Sniffers

Module 8

Engineered by Hackers. Presented by Professionals.
Interclick purchases anonymous audience data from several vendors for the purpose of targeting advertising campaigns. Consequently, it has a number of quality control measures in place to understand the quality and effectiveness of this data. The code observed in the paper was a quality measure being tested.

Study of the Day: Which Websites Spy on Your Stuff?

According to a new study, your browsing history may be even less safe than the last time you heard about how your browsing history is not safe.

Researchers at the University of California trolled through a wide range of popular websites to determine which ones were collecting information ("history sniffing" or "history hijacking") about visitors.

Though it’s not surprising that YouPorn tops the list of spying sites, less racy sources like Technorati, TheSun.co.uk, and Wired were all fingered for tapping into your browsing habits. (Perez Hilton was on there too—but again, not that surprising.)

The information is often used to target advertising campaigns—a very lucrative field that companies like Interclick are capitalizing on. Their official statement is that the guilty script is meant only as a form of quality control.

http://goodmenproject.com
Module Objectives

- Lawful Intercept
- Wiretapping
- Sniffing Threats
- Types of Sniffing
- Hardware Protocol Analyzers
- MAC Attacks

- DHCP Attacks
- ARP Poisoning Attacks
- Spoofing Attack
- DNS Poisoning
- Sniffing Tools
- Countermeasures
Lawful Intercept

Lawful intercept is a process that enables a Law Enforcement Agency (LEA) to perform electronic surveillance on a target as authorized by a judicial or administrative order.

The LEA delivers a request for a wiretap to the target's service provider, who is responsible for intercepting data communication to and from the individual.

The service provider then intercepts the target's traffic as it passes through the router and sends a copy of the intercepted traffic to the LEA without the target's knowledge.

The surveillance is performed through the use of wiretaps on the traditional telecommunications and Internet services in voice, data, and multiservice networks.

The service provider uses the target's IP address or session to determine which of its edge routers handles the target's traffic (data communication).
Benefits of Lawful Intercept

- Allows multiple LEAs to run a lawful intercept on the same target without each other’s knowledge
- Hides information about lawful intercepts from all but the most privileged users
- Supports wiretaps in both the input and output direction
- Does not affect the subscriber’s services on the router
- Supports wiretaps of the individual subscribers who share a single physical interface
- Neither the administrator nor the calling parties are aware that packets are being copied or that the call is being tapped
- Provides two secure interfaces: one for setting up the wiretap and one for sending the intercepted traffic to the LEA
Network Components Used for Lawful Intercept

An intercept access point (IAP) is a device that **provides information** for the lawful intercept.

A mediation device (supplied by a third-party vendor) handles **most of the processing** for the lawful intercept.

The collection function is a program that **stores and processes the traffic** intercepted by the service provider.
Wiretapping

- Wiretapping is the process of monitoring the telephone and Internet conversations by a third party.
- Attackers connect a listening device (hardware, software or combination of both) to the circuit carrying information between two phones or hosts on Internet.

Types of Wiretapping

- Active Wiretapping: It only monitors and records the traffic.
- Passive Wiretapping: It monitors and records and also alters the traffic.

Note: Wiretapping without a warrant or the consent of the concerned person is a criminal offense in most countries.
Sniffing Threats

By placing a packet sniffer on a network in promiscuous mode, an attacker can capture and analyze all of the network traffic.

A packet sniffer can only capture packet information within a given subnet.

Many enterprises’ switch ports are open.

Usually any laptop can plug into the network and gain access to the network.

An attacker can steal sensitive information by sniffing the network.
How a **Sniffer** Works?

- Sniffer turns the NIC of a system to the **promiscuous mode** so that it listens to all the data transmitted on its segment.
- Sniffer can constantly read all information entering the computer through the NIC by **decoding the information** encapsulated in the data packet.
Hacker Attacking a Switch

- MAC Flooding
- DNS Poisoning
- ARP Poisoning
- DHCP Attacks
- Password Sniffing
- Spoofing Attack
Types of Sniffing: Passive Sniffing

“Passive sniffing” means sniffing through a hub. On a hub the traffic is sent to all ports.

Passive sniffing involves sending no packets, and monitoring the packets sent by the others.

Active sniffing involves sending out multiple network probes to identify APs. Hub usage is outdated today.
Types of Sniffing: **Active Sniffing**

- When sniffing is performed on a **switched network**, it is known as active sniffing.
- Active sniffing relies on **injecting packets** (ARP) into the network that causes traffic.

Active Sniffing Techniques:
- **MAC Flooding**
- **ARP Spoofing**
- **MAC Duplciating**
- **DHCP Starvation**

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Protocols Vulnerable to Sniffing

- Telnet and Rlogin: Keystrokes including user names and passwords
- HTTP: Data sent in clear text
- SMTP: Passwords and data sent in clear text
- NNTP: Passwords and data sent in clear text
- POP: Passwords and data sent in clear text
- FTP: Passwords and data sent in clear text
- IMAP: Passwords and data sent in clear text
Sniffers operate at the Data Link layer of the OSI model. They do not adhere to the same rules as applications and services that reside further up the stack.

If one layer is hacked, communications are compromised without the other layers being aware of the problem.
A hardware protocol analyzer is a piece of equipment that captures signals without altering the traffic in a cable segment.

It captures data packet and decodes and analyzes its content according to certain predetermined rules.

It can be used to monitor network usage and identify malicious network traffic generated by hacking software installed in the network.
SPAN port is a port which is configured to receive a copy of every packet that passes through a switch.

When connected to the SPAN port, an attacker can compromise the entire network.
MAC Flooding

1. MAC flooding involves flooding switch with numerous requests.

2. Switches have a limited memory for mapping various MAC addresses to the physical ports on switch.

3. MAC flooding makes use of this limitation to bombard switch with fake MAC addresses until the switch cannot keep up.

4. Switch then acts as a hub by broadcasting packets to all machines on the network and attackers can sniff the traffic easily.
MAC Address/CAM Table

- All Content Addressable Memory (CAM) tables have a **fixed size**
- It **stores information** such as MAC addresses available on physical ports with their associated VLAN parameters

48 Bit Hexadecimal Number Creates Unique Layer

Two Address

1258.3582.8DAB

First 24 bits = Manufacture Code
Assigned by IEEE

0000.0aXX.XXXX

Second 24 bits = Specific Interface,
Assigned by Manufacturer

0000.0aXX.XXXX

Broadcast Address

FFFF.FFFF.FFFF
How CAM Works?

1. CAM Table:
   - MAC: A, PORT: 1
   - MAC: C, PORT: 3
   B is unknown, broadcasts the ARP

2. CAM Table:
   - MAC: A, PORT: 1
   - MAC: B, PORT: 2
   - MAC: C, PORT: 3
   A is on port 1
   Learn: B is on port 2

3. CAM Table:
   - MAC: A, PORT: 1
   - MAC: B, PORT: 2
   - MAC: C, PORT: 3
   B is on port 2
   Does not see traffic to B
What Happens When CAM Table is Full?

- Once the CAM table on the switch is full, additional ARP request traffic will flood every port on the switch.
- This will basically turn a switch into a hub.
- This attack will also fill the CAM tables of adjacent switches.

<table>
<thead>
<tr>
<th>MAC</th>
<th>PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>3</td>
</tr>
<tr>
<td>Z</td>
<td>3</td>
</tr>
<tr>
<td>C</td>
<td>3</td>
</tr>
</tbody>
</table>

MAC A

Y is on Port 3

Traffic A → B

Port 1

MAC B

Traffic A → B

Port 2

MAC C

Z is on Port 3

Traffic A → B

Port 3

MAC C can see the traffic from A to B
Mac Flooding Switches with `macof`

- `macof` is a Linux tool that is a part of dsniff collection
- Macof sends random `source MAC` and `IP addresses`
- This tool `floods the switch’s CAM tables` (131,000 per min) by sending bogus MAC entries

```
macof -i eth1
```

```
18:b1:22:12:85:15 13:15:5a:6b:45:c4 0.0.0.0.0.25684 > 0.0.0.0.86254: s 2658741236:1235486715(0) win 512
12:a8:d8:15:4d:3b ab:4c:cd:5f:ad:cd 0.0.0.0.12387 > 0.0.0.0.78962: s 1238569742:782563145(0) win 512
13:3f:ab:14:25:95 66:ab:6d:4:b2:85 0.0.0.0.45638 > 0.0.0.0.4568: s 123587152:456312589(0) win 512
a2:2f:85:12:ac:2 12:85:2f:52:41:25 0.0.0.0.42358 > 0.0.0.0.35842: s 3256789512:3568742158(0) win 512
96:25:a3:5c:52:af 82:12:41:1:a0:d6 0.0.0.0.45213 > 0.0.0.0.2358: s 3684125687:3256874125(0) win 512
a2:8b:5c:6d:2a 5a:cc:fe:61:8a:df 0.0.0.0.12354 > 0.0.0.0.78521: s 1236542358:3698521475(0) win 512
55:42:ac:85:c5:96 a5:5f:ad:9d:12:aa 0.0.0.0.123 > 0.0.0.0.12369: s 8523695412:8523698742(0) win 512
a9:4d:4c:5a:5d:ad a4:ad:5f:4d:e9:ad 0.0.0.0.23685 > 0.0.0.0.45686: s 236854125:365145752(0) win 512
a3:e5:1a:25:2:a 25:35:a8:5d:af:fe 0.0.0.0.23685 > 0.0.0.0.85236: s 8623574125:3698521456(0) win 512
```
MAC Flooding Tool: Yersinia

Command Prompt

yersinia> en
Password:
yersinia# sh
  attacks       Show running attacks
  cdp           Cisco Discovery Protocol (CDP) information
  dhcp          Dynamic Host Configuration Protocol (DHCP) information
  dot1q         802.10 information
  dtp           Dynamic Trunking Protocol (DTP) information
  history       Display the session command history
  hsrp          Hot Standby Router Protocol (HSRP) information
  interfaces    Interface status
  stats         Show statistics
  stp           Spanning Tree Protocol (STP) information
  users         Display information about terminal lines
  version       System hardware and software status
  vtp           Virtual Trunking Protocol (VTP) information
How to Defend against MAC Attacks?

Configuring Port Security on Cisco switch:
1. switchport port-security
2. switchport port-security maximum 1 vlan access
3. switchport port-security violation restrict
4. switchport port-security aging time 2
5. switchport port-security aging type inactivity
6. snmp-server enable traps port-security trap-rate 5

Port security limits MAC flooding attack and locks down port and sends an SNMP trap
Module Flow

Sniffing Concepts
MAC Attacks
DHCP Attacks
ARP Poisoning Attacks
Sniffing Tools
Spoofing Attack
DNS Poisoning
Counter measures

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
How DHCP Works?

- DHCP servers maintain **TCP/IP configuration information** in a database such as valid TCP/IP configuration parameters, valid IP addresses, and duration of the lease offered by the server.
- It provides address configuration to DHCP-enabled clients in the form of a **lease offer**.

DHCP Discover (Broadcast) → DHCP Request (Broadcast) → DHCP Offer (Unicast) → DHCP Ack (Unicast) → Here Is Your Configuration

IP Address: 10.10.11.120
Subnet Mask: 255.255.255.16
Default Routers: 10.10.11.1
DNS Servers: 192.168.168.6, 192.168.168.7
Lease Time: 12 days
## DHCP Request/Reply Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPDISCOVER</td>
<td>Client Broadcast to Locate Available Servers</td>
</tr>
<tr>
<td>DHCPOFFER</td>
<td>Server to Client in Response to DHCPDISCOVER with Offer of Configuration Parameters</td>
</tr>
<tr>
<td>DHCPREQUEST</td>
<td>Client Message to Servers Either (a) Requesting Offered Parameters, (b) Confirming Correctness of Previously Allocated Address, or (c) Extending the Lease period</td>
</tr>
<tr>
<td>DHCPACK</td>
<td>Server to Client with Configuration Parameters, Including Committed Network Address</td>
</tr>
<tr>
<td>DHCPNAK</td>
<td>Server to Client Indicating Client’s Notion of Network Address Is Incorrect (e.g., Client Has Moved to New Subnet) or Client’s Lease As Expired</td>
</tr>
<tr>
<td>DHCPDECLINE</td>
<td>Client to Server Indicating Network Address Is Already in Use</td>
</tr>
<tr>
<td>DHCPRELEASE</td>
<td>Client to Server Relinquishing Network Address and Canceling Remaining Lease</td>
</tr>
<tr>
<td>DHCPINFORM</td>
<td>Client to Server, Asking Only for Local Configuration Parameters; Client Already Has Externally Configured Network Address</td>
</tr>
<tr>
<td>OP Code</td>
<td>Hardware Type</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Transaction ID (XID)</td>
<td></td>
</tr>
<tr>
<td>Seconds</td>
<td></td>
</tr>
<tr>
<td>Client IP Address (CIADDR)</td>
<td></td>
</tr>
<tr>
<td>Your IP Address (YIADDR)</td>
<td></td>
</tr>
<tr>
<td>Server IP Address (SIADDR)</td>
<td></td>
</tr>
<tr>
<td>Gateway IP Address (GIADDR)</td>
<td></td>
</tr>
<tr>
<td><strong>Client Hardware Address (CHADDR) — 16 bytes</strong></td>
<td></td>
</tr>
<tr>
<td>Server Name (SNAME) — 64 bytes</td>
<td></td>
</tr>
<tr>
<td>Filename — 128 bytes</td>
<td></td>
</tr>
<tr>
<td>DHCP Options</td>
<td></td>
</tr>
</tbody>
</table>
DHCP Starvation Attack

- Attacker broadcasts *discovery request for the entire DHCP scope* and tries to lease all of the DHCP addresses available in the DHCP scope.
- This is a *Denial of Service (DoS)* attack using DHCP leases.

1. DHCP Discovery (Broadcast) x (Size of Scope)
2. DHCP Offer (Unicast) x (Size of DHCPScope)
3. DHCP Request (Broadcast) x (Size of Scope)
4. DHCP Ack (Unicast) x (Size of Scope)
Rogue DHCP Server Attack

Attacker sets rogue DHCP server in the network and provides DHCP address to the user.

1. DHCP Discovery (Broadcast)
2. DHCP Offer (Unicast) from Rogue Server
3. DHCP Request (Broadcast)
4. DHCP Ack (Unicast) from Rogue Server

By running a rough DHCP server, an attacker can send incorrect TCP/IP settings:
- Wrong Default Gateway → Attacker is the gateway
- Wrong DNS server → Attacker is DNS server
- Wrong IP Address → Denial-of-Service with incorrect IP

IP Address: 10.10.11.120
Subnet Mask: 255.255.255.10
Default Routers: 10.10.11.130
DNS Servers: 192.168.168.6, 192.168.168.7
Lease Time: 12 days
DHCP Starvation Attack Tool: Gobbler

DHCP Scope
10.10.10.1
10.10.10.2
10.10.10.3
10.10.10.4
10.10.10.5
10.10.10.254
How to Defend Against **DHCP Starvation** and **Rogue Server Attack**?

Enable port security to defend against DHCP starvation attack

Enable DHCP snooping to defend against DHCP rogue server attack

**IOS Switch Commands**

- switchport port-security
- switchport port-security maximum 1
- switchport port-security violation restrict
- switchport port-security aging time 2
- switchport port-security aging type inactivity

**IOS Global Commands**

- ip dhcp snooping vlan 4,104
- no ip dhcp snooping information option
- ip dhcp snooping
Module Flow

Sniffing Concepts
MAC Attacks
DHCP Attacks
ARP Poisoning Attacks
Spoofing Attack
DNS Poisoning
Sniffing Tools
Counter measures

Sniffing
Techniques
Sniffing
Techniques
**What is Address Resolution Protocol (ARP)?**

1. **Address Resolution Protocol (ARP)** is a protocol for mapping an IP address to a physical machine address that is recognized in the local network.

2. The ARP protocol broadcasts the network machines to find out their physical MAC address.

3. When one machine needs to communicate with another, it looks up the ARP table. If the MAC address is not found in the table, the ARP is broadcasted over the network.

4. All machines on the network will compare this IP address to their MAC address.

5. If one of them identifies with this address, the machine will respond to ARP which will store the address pair in the ARP table and communication will take place.

---

**Example:**

**Hello,** I need the MAC address of 172.15.3.1. Think I’ll broadcast.

**Hi,** I’m 172.15.3.1, here is my MAC address: MAC: 0800.0400.1111.
ARP Spoofing Attack

ARP packets can be forged to send data to the attacker’s machine.

Switch is set in ‘forwarding mode’ after ARP table is flooded with spoofed ARP replies and attackers can sniff all the network packets.

ARP Spoofing involves constructing a large number of forged ARP request and reply packets to overload a switch.

Attackers flood a target computer’s ARP cache with forged entries which is also known as poisoning.
How Does ARP Spoofing Work?

1. Hey 10.1.1.1 are you there?
   
   User A (10.1.1.0)

2. Switch broadcasts ARP request onto the wire
   
   User B

3. Malicious user eavesdrops on the ARP request and responses and spoofs as the legitimate user
   
   Attacker

4. Information for IP address 10.1.1.1 is now being sent to MAC address 9:8:7:6:5:4

   User D

When a user A initiates a session with user B in the same Layer 2 broadcast domain, an ARP request is broadcasted using the user B's IP addresses and the user A waits for the user B to respond with a MAC address.
Threats of ARP Poisoning

Using fake ARP messages, an attacker can divert all communications between two machines so that all traffic is exchanged via his/her PC.

- Denial of Service (DoS) Attack
- Data Interception
- VoIP Call Tapping
- Stealing Passwords
- Manipulating Data
ARP Poisoning Tool: Cain and Abel

http://www.oxid.it
ARP Poisoning Tool: WinArpAttacker

http://www.xfocus.net
ARP Poisoning Tool: Ufasoft Snif

Ufasoft Snif is an automated ARP poisoning tool that sniffs passwords and email messages on the network. Works on Wi-Fi network as well.

http://www.ufasoft.com
How to Defend Against **ARP Poisoning**?

Use **DHCP Snooping Binding Table and Dynamic ARP Inspection**

```
sh ip dhcp snooping binding

<table>
<thead>
<tr>
<th>MacAddress</th>
<th>IpAddress</th>
<th>Lease</th>
<th>Type</th>
<th>VLAN</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0a:12:3b:2f:df:1c</td>
<td>10.10.10.8</td>
<td>125864</td>
<td>dhcp-</td>
<td>4</td>
<td>FastEthernet</td>
</tr>
<tr>
<td></td>
<td>10.10.8</td>
<td></td>
<td>snooping</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**DHCP Snooping Enabled**

**Dynamic ARP Inspection Enabled**

10.10.10.1
MAC A

No ARP entry in the binding table then discard the packet

10.10.10.2
MAC B

ARP 10.10.10.1 Saying 10.10.10.2 is MAC C

ARP 10.10.10.2 Saying 10.10.10.1 is MAC C

10.10.10.5
MAC C

Check the **MAC** and **IP** fields to see if the ARP from the interface is in the binding; if not, **traffic is blocked**.
Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)#
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 10
DHCP snooping is operational on following VLANs: 10
DHCP snooping is configured on the following L3 Interfaces:

DHCP snooping trust/rate is configured on the following Interfaces:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Trusted</th>
<th>Rate limit (pps)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Switch# show ip dhcp snooping binding

MacAddress      IpAddress  Lease  Type  VLAN  Interface
---------------------------------------------|---------|------|------|-------|---------|
1a:12:3b:2f:df:10  10.10.10.8  125864  dhcp-  4  FastEthernet  0/3

Total number of bindings: 1

Switch(config)# ip arp inspection vlan 10
Switch(config)#
Switch# show ip arp inspection
Source Mac Validation : Disabled
Destination Mac Validation : Disabled
IP Address Validation : Disabled
Vlan Configuration Operation ACL Match Static ACL
10    Enabled    Active
Vlan ACL Logging DHCP Logging Probe Logging
10    Deny     Deny     Off
Vlan Forwarded Dropped DHCP Drops ACL Drops
10    0   0   0
Vlan DHCP Permits ACL Permits Probe Permits Source MAC Failures
10    0   0   0   0
Vlan Dest MAC Failures IP Validation Failures Invalid Protocol Data
10    0   0   0   0
MAC Spoofing/Duplicating

- MAC duplicating attack is launched by **sniffing network for MAC addresses** of clients who are actively associated with a switch port and re-using one of those addresses.
- By listening to the traffic on the network, a malicious user can **intercept and use a legitimate user's MAC address** to receive all the traffic destined for the user.

**Switch Rule:**
- Allow access to the network only if your MAC address is A:B:C:D:E.

**No! My MAC Address is A:B:C:D:E**

**Attacker:**
- Sniffs the network for MAC addresses of the currently associated users and then uses that MAC address to attack other users associated to the same switch port.

**Note:** This technique works on Wireless Access Points with MAC filtering enabled.
Spoofing Attack Threats

MAC spoofing
- If MACs are used for network access, an attacker can gain access to the network.
- An attacker can take over someone's identity already on the network.

IP spoofing
- Ping of death
- ICMP unreachable storm
- SYN flood
- Trusted IP addresses can be spoofed
MAC Spoofing Tool: **SMAC**

![SMAC 2.0 GUI](image)

<table>
<thead>
<tr>
<th>Active</th>
<th>Spoofed</th>
<th>Network Adapter</th>
<th>IP Address</th>
<th>Active MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Bluetooth Personal Area Network from TOSHIBA</td>
<td>0.0.0.0</td>
<td>00-10-C6-EE-D6-91</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>VMware Virtual Ethernet Adapter for VMnet8</td>
<td>192.168.0.107</td>
<td>00-50-0B-F5-BD-23</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td></td>
<td>192.168.17.1</td>
<td>00-50-56-C0-00-08</td>
</tr>
</tbody>
</table>

**New Spoofed MAC Address:**

```
00 - 10 - FE - 81 - D6 - 91
```

**Digital Equipment Corporation [0010FE]**

- **Show Only Active Network Adapters**
- **Update MAC**
- **Remove MAC**
- **Restart Adapter**
- **Random**
- **IP Config**
- **MAC List**
- **Refresh**
- **Exit**

**Disclaimer:**

Use this program at your own risk. We are not responsible for any damage that may occur to any system. This program is not to be used for any illegal or unethical purpose. Do not use this program if you do not agree with the terms and conditions.

http://www.klcconsulting.net
How to Defend Against MAC Spoofing?

Use DHCP Snooping Binding Table, Dynamic ARP Inspection and IP Source Guard

DHCP Snooping Enabled
Dynamic ARP Inspection Enabled
IP Source Guard Enabled

IP and MAC entry in the binding table does not match then discard the packet

Traffic Sent with IP 10.10.10.5 Mac B

Traffic Sent with IP 10.10.10.2 Mac C

Received Traffic Source IP 10.10.10.2 Mac B

Check the MAC and IP fields to see if the traffic from the interface is in the binding table; if not, traffic is blocked
DNS Poisoning Techniques

1. DNS poisoning is a technique that **tricks a DNS server** into believing that it has received authentic information when, in reality, it has not.

2. It results in **substitution of a false Internet provider address** at the domain name service level where web addresses are converted into numeric Internet provider addresses.
Intranet DNS Spoofing

- For this technique, you must be connected to the local area network (LAN) and be able to sniff packets.
- It works well against switches with ARP poisoning the router.
Intranet DNS Spoofing

Internet DNS Spoofing, attacker **infects Rebecca’s machine** with a Trojan and changes her **DNS IP address** to that of the attacker’s.

1. **Attacker runs DNS Server in Russia (IP: 200.0.0.2)**
   - Attacker infects Rebecca’s computer by changing her DNS IP address to: 200.0.0.2
2. **DNS Request do to 200.0.0.2**
   - DNS Response located at 65.0.0.2
3. **Rebecca’s Browser connects to 65.0.0.2**
4. **Rebecca’s Browser connects to 65.0.0.2**
5. **Attacker sniffs the credential and redirects the request to real website**

What is the IP address of www.xsecurity.com

Real Website www.xsecurity.com
IP: 200.0.0.45

Fake Website
IP: 65.0.0.2

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Attacker sends a Trojan to Rebecca’s machine and changes her proxy server settings in Internet Explorer to that of the attacker’s.

**Diagram:**
- **Rebecca** (IP: 10.0.0.5)
- **Attacker** runs Proxy Server in Russia (IP: 200.0.0.2)
- **Real Website** (www.xsecurity.com, IP: 200.0.0.45)
- **Fake Website** (IP: 65.0.0.2)

1. Attacker infects Rebecca’s computer by changing her IE proxy address to 200.0.0.2.
2. All Rebecca’s Web requests go through the attacker’s machine.
3. Hacker sends Rebecca’s request to Fake Website.
4. Attacker’s fake website sniffs the credential and redirects the request to the real website.
DNS Cache Poisoning

DNS cache poisoning involves changing or adding records in the resolver cache of a DNS, so that a DNS query for a domain returns an IP address of a fake website set by the attacker.

If the server cannot validate that DNS responses have come from an authoritative source, it will cache the incorrect entries locally and serve them to users who make the same request.
How to Defend Against DNS Spoofing?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Resolve all DNS queries to local DNS server</td>
</tr>
<tr>
<td>02</td>
<td>Block DNS requests from going to external servers</td>
</tr>
<tr>
<td>03</td>
<td>Implement DNSSEC</td>
</tr>
<tr>
<td>04</td>
<td>Configure DNS resolver to use a new random source port from its available range for each outgoing query</td>
</tr>
<tr>
<td>05</td>
<td>Configure firewall to restrict external DNS lookup</td>
</tr>
<tr>
<td>06</td>
<td>Restrict DNS recursing service, either full or partial, to authorized users</td>
</tr>
<tr>
<td>07</td>
<td>Use DNS Non-Existent Domain (NXDOMAIN) Rate Limiting</td>
</tr>
</tbody>
</table>
Sniffing Tool: Wireshark

1. Wireshark is a free packet sniffing tool. Wireshark uses Winpcap to capture packets, so it can only capture the packets on the networks supported by Winpcap.


3. Captured files can be programmatically edited via command-line. A set of filters for customized data display can be refined using a display filter.

Attacker  Wireshark Tool  Network  Victim
Sniffing Tool: Wireshark

http://www.wireshark.org
Follow TCP Stream in Wireshark

Password revealed in TCP Stream
Display Filters in **Wireshark**

Display filters are used to **change the view of packets** in the captured files.

**Example:** Type the protocol in the filter box: **arp, http, tcp, udp, dns**

- **Specific Ports**
  - `tcp.port==23`
  - `ip.addr==192.168.1.100` or `machine`
  - `ip.addr==192.168.1.100 && tcp.port==23`

- **Addresses**
  - `ip.addr == 10.0.0.4` or `ip.addr == 10.0.0.5`

- **Filtering by IP Address**
  - `ip.addr == 10.0.0.4`
  - `ip.dst == 10.0.1.50 && frame.pkt_len > 400`
  - `ip.addr == 10.0.1.12 && icmp && frame.number > 15 && frame.number < 30`
  - `ip.src==205.153.63.30` or `ip.dst==205.153.63.30`

---

**CEH**

Certified Ethical Hacker

```
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
```

**ATHENA**

TRUNG TÂM BÀO TÀO AN NINH MẠNG & QUẢN TRI MẠNG

WWW.ATHENA.EDU.VN
Additional Wireshark Filters

1. Displays all TCP resets
   tcp.flags.reset==1

2. Displays all HTTP GET requests
   http.request

3. Displays all TCP packets that contain the word ‘traffic’
   tcp contains traffic

4. Sets a filter for the HEX values of 0x33 0x27 0x58 at any offset
   udp contains 33:27:58

5. Displays all retransmissions in the trace
   tcp.analysis.retransmission
Shifting Tool: CACE Pilot

http://www.cacotech.com
Sniffing Tool: **Tcpdump/Windump**

TCPdump is a very powerful command line interface packet sniffer which runs on Linux and Windows.

**TCPDump**
- Runs on Linux and UNIX systems

**Windump**
- Runs on Windows systems

```
tcpdump -i eth0
13:13:40.407606 10.20.21.09 > R1P2-ROUTERS.MCAST.NET.router = RIPv2
13:13:55.311192 :: > E92::1: icmpv: neighbor solic who has fe80:1
13:14:08.179269 :: > E92::1: icmp: neighbor solic who has fe80:1
13:14:09.374309 fe80::2eef:ff:fe00:1300:124 > iproute-allrouters: icmp: router ac
10:20:21.685725 10.20.21.55 > RIPv2-ROUTERS.MCAST.NET.udp
10:20:24.952408 vmsl.endicott.juggboy.com.router = RIPv2-ROUTERS.MCAST.NET.udp
```
Discovery Tool: **NetworkView**

- NetworkView is a network discovery and management tool for Windows
- **Discover TCP/IP nodes and routes** using DNS, SNMP, Ports, NetBIOS and WMI

[Image: NetworkView Screenshot](http://www.networkview.com)
Discovery Tool: The Dude Sniffer

The Dude sniffer scans all devices within the specified subnets and draws a detailed layout map.
Password Sniffing Tool: **Ace**

Ace Password Sniffer can *monitor and capture passwords* through FTP, POP3, HTTP, SMTP, Telnet, and webmail passwords.
Packet Sniffing Tool: Capsa Network Analyzer

Capsa network analyzer captures all data transmitted over the network and provides a wide range of analysis statistics in an intuitive and graphic way.

http://www.colasoft.com

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

ATHENA
TRUNG TÂM BÀO TÀO AN NINH MẠNG & QUẢN TRỊ MẠNG
WWW.ATHENA.EDU.VN
OmniPeek Network Analyzer

OmniPeek sniffer displays a Google Map in the OmniPeek capture window showing the locations of all the public IP addresses of captured packets.

This feature is a great way to monitor the network in real time, and show from where in the world that traffic is coming.
Network Packet Analyzer: Observer

Observer provides a comprehensive drill-down into network traffic and provides back-in-time analysis, reporting, trending, alarms, application tools, and route monitoring capabilities.
Session Capture Sniffer: **NetWitness**

NetWitness Investigator can locally capture live traffic and process packet files from virtually any existing network collection device for quick and easy analysis.

- Real-time, Patented Layer 7 Analytics
- Analyze data starting from application layer entities
- Extensive network and application layer filtering
- Integrated GeoIP for resolving IP addresses to city/county
- SSL Decryption (with server certificate)
- Interactive time charts, and summary view

---

**Filter Network**

**Capture Traffic**

**Analyze Traffic**

**Layer 7 Analytics**

**Summary View**
Session Capture Sniffer: NetWitness

http://www.netwitness.com

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Email Message Sniffer: **Big-Mother**

Big-Mother is an eavesdropping program that uses a switch sniffer to capture and analyze communication traffic over a home network. It logs in real time URL visits, Email, chats, games, FTP, and data flows, and also takes webpage snapshots, duplicates Email and FTP copies, records MSN messenger content, and gives statistical reports.

[Website: www.tupsoft.com]

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
TCP/IP Packet Crafter: Packet Builder

http://www.colasoft.com

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.
Additional Sniffing Tools

- EtherDetect Packet Sniffer
  http://www.etherdetect.com

- Ettercap
  http://ettercap.sourceforge.net

- dsniff
  http://monkey.org

- Windump
  http://www.winpcap.org

- EffeTech HTTP Sniffer
  http://www.effetech.com

- SmartSniff
  http://www.nirsoft.net

- Ntop
  http://www.ntop.org

- EtherApe
  http://etherape.sourceforge.net
Additional Sniffing Tools

- Network Probe
  http://www.objectplanet.com

- Snort
  http://www.snort.org

- Colasoft MSN Monitor
  http://www.colasoft.com

- Sniff'em
  http://www.sniff-em.com

- MaaTec Network Analyzer
  http://www.maatec.com

- Alchemy Network Monitor
  http://www.mishelpers.com

- CommView
  http://www.tamos.com

- NetResident
  http://www.tamos.com
Additional Sniffing Tools

- **Kismet**
  - http://www.kismetwireless.net

- **IE HTTP Analyzer**
  - http://www.ieinspector.com

- **AIM Sniffer**
  - http://www.effetech.com

- **MiniStumbler**
  - http://www.stumbler.net

- **Netstumbler**
  - http://www.stumbler.net

- **PacketMon**
  - http://www.analogx.com

- **Packet Sniffer**

- **EtherScan Analyzer**
  - http://www.etherscan.com
Additional Sniffing Tools

- NADetector
  - http://www.nsauditor.com

- Microsoft Network Monitor
  - http://www.microsoft.com

- NetworkMiner

- Jitbit Network Sniffer
  - http://www.jitbit.com

- PRTG Network Monitor
  - http://www.paessler.com

- Sniff-O-Matic
  - http://www.kwakkelflap.com

- Network Security Toolkit
  - http://www.networksecuritytoolkit.org

- Atelier Web Ports Traffic Analyzer (AWPTA)
  - http://www.atelierweb.com
How an Attacker Hacks the Network Using Sniffers?

1. An attacker connects his laptop to a switch port
2. He runs discovery tools to learn about network topology
3. He identifies victim’s machine to target his attacks
4. He poisons the victim machine by using ARP spoofing techniques
5. The traffic destined for the victim machine is redirected to the attacker
6. The hacker extracts passwords and sensitive data from the redirected traffic
How to Defend Against Sniffing?

- Restrict the physical access to the network media to ensure that a packet sniffer cannot be installed.
- Use encryption to protect confidential information.
- Permanently add the MAC address of the gateway to the ARP cache.
- Use static IP addresses and static ARP tables to prevent attackers from adding the spoofed ARP entries for machines in the network.
- Turn off network identification broadcasts and if possible restrict the network to authorized users in order to protect network from being discovered with sniffing tools.
- Use IPv6 instead of IPv4 protocol.
- Use encrypted sessions such as SSH instead of Telnet, Secure Copy (SCP) instead of FTP, SSL for e-mail connection, etc to protect wireless network users against sniffing attacks.
Sniffing Prevention Techniques

- Use PGP and S/MIME
- Use VPNs (Virtual Private Networks)
- Use Secure Shell (SSH)
- Use IP Security (IPSec)
- Use One-time passwords (OTP)
- Use SSL/TLS Protocol
How to Detect Sniffing?

**Promiscuous Mode**
You will need to check which machines are running in the promiscuous mode.

Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety.

**Network Tools**
Run network tools such as HP Performance Insight to monitor the network for strange packets.

It enables you to collect, consolidate, centralize and analyze traffic data across different network resources and technologies.

**IDS**
Run IDS and notice if the MAC address of certain machines has changed (Example: router’s MAC address).

IDS can alert the administrator about suspicious activities.
Promiscuous Detection Tool: **PromqryUI**

PromqryUI is a security tool from Microsoft that can be used to **detect network interfaces** that are running in promiscuous mode.

http://www.microsoft.com
Promiscuous Detection Tool: PromiScan
By placing a packet sniffer in a network, attackers can capture and analyze all the network traffic.

Attackers can sniff confidential information such as email and chat conversations, passwords, and web traffic.

Sniffing is broadly categorized as passive and active; passive sniffing refers to sniffing from a hub-based network whereas active sniffing refers to sniffing from a switch-based network.

Sniffers operate at the Data Link layer of the OSI model and do not adhere to the same rules as applications and services that reside further up the stack.

Attackers use MAC Attacks, DHCP Attacks, ARP Poisoning Attacks, Spoofing Attack and DNS Poisoning techniques to sniff network traffic.

Major countermeasures for sniffing include using static IP addresses and static ARP tables, and using encrypted sessions such as SSH instead of Telnet, Secure Copy (SCP) instead of FTP, SSL for data transmission.
“The young security pro knows the rules, but the old security pro knows the exceptions.”

- Oliver Wendell Holmes,
  An American Physician,
  Professor, Lecturer, and
  Author