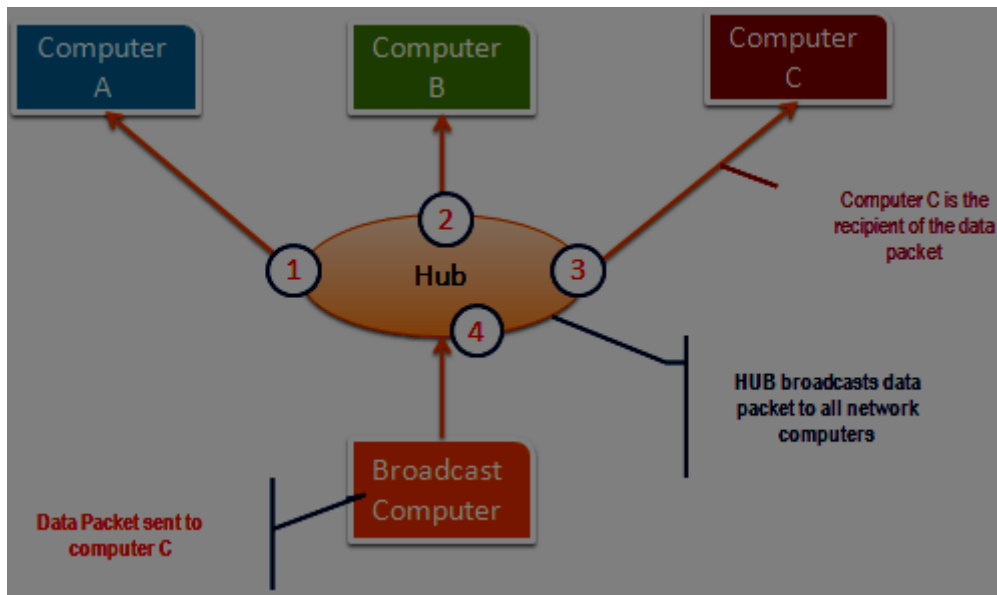


Figure 4: How the Hub works.

A switch works differently; it maps IP/MAC addresses to physical ports on it. Broadcast messages are sent to the physical ports that match the IP/MAC address configurations for the recipient computer. This means broadcast messages are only seen by the recipient computer. Switches operate at the data link layer (layer 2) and network layer (layer 3).

Figure 5 below illustrates how the switch works.

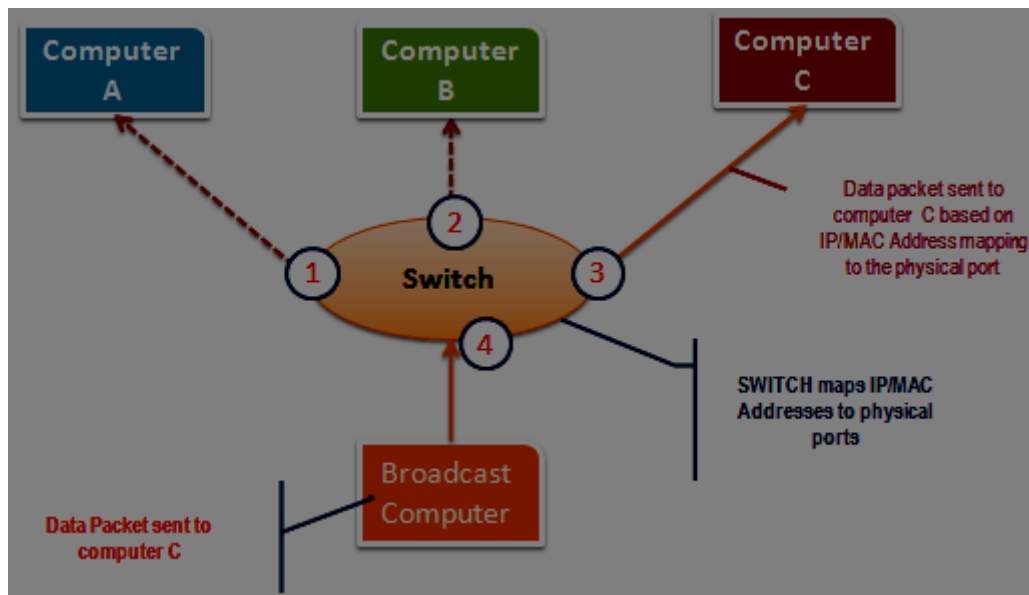


Figure 5: How the Switch works.

Passive sniffing is intercepting packages transmitted over a network that uses a hub. It is called passive sniffing because it is difficult to detect. It is also easy to perform as the hub sends broadcast messages to all the computers on the network.

Active sniffing is intercepting packages transmitted over a network that uses a switch.

There are two main methods used to sniff switch linked networks, ARP poisoning and MAC flooding.

What is ARP Poisoning?

ARP is the acronym for Address Resolution Protocol. It is used to convert IP address to physical addresses [MAC address] on a switch. The host computer sends an ARP broadcast on the network and the recipient computer responds with its physical address [MAC Address]. The resolved IP/MAC address is then used to communicate. **ARP poisoning is sending fake MAC addresses to the switch so that it can associate the fake MAC addresses with the IP address of a genuine computer on a network and hijack the traffic.**

ARP Poisoning Countermeasures

Static ARP entries: these can be defined in the local ARP cache and the switch configured to ignore all auto ARP reply packets. The disadvantage of this method is, it's difficult to maintain on large networks. IP/MAC address mapping have to be distributed to all the computers on the network.

ARP poisoning detection software: these systems can be used to cross check the IP/MAC address resolution and certify them if they are authenticate. Unidentified IP/MAC address resolutions can then be blocked.

Operating System Security: this measure is dependent on the operating system being used. The following are the basic techniques used by various operating systems.

- **Linux based:** these work by ignoring unsolicited ARP reply packets.
- **Microsoft windows:** the ARP cache behavior can be configured via the registry. The following list includes some of the software that can be used to protect networks against sniffing;
 - **AntiARP**– provides protection against both passive and active sniffing
 - **Agnitum Outpost Firewall**–provides protection against passive sniffing
 - **XArp**– provides protection against both passive and active sniffing
- **Mac OS:** ArpGuard can be used to provide protection. It protects against both active and passive sniffing.

Lab Activity: Configure ARP entries in Windows

We are using Windows 7 for this exercise but the commands should be able to work on other versions of windows as well.

Open the command prompt and enter the following command:

```
arp -a
```

Explanation,

- **arp** calls the ARP configure program located in Windows/System32 directory.
- **The -a** is the parameter to display to contents of the ARP cache.

After running the above command, you will get result similar to Figure 6 below:

```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\DAEMON>arp -a

Interface: 192.168.1.38 --- 0xc
Internet Address      Physical Address      Type
192.168.1.1           00-23-f8-ce-fd-96     dynamic
192.168.1.33          64-27-37-1a-6a-05     dynamic
192.168.1.34          24-b6-fd-0f-49-e3     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-fc     static
224.0.0.253           01-00-5e-00-00-fd     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\DAEMON>
  
```

Figure 6: Calling and displaying ARP cache.

Note: dynamic entries are added and deleted automatically when using TCP/IP sessions with remote computers. Static entries are added manually and are deleted when the computer is restarted, the network interface card restarted or other activities that affect it.

Adding static entries

Open the command prompt then use the **ipconfig /all** command to get the IP and MAC address

```

Administrator: C:\Windows\system32\cmd.exe

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Centrino(R) Wireless-N 2230
Physical Address. . . . . : 60-36-DD-A6-C5-43
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b899:74a:33df:8cc5%12(Preferred)
IPv4 Address. . . . . : 192.168.1.33(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 03 January 2014 12:39:30
Lease Expires . . . . . : 06 January 2014 14:13:39
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 291518173
DHCPv6 Client DUID. . . . . : 00-01-00-01-19-9F-A9-BF-60-36-DD-A6-C5-43

DNS Servers . . . . . : 41.220.128.6
                     : 41.220.128.8
NetBIOS over Tcpip. . . . . : Enabled
  
```

Figure 7: Displaying IP and MAC addresses.

The MAC address is represented using the Physical Address and the IP address is IPv4Address.

Enter the following command

```
arp -s 192.168.1.38 60-36-DD-A6-C5-43
```

Note: The IP and MAC address will be different from the ones used here. This is because they are unique.

Use the following command to view the ARP cache: **arp -a**

You will get the following result as shown in Figure 8 below

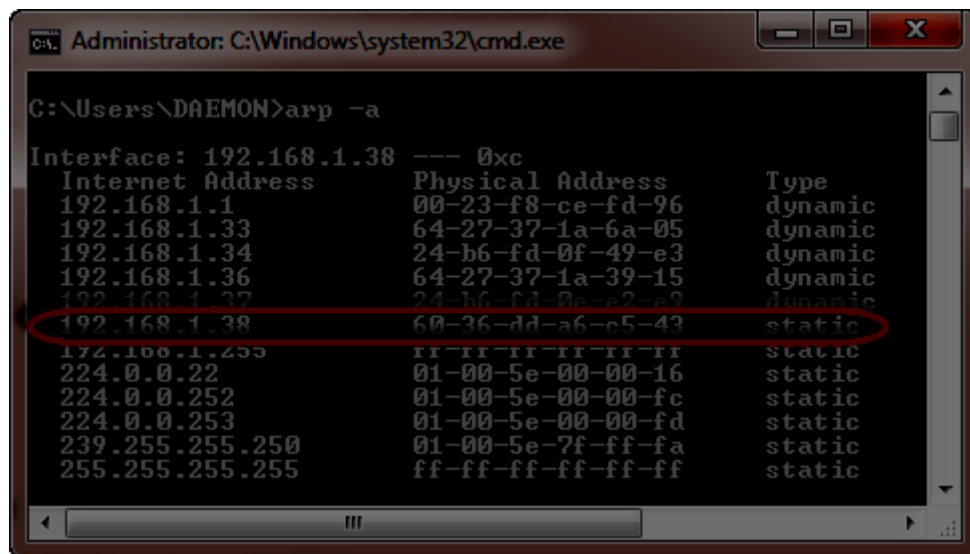


Figure 8: Resolving MAC and IP address.

Note the IP address has been resolved to the MAC address we provided and it is of a static type.

Deleting an ARP cache entry

Use the following command to remove an IP address entry

```
arp -d 192.168.1.38
```

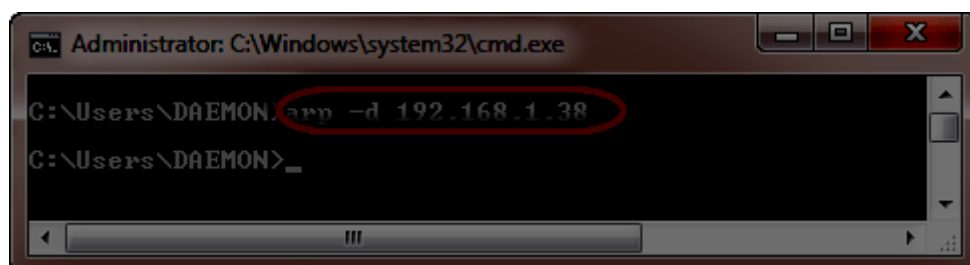


Figure 9: Removing IP address.

What is a MAC Flooding?

MAC flooding is a network sniffing technique that floods the switch MAC table with fake MAC addresses. This leads to overloading the switch memory and makes it act as a hub. Once the switch has been compromised, it sends the broadcast messages to all computers on a network. This makes it possible to sniff data packets as they sent on the network.

Counter Measures against MAC flooding

- **Some switches have port security feature.** This feature can be used to limit the number of MAC addresses on the ports. It can also be used to maintain a secure MAC address table in addition to the one provided by the switch.
- **Authentication, Authorization and Accounting servers** can be used to filter discovered MAC addresses.

Sniffing Counter Measures

- **Restriction to network physical media** highly reduces the chances of a network sniffer been installed
- **Encrypting messages** as they are transmitted over the network greatly reduces their value as they are difficult to decrypt.
- **Changing the network to a Secure Shell (SSH) network** also reduces the chances of the network been sniffed.

Hacking Activity: Sniff network traffic

In this practical scenario, we are going to **use Wireshark to sniff data packets as they are been transmitted over HTTP protocol.** For this example, we will sniff the network using Wireshark, then login to a web application that does not use secure communication. We will login to a web application on <http://www.techpanda.org/>

The login address is **admin@google.com** and the password is **Password2010**.

Note: We will login to the web app for demonstration purposes only. The technique can also sniff data packets from other computers that are on the same network as the one that you are using to sniff. The sniffing is not only limited to techpanda.org, it sniffs all HTTP and other protocols data packets.

Sniffing the network using Wireshark

The illustration in Figure 10 below shows you the steps that you will carry out in order to complete this exercise without confusion.

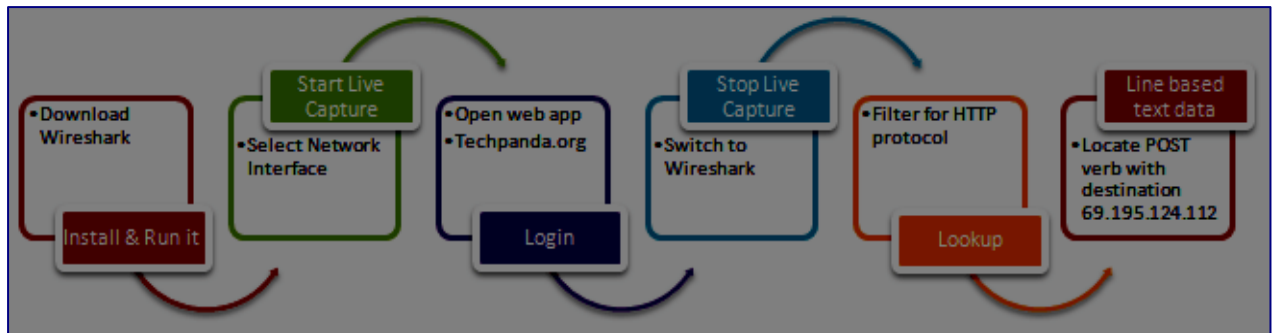


Figure 10: Data packet sniffing steps.

Download Wireshark from this link <http://www.wireshark.org/download.html>

- Install and open the Wireshark application.
- You will get the screen shown in Figure 11 below.

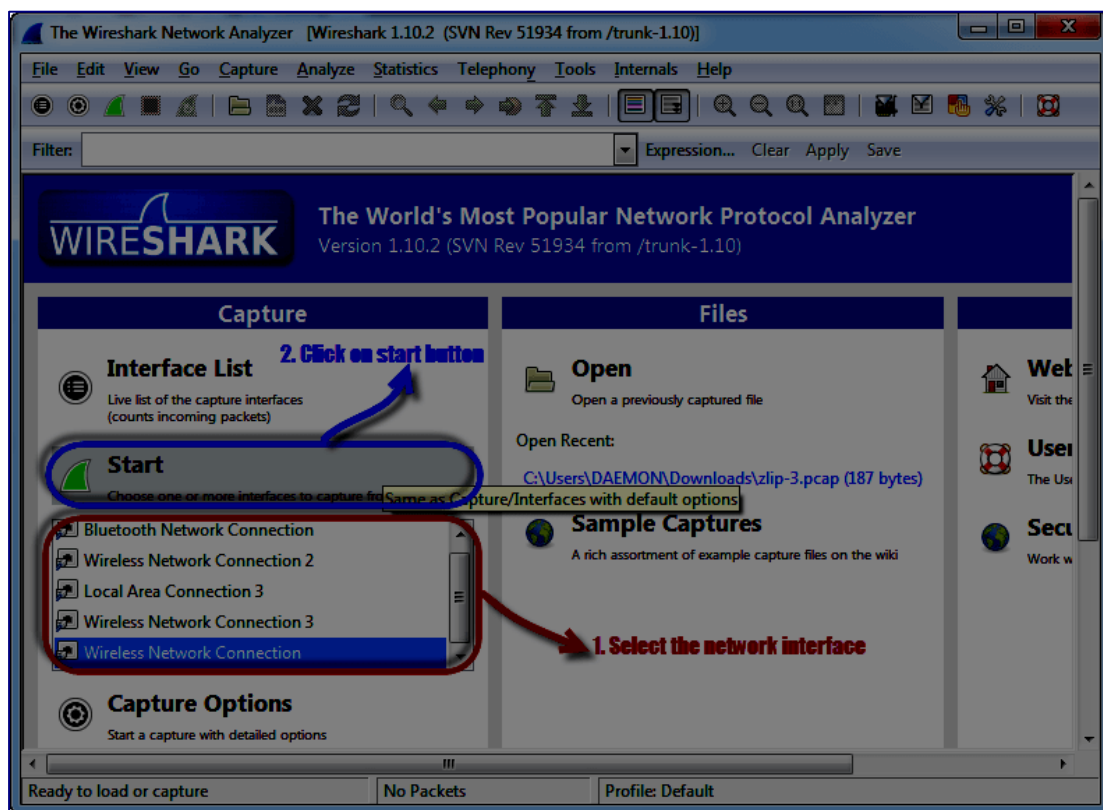


Figure 11: Wireshark application.

- Select the network interface you want to sniff. Note for this demonstration, we are using a wireless network connection. If you are on a local area network, then you should select the local area network interface.

- Click on start button as shown above.

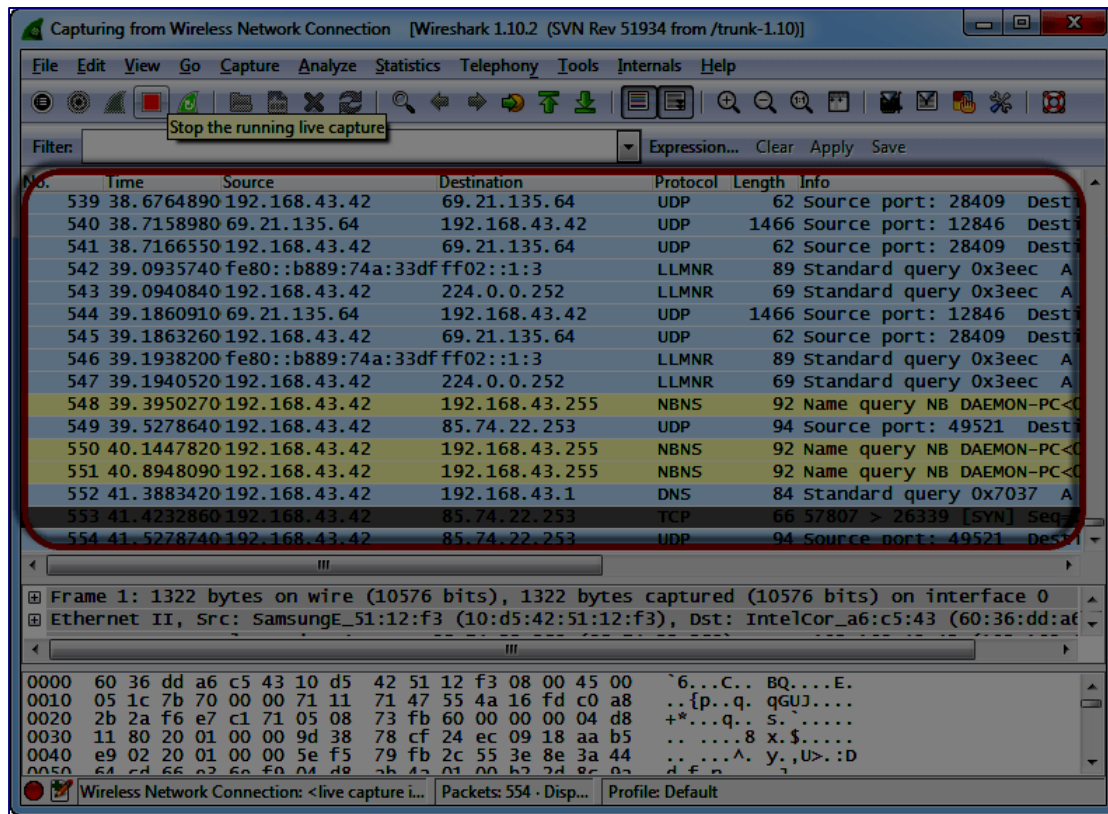


Figure 12: Wireshark capturing data.

- Open your web browser and type in <http://www.techpanda.org/>

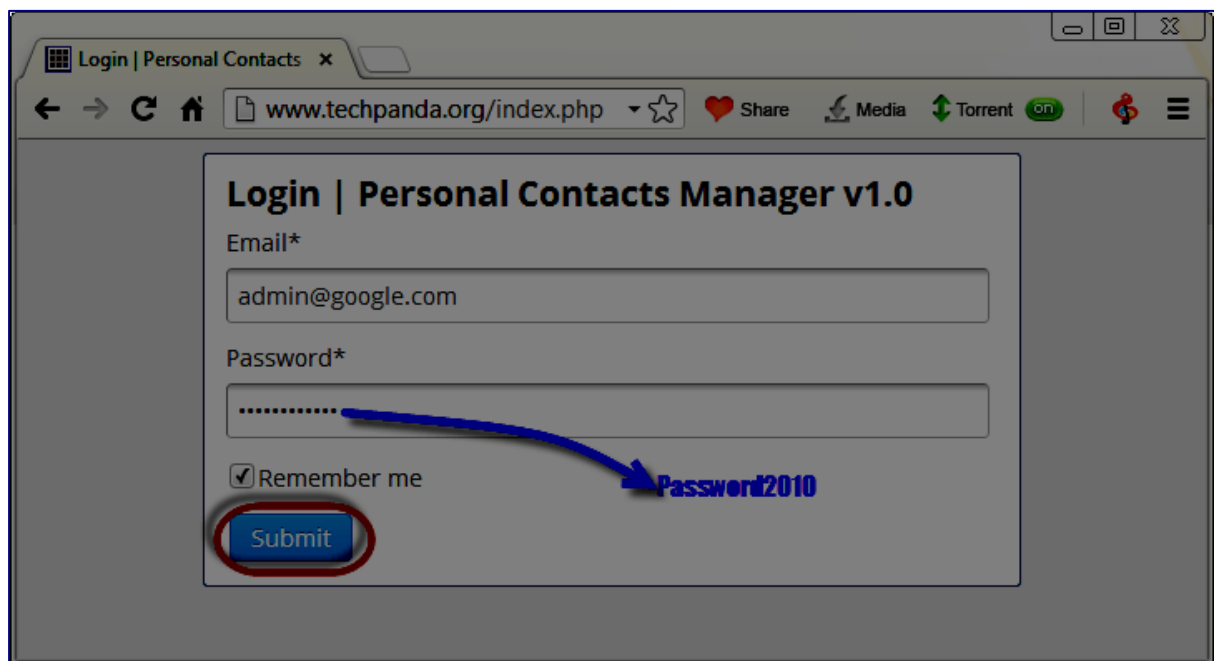


Figure 13: Login to techpanda.

- The login email is admin@google.com, the password is Password2010.
- Click on submit button.
- A successful login should give you the following dashboard:

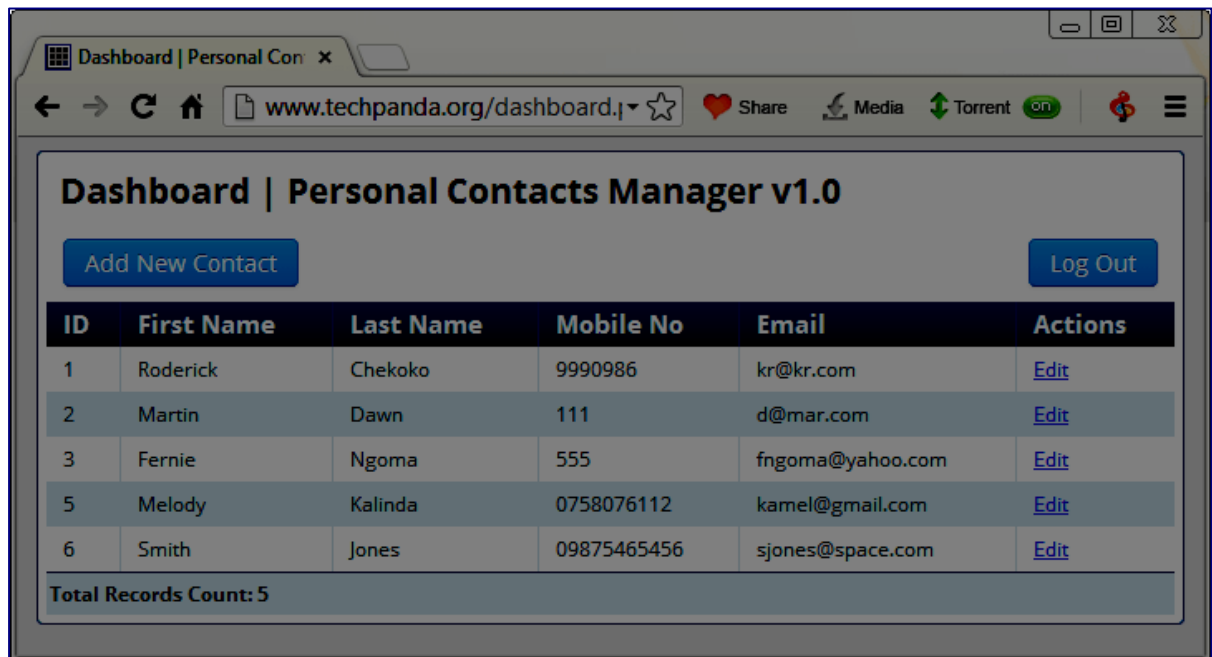


Figure 14: Successful login to techpanda.

- Go back to Wireshark and stop the live capture

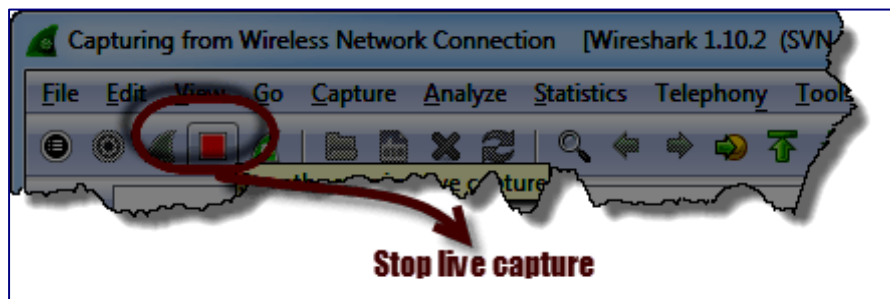


Figure 15: Stopping Wireshark data capture.

- Filter for HTTP protocol results only using the filter textbox.

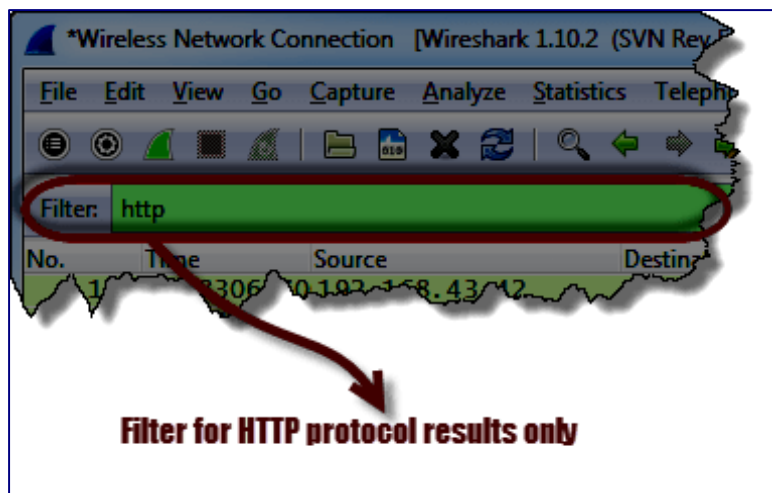


Figure 16: Filtering HTTP protocol results only.

- Locate the Info column and look for entries with the HTTP verb **POST** and click on it

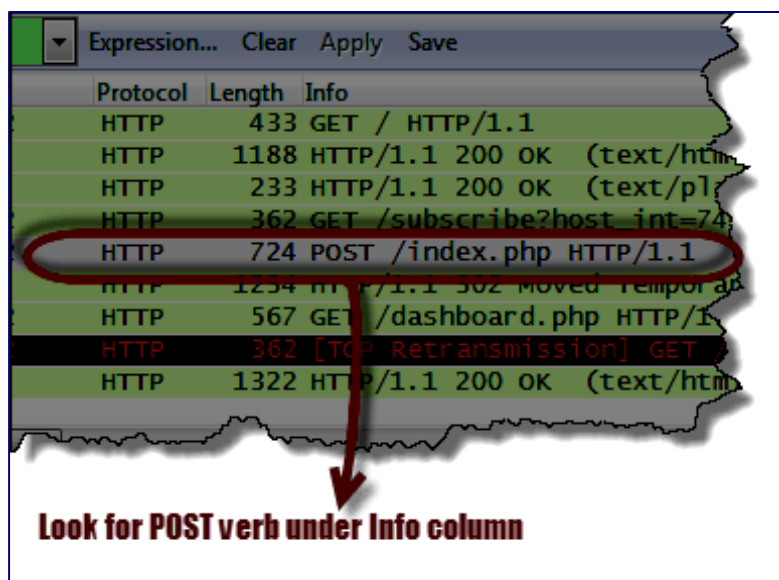


Figure 17: Identifying the “POST” verb.

- Just below the log entries, there is a panel with a summary of captured data. Look for the summary that says Line-based text data: application/x-www-form-urlencoded.

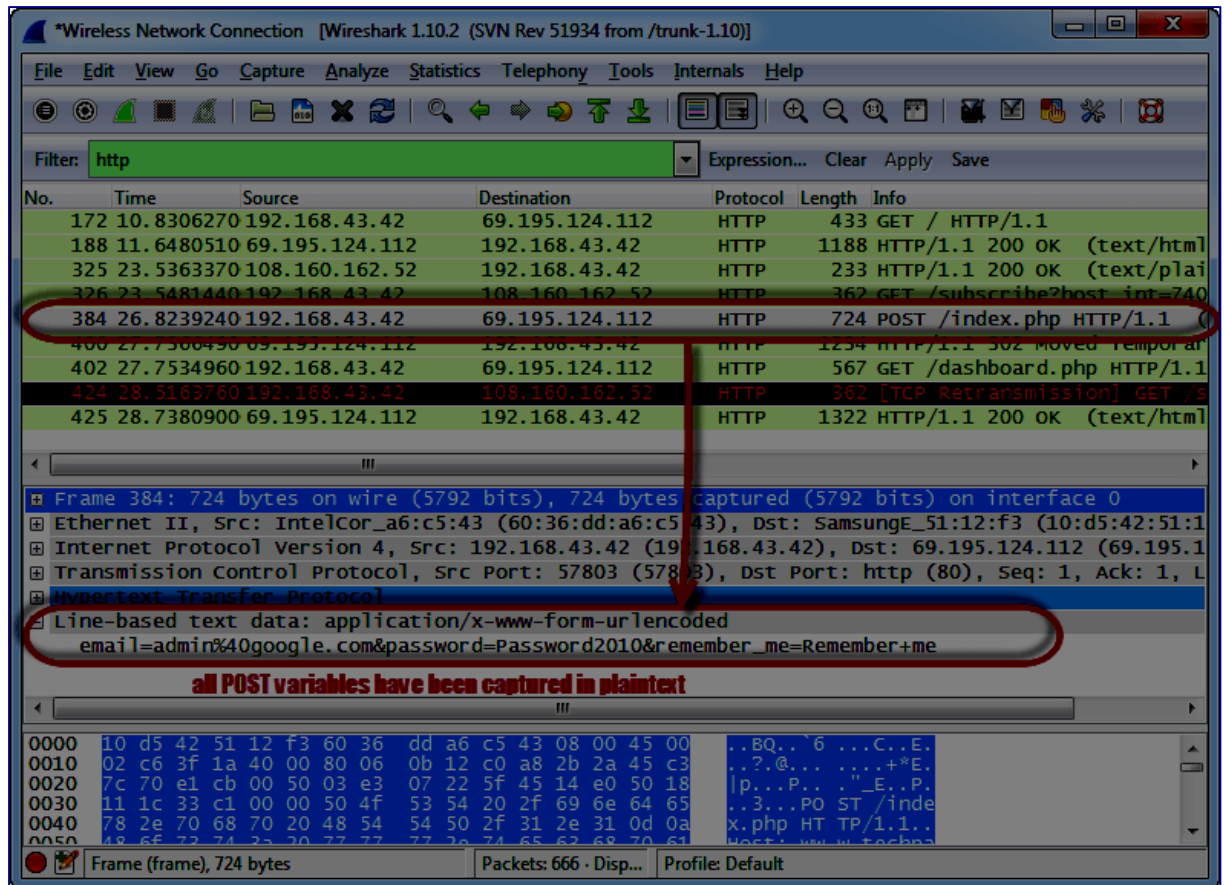


Figure 18: Viewing the plaintext value of “POST”.

- You should be able to view the plaintext values of all the POST variables submitted to the server via HTTP protocol.

Conclusion

- Network sniffing is intercepting packages as they are transmitted over the network.
- Passive sniffing is done on a network that uses a hub. It is difficult to detect.
- Active sniffing is done on a network that uses a switch. It is easy to detect.
- ARP poisoning works by sending fake MAC addresses to the switch.
- MAC flooding works by flooding the MAC table address list with fake MAC addresses. This makes the switch to operate like a HUB.
- Security measures as outlined above can help protect the network against data sniffing.

Credit: This lab exercise has been adapted from Guuru 99.