Sniffers

Module 8

Engineered by Hackers. Presented by Professionals.

CEH™

Certified Ethical Hacker

SECURITY NEWS

December 2, 2010

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.

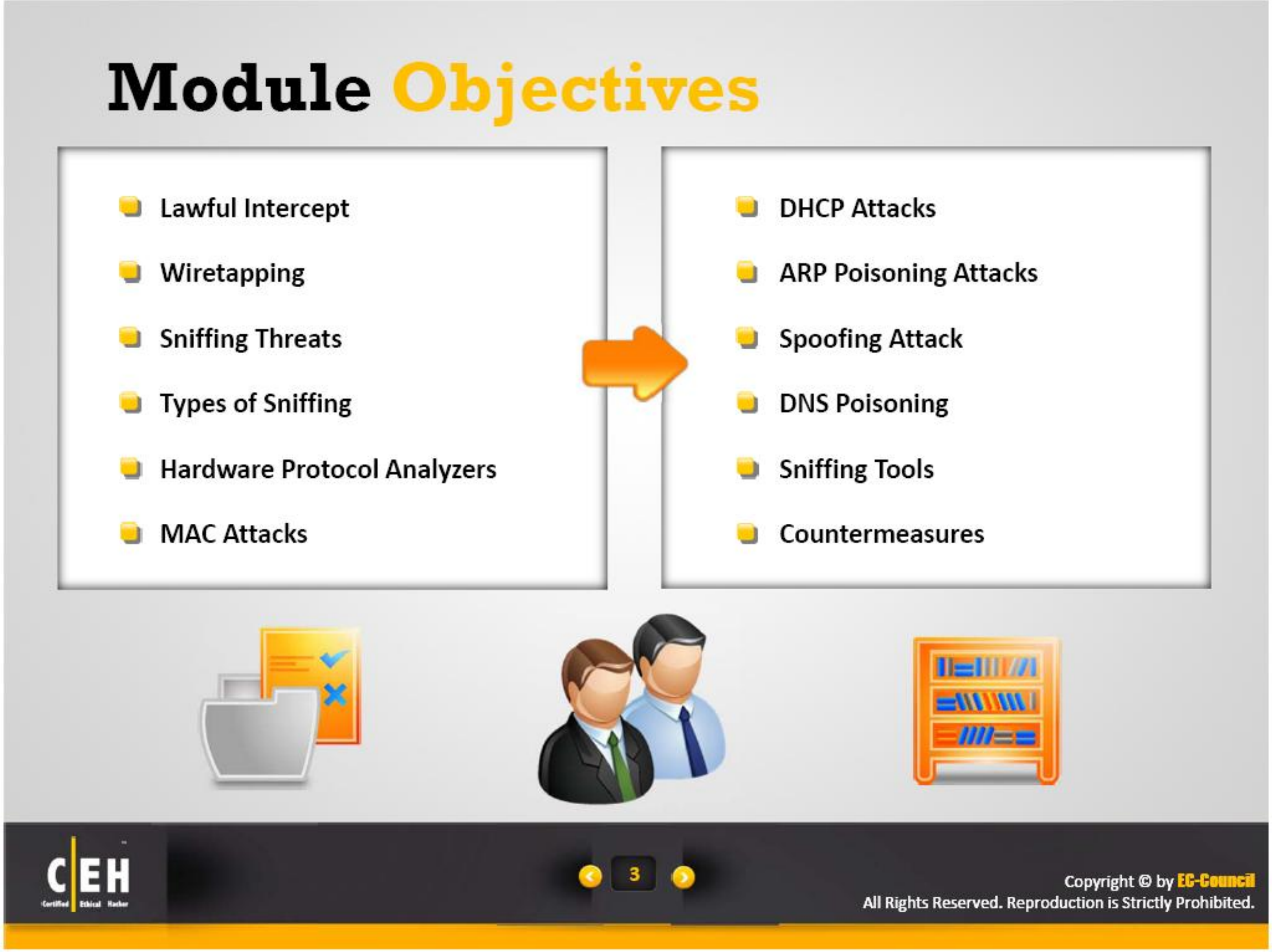
Though it's not surprising that YouPorn tops the list of spying sites, less racy sources like Technorati, TheSun.co.uk, and *Wired* were all fingered for tapping into your browsing habits. (Perez Hilton was on there too—but again, not that surprising.)

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

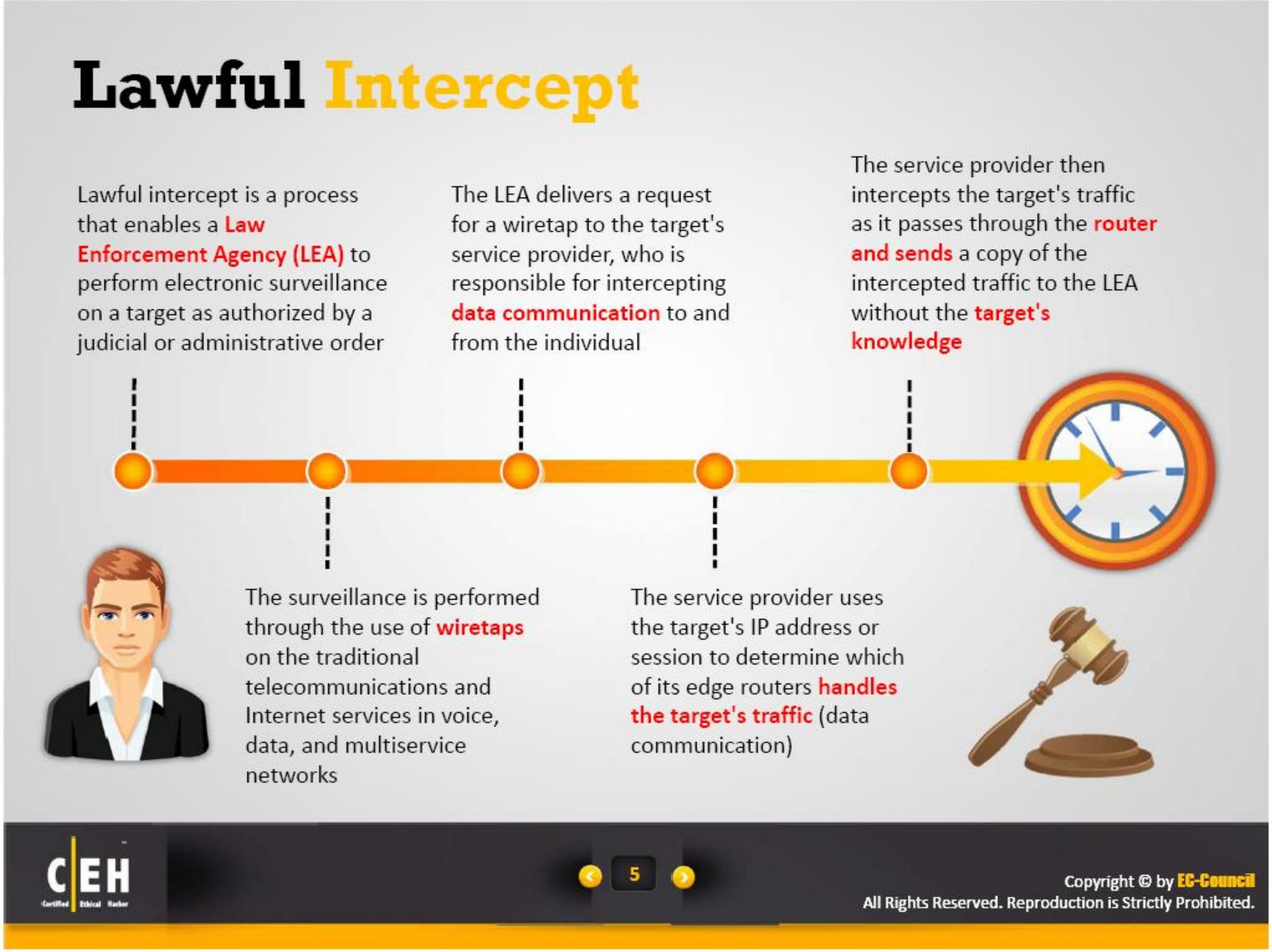


Module Objectives

- 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

CEH
Certified Ethical Hacker



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

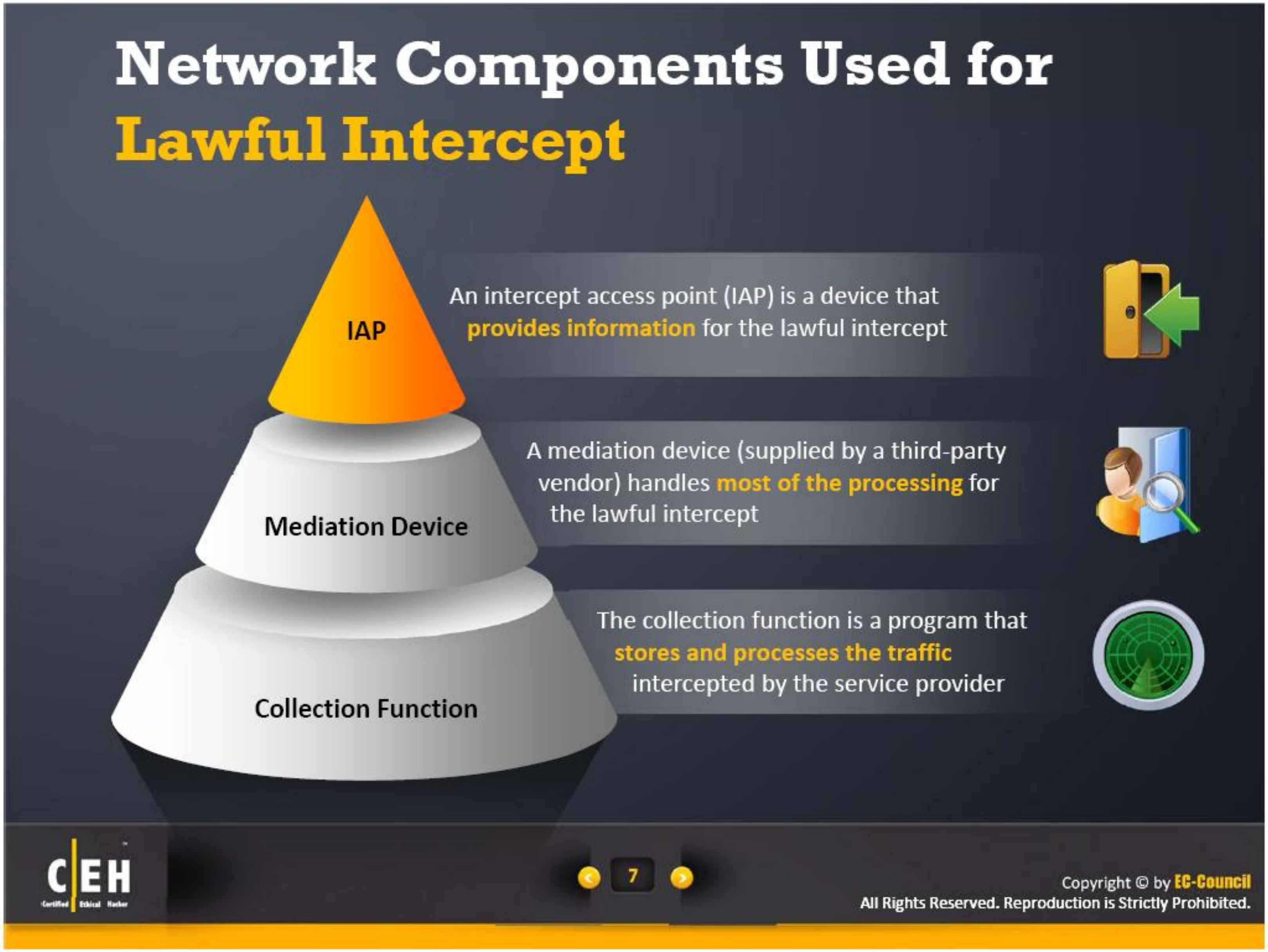
The LEA delivers a request for a wiretap to the target's service provider, who is responsible for intercepting **data communication** to and from the individual

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

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**

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

IAP

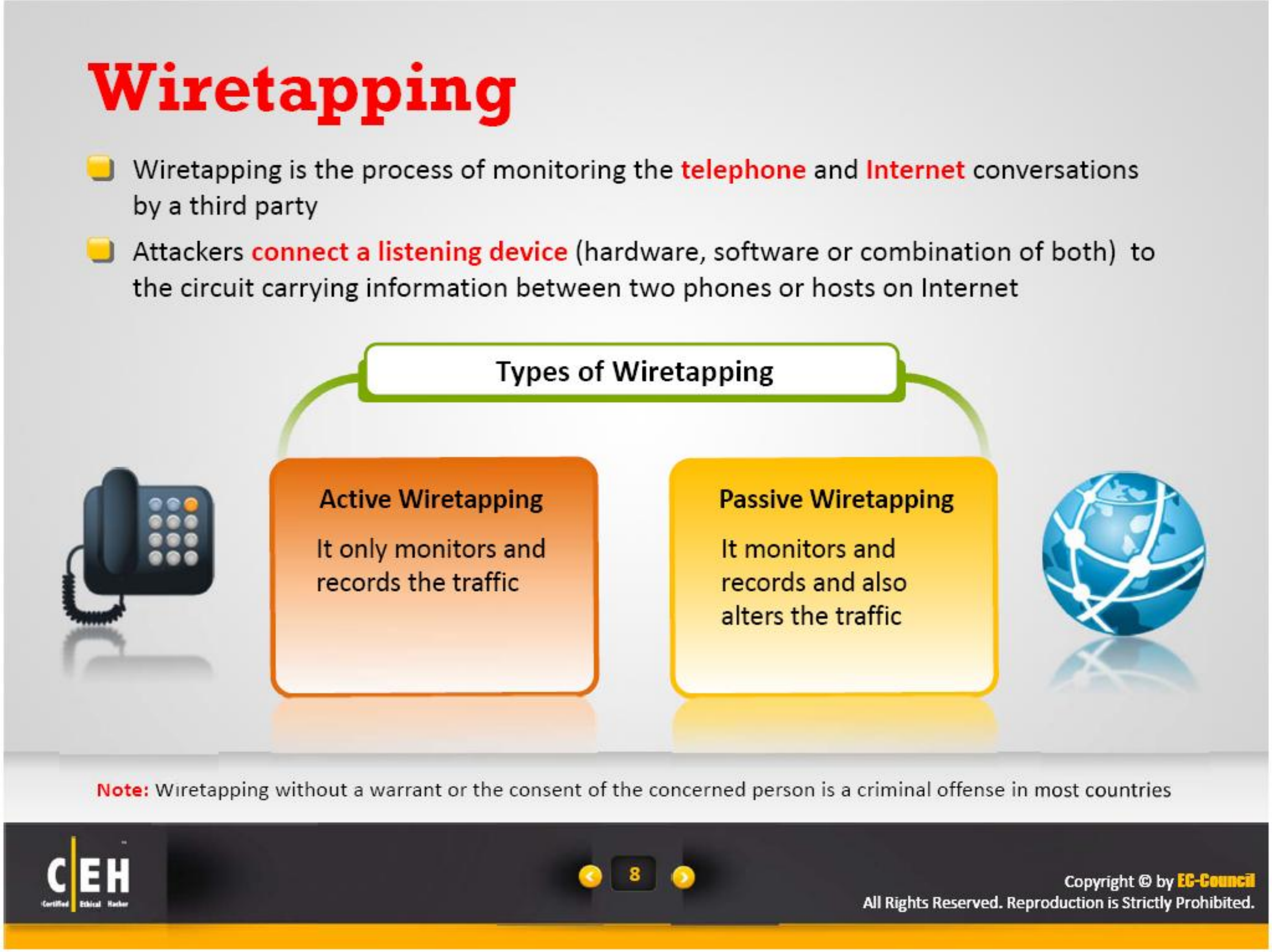
An intercept access point (IAP) is a device that **provides information** for the lawful intercept

Mediation Device

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

Collection Function

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

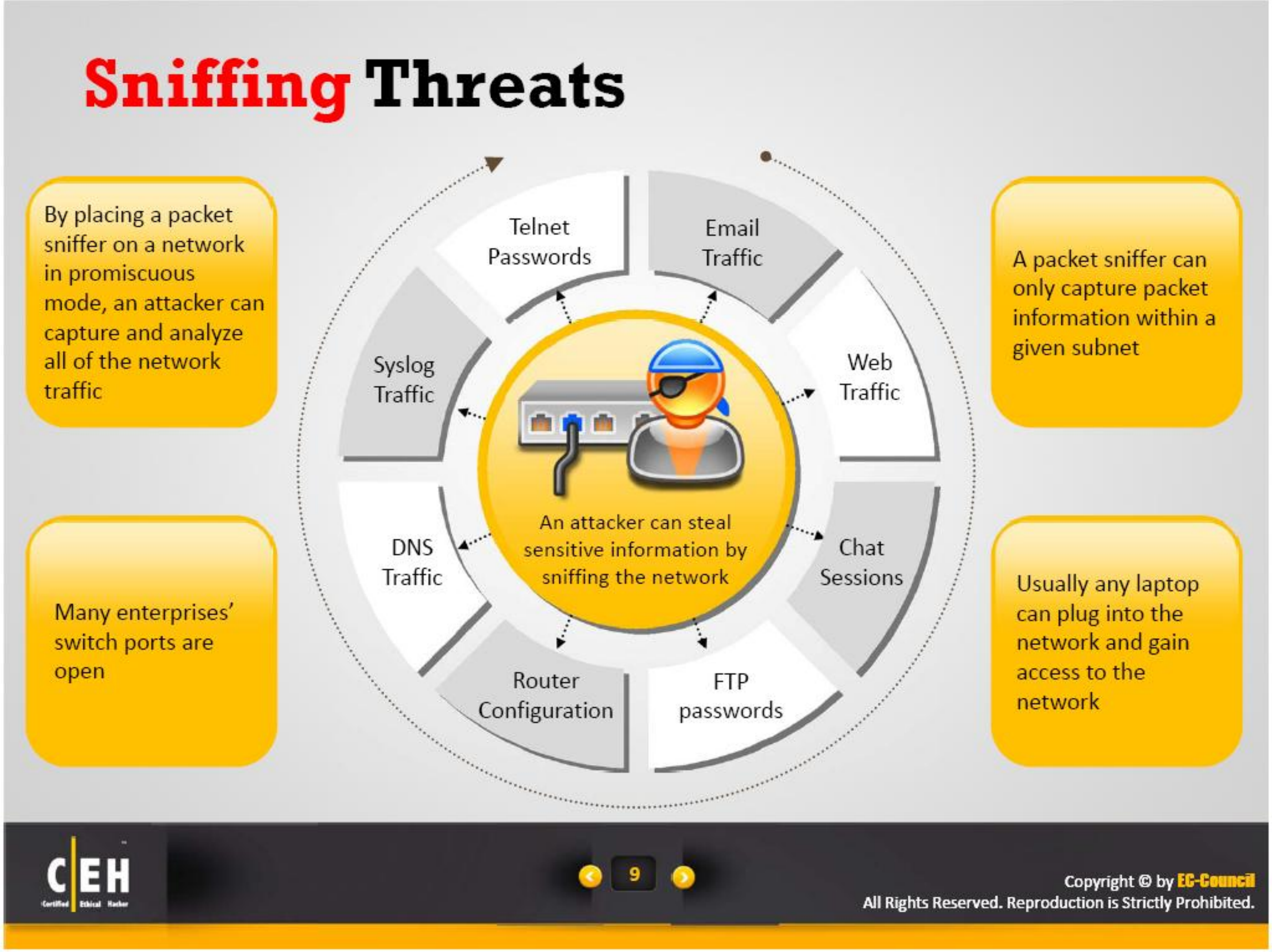
Active Wiretapping

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

Many enterprises' switch ports are open

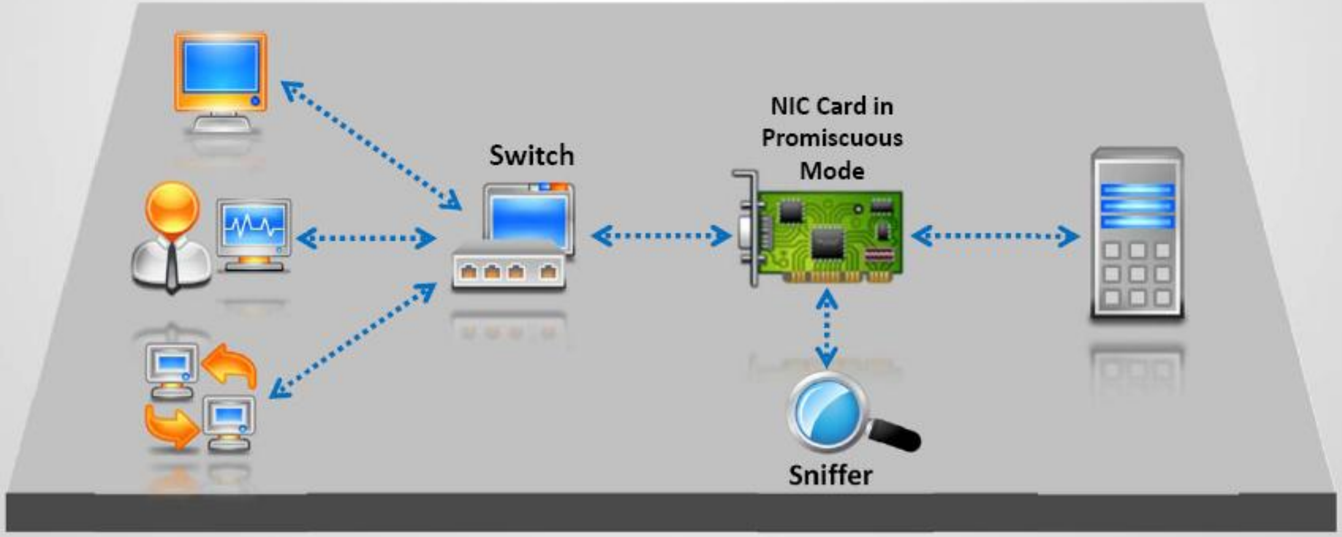
An attacker can steal sensitive information by sniffing the network

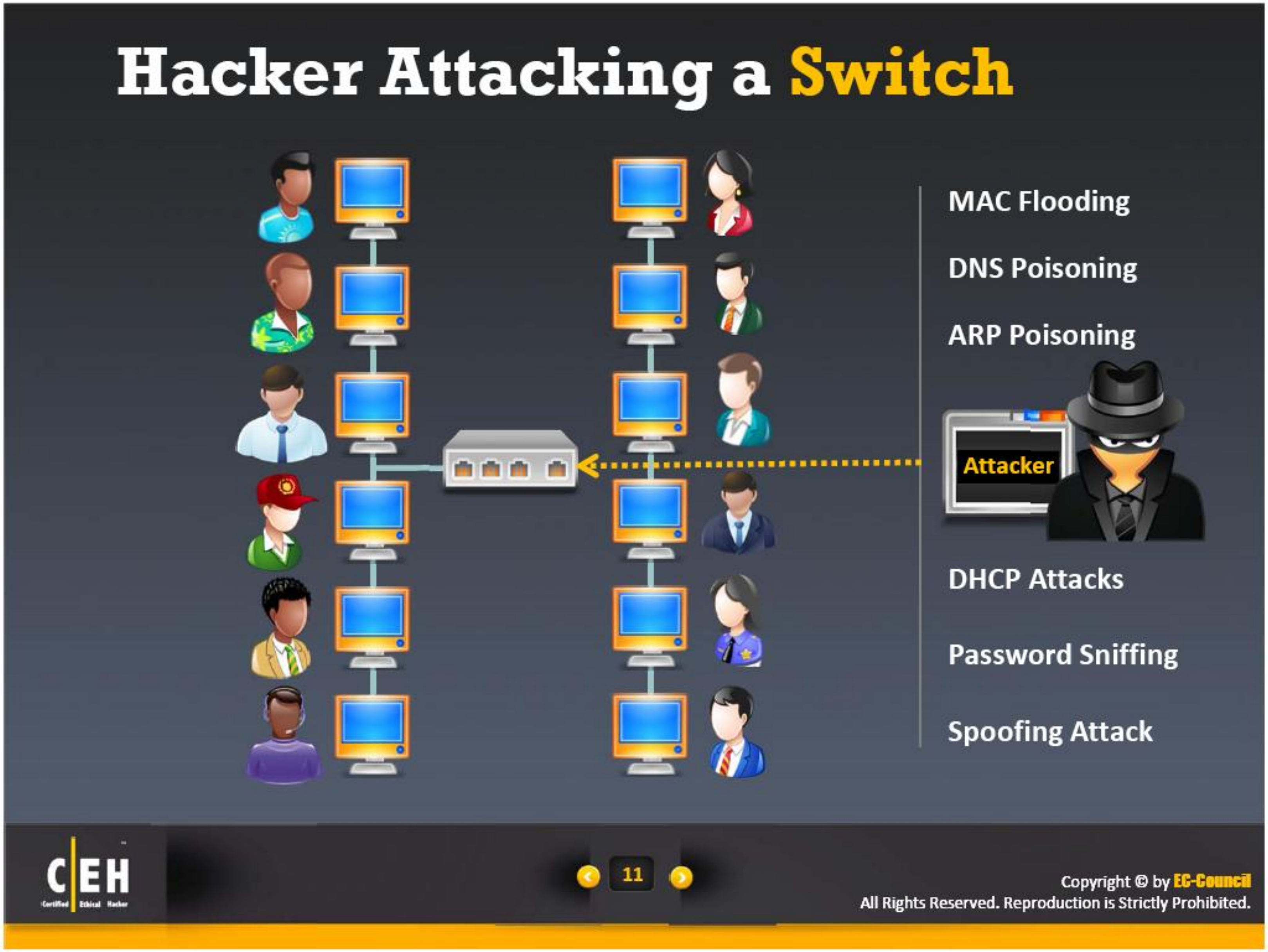
A packet sniffer can only capture packet information within a given subnet

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

How a Sniffer Works?

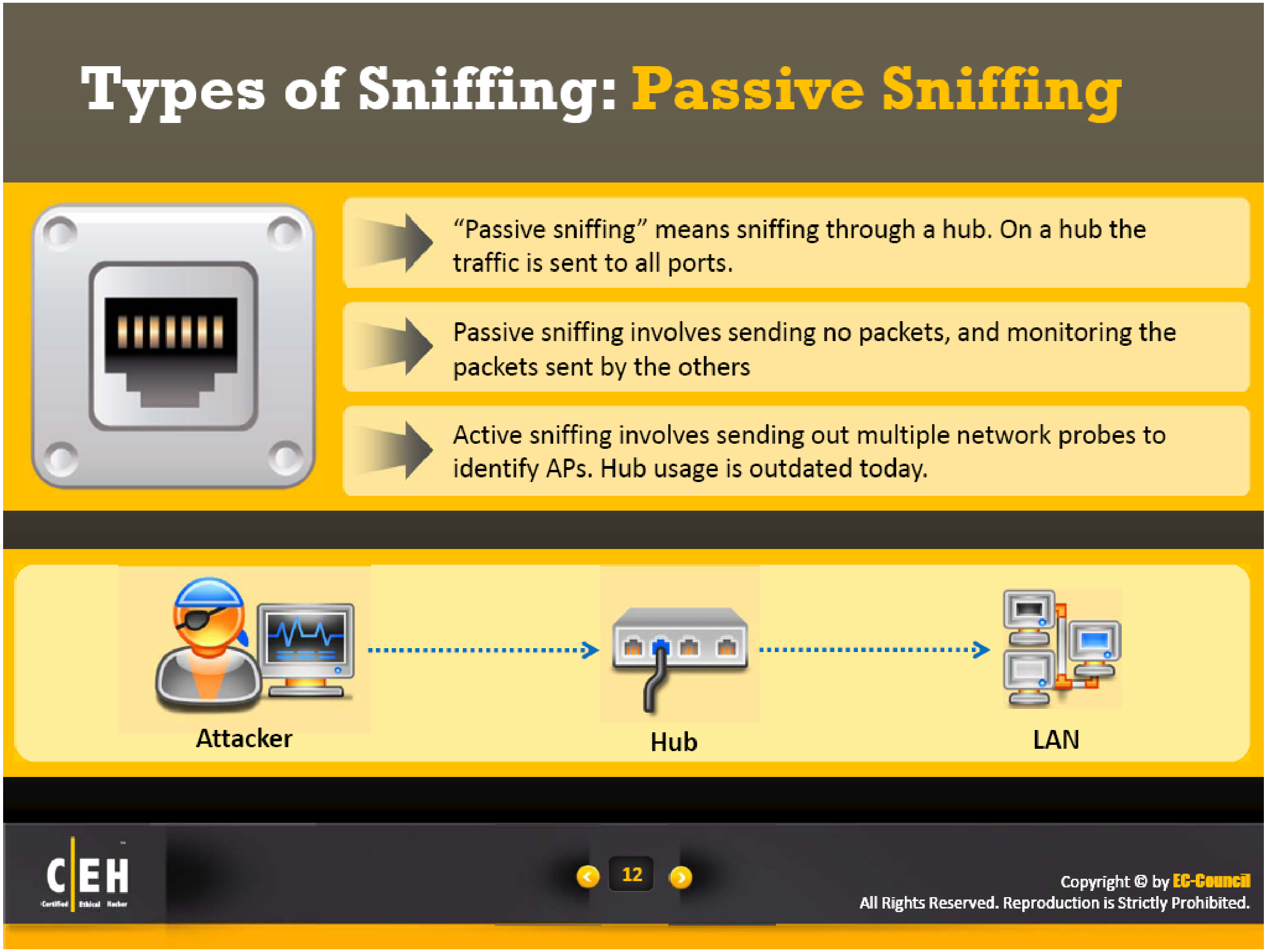
- Sniffer turns the NIC of a system to the **promiscuous mode** so that it listens to all the data transmitted on its segment
- Sniffer can constantly read all information entering the computer through the NIC by **decoding the information** encapsulated in the data packet





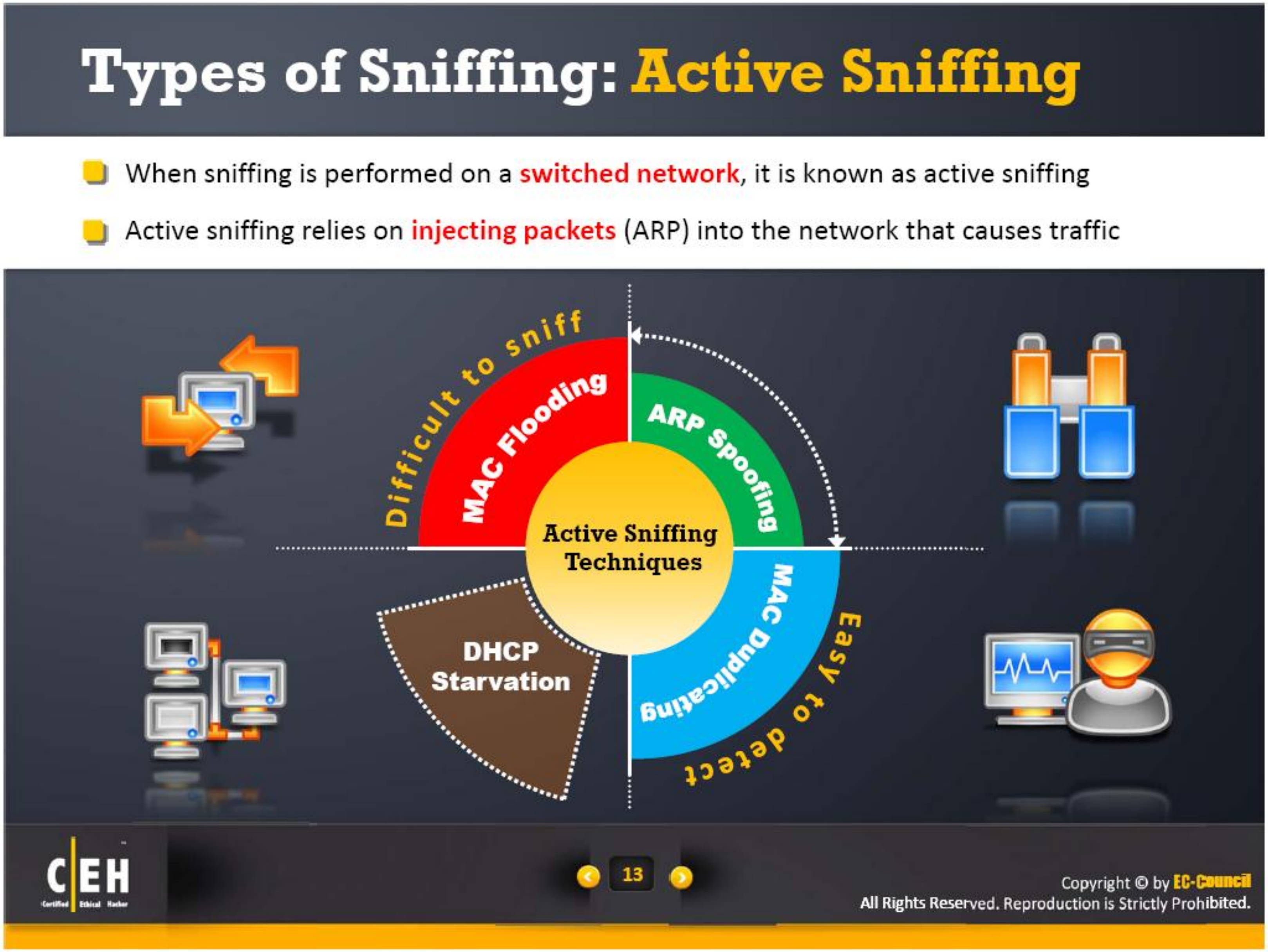
Hacker Attacking a Switch

- MAC Flooding
- DNS Poisoning
- ARP Poisoning
- DHCP Attacks
- Password Sniffing
- Spoofing Attack



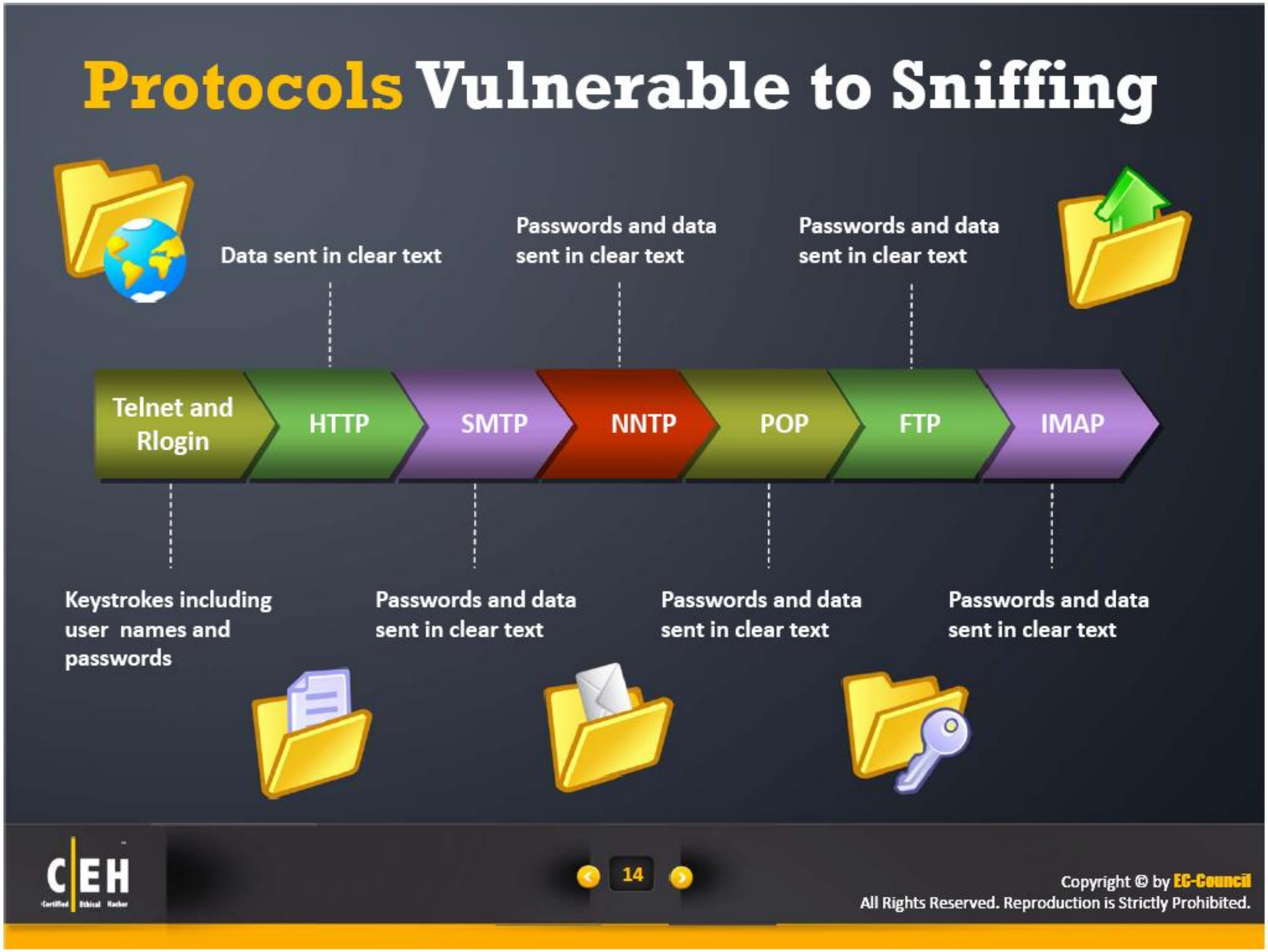
Types of Sniffing: Passive Sniffing

- "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



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

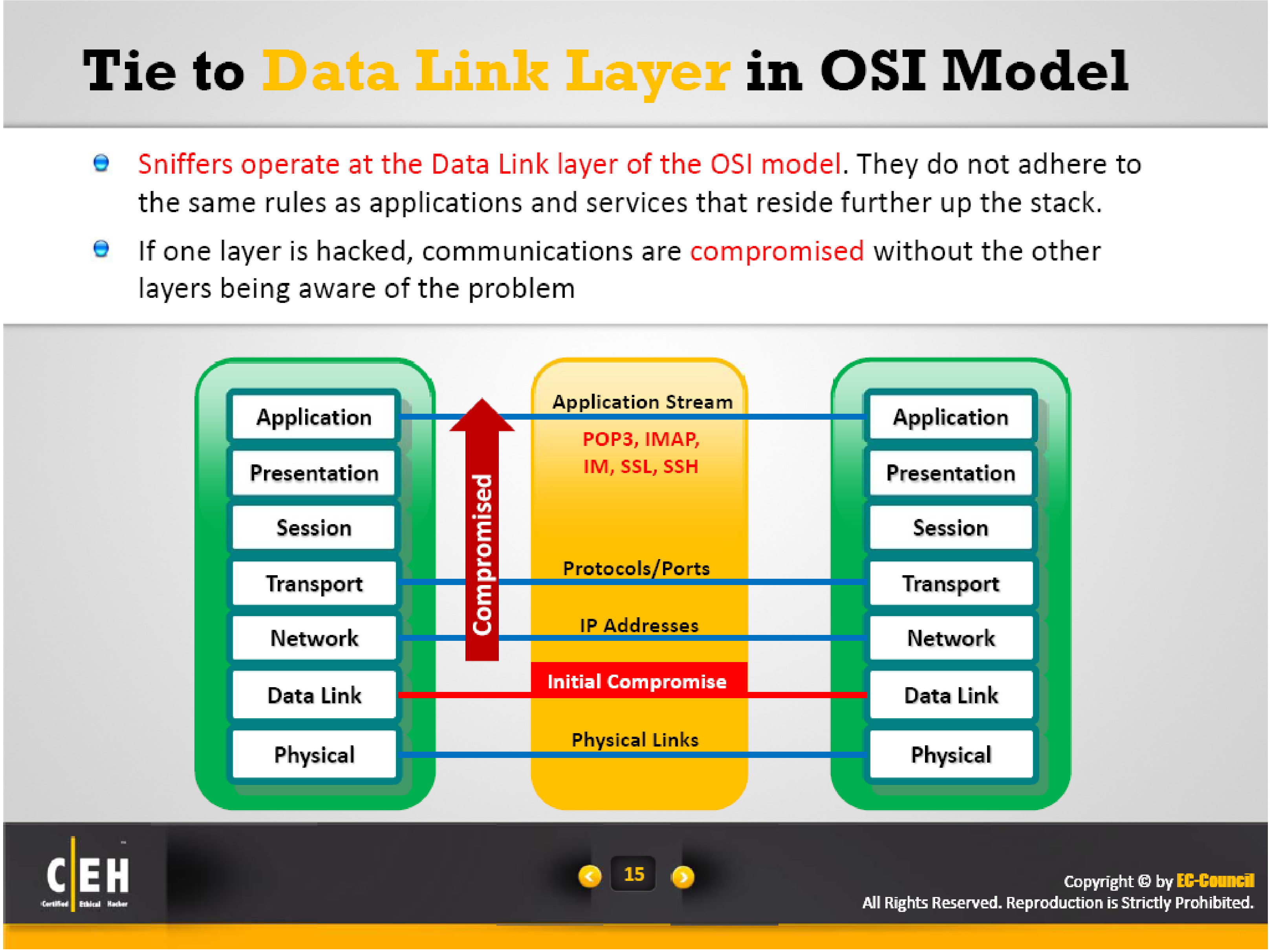
Passwords and data sent in clear text

FTP

Passwords and data sent in clear text

IMAP

Passwords and data sent in clear text



Tie to Data Link Layer in OSI Model

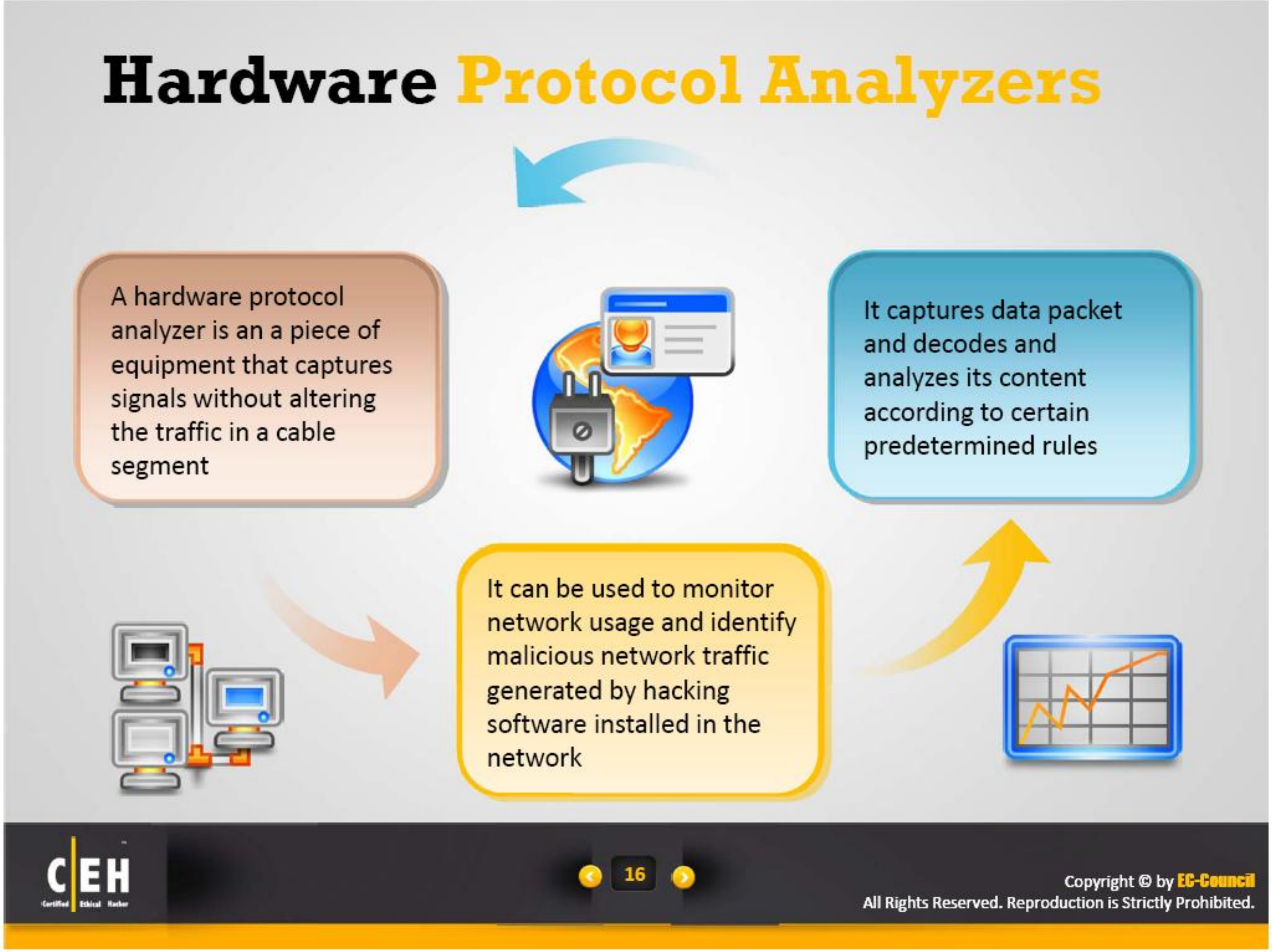
- Sniffers operate at the Data Link layer of the OSI model. They do not adhere to the same rules as applications and services that reside further up the stack.
- If one layer is hacked, communications are compromised without the other layers being aware of the problem

Application
Presentation
Session
Transport
Network
Data Link
Physical

Compromised

Application Stream
POP3, IMAP, IM, SSL, SSH
Protocols/Ports
IP Addresses
Initial Compromise
Physical Links

Application
Presentation
Session
Transport
Network
Data Link
Physical



Hardware Protocol Analyzers

A hardware protocol analyzer is an 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

Agilent N2X N5540A

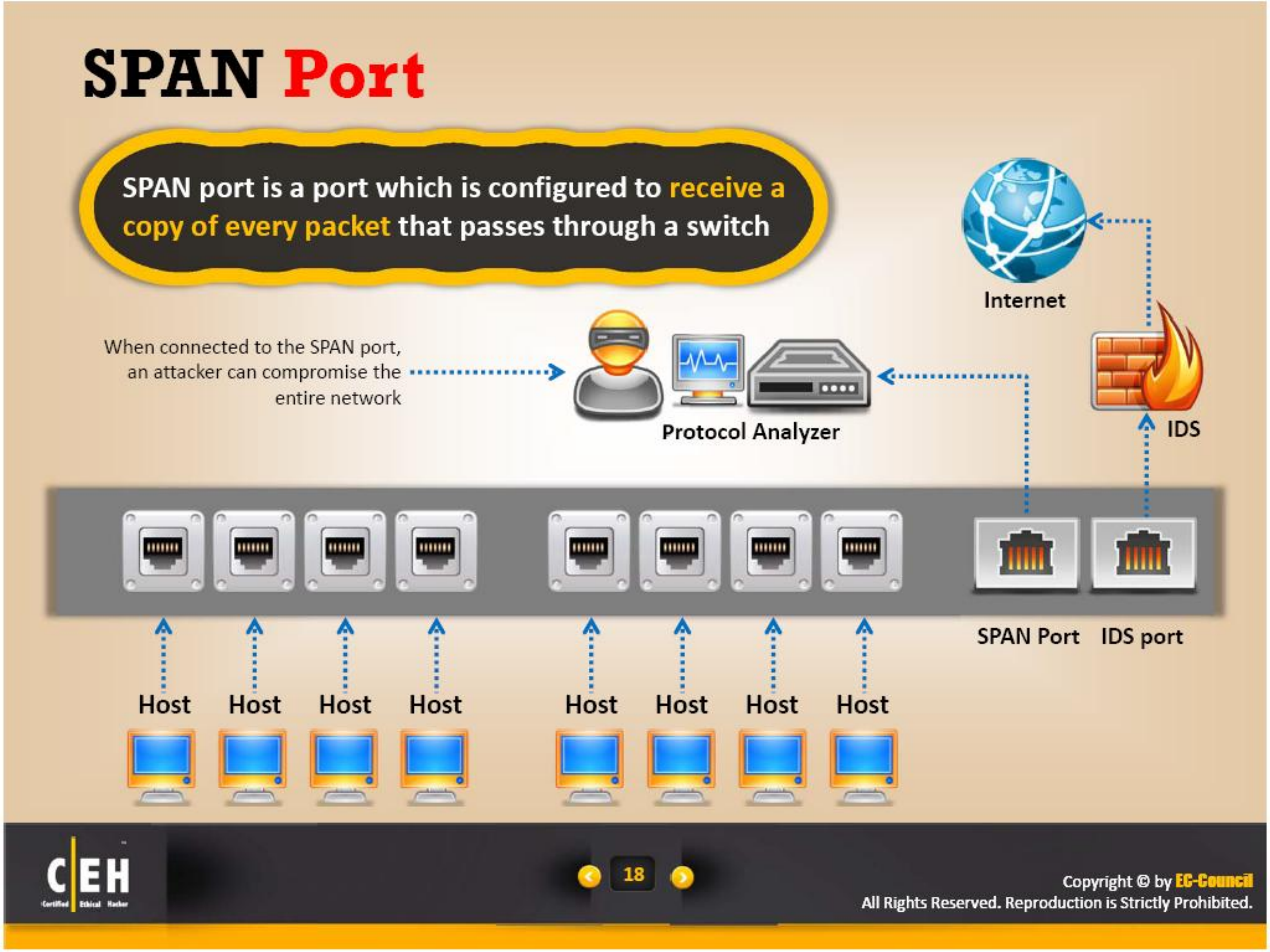
Agilent E2960B

RADCOM PrismLite Protocol Analyzer

RADCOM Prism UltraLite Protocol Analyzer

FLUKE Networks OptiView® Network Analyzer

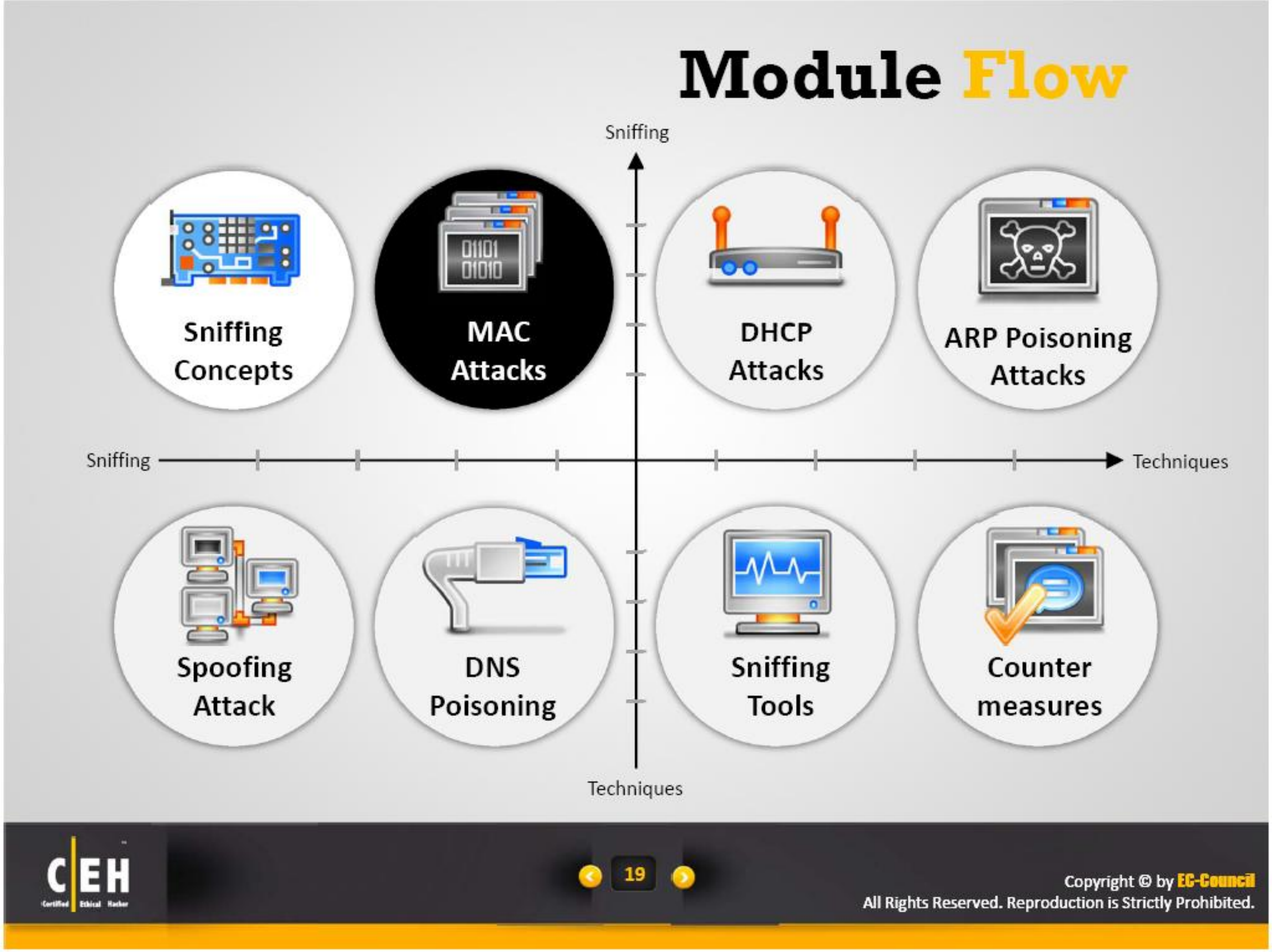
FLUKE Networks EtherScope™ Series II Network Assistant



SPAN Port

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



Module Flow

Sniffing Concepts

MAC Attacks

DHCP Attacks

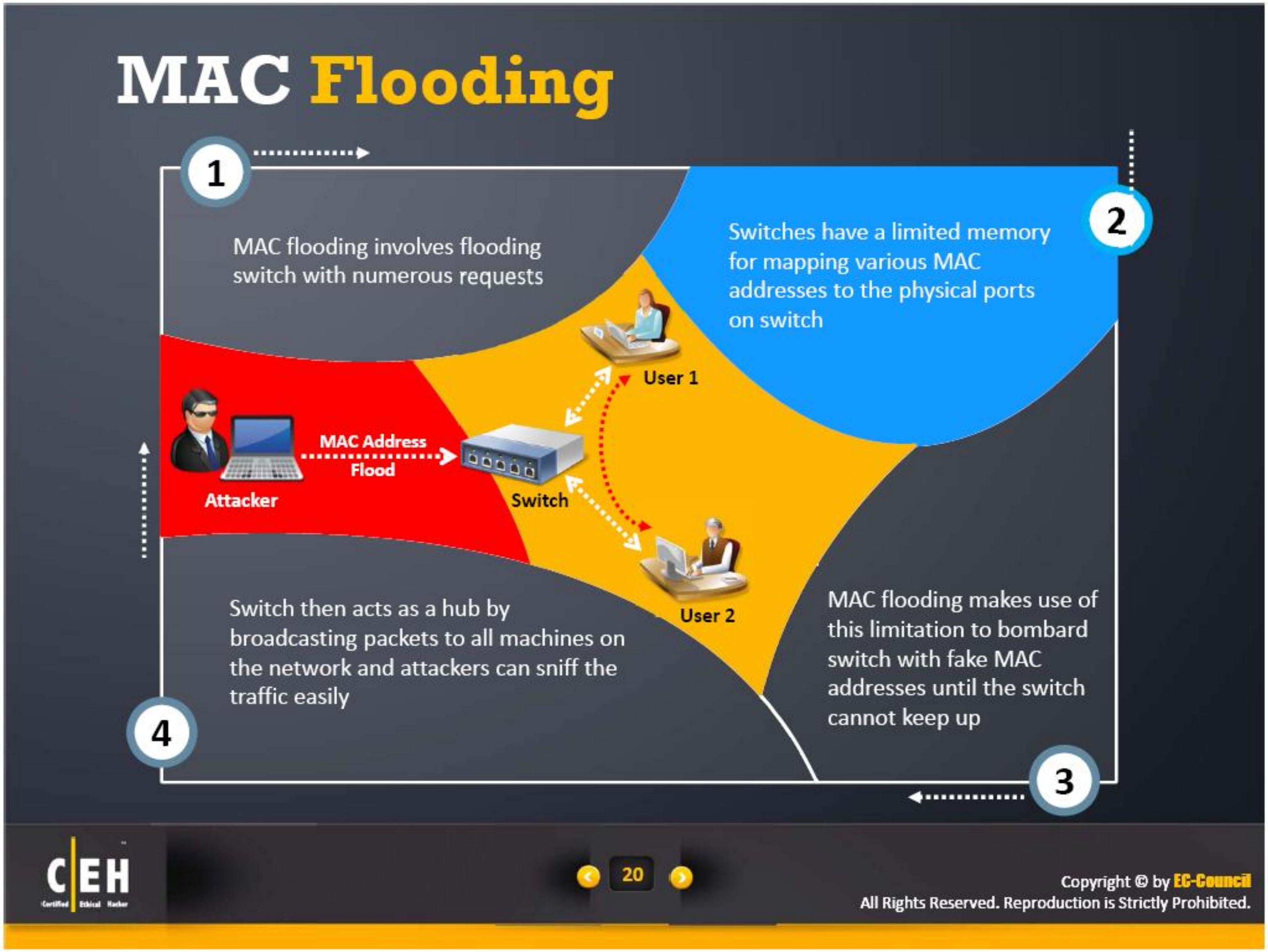
ARP Poisoning Attacks

Spoofing Attack

DNS Poisoning

Sniffing Tools

Counter measures



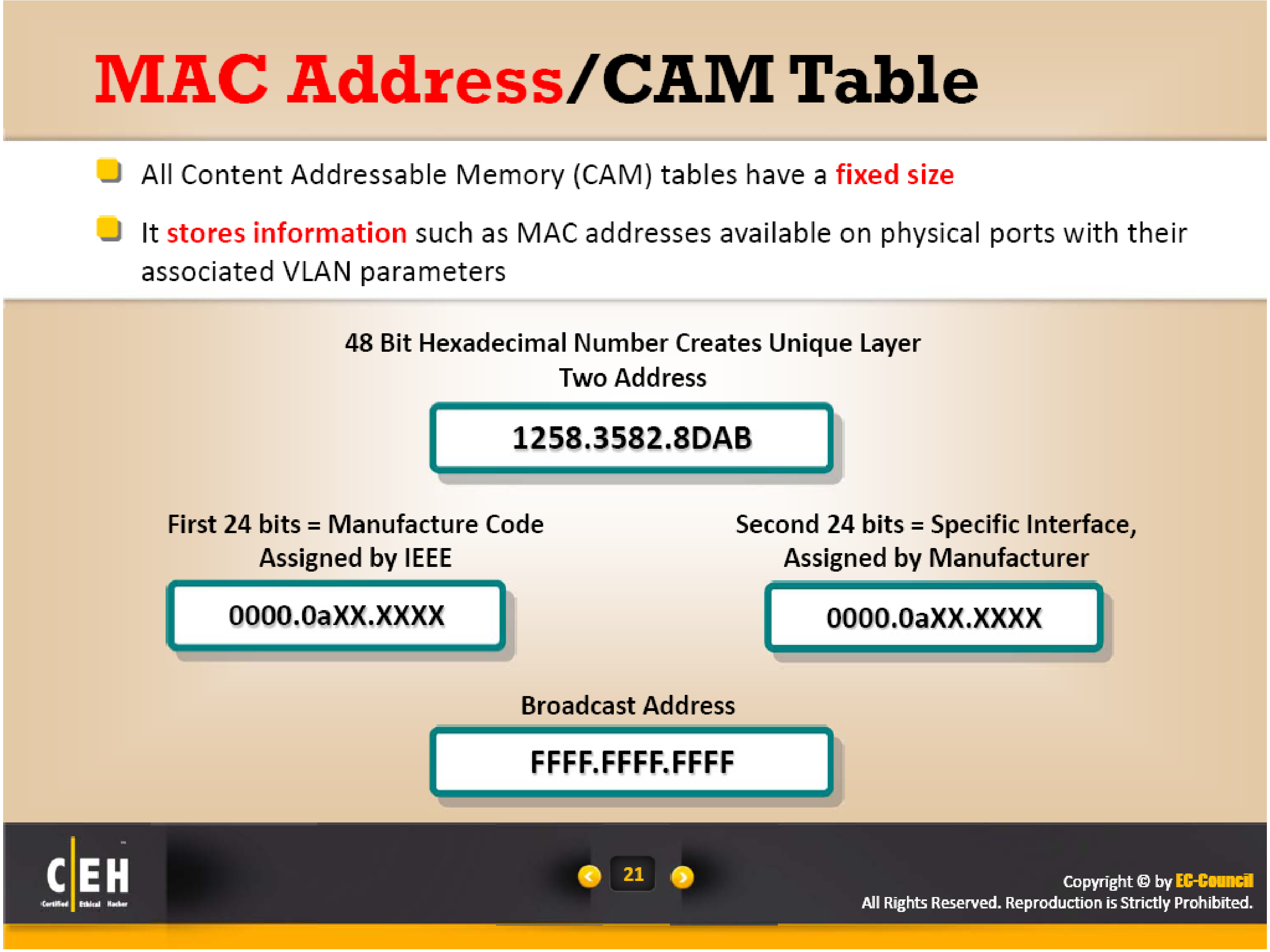
MAC Flooding

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

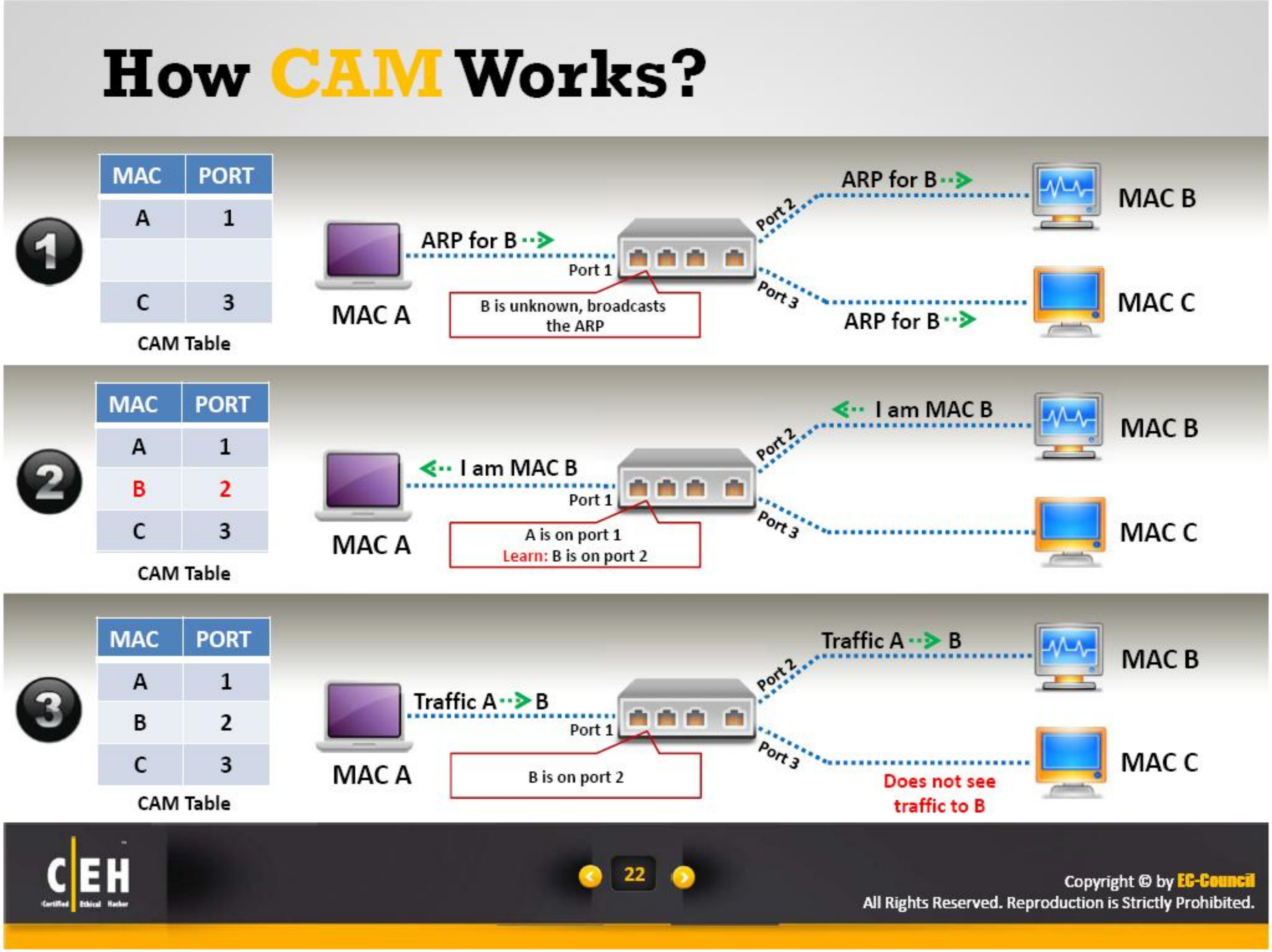
0000.0aXX.XXXX

Second 24 bits = Specific Interface, Assigned by Manufacturer

0000.0aXX.XXXX

Broadcast Address

FFFF.FFFF.FFFF



How CAM Works?

1

MAC	PORT
A	1
C	3

CAM Table

MAC A

ARP for B

Port 1

B is unknown, broadcasts the ARP

Port 2

ARP for B

MAC B

Port 3

ARP for B

MAC C

2

MAC	PORT
A	1
B	2
C	3

CAM Table

MAC A

I am MAC B

Port 1

A is on port 1
Learn: B is on port 2

Port 2

I am MAC B

MAC B

Port 3

MAC C

3

MAC	PORT
A	1
B	2
C	3

CAM Table

MAC A

Traffic A B

Port 1

B is on port 2

Port 2

Traffic A B

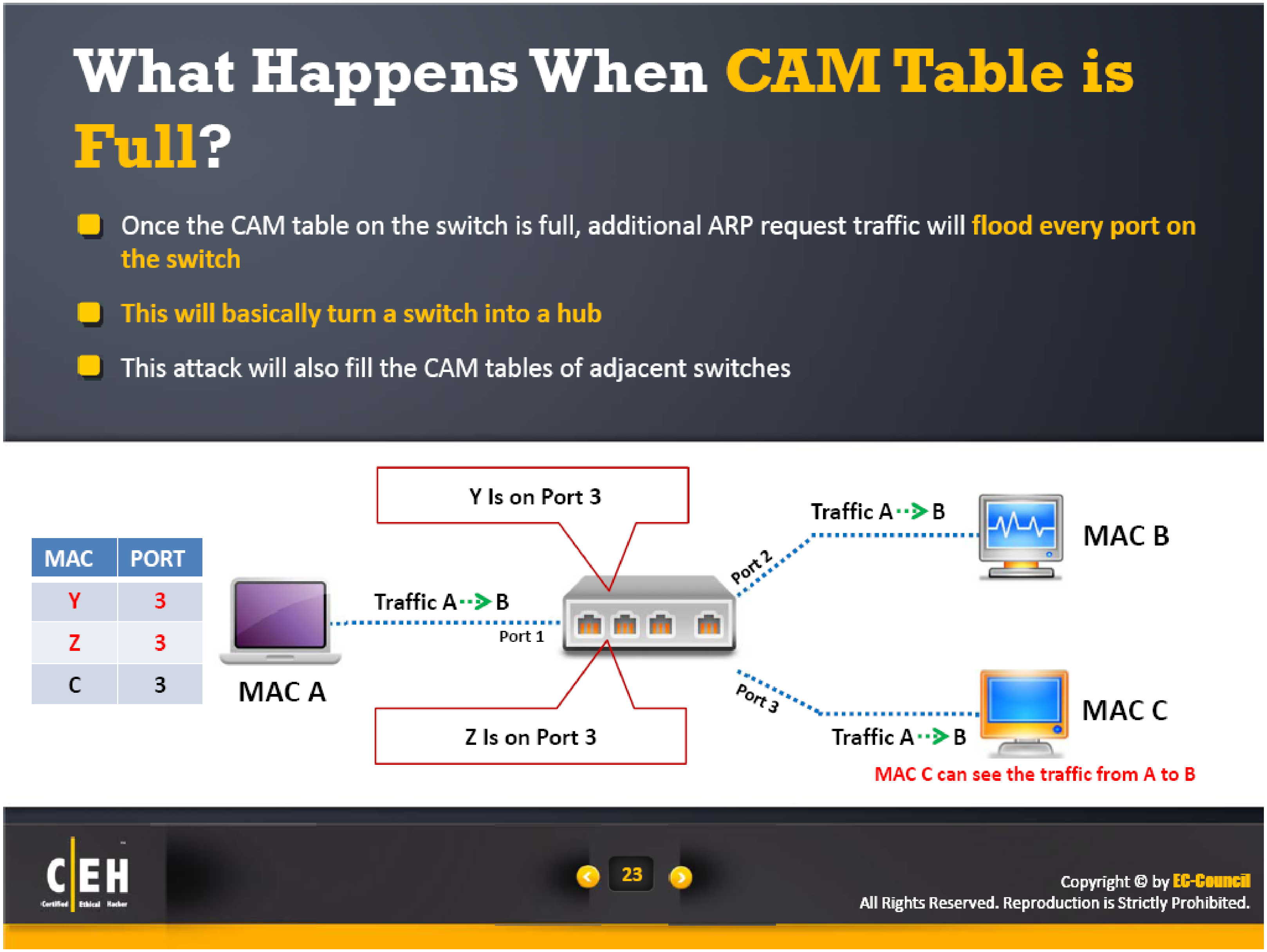
MAC B

Port 3

MAC C

Does not see traffic to B

CEH Certified Ethical Hacker



What Happens When CAM Table is Full?

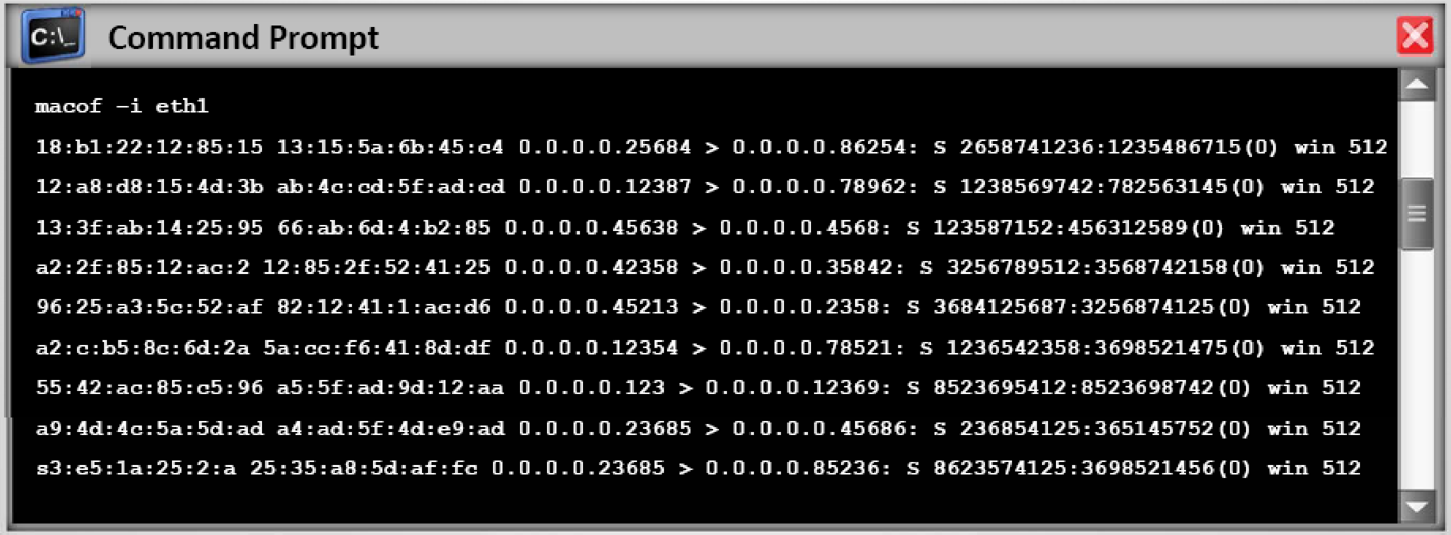
- Once the CAM table on the switch is full, additional ARP request traffic will flood every port on the switch
- This will basically turn a switch into a hub
- This attack will also fill the CAM tables of adjacent switches

MAC	PORT
Y	3
Z	3
C	3

MAC C can see the traffic from A to B

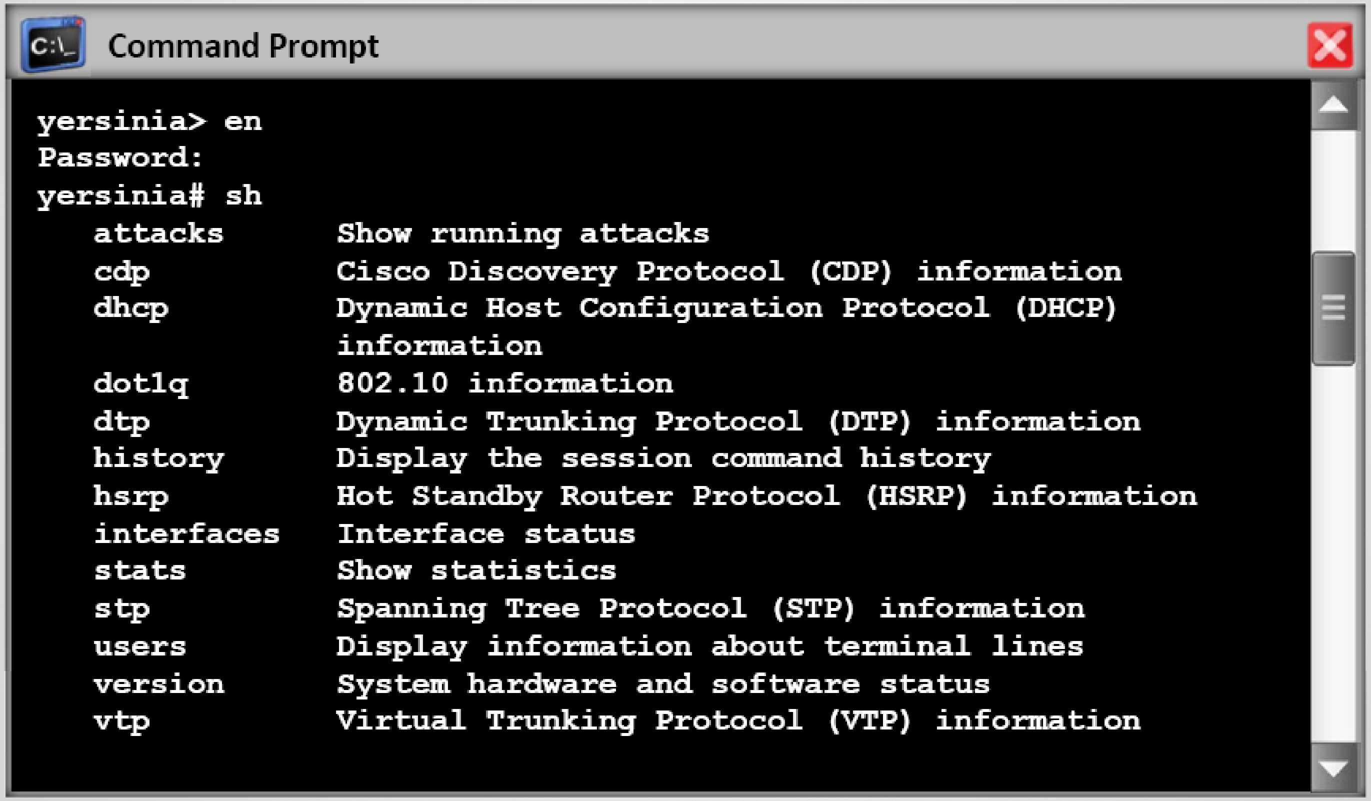
Mac Flooding Switches with macof

- 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

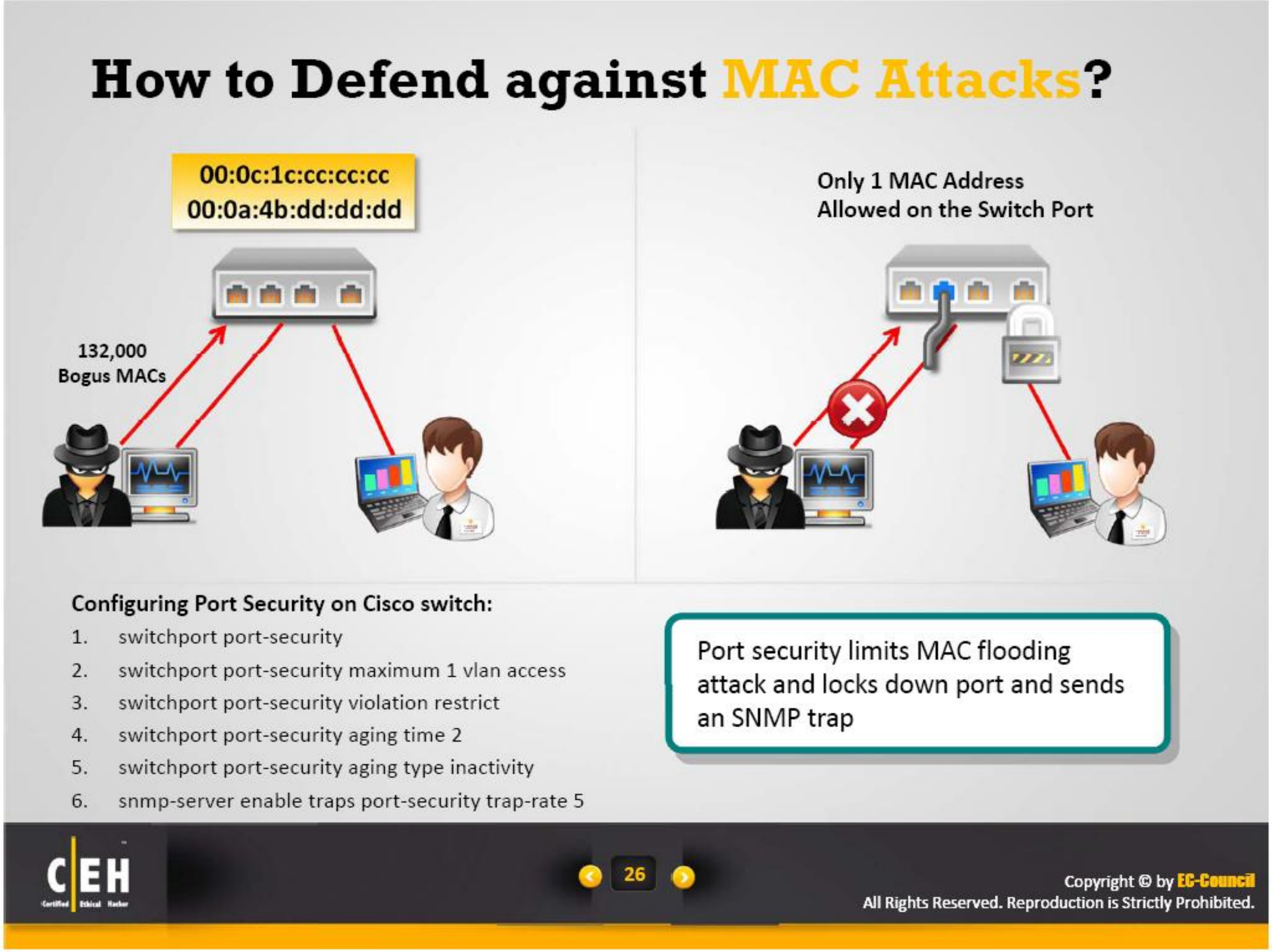


```
macof –i eth1
18:b1:22:12:85:15 13:15:5a:6b:45:c4 0.0.0.0.25684 > 0.0.0.0.86254: S 2658741236:1235486715(0) win 512
12:a8:d8:15:4d:3b ab:4c:cd:5f:ad:cd 0.0.0.0.12387 > 0.0.0.0.78962: S 1238569742:782563145(0) win 512
13:3f:ab:14:25:95 66:ab:6d:4:b2:85 0.0.0.0.45638 > 0.0.0.0.4568: S 123587152:456312589(0) 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:ac:d6 0.0.0.0.45213 > 0.0.0.0.2358: S 3684125687:3256874125(0) win 512
a2:c:b5:8c:6d:2a 5a:cc:f6:41:8d: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
s3:e5:1a:25:2:a 25:35:a8:5d:af:fc 0.0.0.0.23685 > 0.0.0.0.85236: S 8623574125:3698521456(0) win 512
```

MAC Flooding Tool: Yersinia



```
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?

00:0c:1c:cc:cc:cc
00:0a:4b:dd:dd:dd

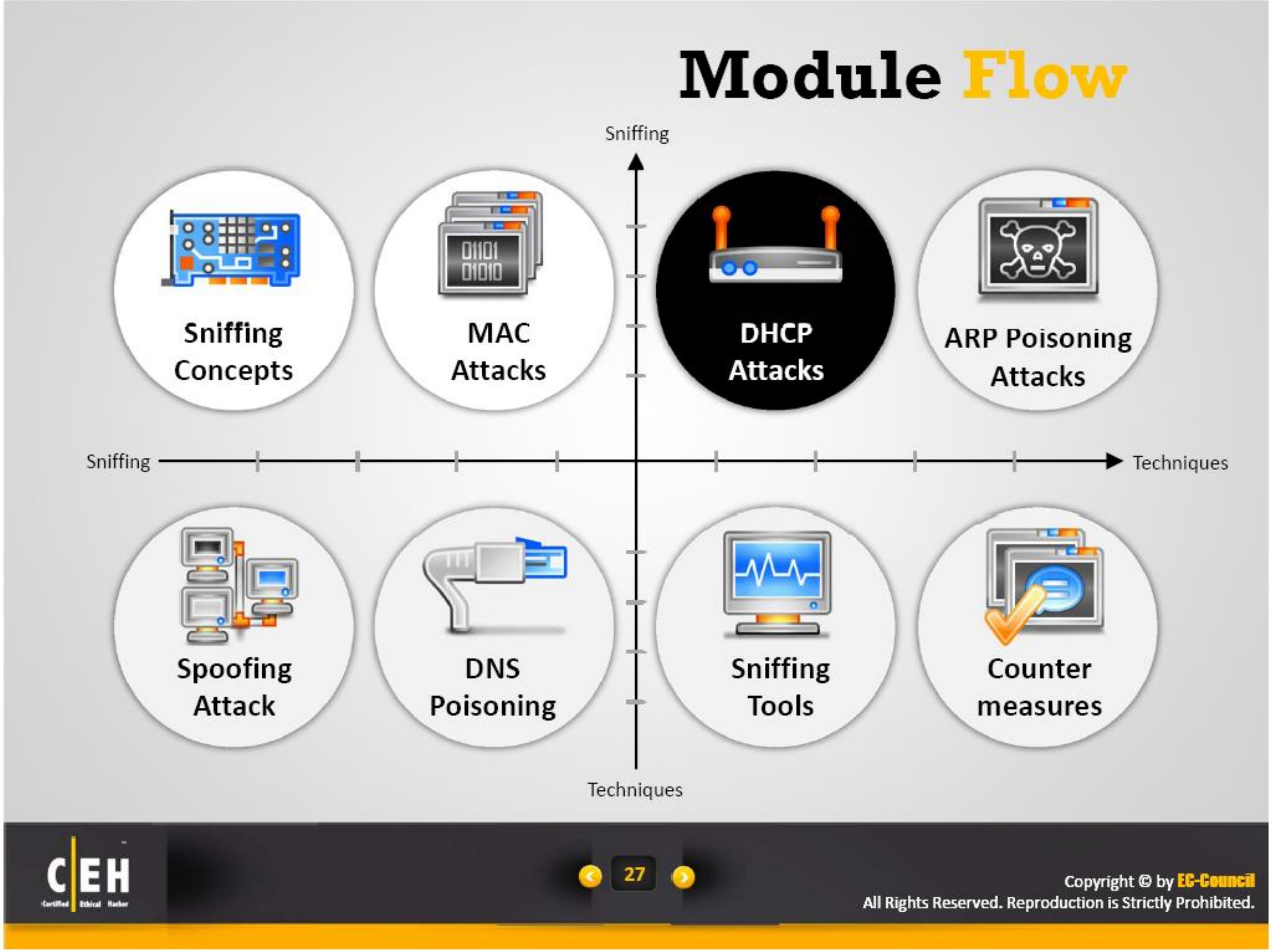
132,000
Bogus MACs

Only 1 MAC Address
Allowed on the Switch Port

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

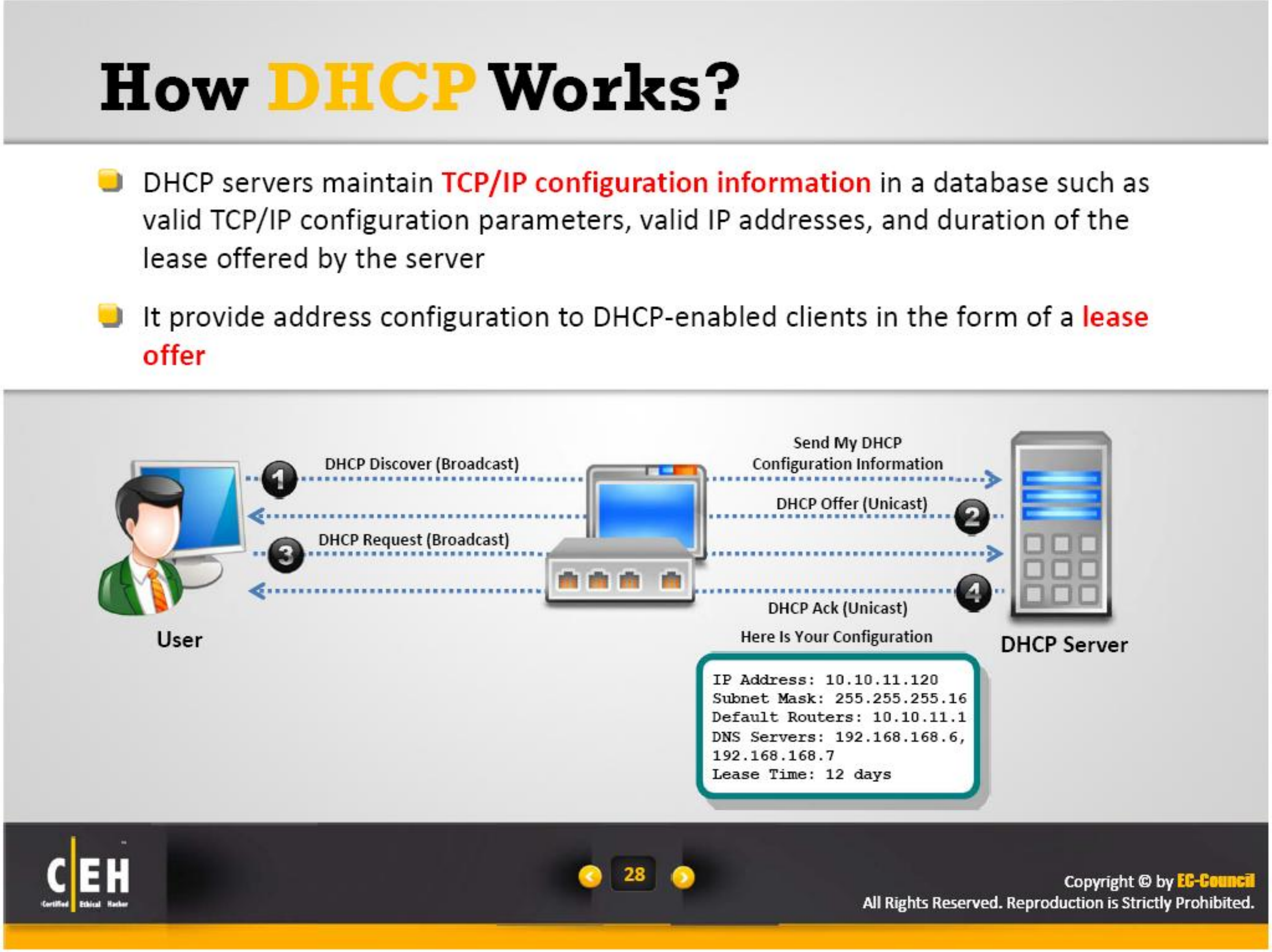
ARP Poisoning Attacks

Spoofing Attack

DNS Poisoning

Sniffing Tools

Counter measures

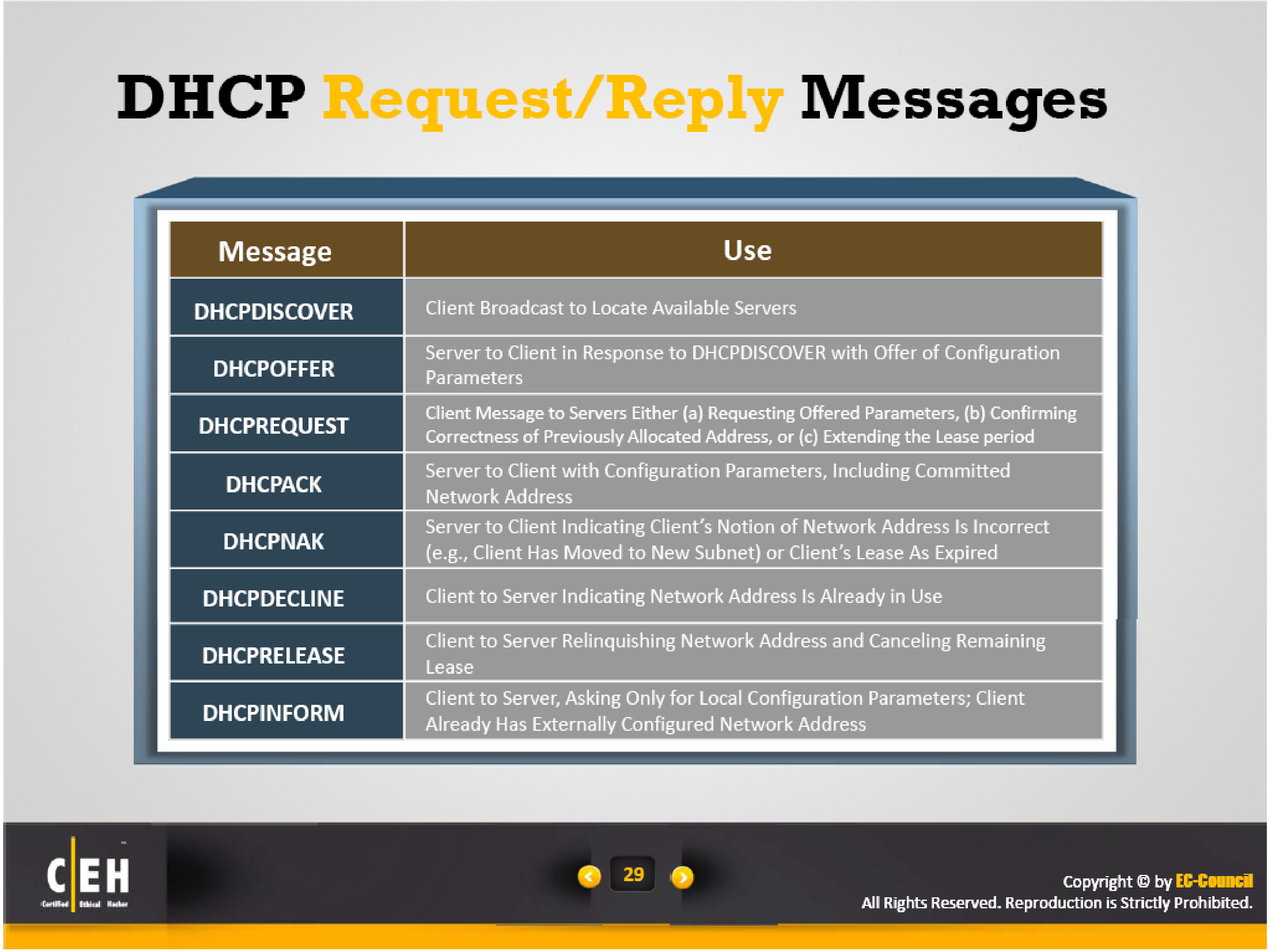


How DHCP Works?

- 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 provide address configuration to DHCP-enabled clients in the form of a **lease offer**

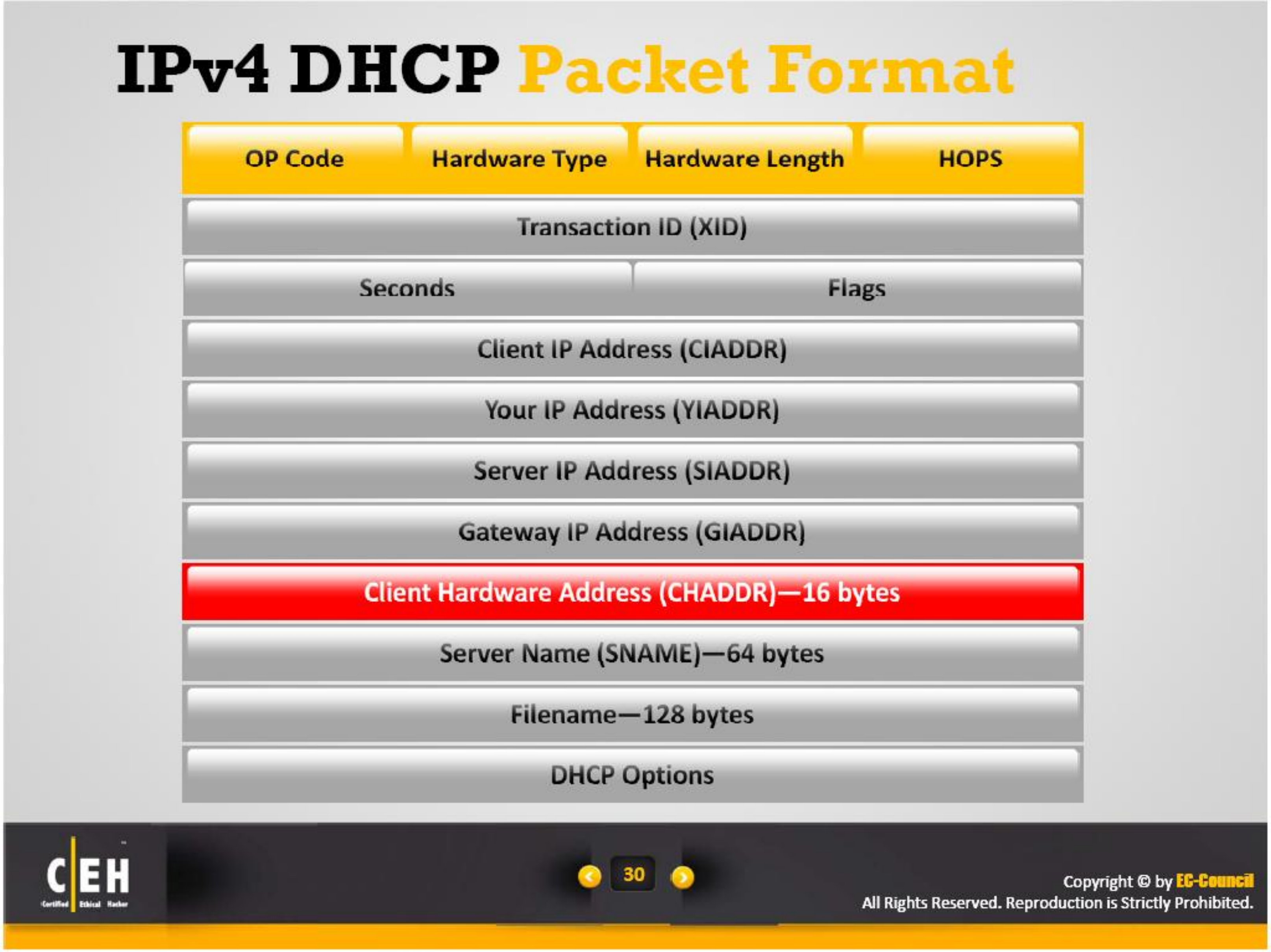
User
1
DHCP Discover (Broadcast)
Send My DHCP Configuration Information
DHCP Offer (Unicast)
2
3
DHCP Request (Broadcast)
4
DHCP Ack (Unicast)
Here Is Your Configuration
DHCP Server

```
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
```



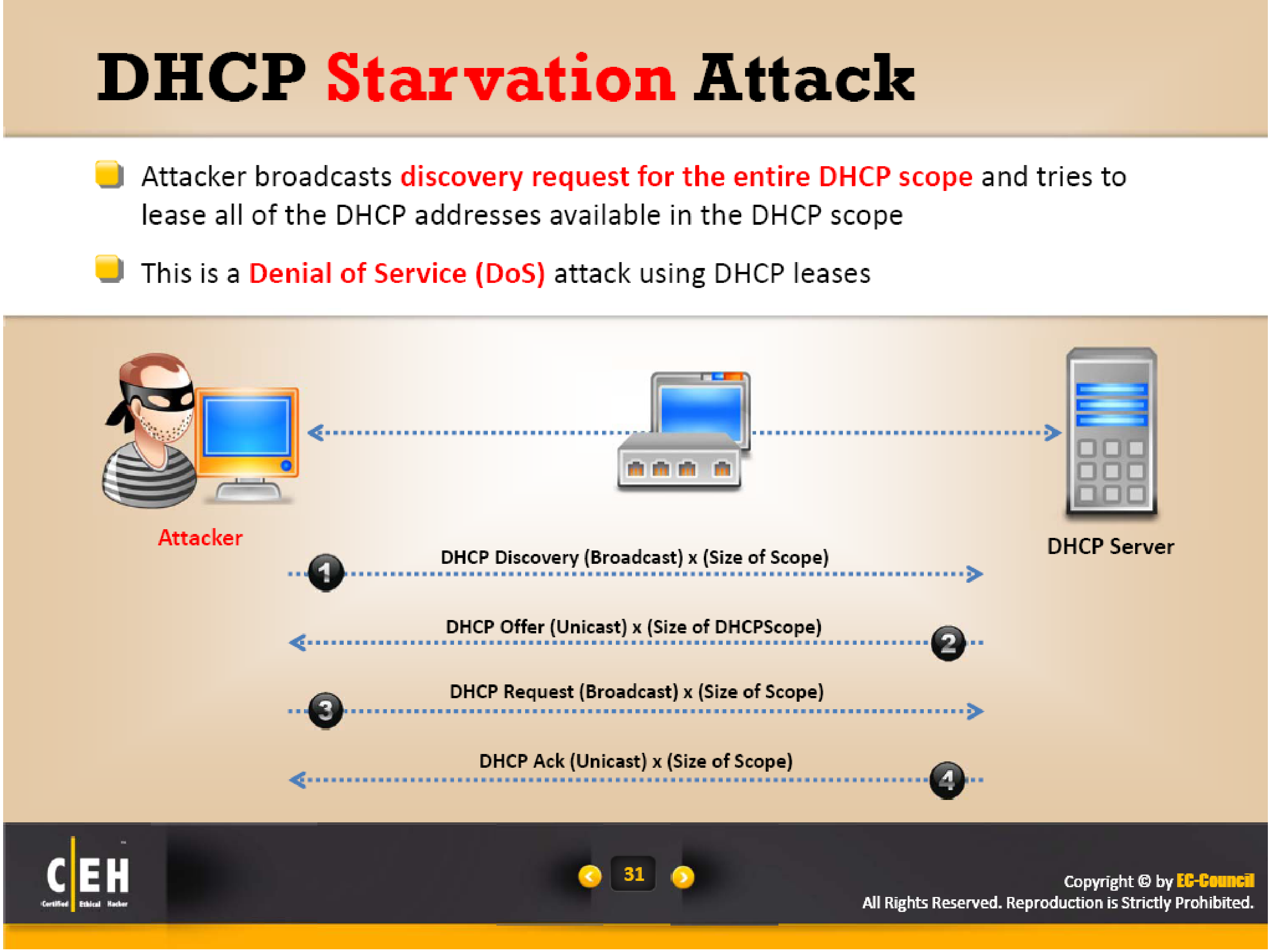
DHCP Request/Reply Messages

Message	Use
DHCPDISCOVER	Client Broadcast to Locate Available Servers
DHCPOFFER	Server to Client in Response to DHCPDISCOVER with Offer of Configuration Parameters
DHCPREQUEST	Client Message to Servers Either (a) Requesting Offered Parameters, (b) Confirming Correctness of Previously Allocated Address, or (c) Extending the Lease period
DHCPACK	Server to Client with Configuration Parameters, Including Committed Network Address
DHCPNAK	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
DHCPDECLINE	Client to Server Indicating Network Address Is Already in Use
DHCPRELEASE	Client to Server Relinquishing Network Address and Canceling Remaining Lease
DHCPINFORM	Client to Server, Asking Only for Local Configuration Parameters; Client Already Has Externally Configured Network Address



IPv4 DHCP Packet Format

OP Code	Hardware Type	Hardware Length	HOPS
Transaction ID (XID)			
Seconds		Flags	
Client IP Address (CIADDR)			
Your IP Address (YIADDR)			
Server IP Address (SIADDR)			
Gateway IP Address (GIADDR)			
Client Hardware Address (CHADDR)—16 bytes			
Server Name (SNAME)—64 bytes			
Filename—128 bytes			
DHCP Options			



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

Attacker

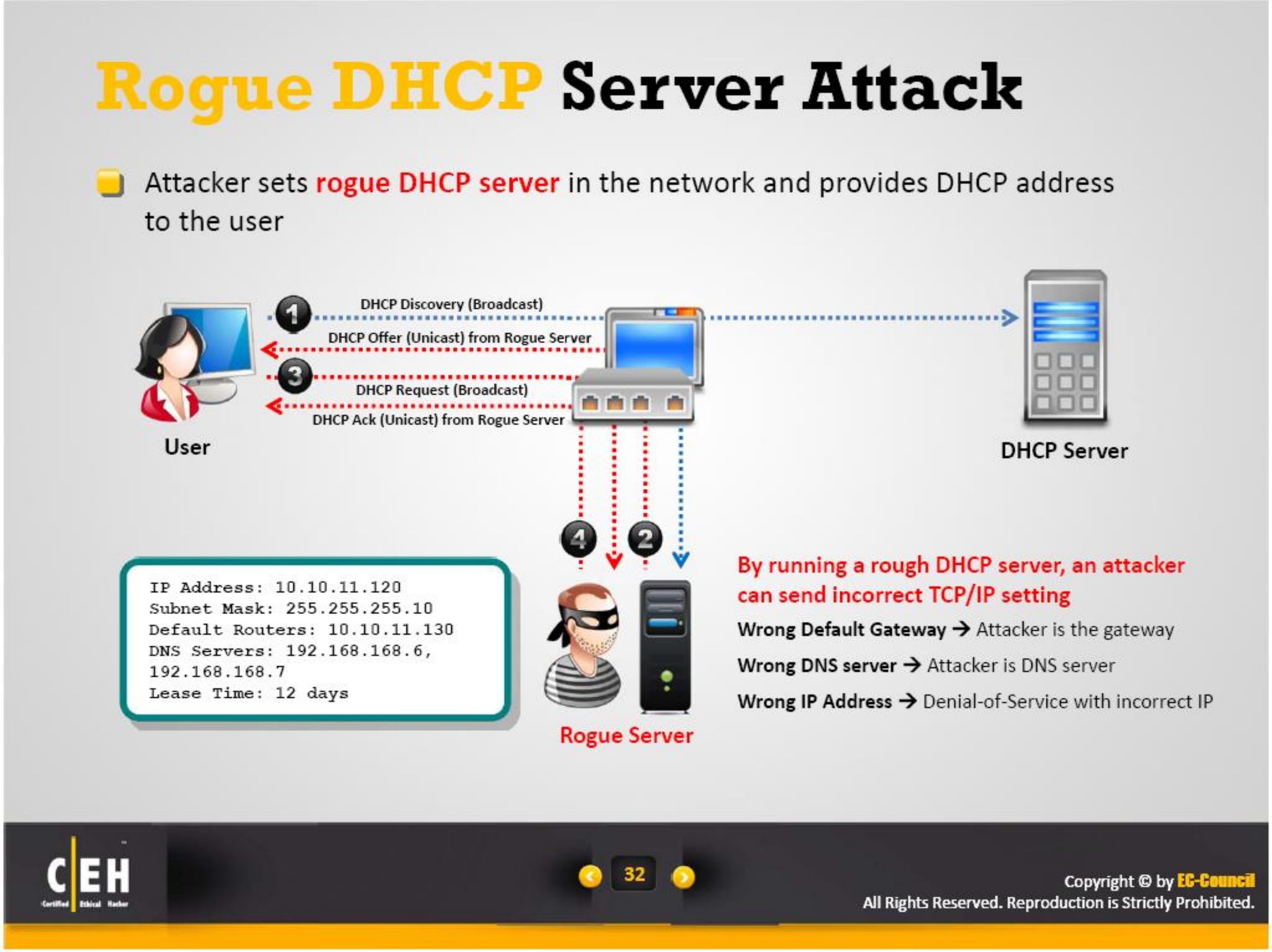
DHCP Server

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)
DHCP Offer (Unicast) from Rogue Server
3
DHCP Request (Broadcast)
DHCP Ack (Unicast) from Rogue Server
User
DHCP Server
4
2
Rogue Server

```
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
```

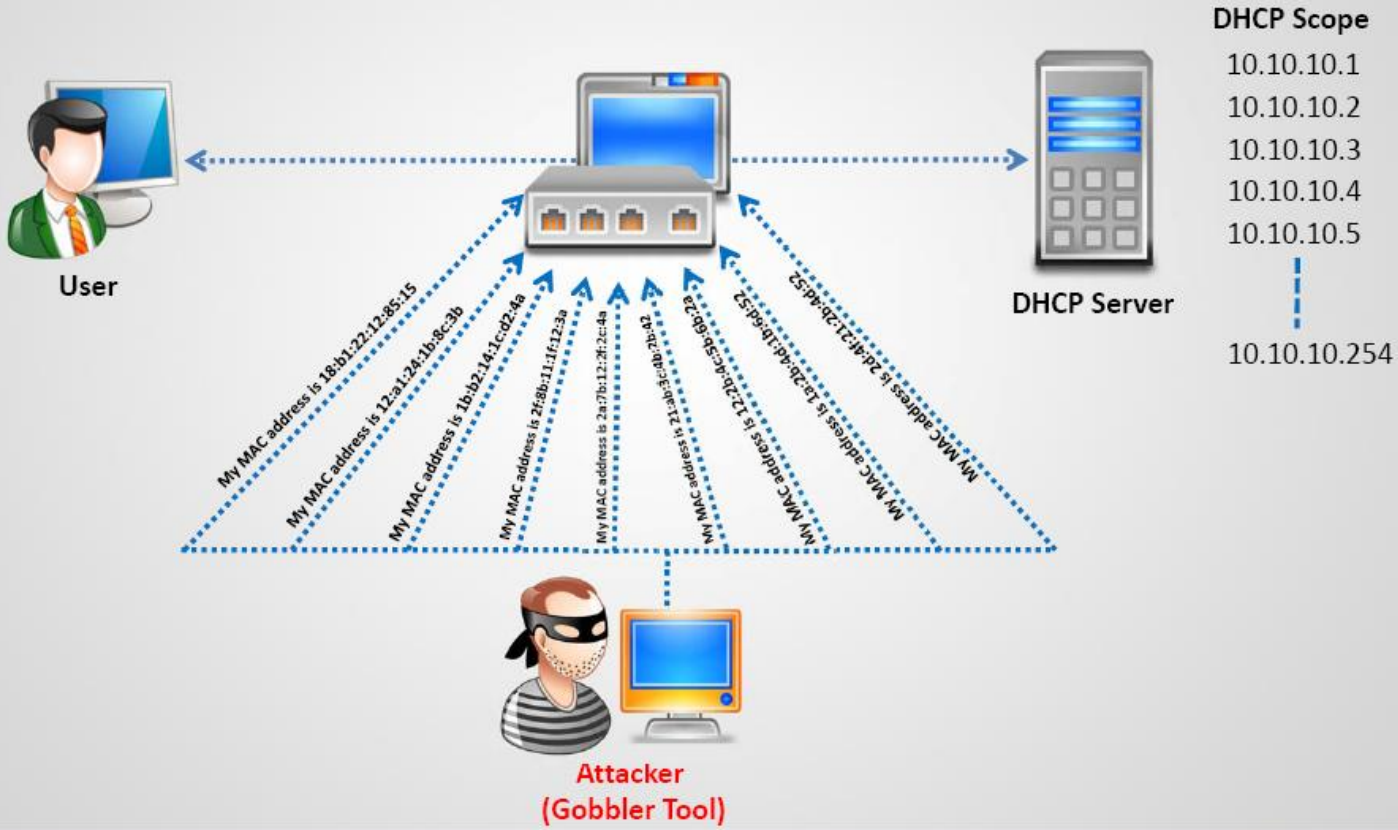
By running a rough DHCP server, an attacker can send incorrect TCP/IP setting

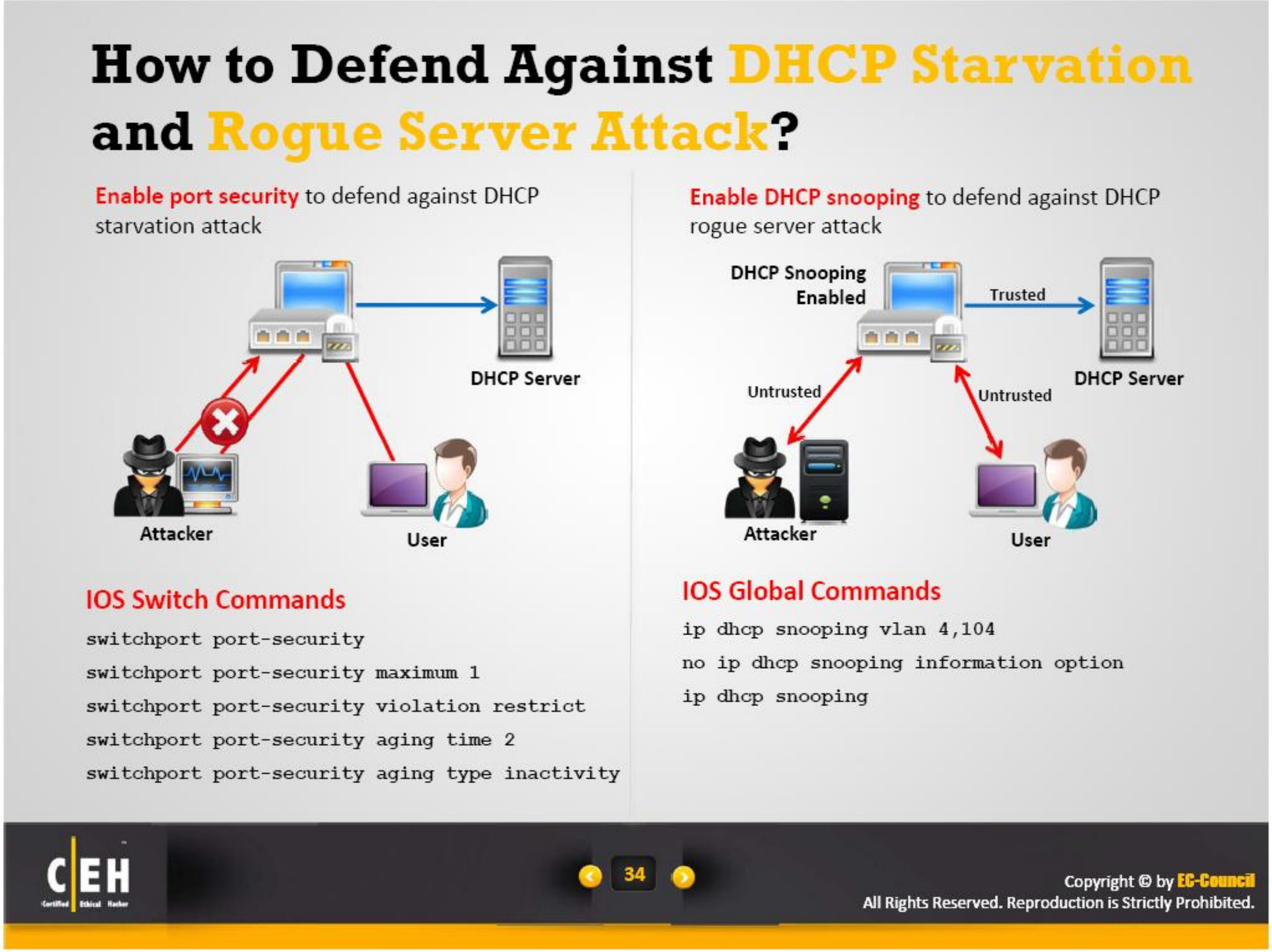
Wrong Default Gateway → Attacker is the gateway

Wrong DNS server → Attacker is DNS server

Wrong IP Address → Denial-of-Service with incorrect IP

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
User
DHCP Server
My MAC address is 18:b1:22:12:85:15
My MAC address is 12:a1:24:1b:8c:3b
My MAC address is 1b:b2:14:1c:d2:4a
My MAC address is 2f:8b:11:1f:12:3a
My MAC address is 2a:7b:12:2f:2c:4a
My MAC address is 21:ab:3c:4b:7b:42
My MAC address is 12:2b:4C:5b:6b:2a
My MAC address is 1a:2b:4d:1b:6d:52
My MAC address is 2d:4f:21:2b:4d:52
Attacker
(Gobbler Tool)



How to Defend Against DHCP Starvation and Rogue Server Attack?

Enable port security to defend against DHCP starvation attack

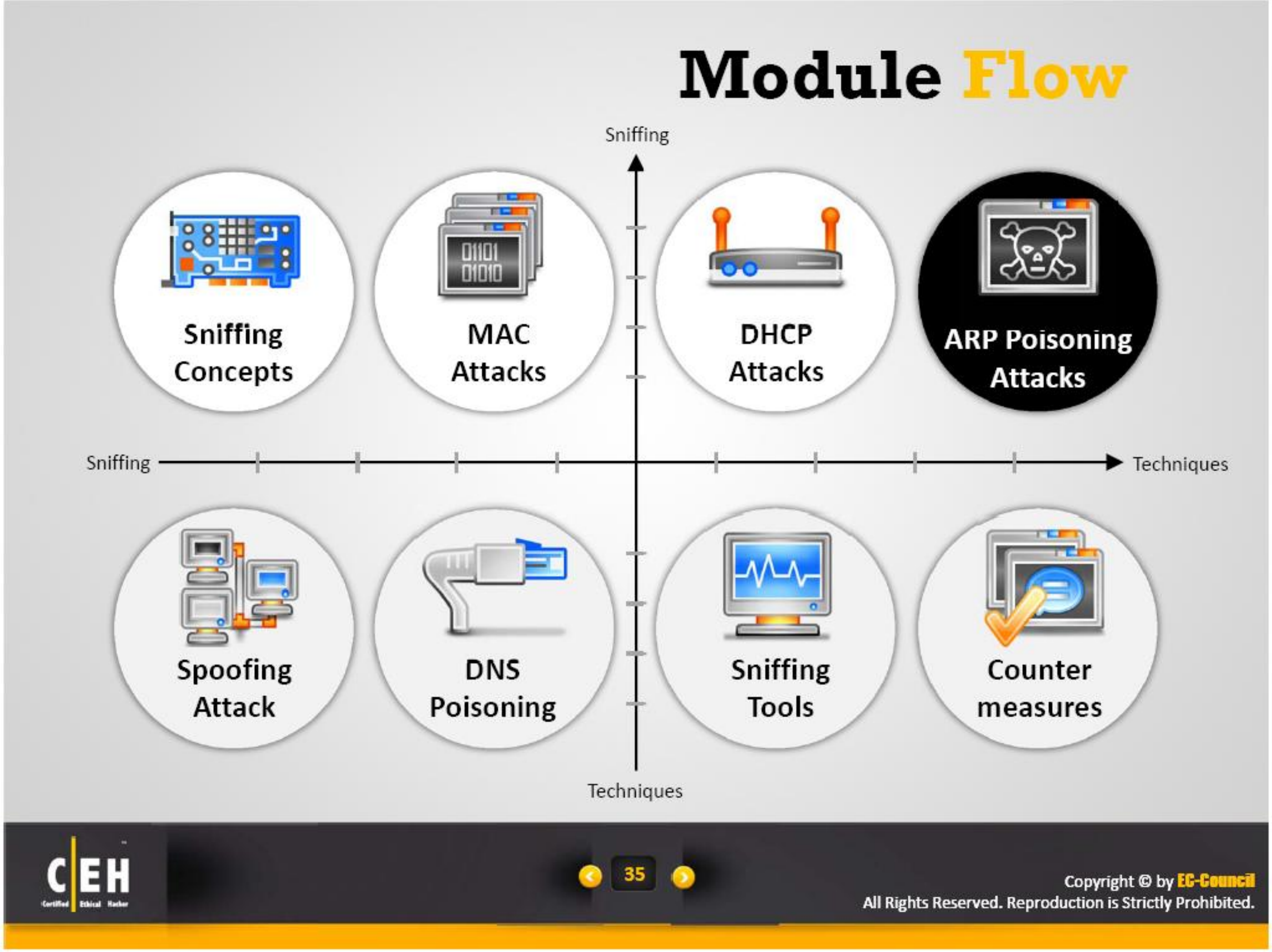
IOS Switch Commands

```
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
```

Enable DHCP snooping to defend against DHCP rogue server attack

IOS Global Commands

```
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
```



Module Flow

Sniffing

Sniffing Concepts

MAC Attacks

DHCP Attacks

ARP Poisoning Attacks

Sniffing

Techniques

Spoofing Attack

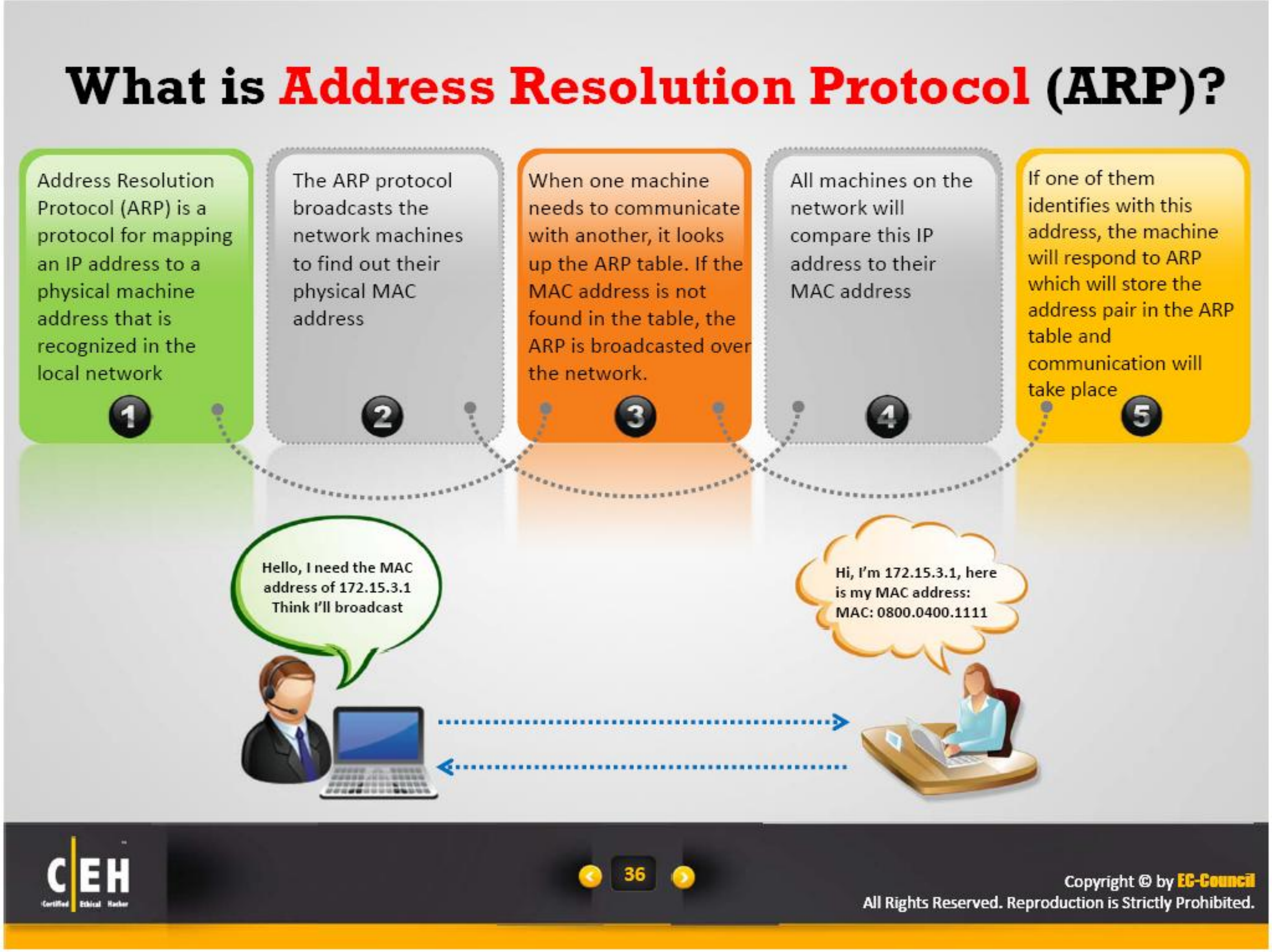
DNS Poisoning

Sniffing Tools

Counter measures

Techniques

CEH Certified Ethical Hacker



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

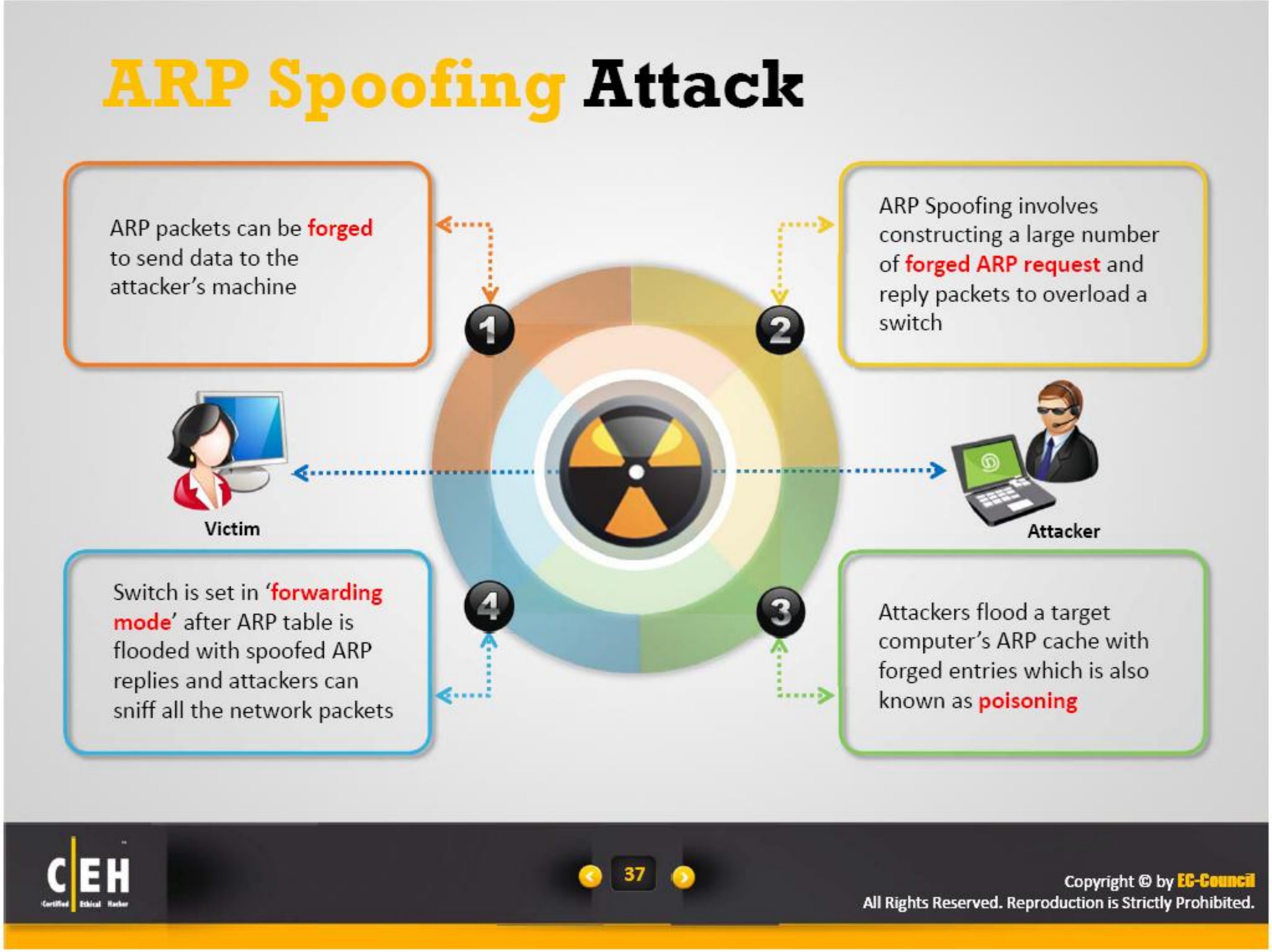
2. The ARP protocol broadcasts the network machines to find out their physical MAC address

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

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



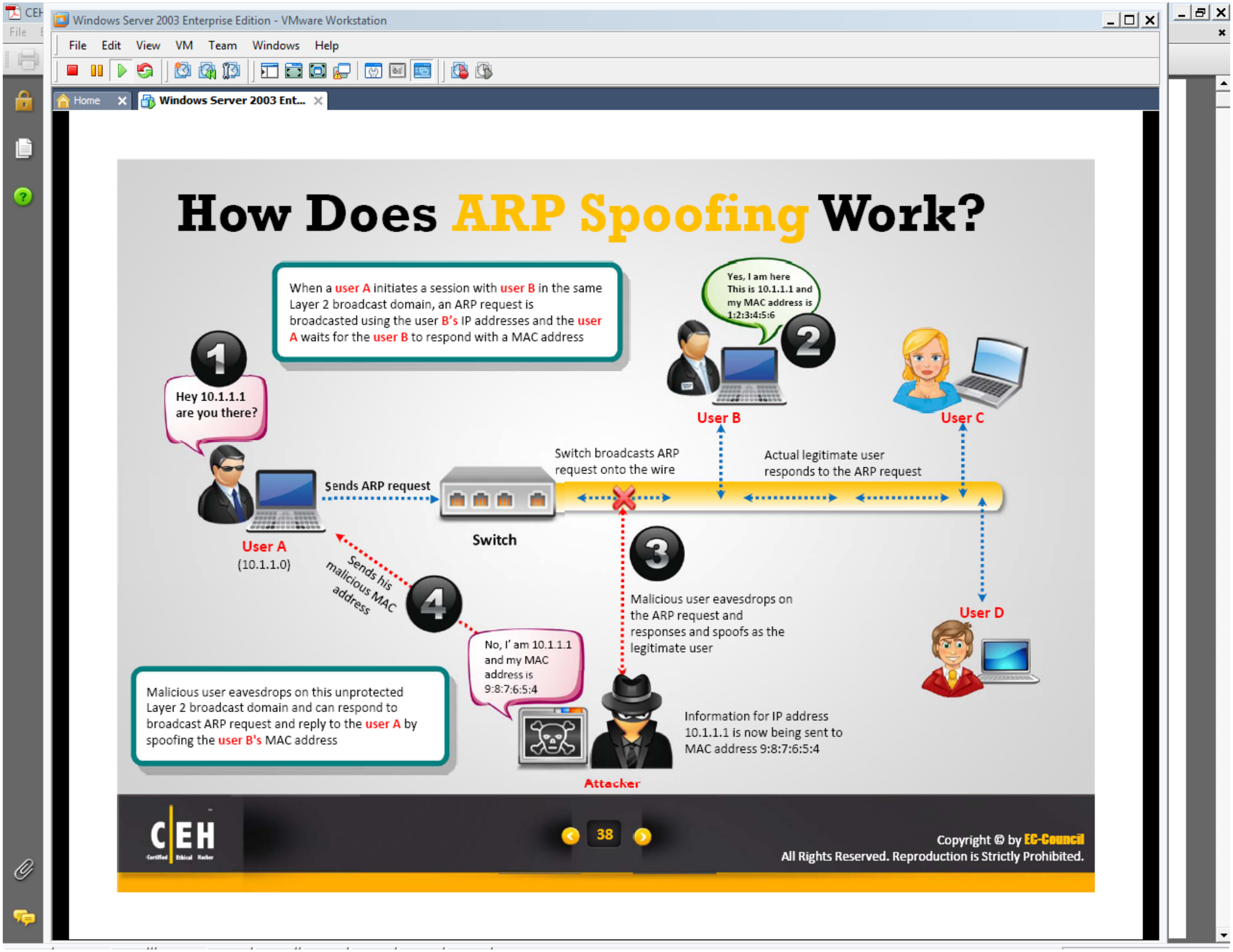
ARP Spoofing Attack

1. ARP packets can be **forged** to send data to the attacker's machine

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

3. Attackers flood a target computer's ARP cache with forged entries which is also known as **poisoning**

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


CEH
File
Windows Server 2003 Enterprise Edition - VMware Workstation
File Edit View VM Team Windows Help
Home
Windows Server 2003 Ent...

How Does ARP Spoofing Work?

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

1 Hey 10.1.1.1 are you there?

2 Yes, I am here This is 10.1.1.1 and my MAC address is 1:2:3:4:5:6

User A (10.1.1.0)

Sends ARP request

Switch

Switch broadcasts ARP request onto the wire

User B

User C

Actual legitimate user responds to the ARP request

User D

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

4 Sends his malicious MAC address

No, I' am 10.1.1.1 and my MAC address is 9:8:7:6:5:4

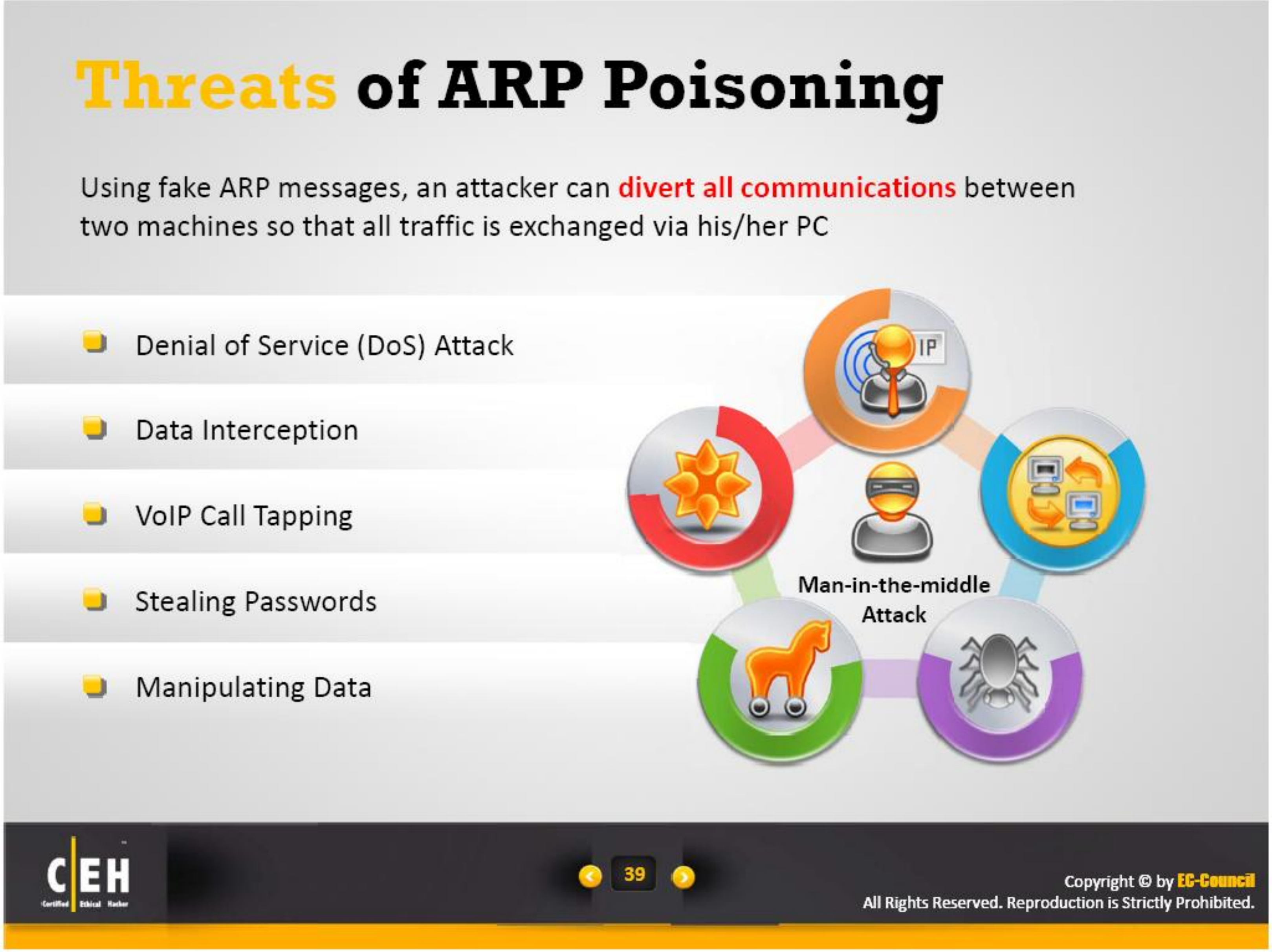
Malicious user eavesdrops on this unprotected Layer 2 broadcast domain and can respond to broadcast ARP request and reply to the user A by spoofing the user B's MAC address

Attacker

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

CEH Certified Ethical Hacker

38



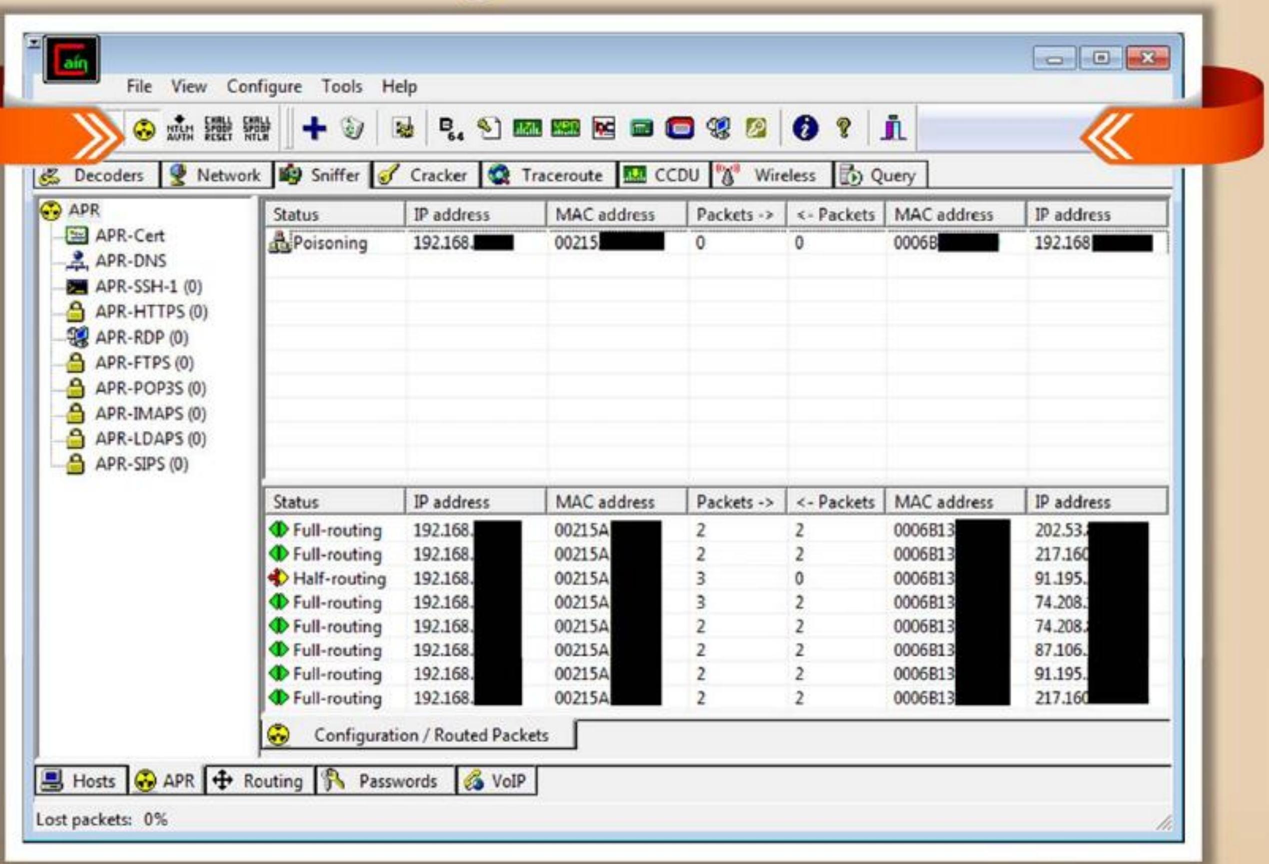
Threats of ARP Poisoning

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

Man-in-the-middle Attack

ARP Poisoning Tool: Cain and Abel



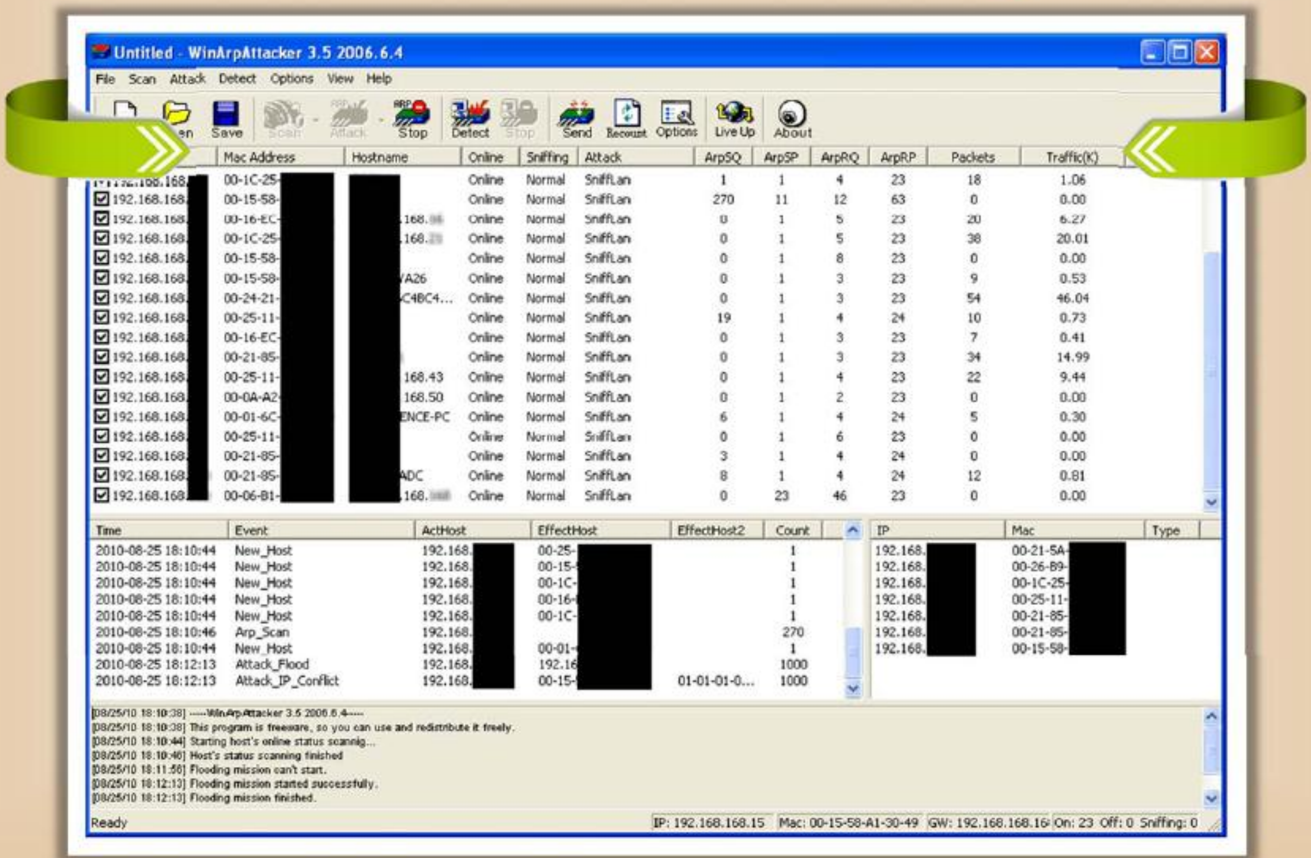
Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.[redacted]	00215[redacted]	0	0	0006B[redacted]	192.168[redacted]

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	202.53.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	217.160[redacted]
Half-routing	192.168.[redacted]	00215A[redacted]	3	0	0006B13[redacted]	91.195.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	3	2	0006B13[redacted]	74.208.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	74.208.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	87.106.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	91.195.[redacted]
Full-routing	192.168.[redacted]	00215A[redacted]	2	2	0006B13[redacted]	217.160[redacted]

Lost packets: 0%

http://www.oxid.it

ARP Poisoning Tool: WinArpAttacker



Untitled - WinArpAttacker 3.5 2006.6.4

	Mac Address	Hostname	Online	Sniffing	Attack	ArpSQ	ArpSP	ArpRQ	ArpRP	Packets	Traffic(K)
192.168.168.[redacted]	00-1C-25-[redacted]	[redacted]	Online	Normal	SniffLan	1	1	4	23	18	1.06
☑ 192.168.168.[redacted]	00-15-58-[redacted]	[redacted]	Online	Normal	SniffLan	270	11	12	63	0	0.00
☑ 192.168.168.[redacted]	00-16-EC-[redacted]	[redacted].168.[redacted]	Online	Normal	SniffLan	0	1	5	23	20	6.27
☑ 192.168.168.[redacted]	00-1C-25-[redacted]	[redacted].168.[redacted]	Online	Normal	SniffLan	0	1	5	23	38	20.01
☑ 192.168.168.[redacted]	00-15-58-[redacted]	[redacted]	Online	Normal	SniffLan	0	1	8	23	0	0.00
☑ 192.168.168.[redacted]	00-15-58-[redacted]	[redacted]A26	Online	Normal	SniffLan	0	1	3	23	9	0.53
☑ 192.168.168.[redacted]	00-24-21-[redacted]	[redacted]C4BC4...	Online	Normal	SniffLan	0	1	3	23	54	46.04
☑ 192.168.168.[redacted]	00-25-11-[redacted]	[redacted]	Online	Normal	SniffLan	19	1	4	24	10	0.73
☑ 192.168.168.[redacted]	00-16-EC-[redacted]	[redacted]	Online	Normal	SniffLan	0	1	3	23	7	0.41
☑ 192.168.168.[redacted]	00-21-85-[redacted]	[redacted]	Online	Normal	SniffLan	0	1	3	23	34	14.99
☑ 192.168.168.[redacted]	00-25-11-[redacted]	[redacted].168.43	Online	Normal	SniffLan	0	1	4	23	22	9.44
☑ 192.168.168.[redacted]	00-0A-A2-[redacted]	[redacted].168.50	Online	Normal	SniffLan	0	1	2	23	0	0.00
☑ 192.168.168.[redacted]	00-01-6C-[redacted]	[redacted]ENCE-PC	Online	Normal	SniffLan	6	1	4	24	5	0.30
☑ 192.168.168.[redacted]	00-25-11-[redacted]	[redacted]	Online	Normal	SniffLan	0	1	6	23	0	0.00
☑ 192.168.168.[redacted]	00-21-85-[redacted]	[redacted]	Online	Normal	SniffLan	3	1	4	24	0	0.00
☑ 192.168.168.[redacted]	00-21-85-[redacted]	[redacted]ADC	Online	Normal	SniffLan	8	1	4	24	12	0.81
☑ 192.168.168.[redacted]	00-06-B1-[redacted]	[redacted].168.[redacted]	Online	Normal	SniffLan	0	23	46	23	0	0.00

Time	Event	ActHost	EffectHost	EffectHost2	Count
2010-08-25 18:10:44	New_Host	192.168.[redacted]	00-25-[redacted]		1
2010-08-25 18:10:44	New_Host	192.168.[redacted]	00-15-[redacted]		1
2010-08-25 18:10:44	New_Host	192.168.[redacted]	00-1C-[redacted]		1
2010-08-25 18:10:44	New_Host	192.168.[redacted]	00-16-[redacted]		1
2010-08-25 18:10:44	New_Host	192.168.[redacted]	00-1C-[redacted]		1
2010-08-25 18:10:46	Arp_Scan	192.168.[redacted]	[redacted]		270
2010-08-25 18:10:44	New_Host	192.168.[redacted]	00-01-[redacted]		1
2010-08-25 18:12:13	Attack_Flood	192.168.[redacted]	192.16[redacted]		1000
2010-08-25 18:12:13	Attack_IP_Conflict	192.168.[redacted]	00-15-[redacted]	01-01-01-0...	1000

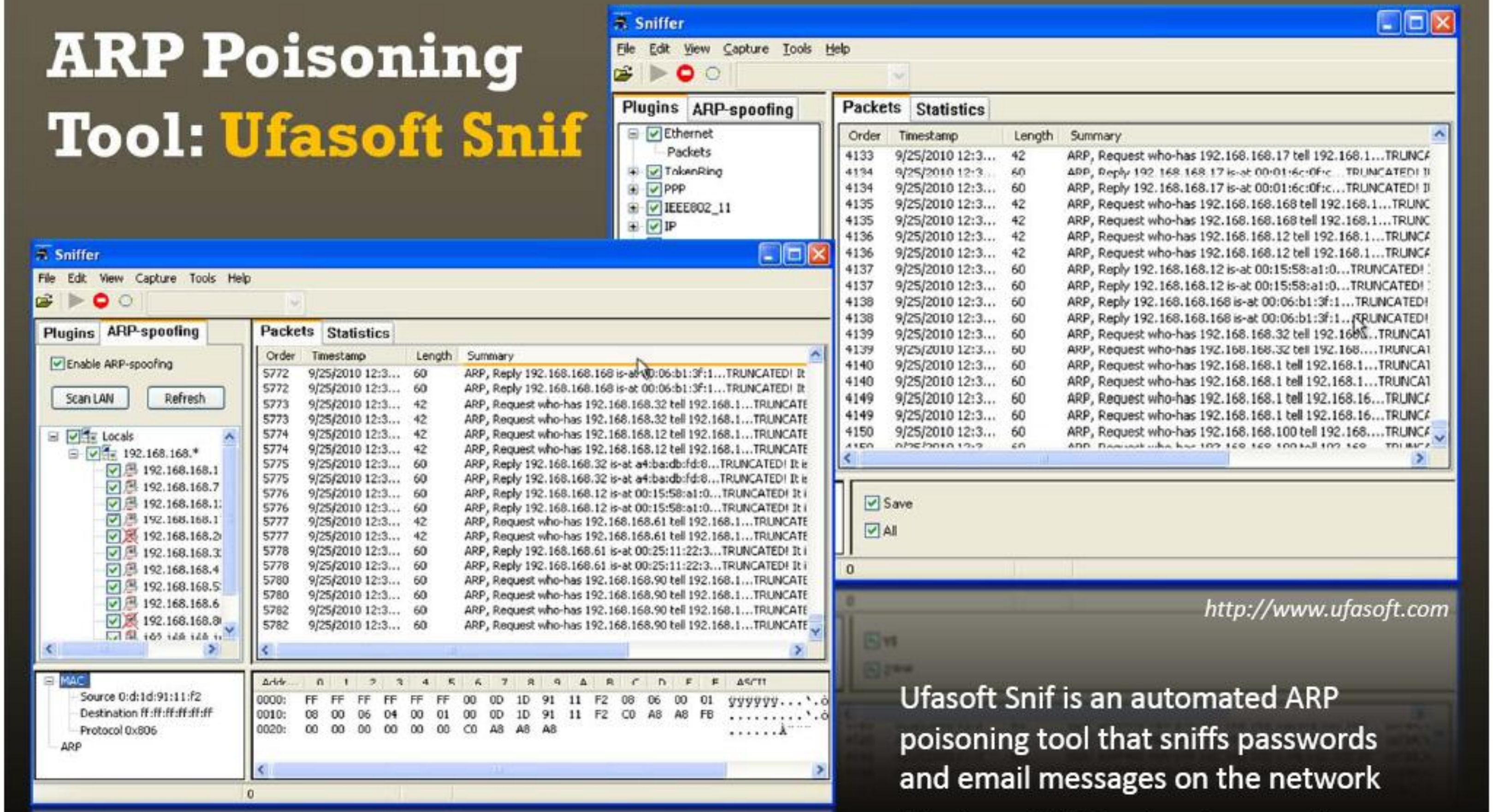
IP	Mac	Type
192.168.[redacted]	00-21-5A-[redacted]	
192.168.[redacted]	00-26-B9-[redacted]	
192.168.[redacted]	00-1C-25-[redacted]	
192.168.[redacted]	00-25-11-[redacted]	
192.168.[redacted]	00-21-85-[redacted]	
192.168.[redacted]	00-21-85-[redacted]	
192.168.[redacted]	00-15-58-[redacted]	

```
[08/25/10 18:10:38] -----WinArpAttacker 3.5 2006.6.4-----
[08/25/10 18:10:38] This program is freeware, so you can use and redistribute it freely.
[08/25/10 18:10:44] Starting host's online status scannig...
[08/25/10 18:10:46] Host's status scanning finished
[08/25/10 18:11:56] Flooding mission can't start.
[08/25/10 18:12:13] Flooding mission started successfully.
[08/25/10 18:12:13] Flooding mission finished.
```

Ready | IP: 192.168.168.15 | Mac: 00-15-58-A1-30-49 | GW: 192.168.168.16 | On: 23 Off: 0 Sniffing: 0

http://www.xfocus.net

ARP Poisoning Tool: Ufasoft Snif



```
Order  Timestamp          Length  Summary
4133   9/25/2010 12:3...  42      ARP, Request who-has 192.168.168.17 tell 192.168.1...TRUNCA
4134   9/25/2010 12:3...  60      ARP, Reply 192.168.168.17 is-at 00:01:6c:0f:c...TRUNCATED! I
4134   9/25/2010 12:3...  60      ARP, Reply 192.168.168.17 is-at 00:01:6c:0f:c...TRUNCATED! I
4135   9/25/2010 12:3...  42      ARP, Request who-has 192.168.168.168 tell 192.168.1...TRUNC
4135   9/25/2010 12:3...  42      ARP, Request who-has 192.168.168.168 tell 192.168.1...TRUNC
4136   9/25/2010 12:3...  42      ARP, Request who-has 192.168.168.12 tell 192.168.1...TRUNCA
4136   9/25/2010 12:3...  42      ARP, Request who-has 192.168.168.12 tell 192.168.1...TRUNCA
4137   9/25/2010 12:3...  60      ARP, Reply 192.168.168.12 is-at 00:15:58:a1:0...TRUNCATED!
4137   9/25/2010 12:3...  60      ARP, Reply 192.168.168.12 is-at 00:15:58:a1:0...TRUNCATED!
4138   9/25/2010 12:3...  60      ARP, Reply 192.168.168.168 is-at 00:06:b1:3f:1...TRUNCATED!
4138   9/25/2010 12:3...  60      ARP, Reply 192.168.168.168 is-at 00:06:b1:3f:1...TRUNCATED!
4139   9/25/2010 12:3...  60      ARP, Request who-has 192.168.168.32 tell 192.168...TRUNCAT
4139   9/25/2010 12:3...  60      ARP, Request who-has 192.168.168.32 tell 192.168....TRUNCAT
4140   9/25/2010 12:3...  60      ARP, Request who-has 192.168.168.1 tell 192.168.1...TRUNCAT
4140   9/25/2010 12:3...  60      ARP, Request who-has 192.168.168.1 tell 192.168.1...TRUNCAT
4149   9/25/2010 12:3...  60      ARP, Request who-has 192.168.168.1 tell 192.168.16...TRUNCA
4149   9/25/2010 12:3...  60      ARP, Request who-has 192.168.168.1 tell 192.168.16...TRUNCA
4150   9/25/2010 12:3...  60      ARP, Request who-has 192.168.168.100 tell 192.168....TRUNCA
```

☑ Enable ARP-spoofing

```
Locals
  192.168.168.*
    192.168.168.1
    192.168.168.7
    192.168.168.1:
    192.168.168.1
    192.168.168.2
    192.168.168.3:
    192.168.168.4
    192.168.168.5:
    192.168.168.6
    192.168.168.8
```

```
Order  Timestamp          Length  Summary
5772   9/25/2010 12:3...  60      ARP, Reply 192.168.168.168 is-at 00:06:b1:3f:1...TRUNCATED! It
5772   9/25/2010 12:3...  60      ARP, Reply 192.168.168.168 is-at 00:06:b1:3f:1...TRUNCATED! It
5773   9/25/2010 12:3...  42      ARP, Request who-has 192.168.168.32 tell 192.168.1...TRUNCATE
5773   9/25/2010 12:3...  42      ARP, Request who-has 192.168.168.32 tell 192.168.1...TRUNCATE
5774   9/25/2010 12:3...  42      ARP, Request who-has 192.168.168.12 tell 192.168.1...TRUNCATE
5774   9/25/2010 12:3...  42      ARP, Request who-has 192.168.168.12 tell 192.168.1...TRUNCATE
5775   9/25/2010 12:3...  60      ARP, Reply 192.168.168.32 is-at a4:ba:db:fd:8...TRUNCATED! It is
5775   9/25/2010 12:3...  60      ARP, Reply 192.168.168.32 is-at a4:ba:db:fd:8...TRUNCATED! It is
5776   9/25/2010 12:3...  60      ARP, Reply 192.168.168.12 is-at 00:15:58:a1:0...TRUNCATED! It i
5776   9/25/2010 12:3...  60      ARP, Reply 192.168.168.12 is-at 00:15:58:a1:0...TRUNCATED! It i
5777   9/25/2010 12:3...  42      ARP, Request who-has 192.168.168.61 tell 192.168.1...TRUNCATE
5777   9/25/2010 12:3...  42      ARP, Request who-has 192.168.168.61 tell 192.168.1...TRUNCATE
5778   9/25/2010 12:3...  60      ARP, Reply 192.168.168.61 is-at 00:25:11:22:3...TRUNCATED! It i
5778   9/25/2010 12:3...  60      ARP, Reply 192.168.168.61 is-at 00:25:11:22:3...TRUNCATED! It i
5780   9/25/2010 12:3...  60      ARP, Request who-has 192.168.168.90 tell 192.168.1...TRUNCATE
5780   9/25/2010 12:3...  60      ARP, Request who-has 192.168.168.90 tell 192.168.1...TRUNCATE
5782   9/25/2010 12:3...  60      ARP, Request who-has 192.168.168.90 tell 192.168.1...TRUNCATE
5782   9/25/2010 12:3...  60      ARP, Request who-has 192.168.168.90 tell 192.168.1...TRUNCATE
```

```
MAC
  Source 0:d:1d:91:11:f2
  Destination ff:ff:ff:ff:ff:ff
  Protocol 0x806
ARP
```

```
Addr...  0   1   2   3   4   5   6   7   8   9   A   B   C   D   E   F   ASCII
0000:    FF  FF  FF  FF  FF  FF  00  0D  1D  91  11  F2  08  06  00  01  ÿÿÿÿÿÿ...`.ò
0010:    08  00  06  04  00  01  00  0D  1D  91  11  F2  C0  A8  A8  FB  ..........`.ò
0020:    00  00  00  00  00  00  C0  A8  A8  A8                          ......À
```

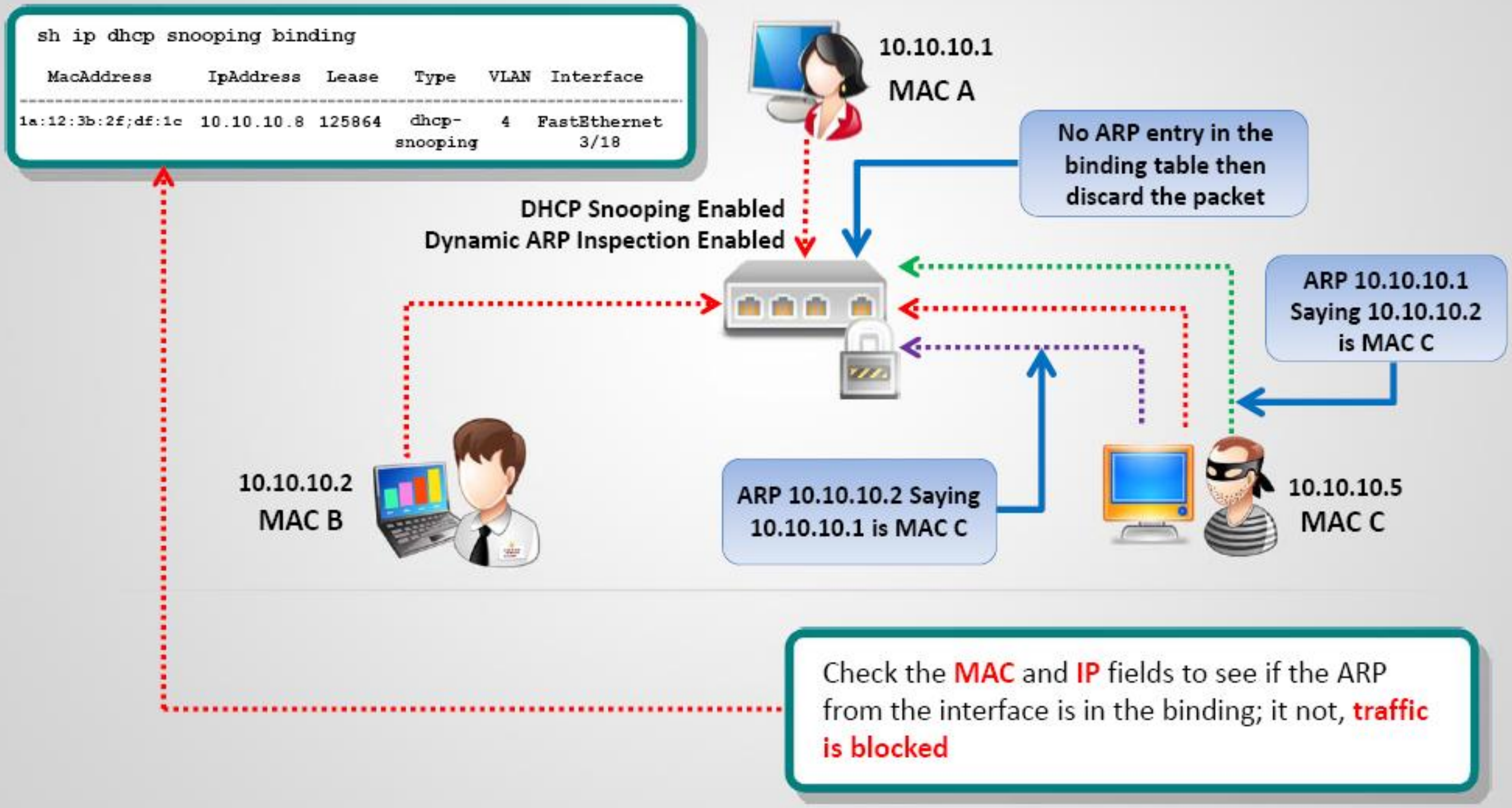
http://www.ufasoft.com

Ufasoft Snif is an automated ARP poisoning tool that sniffs passwords and email messages on the network

Works on Wi-Fi network as well

How to Defend Against ARP Poisoning?

Use DHCP Snooping Binding Table and Dynamic ARP Inspection



```
sh ip dhcp snooping binding

 MacAddress         IpAddress   Lease    Type    VLAN  Interface
--------------------------------------------------------------------
1a:12:3b:2f;df:1c  10.10.10.8  125864   dhcp-    4   FastEthernet
                                       snooping          3/18
```

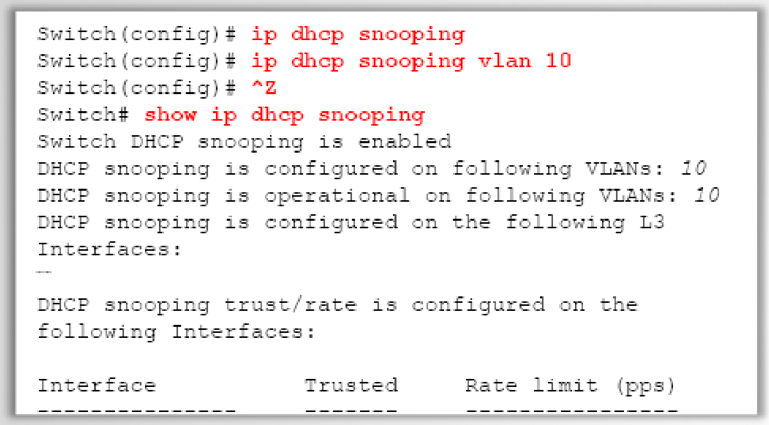
No ARP entry in the binding table then discard the packet

ARP 10.10.10.1 Saying 10.10.10.2 is MAC C

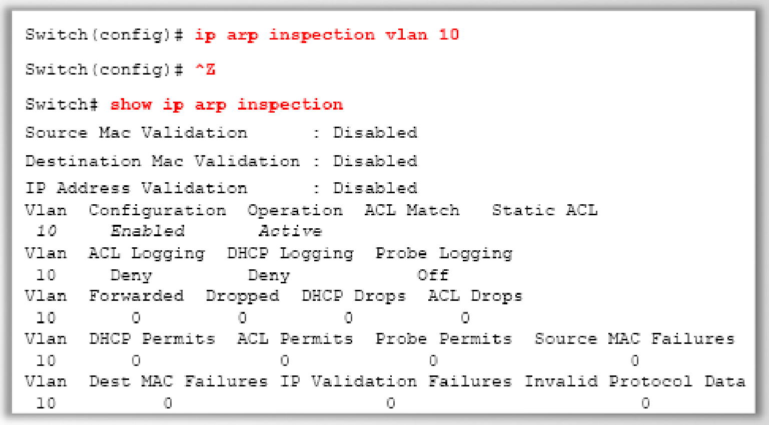
ARP 10.10.10.2 Saying 10.10.10.1 is MAC C

Check the **MAC** and **IP** fields to see if the ARP from the interface is in the binding; it not, **traffic is blocked**

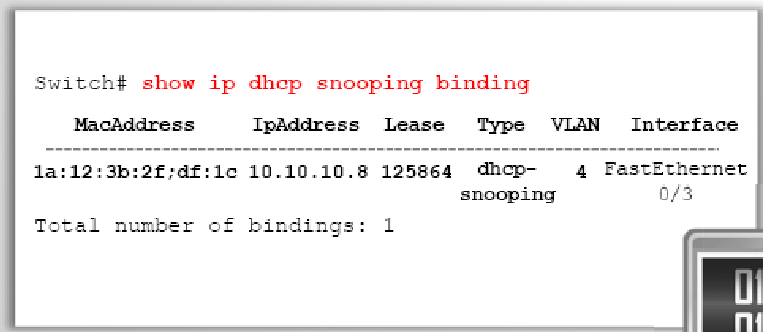
Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches



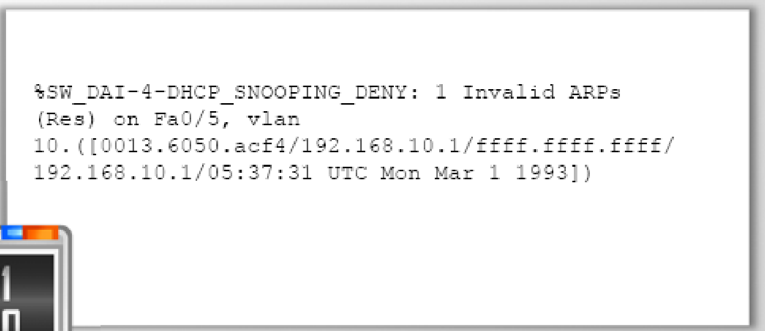
```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ^Z
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs: 10
DHCP snooping is operational on following VLANs: 10
DHCP snooping is configured on the following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

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

Interface             Trusted     Rate limit (pps)
---------------       -------     ----------------
```



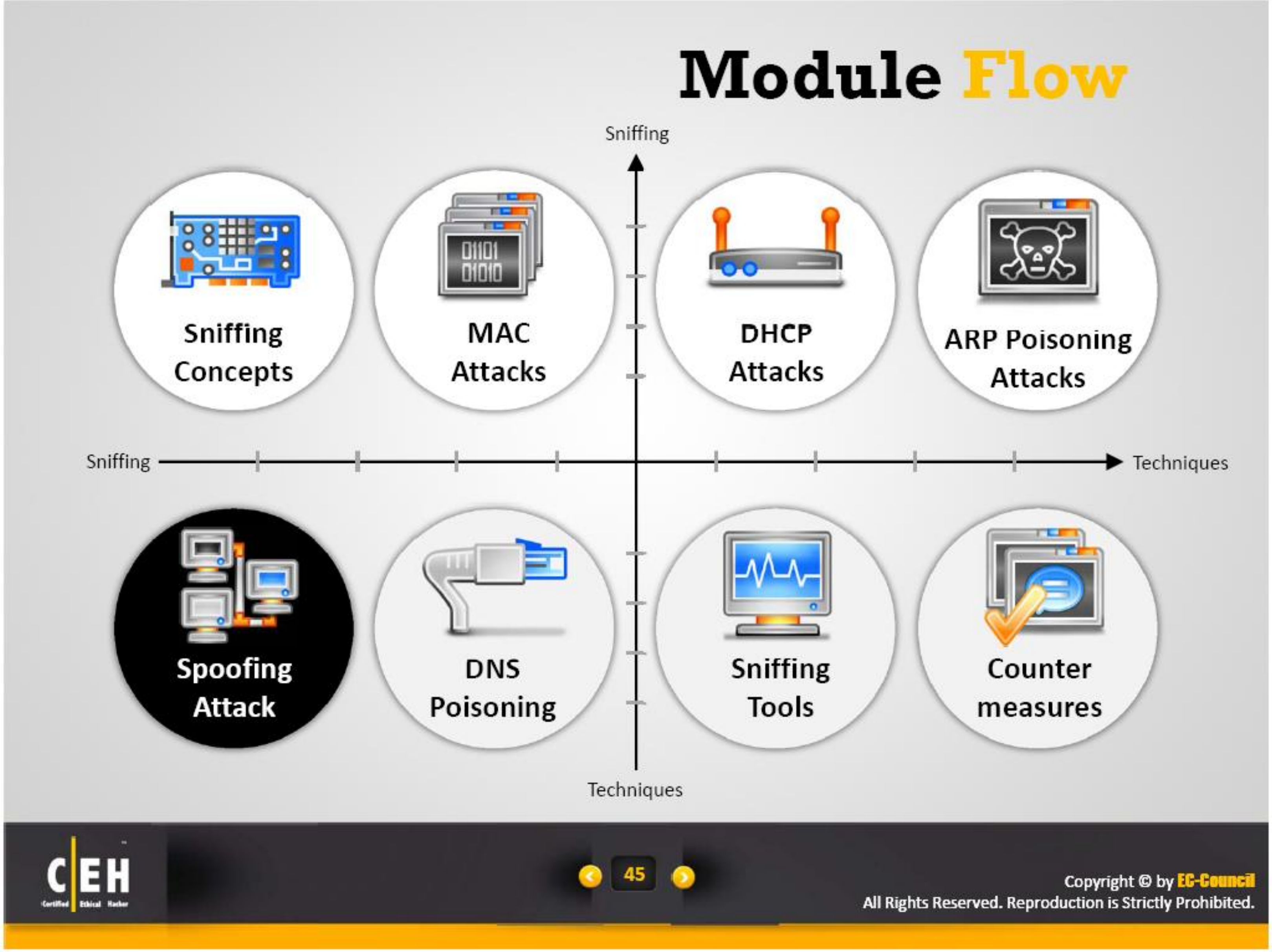
```
Switch(config)# ip arp inspection vlan 10

Switch(config)# ^Z

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          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
```



```
Switch# show ip dhcp snooping binding

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

Total number of bindings: 1
```

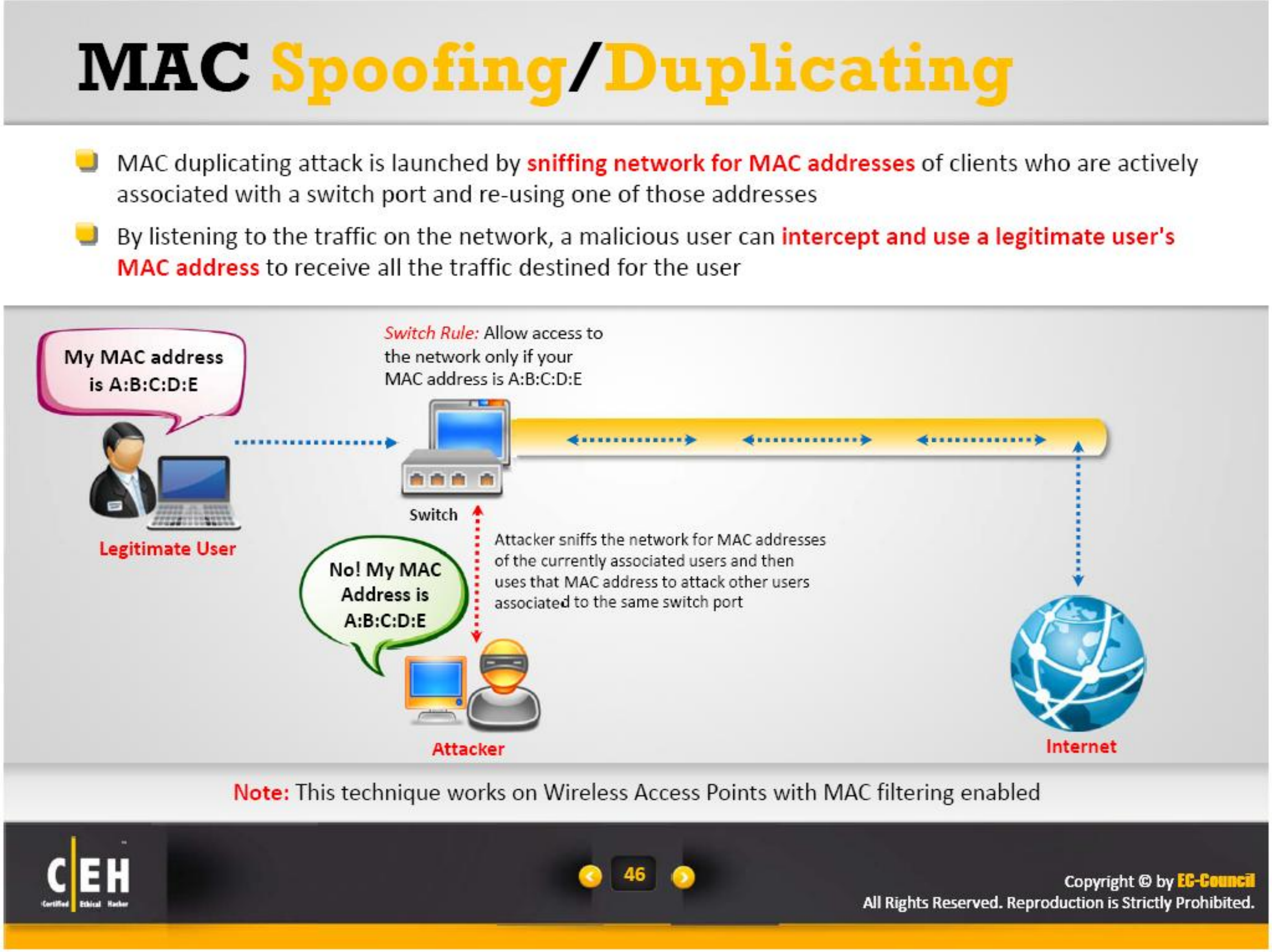


```
%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs
(Res) on Fa0/5, vlan
10.([0013.6050.acf4/192.168.10.1/ffff.ffff.ffff/
192.168.10.1/05:37:31 UTC Mon Mar 1 1993])
```



Module Flow

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



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

My MAC address is A:B:C:D:E

Legitimate User

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

Switch

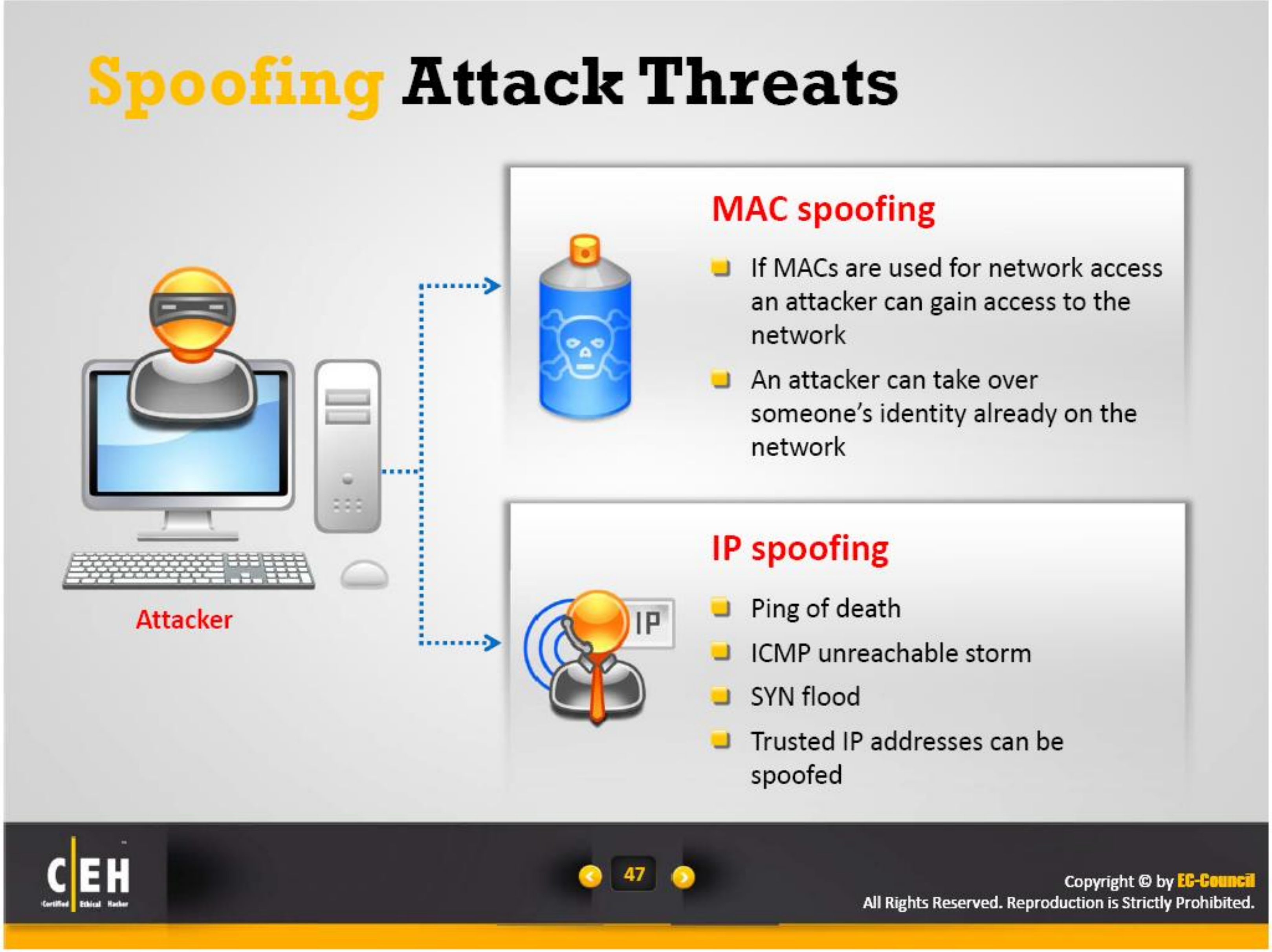
No! My MAC Address is A:B:C:D:E

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

Attacker

Internet

Note: This technique works on Wireless Access Points with MAC filtering enabled



Spoofing Attack Threats

Attacker

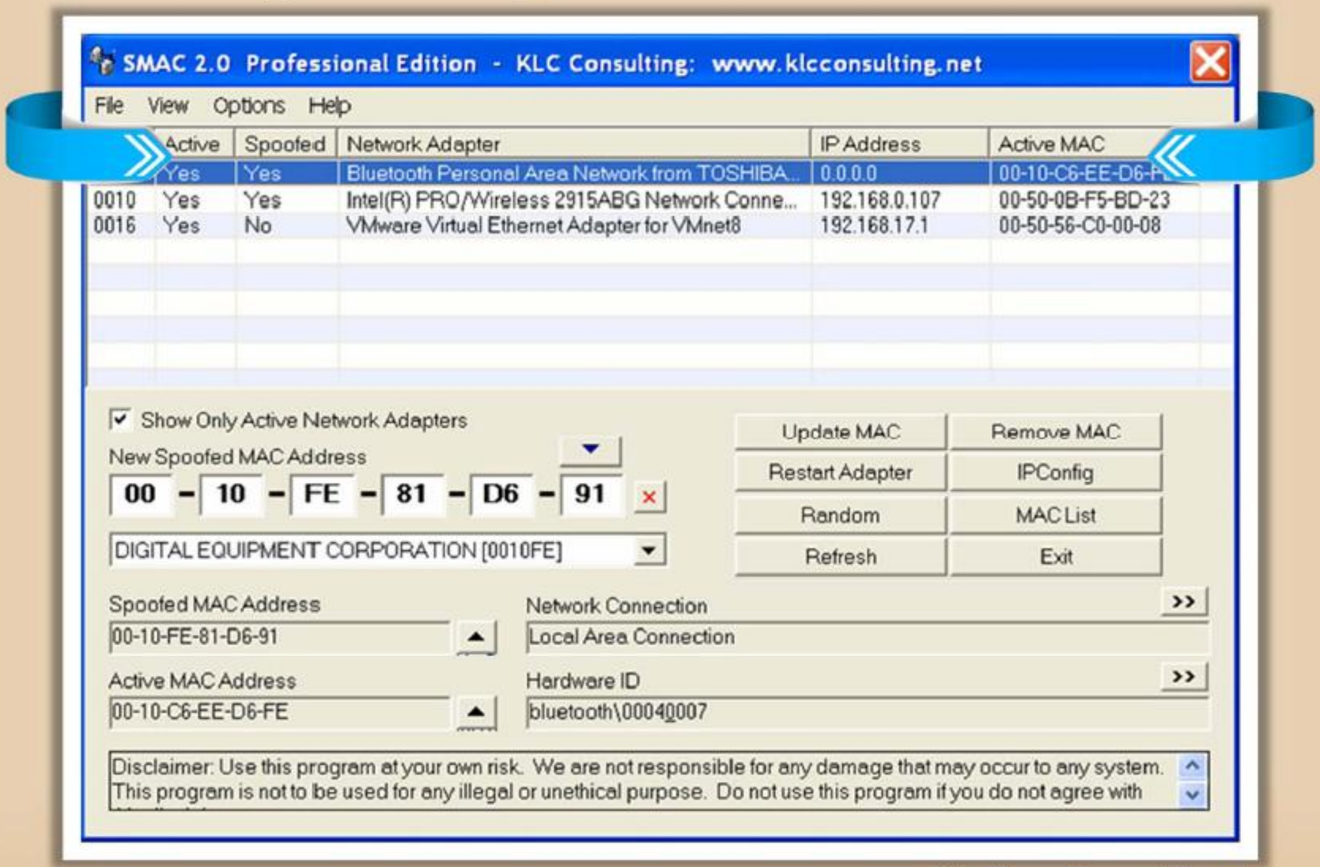
MAC spoofing

- 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 Professional Edition - KLC Consulting: www.klcconsulting.net
File
View
Options
Help

	Active	Spoofed	Network Adapter	IP Address	Active MAC
	Yes	Yes	Bluetooth Personal Area Network from TOSHIBA...	0.0.0.0	00-10-C6-EE-D6-F
0010	Yes	Yes	Intel(R) PRO/Wireless 2915ABG Network Conne...	192.168.0.107	00-50-0B-F5-BD-23
0016	Yes	No	VMware Virtual Ethernet Adapter for VMnet8	192.168.17.1	00-50-56-C0-00-08

☑ Show Only Active Network Adapters

New Spoofed MAC Address: 00 - 10 - FE - 81 - D6 - 91

DIGITAL EQUIPMENT CORPORATION [0010FE]

Spoofed MAC Address: 00-10-FE-81-D6-91

Network Connection: Local Area Connection

Active MAC Address: 00-10-C6-EE-D6-FE

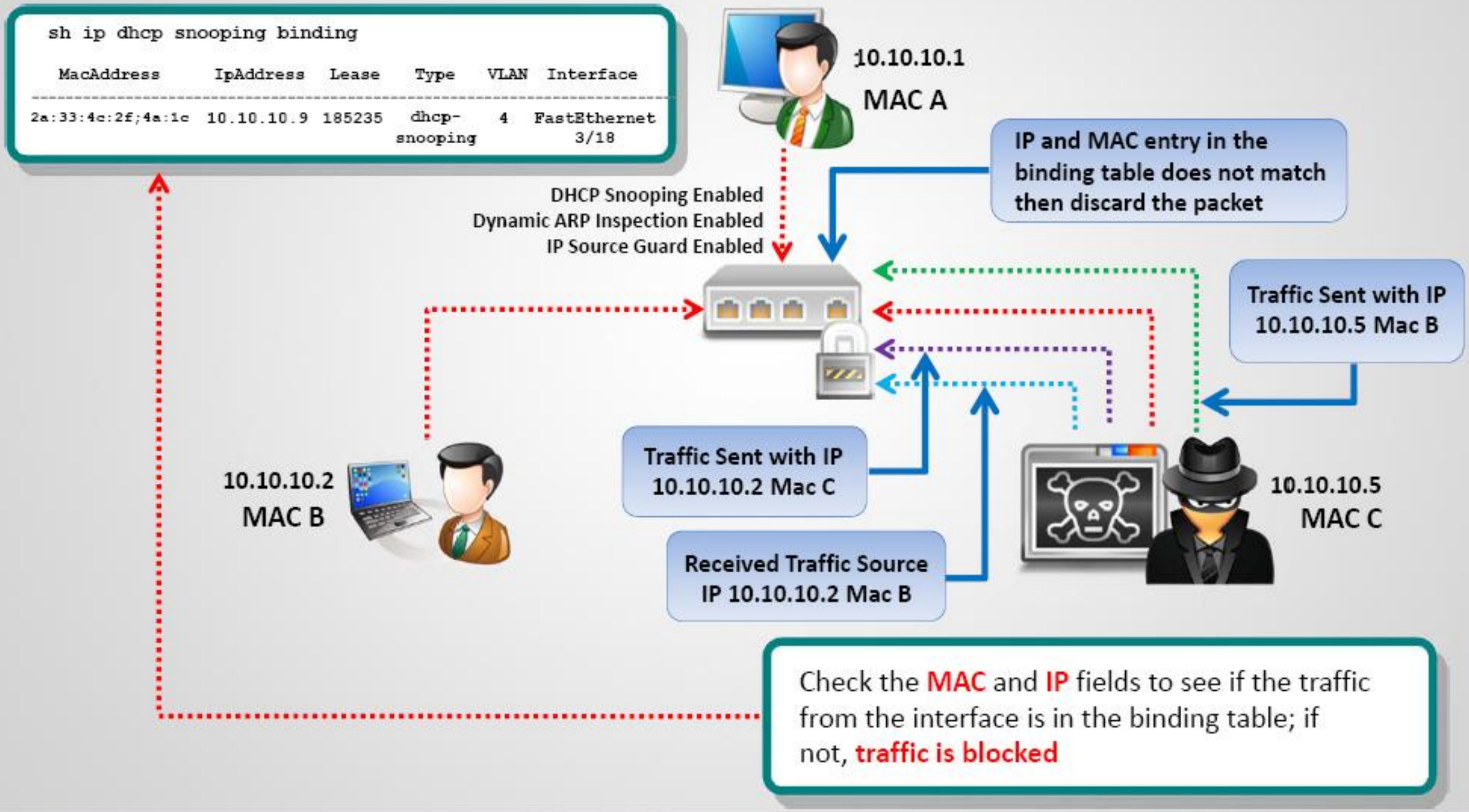
Hardware ID: bluetooth\00040007

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

http://www.klcconsulting.net

How to Defend Against MAC Spoofing?

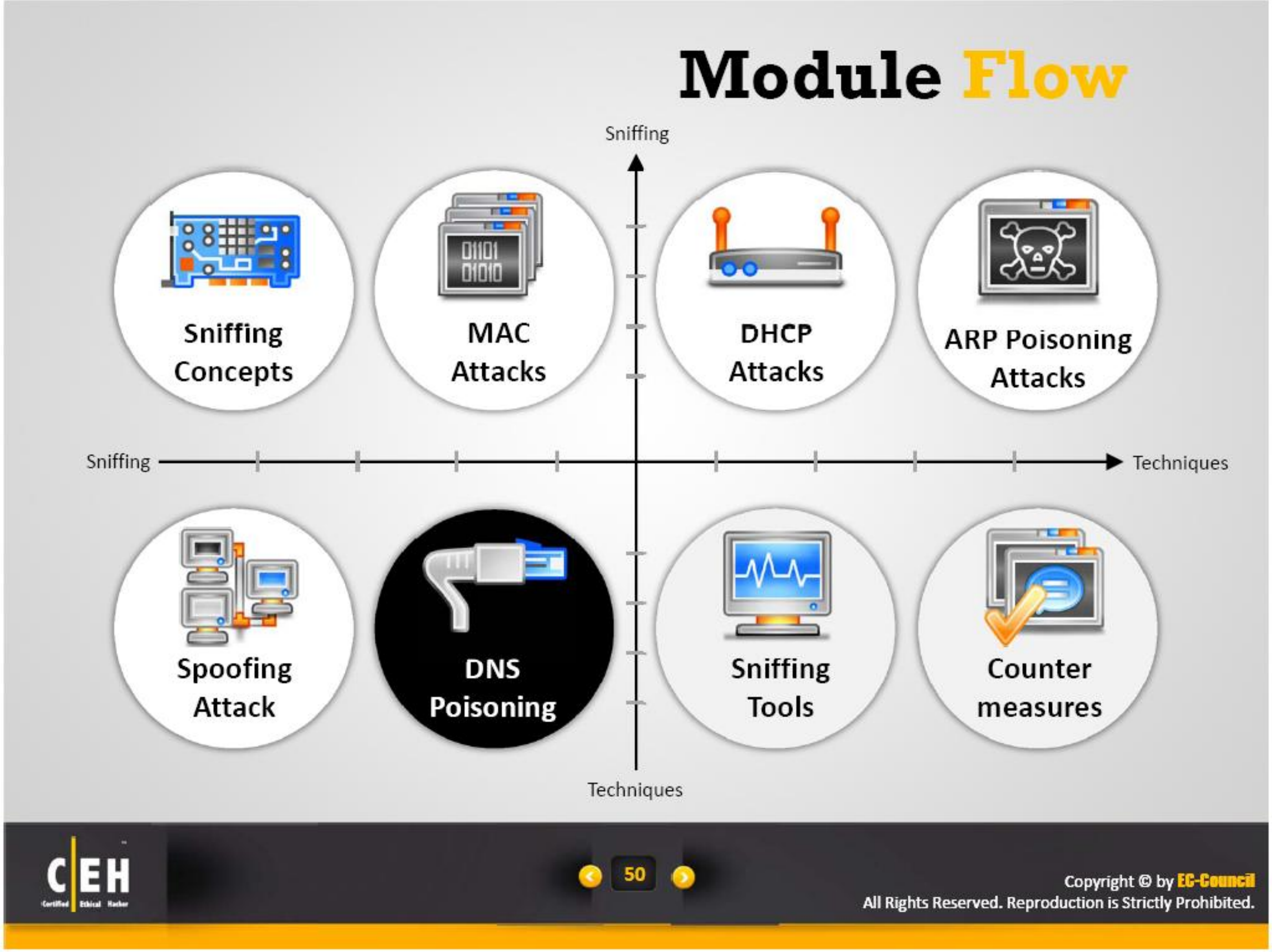
Use DHCP Snooping Binding Table, Dynamic ARP Inspection and IP Source Guard



```
 sh ip dhcp snooping binding

  MacAddress        IpAddress   Lease    Type    VLAN  Interface
------------------------------------------------------------------
2a:33:4c:2f;4a:1c  10.10.10.9  185235   dhcp-     4   FastEthernet
                                       snooping           3/18
```

10.10.10.1
MAC A
IP and MAC entry in the binding table does not match then discard the packet
DHCP Snooping Enabled
Dynamic ARP Inspection Enabled
IP Source Guard Enabled
Traffic Sent with IP 10.10.10.5 Mac B
10.10.10.2
MAC B
Traffic Sent with IP 10.10.10.2 Mac C
Received Traffic Source IP 10.10.10.2 Mac B
10.10.10.5
MAC C

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



Module Flow

Sniffing

Sniffing Concepts

MAC Attacks

DHCP Attacks

ARP Poisoning Attacks

Sniffing

Techniques

Spoofing Attack

DNS Poisoning

Sniffing Tools

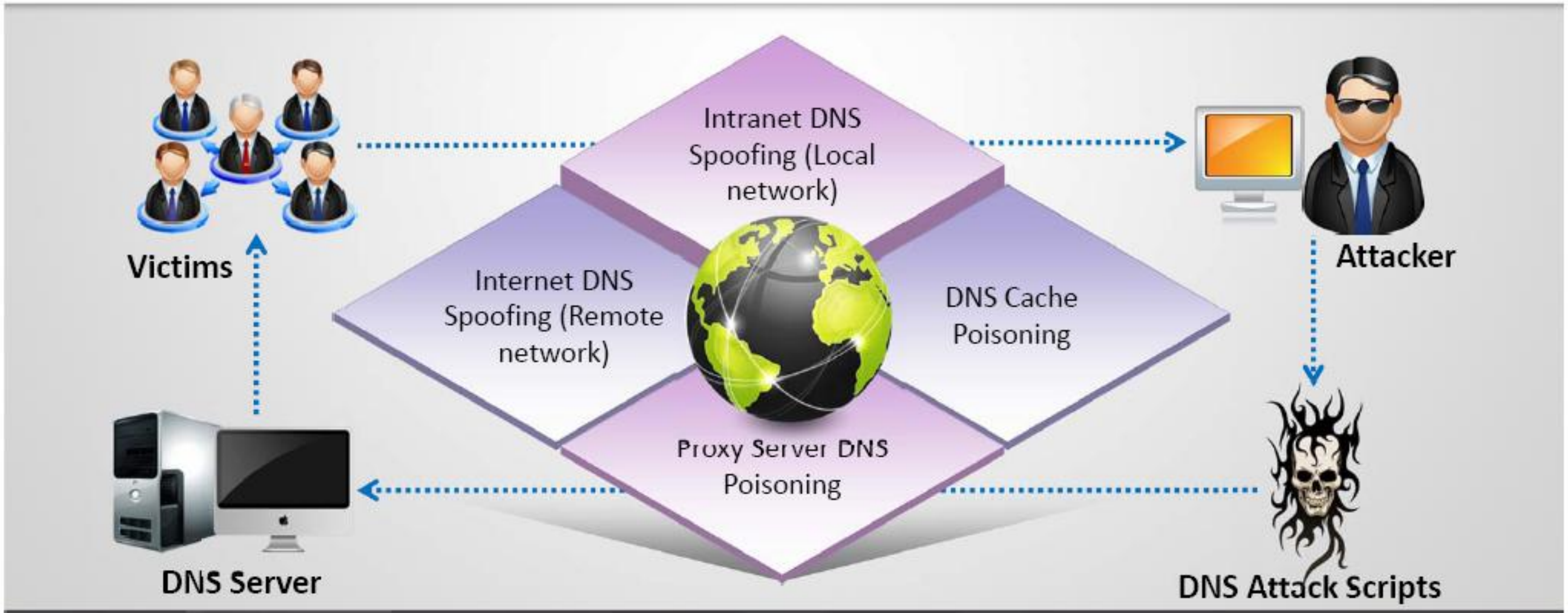
Counter measures

Techniques

50

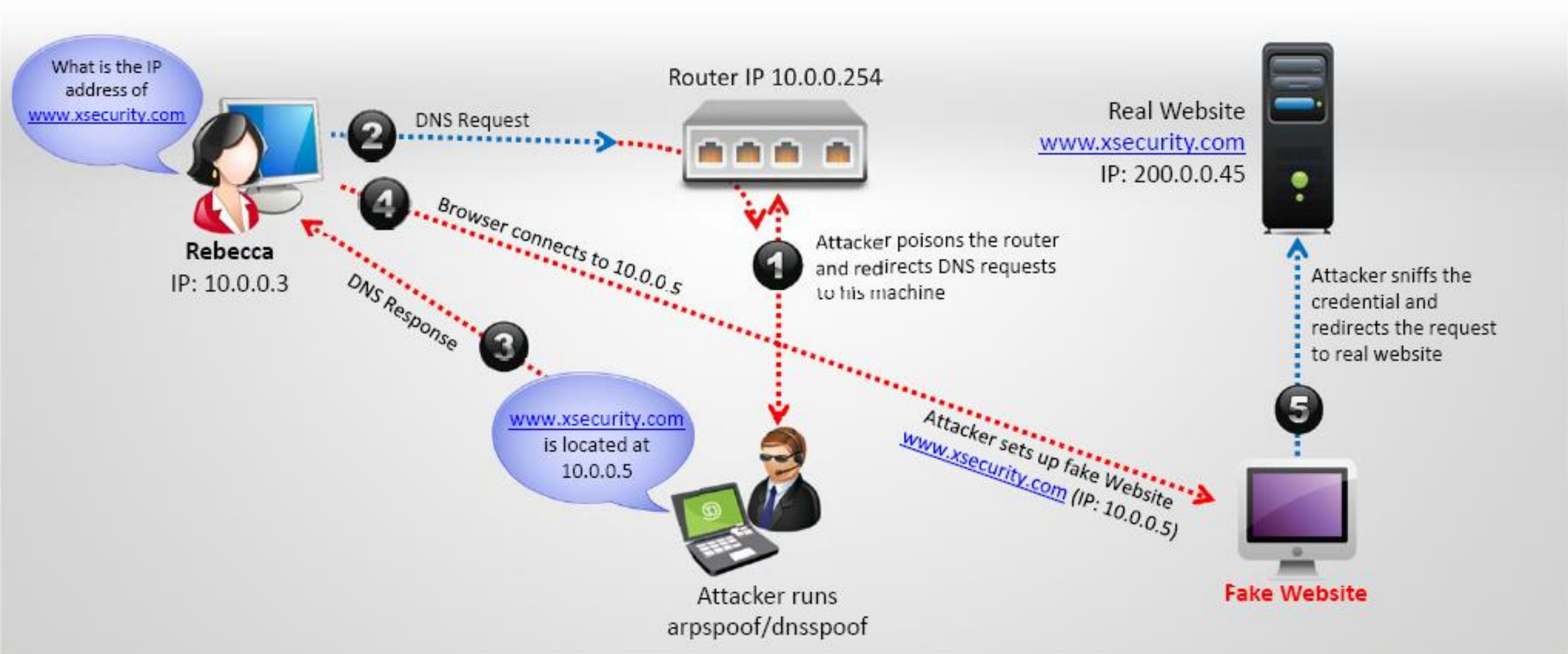
DNS Poisoning Techniques

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


Victims
Intranet DNS Spoofing (Local network)
Attacker
Internet DNS Spoofing (Remote network)
DNS Cache Poisoning
Proxy Server DNS Poisoning
DNS Server
DNS Attack Scripts

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



What is the IP address of www.xsecurity.com

Rebecca
IP: 10.0.0.3

Router IP 10.0.0.254

Real Website
www.xsecurity.com
IP: 200.0.0.45

1 Attacker poisons the router and redirects DNS requests to his machine

2 DNS Request

3 DNS Response

www.xsecurity.com is located at 10.0.0.5

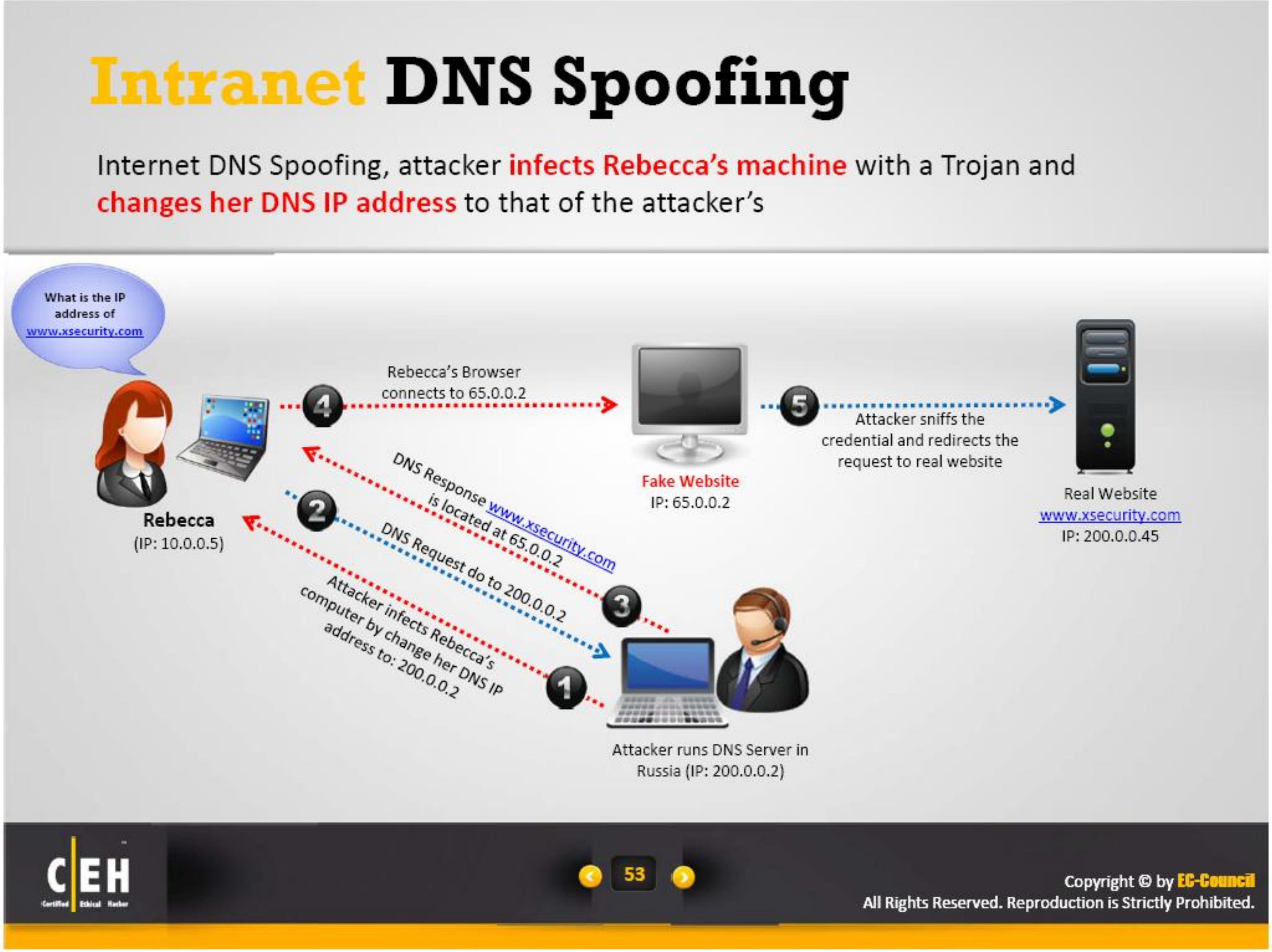
4 Browser connects to 10.0.0.5

5 Attacker sniffs the credential and redirects the request to real website

Attacker sets up fake Website www.xsecurity.com (IP: 10.0.0.5)

Attacker runs arpspoof/dnsspoof

Fake Website



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

What is the IP address of www.xsecurity.com

Rebecca
(IP: 10.0.0.5)

1 Attacker infects Rebecca's computer by change her DNS IP address to: 200.0.0.2

2 DNS Request do to 200.0.0.2

3 DNS Response www.xsecurity.com is located at 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

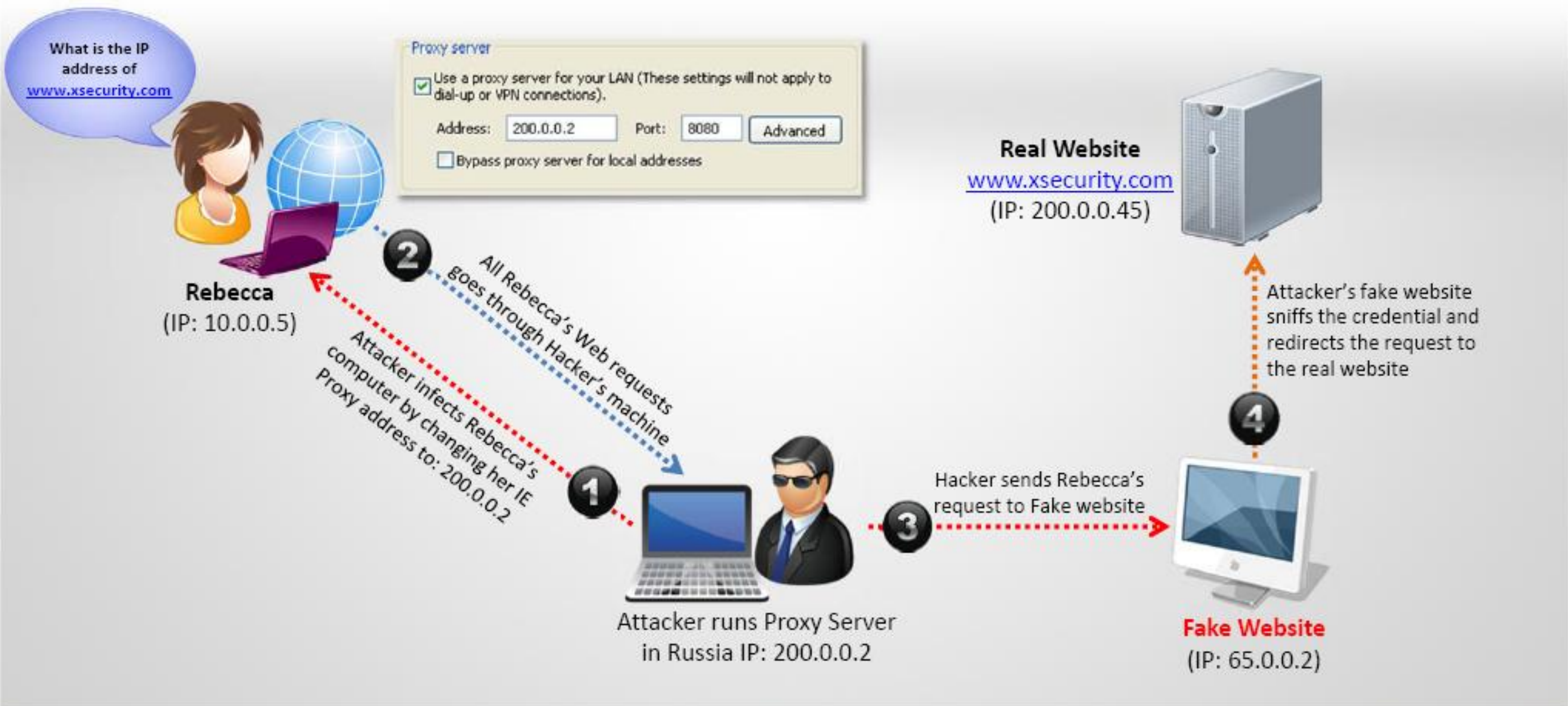
Fake Website
IP: 65.0.0.2

Real Website
www.xsecurity.com
IP: 200.0.0.45

Attacker runs DNS Server in Russia (IP: 200.0.0.2)

Proxy Server DNS Poisoning

- Attacker sends a Trojan to Rebecca's machine and change her **proxy server settings** in Internet Explorer to that of the attacker's


What is the IP address of www.xsecurity.com
Rebecca
(IP: 10.0.0.5)
Real Website
www.xsecurity.com
(IP: 200.0.0.45)
Attacker runs Proxy Server in Russia IP: 200.0.0.2
Fake Website
(IP: 65.0.0.2)

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 200.0.0.2 Port: 8080 Advanced

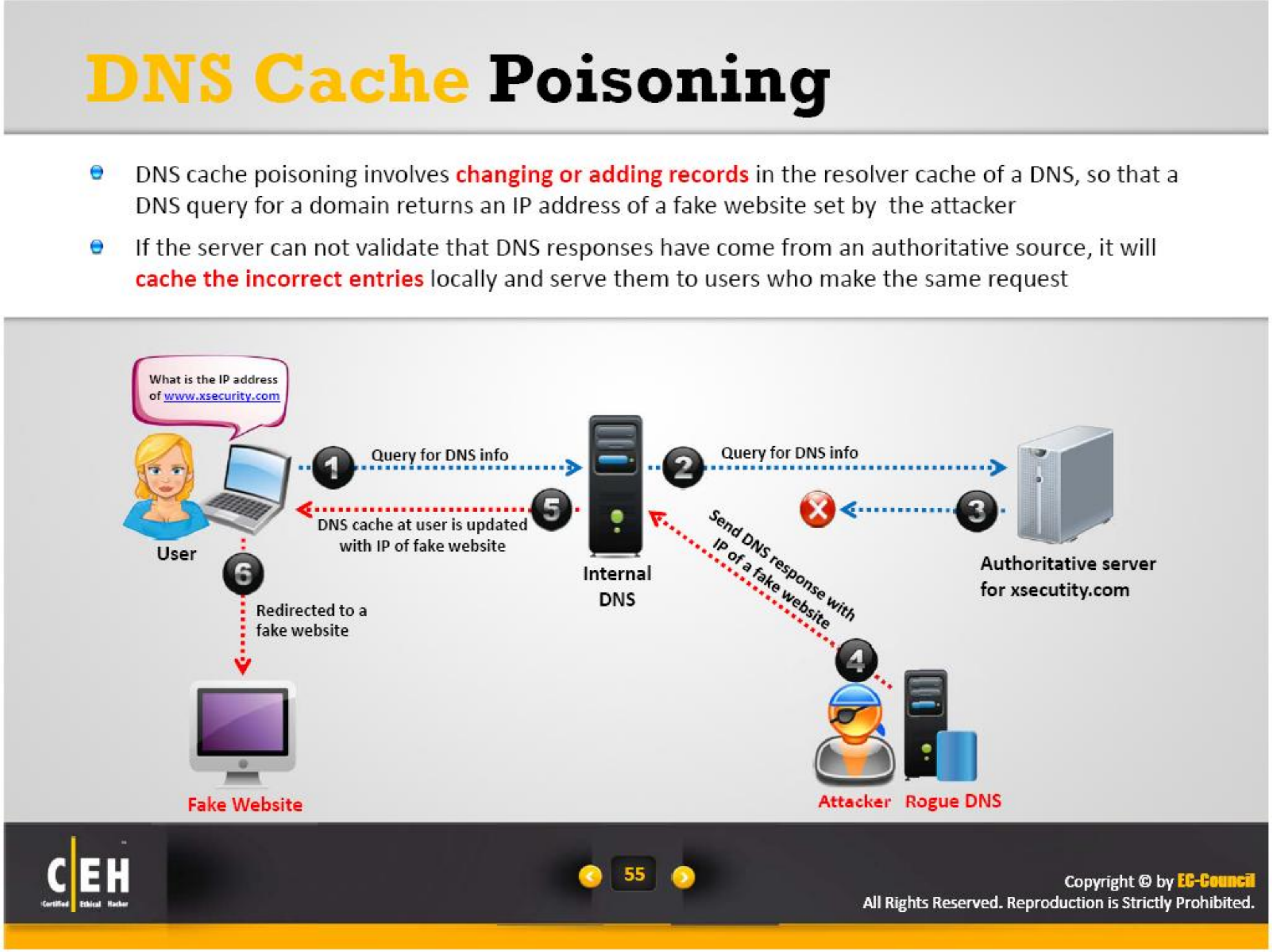
☐ Bypass proxy server for local addresses

1 Attacker infects Rebecca's computer by changing her IE Proxy address to: 200.0.0.2

2 All Rebecca's Web requests goes through Hacker'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 can not 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

What is the IP address of www.xsecurity.com

User

1 Query for DNS info

Internal DNS

2 Query for DNS info

Authoritative server for xsecutity.com

3

4 Send DNS response with IP of a fake website

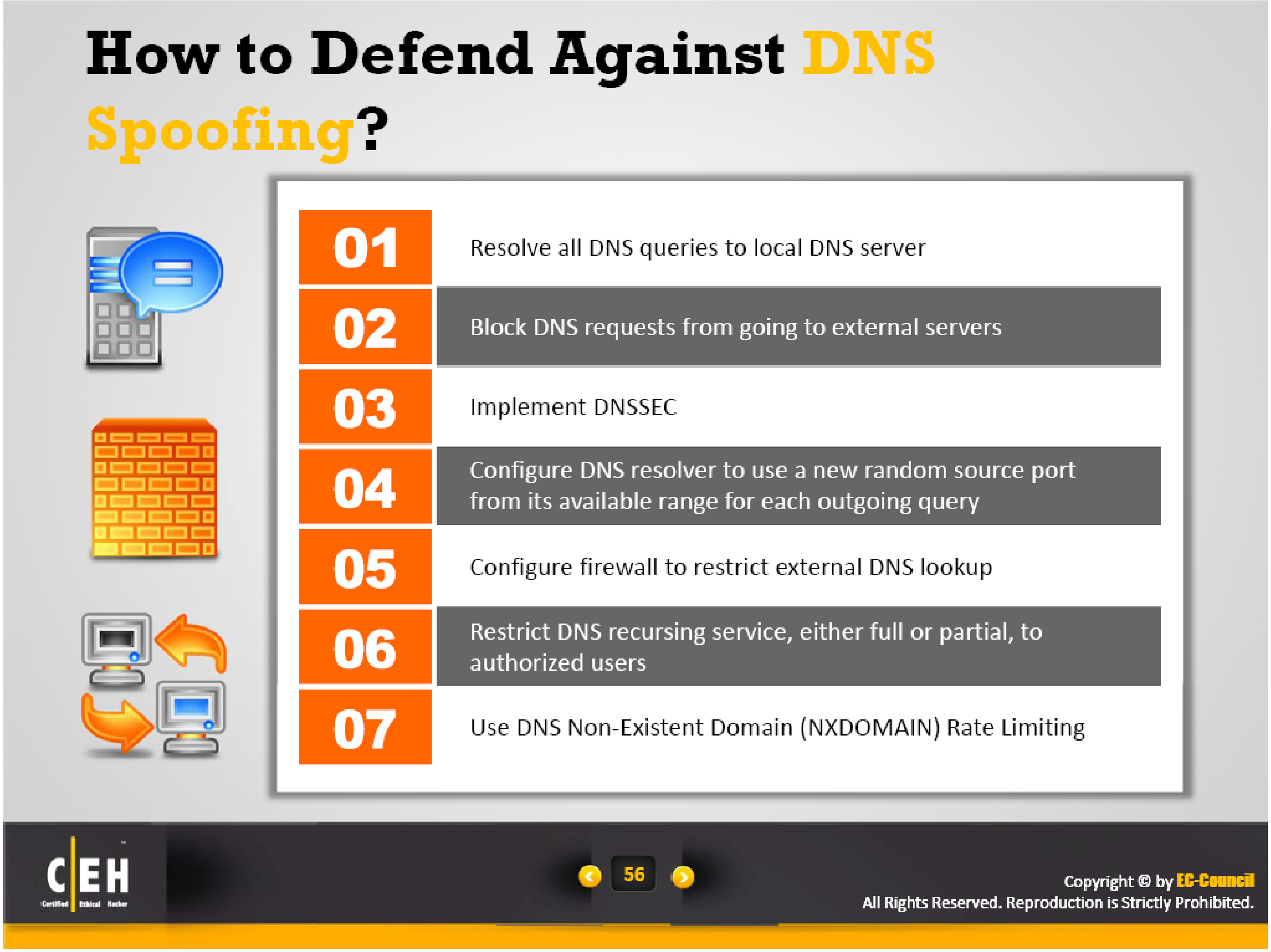
Attacker

Rogue DNS

5 DNS cache at user is updated with IP of fake website

6 Redirected to a fake website

Fake Website



How to Defend Against DNS Spoofing?

01 Resolve all DNS queries to local DNS server

02 Block DNS requests from going to external servers

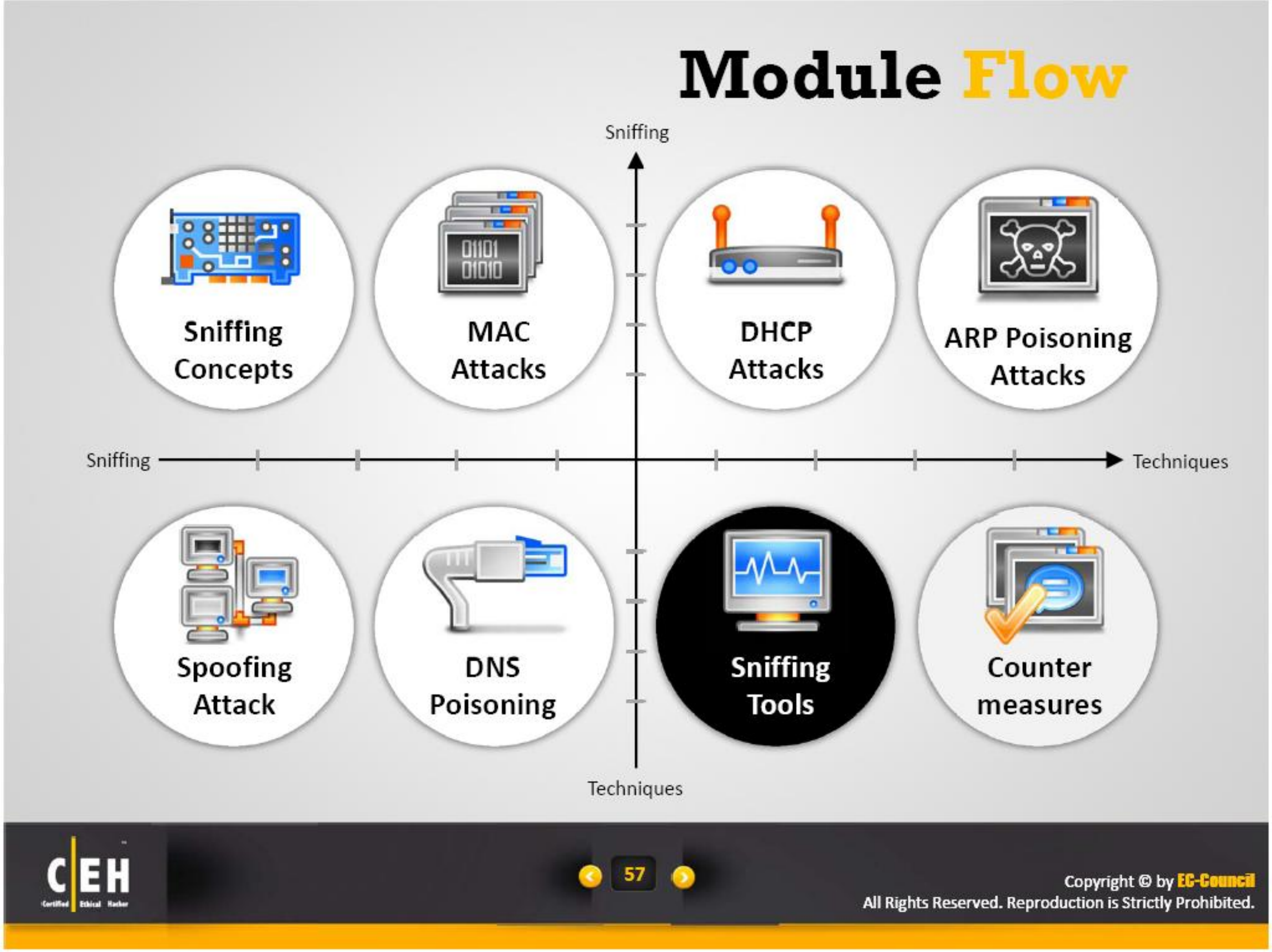
03 Implement DNSSEC

04 Configure DNS resolver to use a new random source port from its available range for each outgoing query

05 Configure firewall to restrict external DNS lookup

06 Restrict DNS recursing service, either full or partial, to authorized users

07 Use DNS Non-Existent Domain (NXDOMAIN) Rate Limiting



Module Flow

Sniffing

Sniffing Concepts

MAC Attacks

DHCP Attacks

ARP Poisoning Attacks

Sniffing

Techniques

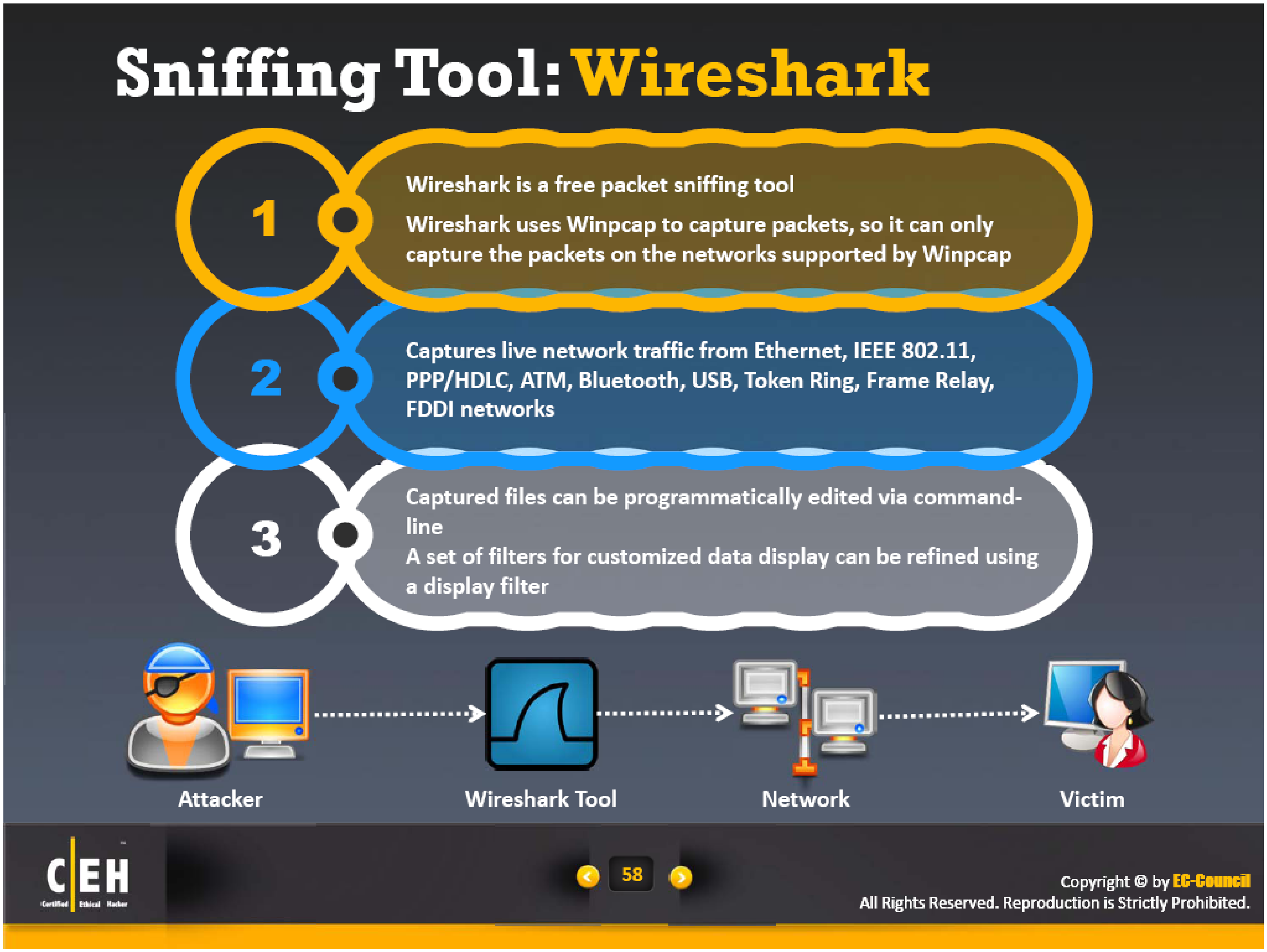
Spoofing Attack

DNS Poisoning

Sniffing Tools

Counter measures

Techniques



Sniffing Tool: Wireshark

1. Wireshark is a free packet sniffing tool

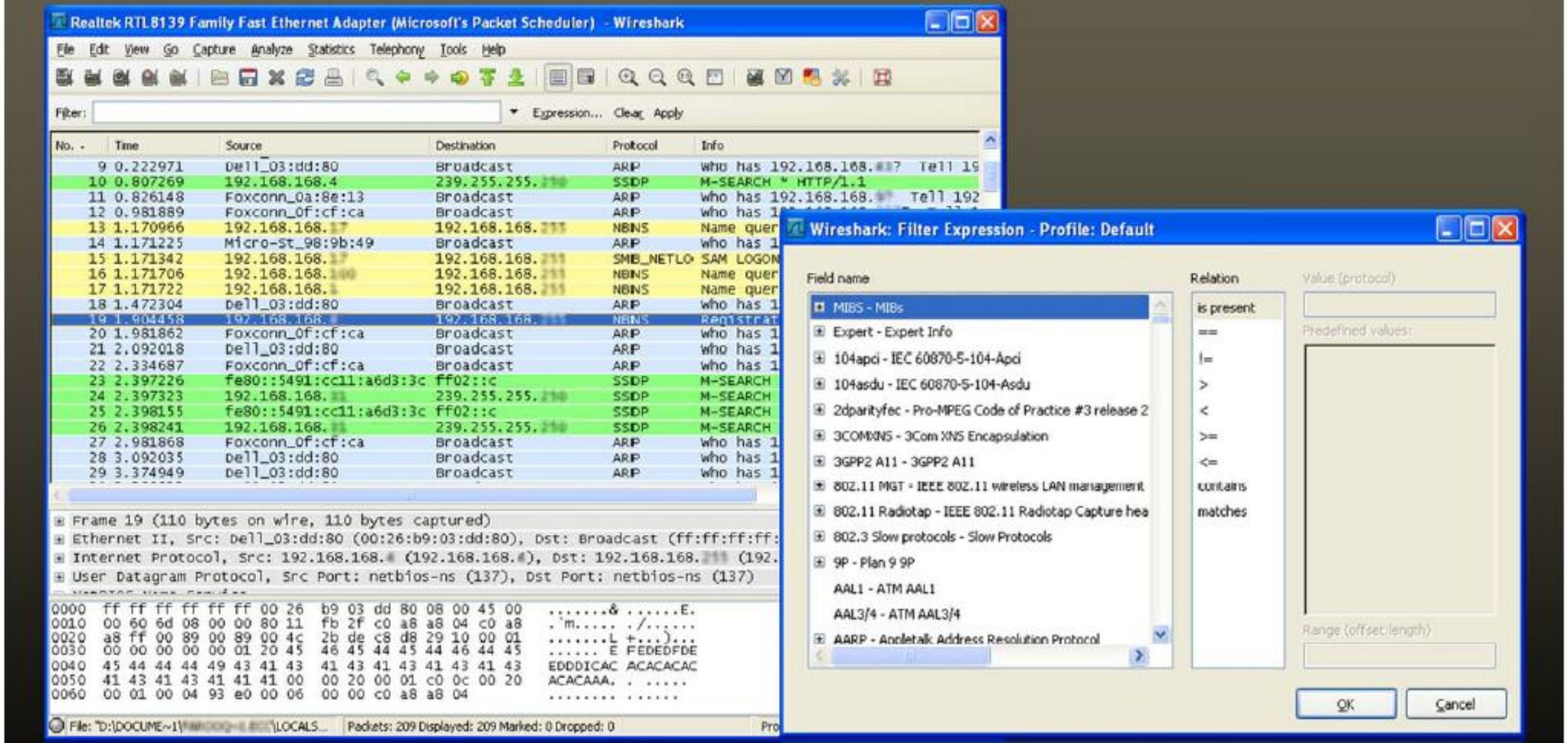
   Wireshark uses Winpcap to capture packets, so it can only capture the packets on the networks supported by Winpcap

2. Captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI networks

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

Sniffing Tool: Wireshark


Realtek RTL8139 Family Fast Ethernet Adapter (Microsoft's Packet Scheduler) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
Wireshark: Filter Expression - Profile: Default
OK
Cancel

```
No. . Time      Source                    Destination            Protocol   Info
    9 0.222971  Dell_03:dd:80             Broadcast              ARP        Who has 192.168.168.[redacted]7  Tell 19
   10 0.807269  192.168.168.4             239.255.255.[redacted] SSDP       M-SEARCH * HTTP/1.1
   11 0.826148  Foxconn_0a:8e:13          Broadcast              ARP        Who has 192.168.168.[redacted]  Tell 192
   12 0.981889  Foxconn_0f:cf:ca          Broadcast              ARP        Who has 1
   13 1.170966  192.168.168.[redacted]    192.168.168.[redacted] NBNS       Name quer
   14 1.171225  Micro-St_98:9b:49         Broadcast              ARP        Who has 1
   15 1.171342  192.168.168.[redacted]    192.168.168.[redacted] SMB_NETLO  SAM LOGON
   16 1.171706  192.168.168.[redacted]    192.168.168.[redacted] NBNS       Name quer
   17 1.171722  192.168.168.[redacted]    192.168.168.[redacted] NBNS       Name quer
   18 1.472304  Dell_03:dd:80             Broadcast              ARP        Who has 1
   19 1.904458  192.168.168.[redacted]    192.168.168.[redacted] NBNS       Registrat
   20 1.981862  Foxconn_0f:cf:ca          Broadcast              ARP        Who has 1
   21 2.092018  Dell_03:dd:80             Broadcast              ARP        Who has 1
   22 2.334687  Foxconn_0f:cf:ca          Broadcast              ARP        Who has 1
   23 2.397226  fe80::5491:cc11:a6d3:3c   ff02::c                SSDP       M-SEARCH
   24 2.397323  192.168.168.[redacted]    239.255.255.[redacted] SSDP       M-SEARCH
   25 2.398155  fe80::5491:cc11:a6d3:3c   ff02::c                SSDP       M-SEARCH
   26 2.398241  192.168.168.[redacted]    239.255.255.[redacted] SSDP       M-SEARCH
   27 2.981868  Foxconn_0f:cf:ca          Broadcast              ARP        Who has 1
   28 3.092035  Dell_03:dd:80             Broadcast              ARP        Who has 1
   29 3.374949  Dell_03:dd:80             Broadcast              ARP        Who has 1
```

```
⊞ Frame 19 (110 bytes on wire, 110 bytes captured)
⊞ Ethernet II, Src: Dell_03:dd:80 (00:26:b9:03:dd:80), Dst: Broadcast (ff:ff:ff:ff:
⊞ Internet Protocol, Src: 192.168.168.[redacted] (192.168.168.[redacted]), Dst: 192.168.168.[redacted] (192.
⊞ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
```

```
0000  ff ff ff ff ff ff 00 26  b9 03 dd 80 08 00 45 00   .......& ......E.
0010  00 60 6d 08 00 00 80 11  fb 2f c0 a8 a8 04 c0 a8   .`m..... ./......
0020  a8 ff 00 89 00 89 00 4c  2b de c8 d8 29 10 00 01   .......L +...)...
0030  00 00 00 00 00 01 20 45  46 45 44 45 44 46 44 45   ...... E FEDEDFDE
0040  45 44 44 44 49 43 41 43  41 43 41 43 41 43 41 43   EDDDICAC ACACACAC
0050  41 43 41 43 41 41 41 00  00 20 00 01 c0 0c 00 20   ACACAAA. . .....
0060  00 01 00 04 93 e0 00 06  00 00 c0 a8 a8 04         ........ ......
```

File: "D:\DOCUME~1\[redacted]\LOCALS... Packets: 209 Displayed: 209 Marked: 0 Dropped: 0

Field name	Relation
⊞ MIBS - MIBs	is present
⊞ Expert - Expert Info	==
⊞ 104apci - IEC 60870-5-104-Apci	!=
⊞ 104asdu - IEC 60870-5-104-Asdu	>
⊞ 2dparityfec - Pro-MPEG Code of Practice #3 release 2	<
⊞ 3COMXNS - 3Com XNS Encapsulation	>=
⊞ 3GPP2 A11 - 3GPP2 A11	<=
⊞ 802.11 MGT - IEEE 802.11 wireless LAN management	contains
⊞ 802.11 Radiotap - IEEE 802.11 Radiotap Capture hea	matches
⊞ 802.3 Slow protocols - Slow Protocols	
⊞ 9P - Plan 9 9P	
AAL1 - ATM AAL1	
AAL3/4 - ATM AAL3/4	
⊞ AARP - Appletalk Address Resolution Protocol	

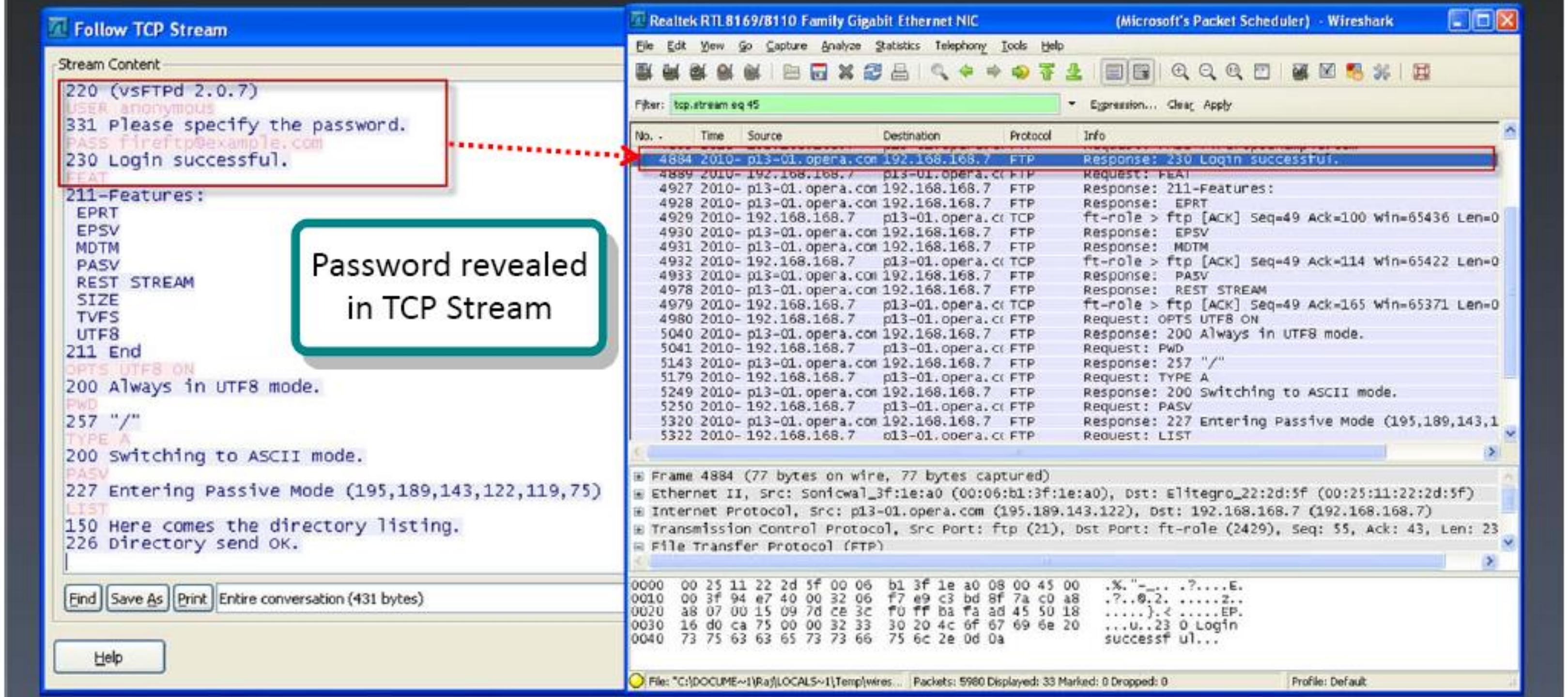
Value (protocol):

Predefined values:

Range (offset:length)

http://www.wireshark.org

Follow TCP Stream in Wireshark



```
220 (vsFTPd 2.0.7)
USER anonymous
331 Please specify the password.
PASS fireftp@example.com
230 Login successful.
FEAT
211-Features:
 EPRT
 EPSV
 MDTM
 PASV
 REST STREAM
 SIZE
 TVFS
 UTF8
211 End
OPTS UTF8 ON
200 Always in UTF8 mode.
PWD
257 "/"
TYPE A
200 Switching to ASCII mode.
PASV
227 Entering Passive Mode (195,189,143,122,119,75)
LIST
150 Here comes the directory listing.
226 Directory send OK.
```

Entire conversation (431 bytes)

Password revealed in TCP Stream

Realtek RTL8169/8110 Family Gigabit Ethernet NIC (Microsoft's Packet Scheduler) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help

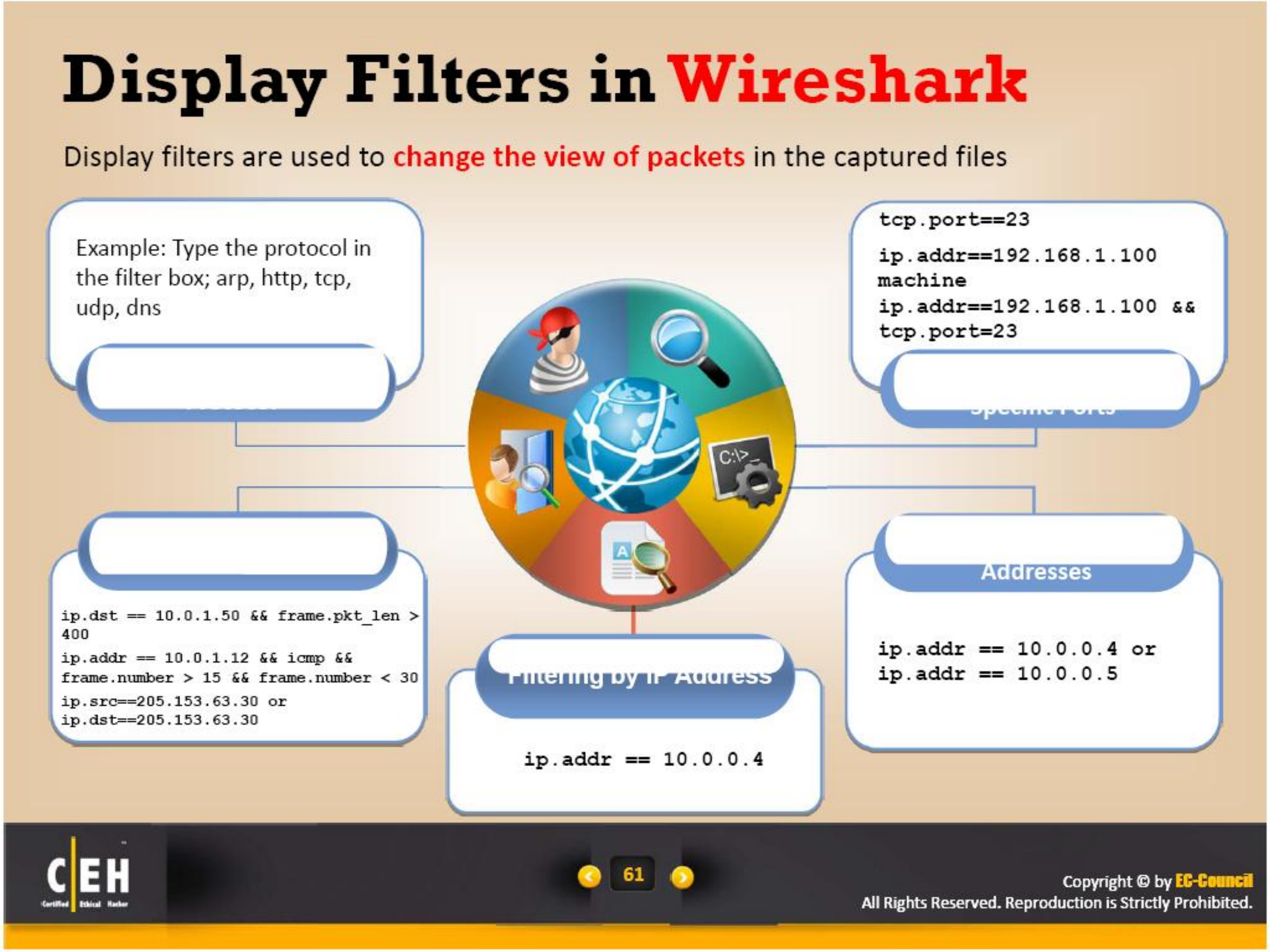
Filter: tcp.stream eq 45

```
No. -  Time  Source             Destination        Protocol  Info
 4884  2010- p13-01.opera.com   192.168.168.7      FTP       Response: 230 Login successful.
 4889  2010- 192.168.168.7      p13-01.opera.c(    FTP       Request: FEAT
 4927  2010- p13-01.opera.com   192.168.168.7      FTP       Response: 211-Features:
 4928  2010- p13-01.opera.com   192.168.168.7      FTP       Response:  EPRT
 4929  2010- 192.168.168.7      p13-01.opera.c(    TCP       ft-role > ftp [ACK] Seq=49 Ack=100 Win=65436 Len=0
 4930  2010- p13-01.opera.com   192.168.168.7      FTP       Response:  EPSV
 4931  2010- p13-01.opera.com   192.168.168.7      FTP       Response:  MDTM
 4932  2010- 192.168.168.7      p13-01.opera.c(    TCP       ft-role > ftp [ACK] Seq=49 Ack=114 Win=65422 Len=0
 4933  2010- p13-01.opera.com   192.168.168.7      FTP       Response:  PASV
 4978  2010- p13-01.opera.com   192.168.168.7      FTP       Response:  REST STREAM
 4979  2010- 192.168.168.7      p13-01.opera.c(    TCP       ft-role > ftp [ACK] Seq=49 Ack=165 Win=65371 Len=0
 4980  2010- 192.168.168.7      p13-01.opera.c(    FTP       Request: OPTS UTF8 ON
 5040  2010- p13-01.opera.com   192.168.168.7      FTP       Response: 200 Always in UTF8 mode.
 5041  2010- 192.168.168.7      p13-01.opera.c(    FTP       Request: PWD
 5143  2010- p13-01.opera.com   192.168.168.7      FTP       Response: 257 "/"
 5179  2010- 192.168.168.7      p13-01.opera.c(    FTP       Request: TYPE A
 5249  2010- p13-01.opera.com   192.168.168.7      FTP       Response: 200 Switching to ASCII mode.
 5250  2010- 192.168.168.7      p13-01.opera.c(    FTP       Request: PASV
 5320  2010- p13-01.opera.com   192.168.168.7      FTP       Response: 227 Entering Passive Mode (195,189,143,1
 5322  2010- 192.168.168.7      p13-01.opera.c(    FTP       Request: LIST
```

```
⊞ Frame 4884 (77 bytes on wire, 77 bytes captured)
⊞ Ethernet II, Src: Sonicwal_3f:1e:a0 (00:06:b1:3f:1e:a0), Dst: Elitegro_22:2d:5f (00:25:11:22:2d:5f)
⊞ Internet Protocol, Src: p13-01.opera.com (195.189.143.122), Dst: 192.168.168.7 (192.168.168.7)
⊞ Transmission Control Protocol, Src Port: ftp (21), Dst Port: ft-role (2429), Seq: 55, Ack: 43, Len: 23
⊟ File Transfer Protocol (FTP)
```

```
0000   00 25 11 22 2d 5f 00 06  b1 3f 1e a0 08 00 45 00   .%."-_.. .?....E.
0010   00 3f 94 e7 40 00 32 06  f7 e9 c3 bd 8f 7a c0 a8   .?..@.2. .....z..
0020   a8 07 00 15 09 7d ce 3c  f0 ff ba fa ad 45 50 18   .....}.< .....EP.
0030   16 d0 ca 75 00 00 32 33  30 20 4c 6f 67 69 6e 20   ...u..23 0 Login
0040   73 75 63 63 65 73 73 66  75 6c 2e 0d 0a            successf ul...
```

File: "C:\DOCUME~1\Raj\LOCALS~1\Temp\wires... Packets: 5980 Displayed: 33 Marked: 0 Dropped: 0 Profile: Default



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
machine
ip.addr==192.168.1.100 &&
tcp.port=23
```

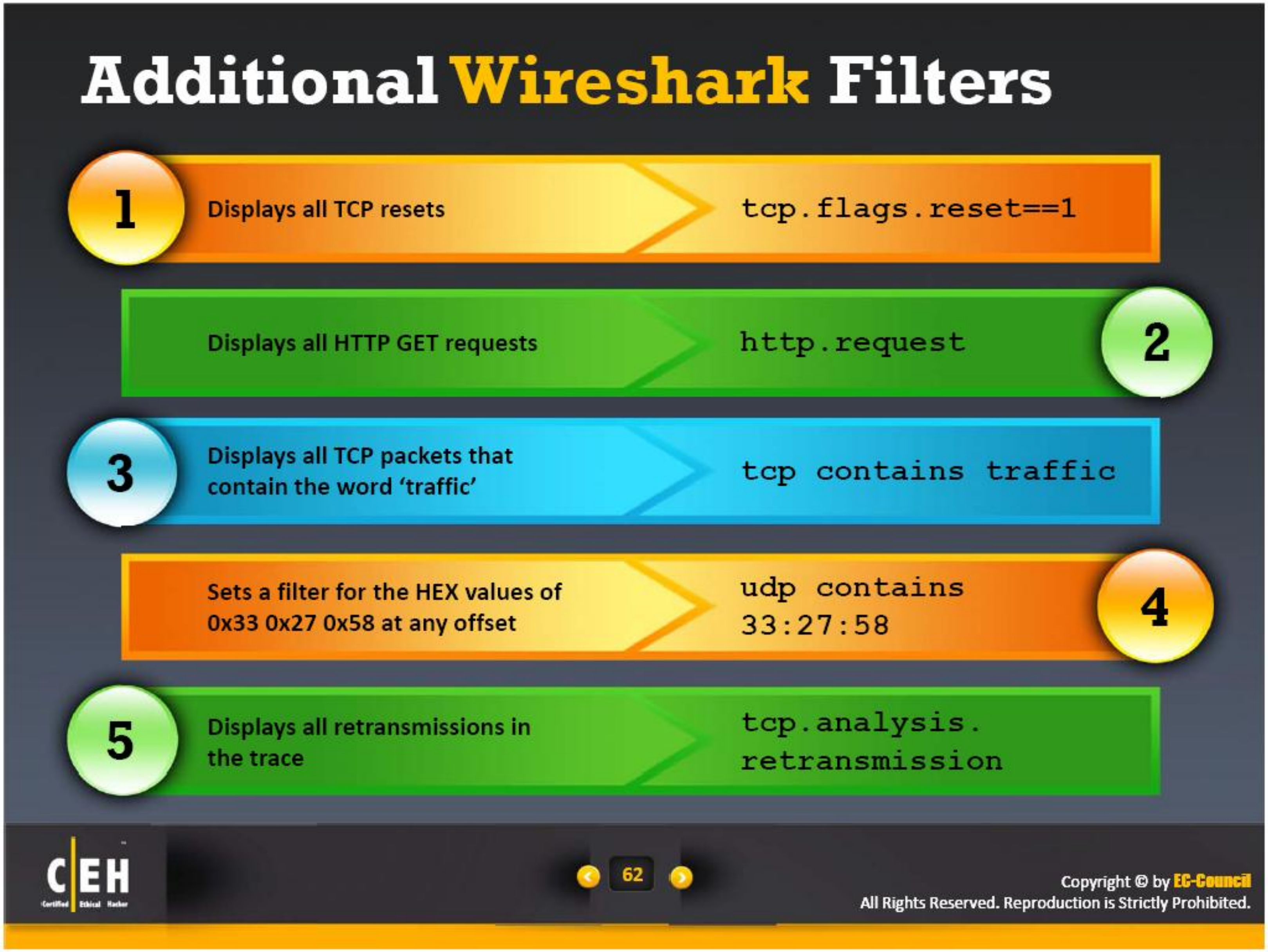
```
ip.dst == 10.0.1.50 && frame.pkt_len >
400
ip.addr == 10.0.1.12 && icmp &&
frame.number > 15 && frame.number < 30
ip.src==205.153.63.30 or
ip.dst==205.153.63.30
```

Filtering by IP Address

```
ip.addr == 10.0.0.4
```

Addresses

```
ip.addr == 10.0.0.4 or
ip.addr == 10.0.0.5
```

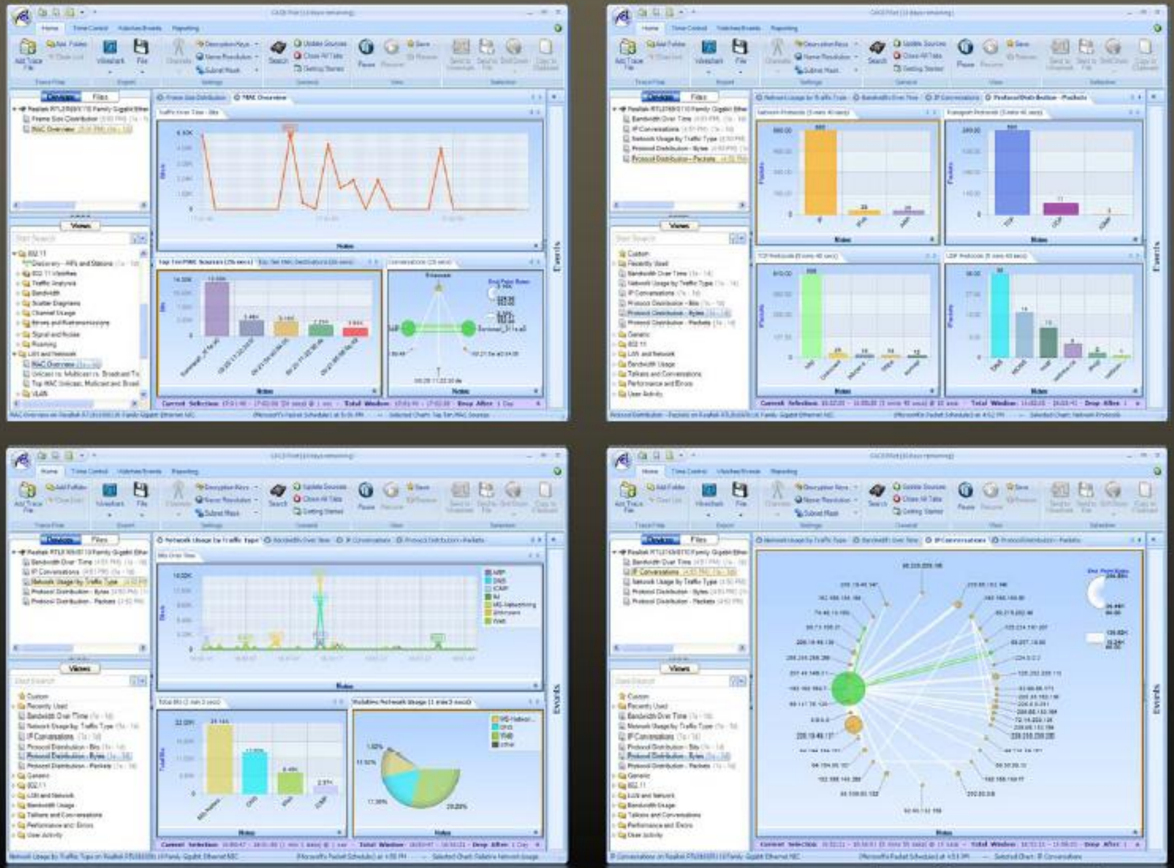


Additional Wireshark Filters

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

CEH
Certified Ethical Hacker

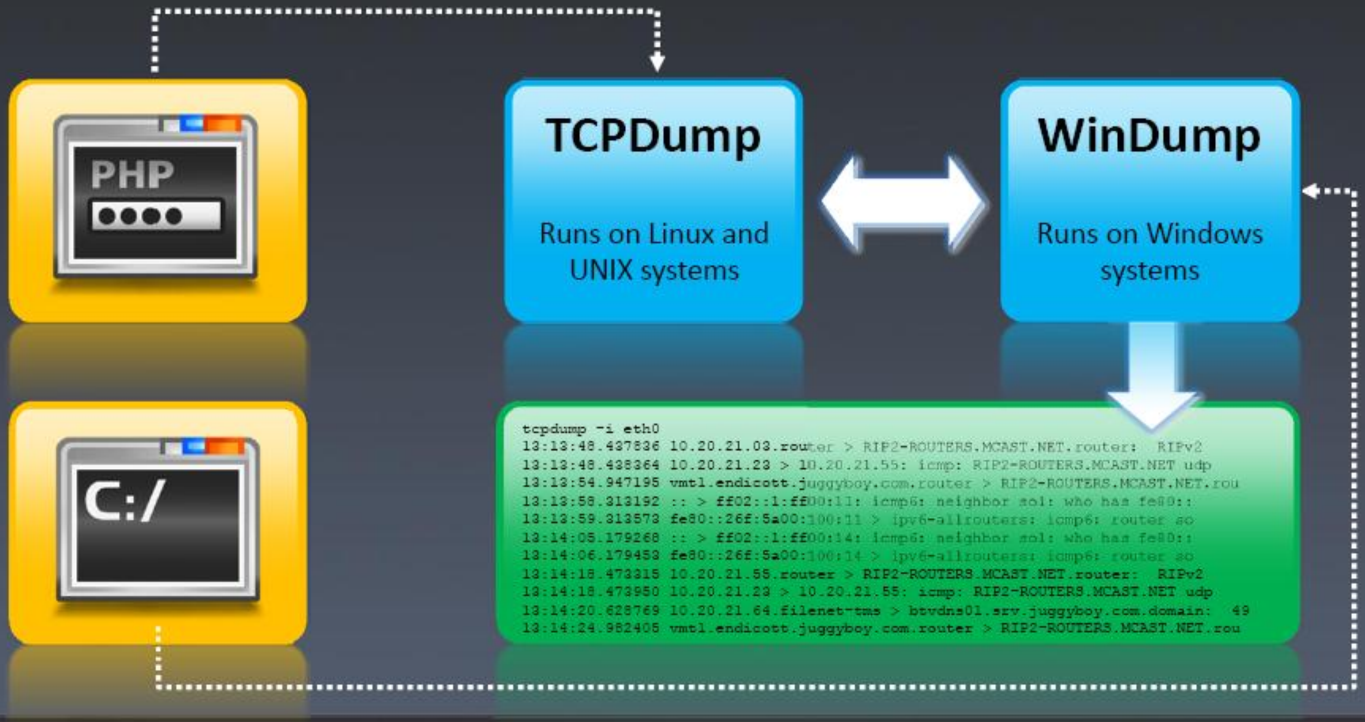
Sniffing Tool: CACE Pilot



http://www.cacetech.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

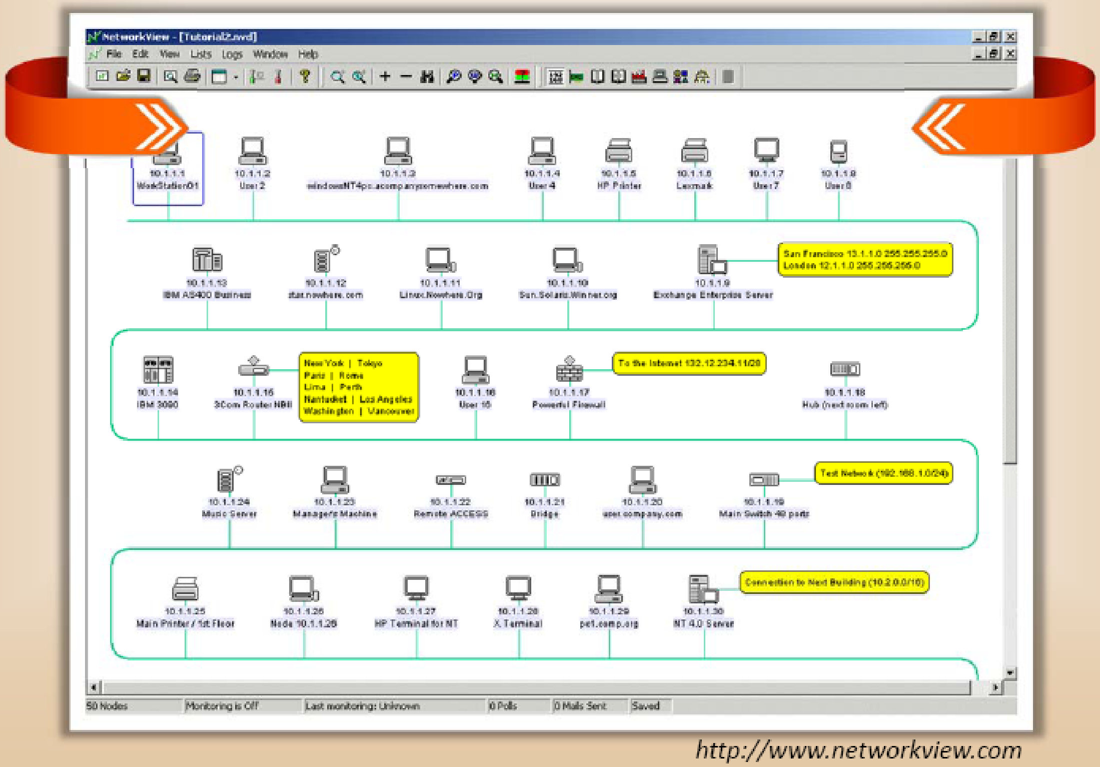
WinDump

Runs on Windows systems

```
tcpdump -i eth0
13:13:48.437836 10.20.21.03.router > RIP2-ROUTERS.MCAST.NET.router:  RIPv2
13:13:48.438364 10.20.21.23 > 10.20.21.55: icmp: RIP2-ROUTERS.MCAST.NET udp
13:13:54.947195 vmtl.endicott.juggyboy.com.router > RIP2-ROUTERS.MCAST.NET.rou
13:13:58.313192 :: > ff02::1:ff00:11: icmp6: neighbor sol: who has fe80::
13:13:59.313573 fe80::26f:5a00:100:11 > ipv6-allrouters: icmp6: router so
13:14:05.179268 :: > ff02::1:ff00:14: icmp6: neighbor sol: who has fe80::
13:14:06.179453 fe80::26f:5a00:100:14 > ipv6-allrouters: icmp6: router so
13:14:18.473315 10.20.21.55.router > RIP2-ROUTERS.MCAST.NET.router:  RIPv2
13:14:18.473950 10.20.21.23 > 10.20.21.55: icmp: RIP2-ROUTERS.MCAST.NET udp
13:14:20.628769 10.20.21.64.filenet-tms > btvdns01.srv.juggyboy.com.domain:  49
13:14:24.982405 vmtl.endicott.juggyboy.com.router > RIP2-ROUTERS.MCAST.NET.rou
```

Discovery Tool: NetworkView

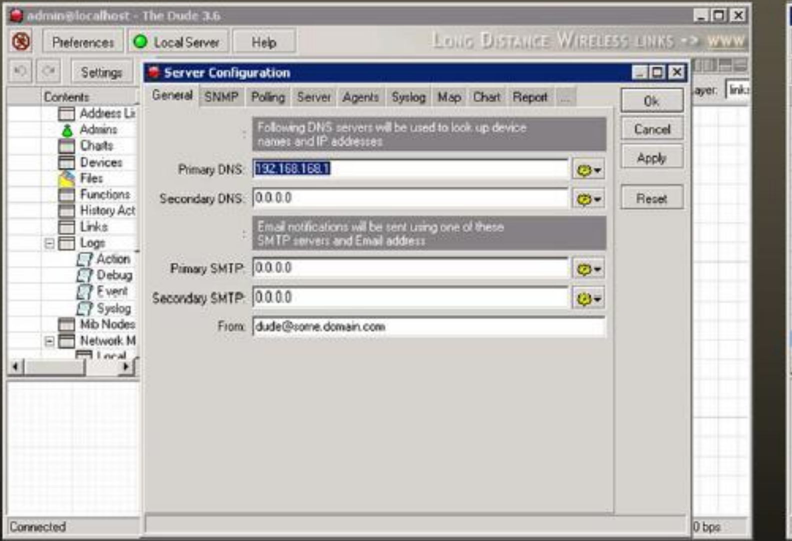
- NetworkView is a network discovery and management tool for Windows
- Discover TCP/IP nodes and routes using DNS, SNMP, Ports, NetBIOS and WMI


NetworkView - [Tutorial2.nvd]
File Edit View Lists Logs Window Help
10.1.1.1 WorkStation01
10.1.1.2 User 2
10.1.1.3 windowsNT4pc.acompanysomewhere.com
10.1.1.4 User 4
10.1.1.5 HP Printer
10.1.1.6 Lexmark
10.1.1.7 User 7
10.1.1.8 User 8
10.1.1.13 IBM AS400 Business
10.1.1.12 stat.nowhere.com
10.1.1.11 Linux.Nowhere.Org
10.1.1.10 Sun.Solaris.Winnet.org
10.1.1.9 Exchange Enterprise Server
San Francisco 13.1.1.0 255.255.255.0
London 12.1.1.0 255.255.255.0
10.1.1.14 IBM 3090
10.1.1.15 3Com Router NBII
New York | Tokyo
Paris | Rome
Lima | Perth
Nantucket | Los Angeles
Washington | Vancouver
10.1.1.16 User 16
10.1.1.17 Powerful Firewall
To the Internet 132.12.234.11/28
10.1.1.18 Hub (next room left)
10.1.1.24 Music Server
10.1.1.23 Manager's Machine
10.1.1.22 Remote ACCESS
10.1.1.21 Bridge
10.1.1.20 user.company.com
10.1.1.19 Main Switch 48 ports
Test Network (192.168.1.0/24)
10.1.1.25 Main Printer / 1st Floor
10.1.1.26 Node 10.1.1.26
10.1.1.27 HP Terminal for NT
10.1.1.28 X Terminal
10.1.1.29 pet.comp.org
10.1.1.30 NT 4.0 Server
Connection to Next Building (10.2.0.0/16)
50 Nodes
Monitoring is Off
Last monitoring: Unknown
0 Polls
0 Mails Sent
Saved

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



Following DNS servers will be used to look up device names and IP addresses

Primary DNS: 192.168.168.1

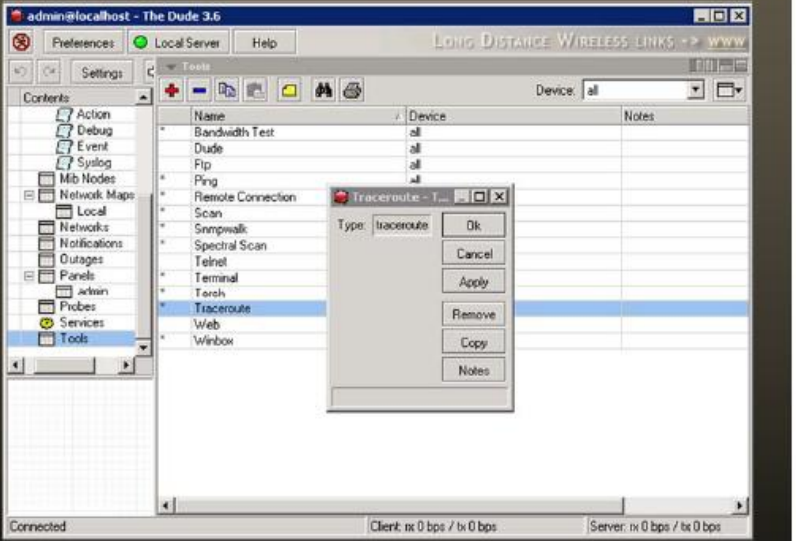
Secondary DNS: 0.0.0.0

Email notifications will be sent using one of these SMTP servers and Email address

Primary SMTP: 0.0.0.0

Secondary SMTP: 0.0.0.0

From: dude@some.domain.com



Device: all

	Name	Device	Notes
*	Bandwidth Test	all	
	Dude	all	
	Ftp	all	
*	Ping	all	
*	Remote Connection		
*	Scan		
*	Snmpwalk		
*	Spectral Scan		
	Telnet		
*	Terminal		
*	Torch		
*	Traceroute		
	Web		
*	Winbox		

Type: traceroute

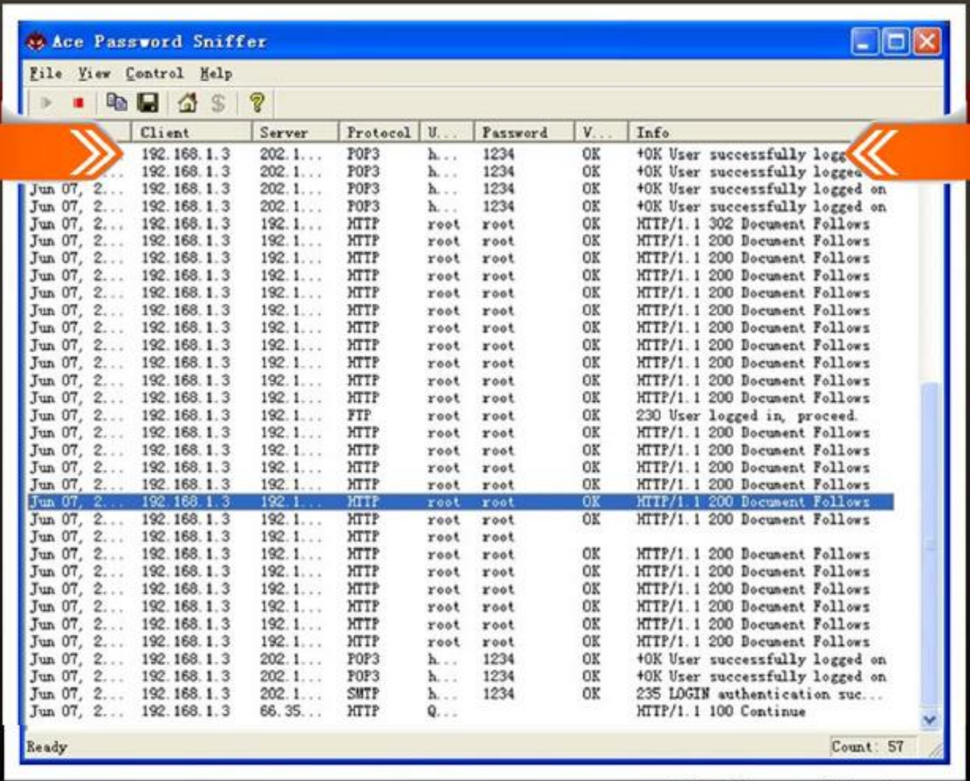
Client: rx 0 bps / tx 0 bps

Server: rx 0 bps / tx 0 bps

http://www.mikrotik.com

Password Sniffing Tool: Ace

Ace Password Sniffer can monitor and capture passwords through FTP, POP3, HTTP, SMTP, Telnet, and webmail passwords



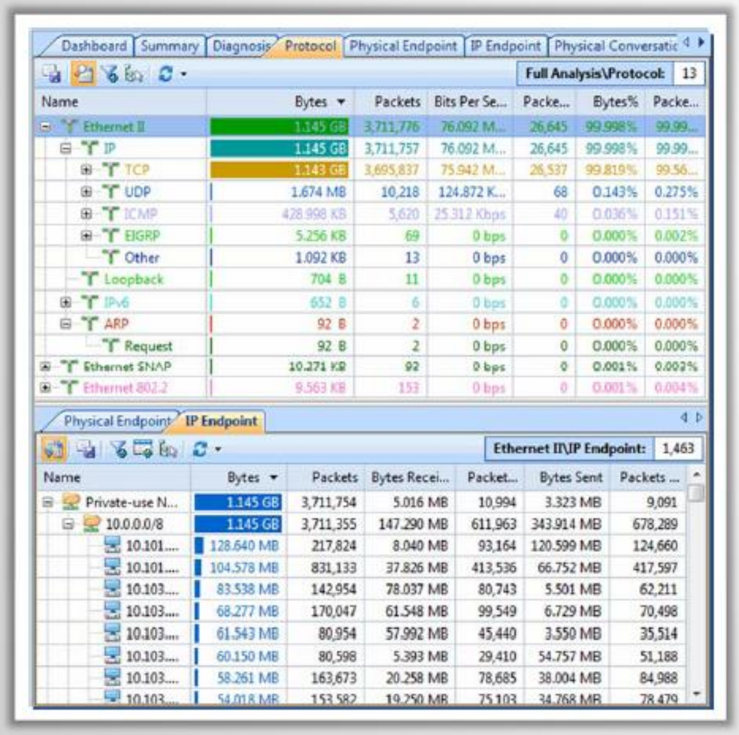
	Client	Server	Protocol	U...	Password	V...	Info
	192.168.1.3	202.1...	POP3	h...	1234	OK	+OK User successfully logg
...	192.168.1.3	202.1...	POP3	h...	1234	OK	+OK User successfully logged
Jun 07, 2...	192.168.1.3	202.1...	POP3	h...	1234	OK	+OK User successfully logged on
Jun 07, 2...	192.168.1.3	202.1...	POP3	h...	1234	OK	+OK User successfully logged on
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 302 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	FTP	root	root	OK	230 User logged in, proceed.
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root		
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	192.1...	HTTP	root	root	OK	HTTP/1.1 200 Document Follows
Jun 07, 2...	192.168.1.3	202.1...	POP3	h...	1234	OK	+OK User successfully logged on
Jun 07, 2...	192.168.1.3	202.1...	POP3	h...	1234	OK	+OK User successfully logged on
Jun 07, 2...	192.168.1.3	202.1...	SMTP	h...	1234	OK	235 LOGIN authentication suc...
Jun 07, 2...	192.168.1.3	66.35...	HTTP	Q...			HTTP/1.1 100 Continue

Ready Count: 57

http://www.effetech.com

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

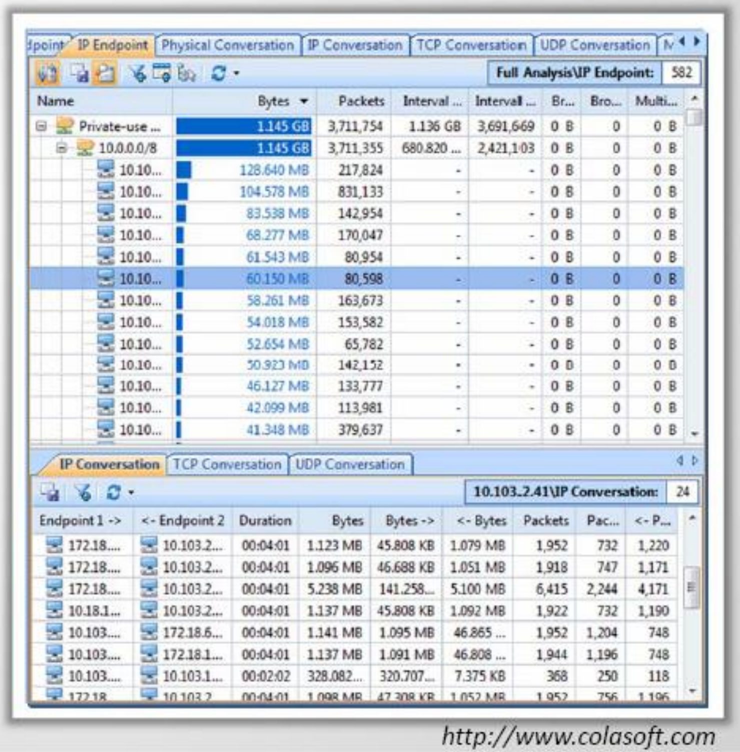


Full Analysis\Protocol: 13

Name	Bytes	Packets	Bits Per Se...	Packe...	Bytes%	Packe...
Ethernet II	1.145 GB	3,711,776	76.092 M...	26,645	99.998%	99.99...
IP	1.145 GB	3,711,757	76.092 M...	26,645	99.998%	99.99...
TCP	1.143 GB	3,695,837	75.942 M...	26,537	99.819%	99.56...
UDP	1.674 MB	10,218	124.872 K...	68	0.143%	0.275%
ICMP	428.998 KB	5,620	25.312 Kbps	40	0.036%	0.151%
EIGRP	5.256 KB	69	0 bps	0	0.000%	0.002%
Other	1.092 KB	13	0 bps	0	0.000%	0.000%
Loopback	704 B	11	0 bps	0	0.000%	0.000%
IPv6	652 B	6	0 bps	0	0.000%	0.000%
ARP	92 B	2	0 bps	0	0.000%	0.000%
Request	92 B	2	0 bps	0	0.000%	0.000%
Ethernet SNAP	10.271 KB	92	0 bps	0	0.001%	0.002%
Ethernet 802.2	9.563 KB	153	0 bps	0	0.001%	0.004%

Ethernet II\IP Endpoint: 1,463

Name	Bytes	Packets	Bytes Recei...	Packet...	Bytes Sent	Packets ...
Private-use N...	1.145 GB	3,711,754	5.016 MB	10,994	3.323 MB	9,091
10.0.0.0/8	1.145 GB	3,711,355	147.290 MB	611,963	343.914 MB	678,289
10.101....	128.640 MB	217,824	8.040 MB	93,164	120.599 MB	124,660
10.101....	104.578 MB	831,133	37.826 MB	413,536	66.752 MB	417,597
10.103....	83.538 MB	142,954	78.037 MB	80,743	5.501 MB	62,211
10.103....	68.277 MB	170,047	61.548 MB	99,549	6.729 MB	70,498
10.103....	61.543 MB	80,954	57.992 MB	45,440	3.550 MB	35,514
10.103....	60.150 MB	80,598	5.393 MB	29,410	54.757 MB	51,188
10.103....	58.261 MB	163,673	20.258 MB	78,685	38.004 MB	84,988
10.103....	54.018 MB	153,582	19.250 MB	75,103	34.768 MB	78,479



Full Analysis\IP Endpoint: 582

Name	Bytes	Packets	Interval ...	Interval ...	Br...	Bro...	Multi...
Private-use ...	1.145 GB	3,711,754	1.136 GB	3,691,669	0 B	0	0 B
10.0.0.0/8	1.145 GB	3,711,355	680.820 ...	2,421,103	0 B	0	0 B
10.10...	128.640 MB	217,824	-	-	0 B	0	0 B
10.10...	104.578 MB	831,133	-	-	0 B	0	0 B
10.10...	83.538 MB	142,954	-	-	0 B	0	0 B
10.10...	68.277 MB	170,047	-	-	0 B	0	0 B
10.10...	61.543 MB	80,954	-	-	0 B	0	0 B
10.10...	60.150 MB	80,598	-	-	0 B	0	0 B
10.10...	58.261 MB	163,673	-	-	0 B	0	0 B
10.10...	54.018 MB	153,582	-	-	0 B	0	0 B
10.10...	52.654 MB	65,782	-	-	0 B	0	0 B
10.10...	50.923 MB	142,152	-	-	0 B	0	0 B
10.10...	46.127 MB	133,777	-	-	0 B	0	0 B
10.10...	42.099 MB	113,981	-	-	0 B	0	0 B
10.10...	41.348 MB	379,637	-	-	0 B	0	0 B

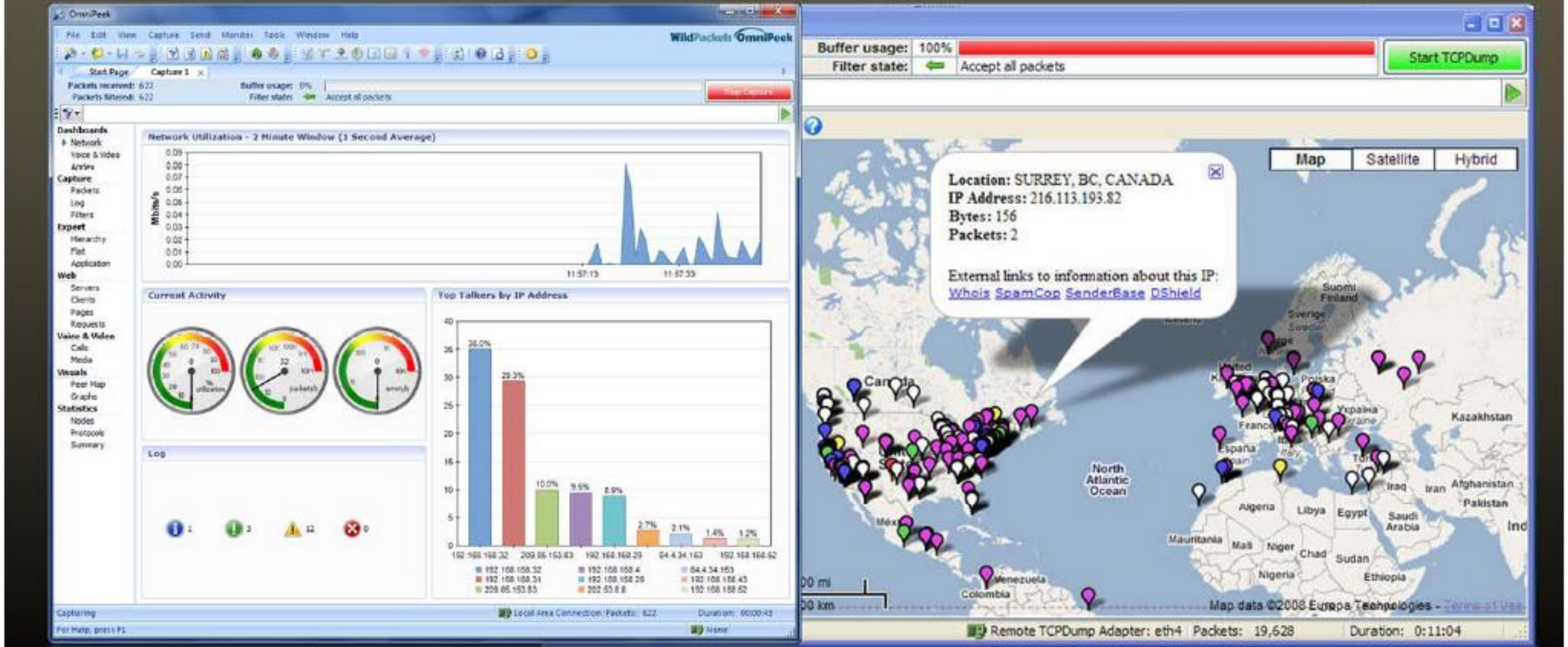
10.103..2.41\IP Conversation: 24

Endpoint 1 ->	<- Endpoint 2	Duration	Bytes	Bytes ->	<- Bytes	Packets	Pac...	<- P...
172.18....	10.103.2...	00:04:01	1.123 MB	45.808 KB	1.079 MB	1,952	732	1,220
172.18....	10.103.2...	00:04:01	1.096 MB	46.688 KB	1.051 MB	1,918	747	1,171
172.18....	10.103.2...	00:04:01	5.238 MB	141.258...	5.100 MB	6,415	2,244	4,171
10.18.1...	10.103.2...	00:04:01	1.137 MB	45.808 KB	1.092 MB	1,922	732	1,190
10.103....	172.18.6...	00:04:01	1.141 MB	1.095 MB	46.865 ...	1,952	1,204	748
10.103....	172.18.1...	00:04:01	1.137 MB	1.091 MB	46.808 ...	1,944	1,196	748
10.103....	10.103.1...	00:02:02	328.082...	320.707...	7.375 KB	368	250	118
172.18	10.103.2	00:04:01	1.098 MB	47.308 KB	1.052 MB	1,952	756	1,196

http://www.colasoft.com

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



Packets received: 622
Packets filtered: 622
Buffer usage: 0%
Filter state: Accept all packets

Buffer usage: 100%
Filter state: Accept all packets

Location: SURREY, BC, CANADA
IP Address: 216.113.193.82
Bytes: 156
Packets: 2

External links to information about this IP:
Whois SpamCop SenderBase DShield

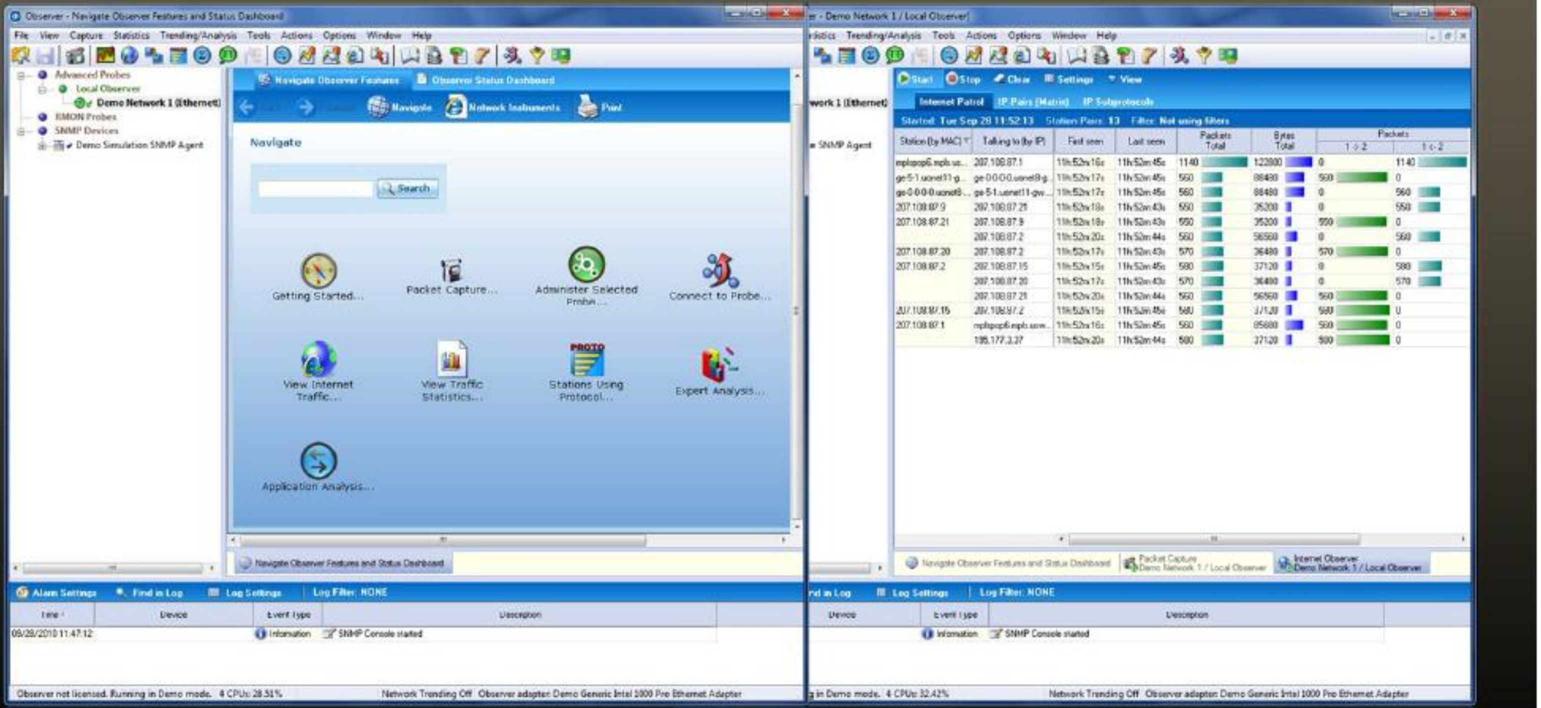
Remote TCPDump Adapter: eth4 Packets: 19,628 Duration: 0:11:04

OmniPeek
File Edit View Capture Send Monitor Tools Window Help
WildPackets OmniPeek
Start Page
Capture 1
Stop Capture
Dashboards
Network
Voice & Video
Capture
Expert
Web
Visuals
Statistics
Network Utilization - 2 Minute Window (1 Second Average)
Current Activity
Top Talkers by IP Address
Log
Start TCPDump
Map
Satellite
Hybrid
Map data ©2008 Europa Technologies - Terms of Use

http://www.wildpackets.com

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


Observer - Navigate Observer Features and Status Dashboard
File View Capture Statistics Trending/Analysis Tools Actions Options Window Help
Advanced Probes
Local Observer
Demo Network 1 (Ethernet)
RMON Probes
SNMP Devices
Demo Simulation SNMP Agent
Navigate Observer Features
Observer Status Dashboard
Navigate
Network Instruments
Print
Search
Getting Started...
Packet Capture...
Administer Selected Probe...
Connect to Probe...
View Internet Traffic...
View Traffic Statistics...
Stations Using Protocol...
Expert Analysis...
Application Analysis...
Demo Network 1 / Local Observer
Start
Stop
Clear
Settings
View
Internet Patrol
IP Pairs (Matrix)
IP Subprotocols
Navigate Observer Features and Status Dashboard
Packet Capture Demo Network 1 / Local Observer
Internet Observer Demo Network 1 / Local Observer
Alarm Settings
Find in Log
Log Settings

Started: Tue Sep 28 11:52:13 Station Pairs: 13 Filter: Not using filters

Station (by MAC)	Talking to (by IP)	First seen	Last seen	Packets Total	Bytes Total	Packets	
						1 -> 2	1 <- 2
mplspop6.mpls.us...	207.108.87.1	11h:52m:16s	11h:52m:45s	1140	122880	0	1140
ge-5-1.uonet11-g...	ge-0-0-0-0.uonet8-g...	11h:52m:17s	11h:52m:45s	560	88480	560	0
ge-0-0-0-0.uonet8-...	ge-5-1.uonet11-gw...	11h:52m:17s	11h:52m:45s	560	88480	0	560
207.108.87.9	207.108.87.21	11h:52m:18s	11h:52m:43s	550	35200	0	550
207.108.87.21	207.108.87.9	11h:52m:18s	11h:52m:43s	550	35200	550	0
	207.108.87.2	11h:52m:20s	11h:52m:44s	560	56560	0	560
207.108.87.20	207.108.87.2	11h:52m:17s	11h:52m:43s	570	36480	570	0
207.108.87.2	207.108.87.15	11h:52m:15s	11h:52m:45s	580	37120	0	580
	207.108.87.20	11h:52m:17s	11h:52m:43s	570	36480	0	570
	207.108.87.21	11h:52m:20s	11h:52m:44s	560	56560	560	0
207.108.87.15	207.108.87.2	11h:52m:15s	11h:52m:45s	580	37120	580	0
207.108.87.1	mplspop6.mpls.usw...	11h:52m:16s	11h:52m:45s	560	85680	560	0
	198.177.3.37	11h:52m:20s	11h:52m:44s	580	37120	580	0

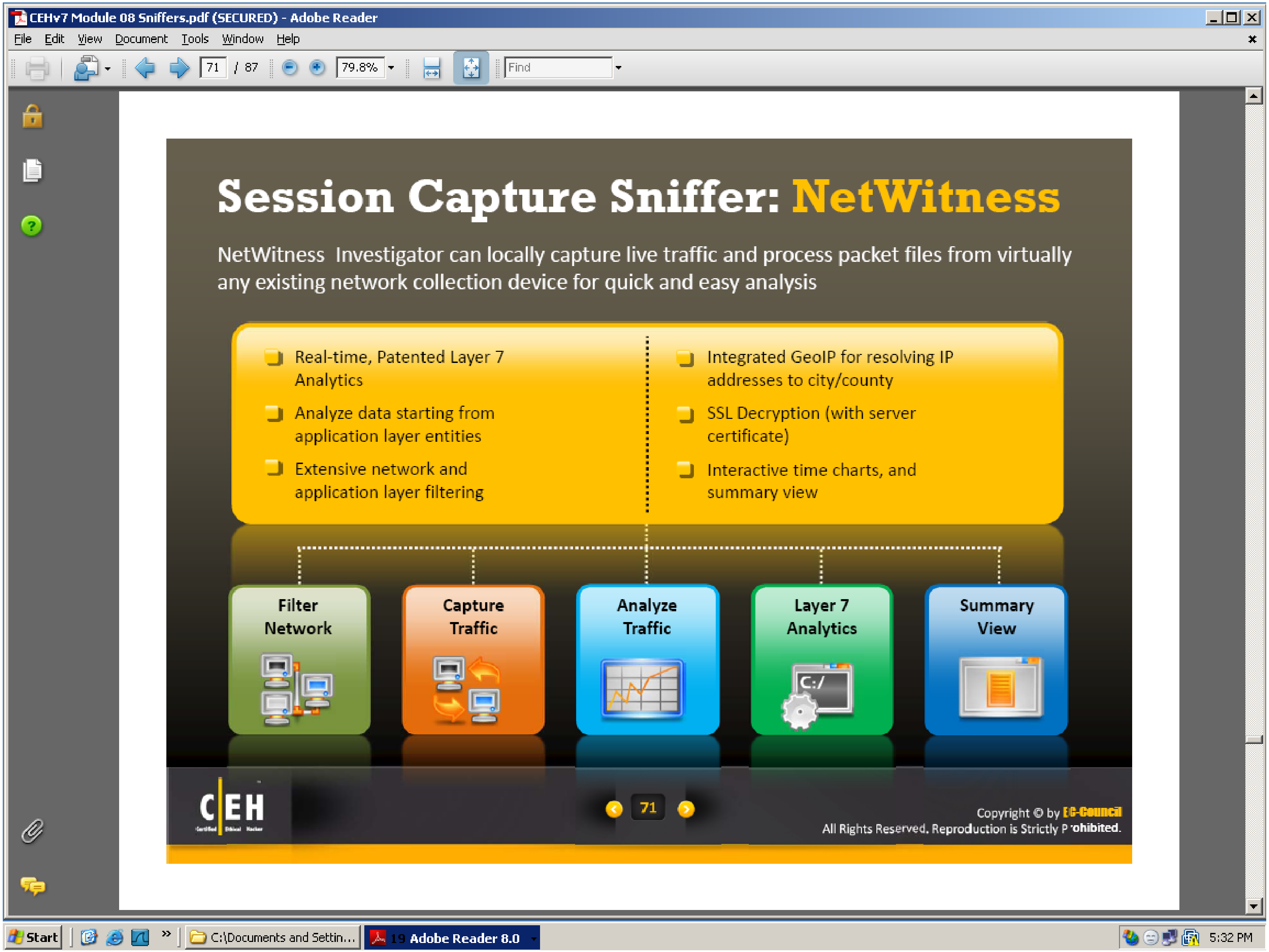
Log Filter: NONE

Time	Device	Event Type	Description
09/28/2010 11:47:12		Information	SNMP Console started

Observer not licensed. Running in Demo mode. 4 CPUs: 28.51% Network Trending Off Observer adapter: Demo Generic Intel 1000 Pro Ethernet Adapter

in Demo mode. 4 CPUs: 32.42% Network Trending Off Observer adapter: Demo Generic Intel 1000 Pro Ethernet Adapter

http://www.netinst.com


CEHv7 Module 08 Sniffers.pdf (SECURED) - Adobe Reader
File Edit View Document Tools Window Help
71 / 87
79.8%
Find
Start
C:\Documents and Settin...
19 Adobe Reader 8.0
5:32 PM

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

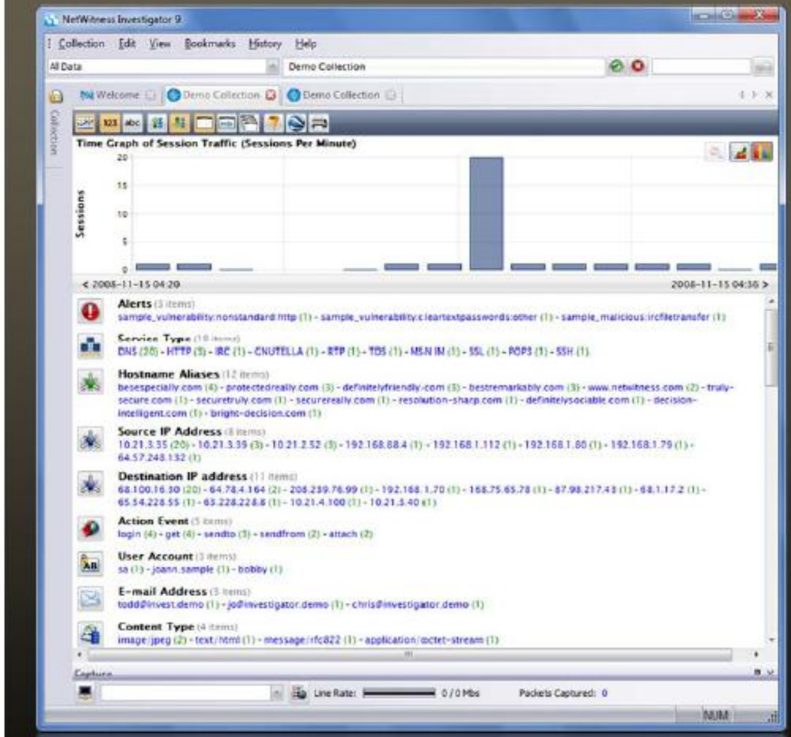
Capture Traffic

Analyze Traffic

Layer 7 Analytics

Summary View

Session Capture Sniffer: NetWitness



Time Graph of Session Traffic (Sessions Per Minute)

Alerts (3 items)
sample_vulnerability:nonstandard:http (1) - sample_vulnerability:cleartextpasswords:other (1) - sample_malicious:ircfiletransfer (1)

Service Type (10 items)
DNS (20) - HTTP (3) - IRC (1) - GNUTELLA (1) - RTP (1) - TDS (1) - MSN IM (1) - SSL (1) - POP3 (1) - SSH (1)

Hostname Aliases (12 items)
besespecially.com (4) - protectedreally.com (3) - definitelyfriendly.com (3) - bestremarkably.com (3) - www.netwitness.com (2) - truly-secure.com (1) - securetruly.com (1) - securereally.com (1) - resolution-sharp.com (1) - definitelysociable.com (1) - decision-intelligent.com (1) - bright-decision.com (1)

Source IP Address (8 items)
10.21.3.35 (20) - 10.21.3.39 (3) - 10.21.2.52 (3) - 192.168.88.4 (1) - 192.168.1.112 (1) - 192.168.1.80 (1) - 192.168.1.79 (1) - 64.57.248.132 (1)

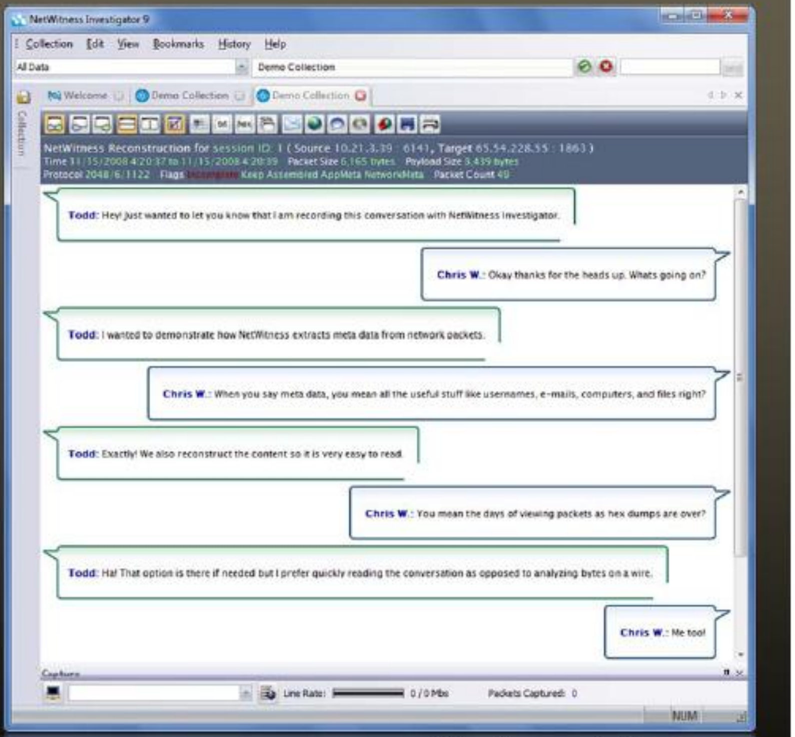
Destination IP address (11 items)
68.100.16.30 (20) - 64.78.4.164 (2) - 208.239.76.99 (1) - 192.168.1.70 (1) - 168.75.65.78 (1) - 87.98.217.43 (1) - 68.1.17.2 (1) - 65.54.228.55 (1) - 63.228.228.8 (1) - 10.21.4.100 (1) - 10.21.5.40 (1)

Action Event (5 items)
login (4) - get (4) - sendto (3) - sendfrom (2) - attach (2)

User Account (3 items)
sa (1) - joann.sample (1) - bobby (1)

E-mail Address (3 items)
todd@invest.demo (1) - jo@investigator.demo (1) - chris@investigator.demo (1)

Content Type (4 items)
image/jpeg (2) - text/html (1) - message/rfc822 (1) - application/octet-stream (1)



NetWitness Reconstruction for session ID: 1 (Source 10.21.3.39 : 6141, Target 65.54.228.55 : 1863)
Time 11/15/2008 4:20:37 to 11/15/2008 4:20:39 Packet Size 6,165 bytes Payload Size 3,439 bytes
Protocol 2048/6/1122 Flags [illegible] Keep Assembled AppMeta NetworkMeta Packet Count 49

Todd: Hey! Just wanted to let you know that I am recording this conversation with NetWitness Investigator.

Chris W.: Okay thanks for the heads up. Whats going on?

Todd: I wanted to demonstrate how NetWitness extracts meta data from network packets.

Chris W.: When you say meta data, you mean all the useful stuff like usernames, e-mails, computers, and files right?

Todd: Exactly! We also reconstruct the content so it is very easy to read.

Chris W.: You mean the days of viewing packets as hex dumps are over?

Todd: Ha! That option is there if needed but I prefer quickly reading the conversation as opposed to analyzing bytes on a wire.

Chris W.: Me too!

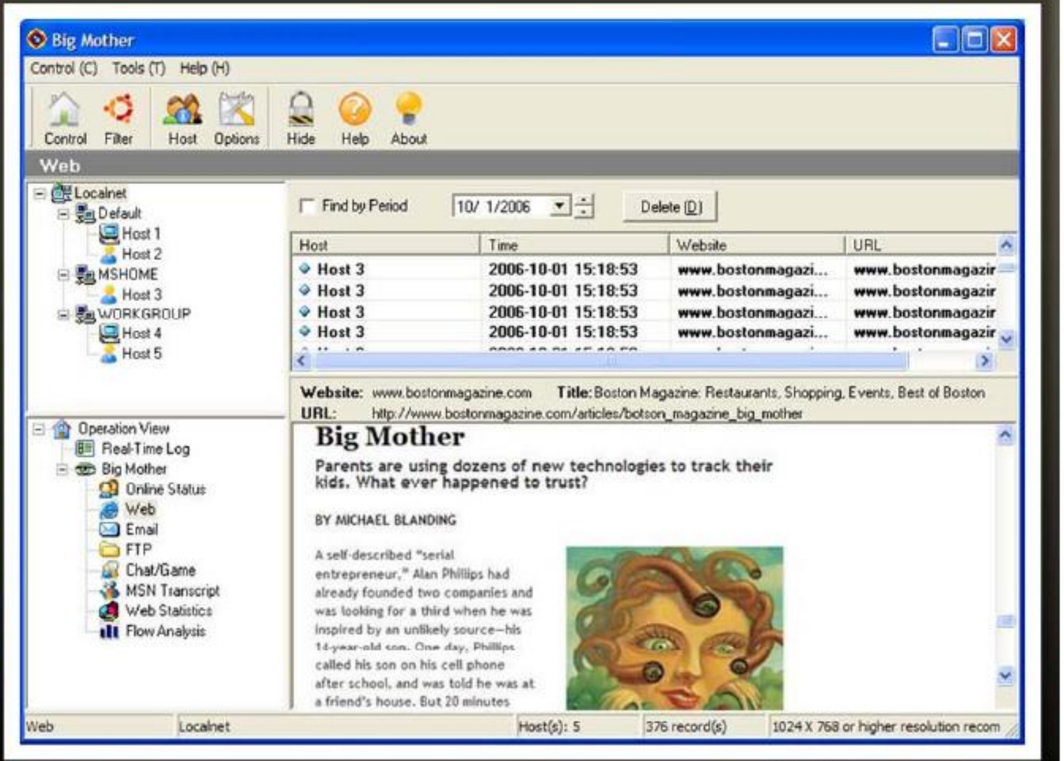
http://www.netwitness.com

CEH Certified Ethical Hacker

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



□ Find by Period 10/ 1/2006

Host	Time	Website	URL
Host 3	2006-10-01 15:18:53	www.bostonmagazi...	www.bostonmagazir
Host 3	2006-10-01 15:18:53	www.bostonmagazi...	www.bostonmagazir
Host 3	2006-10-01 15:18:53	www.bostonmagazi...	www.bostonmagazir
Host 3	2006-10-01 15:18:53	www.bostonmagazi...	www.bostonmagazir

Website: www.bostonmagazine.com **Title:** Boston Magazine: Restaurants, Shopping, Events, Best of Boston
URL: http://www.bostonmagazine.com/articles/botson_magazine_big_mother

Big Mother

Parents are using dozens of new technologies to track their kids. What ever happened to trust?

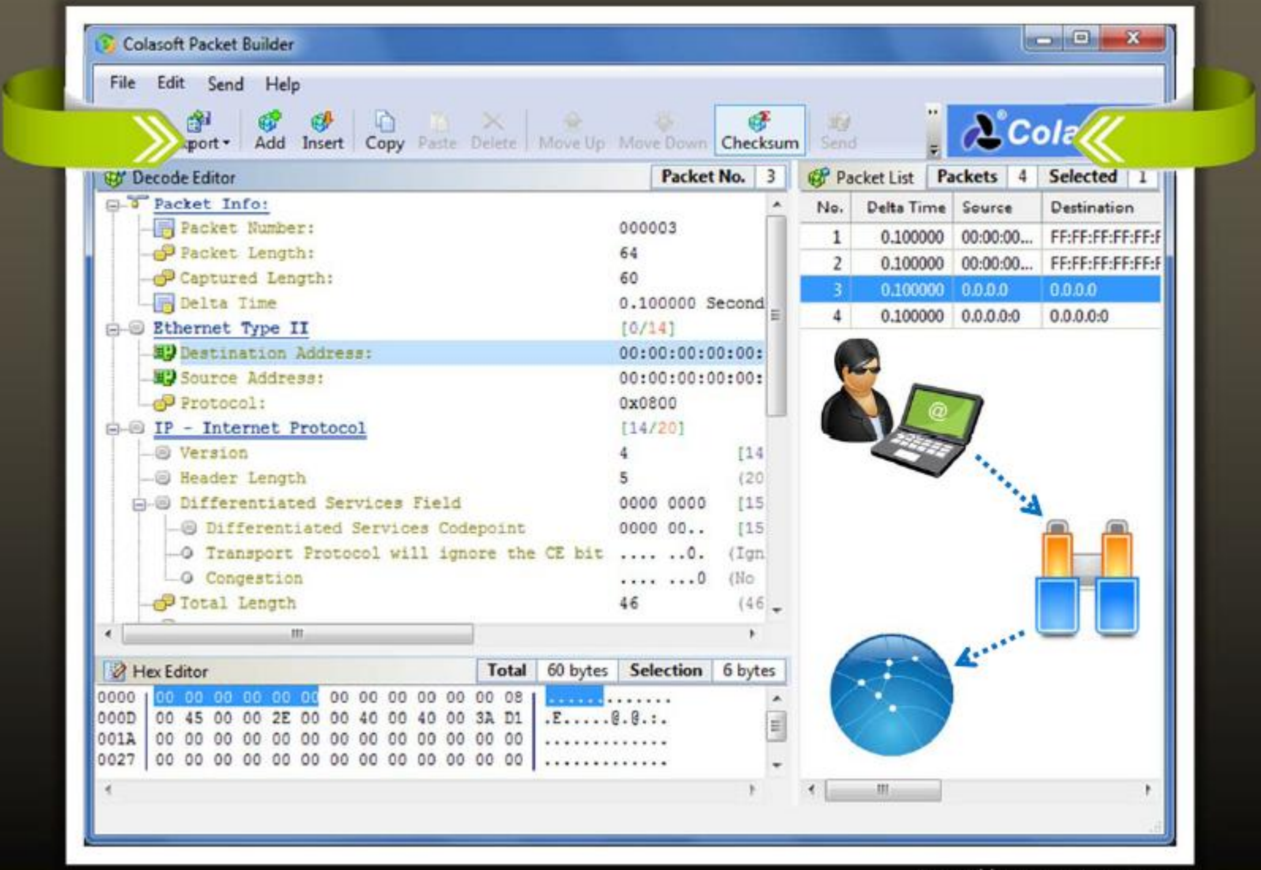
BY MICHAEL BLANDING

A self-described "serial entrepreneur," Alan Phillips had already founded two companies and was looking for a third when he was inspired by an unlikely source—his 14-year-old son. One day, Phillips called his son on his cell phone after school, and was told he was at a friend's house. But 20 minutes

Web | Localnet | Host(s): 5 | 376 record(s) | 1024 X 768 or higher resolution recom

http://www.tupsoft.com

TCP/IP Packet Crafter: Packet Builder

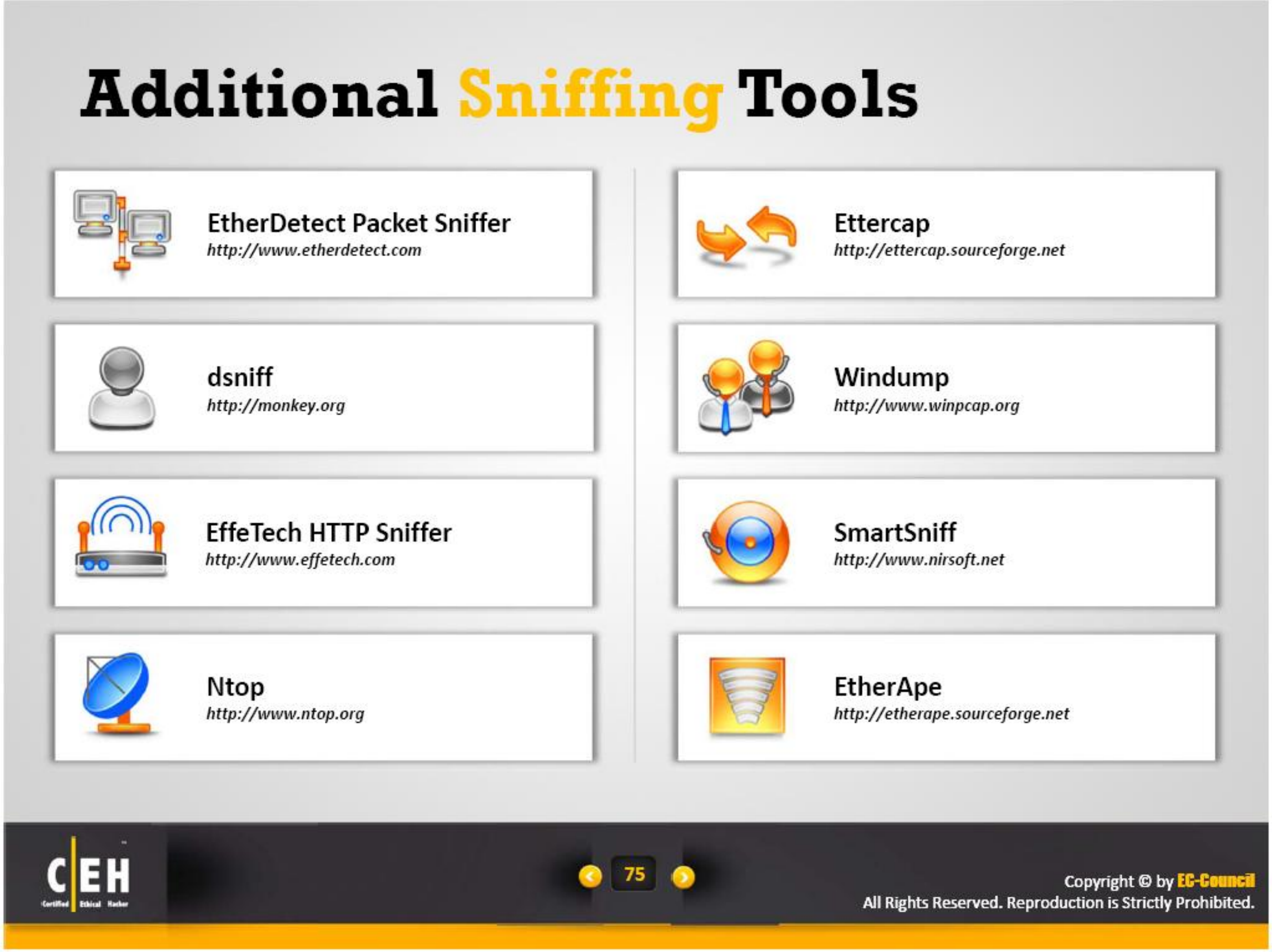


```
Packet Info:
    Packet Number:                                   000003
    Packet Length:                                   64
    Captured Length:                                 60
    Delta Time                                       0.100000 Second
Ethernet Type II                                     [0/14]
    Destination Address:                             00:00:00:00:00:
    Source Address:                                  00:00:00:00:00:
    Protocol:                                        0x0800
IP - Internet Protocol                               [14/20]
    Version                                          4          [14
    Header Length                                    5          (20
    Differentiated Services Field                    0000 0000  [15
        Differentiated Services Codepoint            0000 00..  [15
        Transport Protocol will ignore the CE bit    .... ..0.  (Ign
        Congestion                                   .... ...0  (No
    Total Length                                     46         (46
```

```
0000 | 00 00 00 00 00 00 00 00 00 00 00 00 08 | .............
000D | 00 45 00 00 2E 00 00 40 00 40 00 3A D1 | .E.....@.@.:.
001A | 00 00 00 00 00 00 00 00 00 00 00 00 00 | .............
0027 | 00 00 00 00 00 00 00 00 00 00 00 00 00 | .............
```

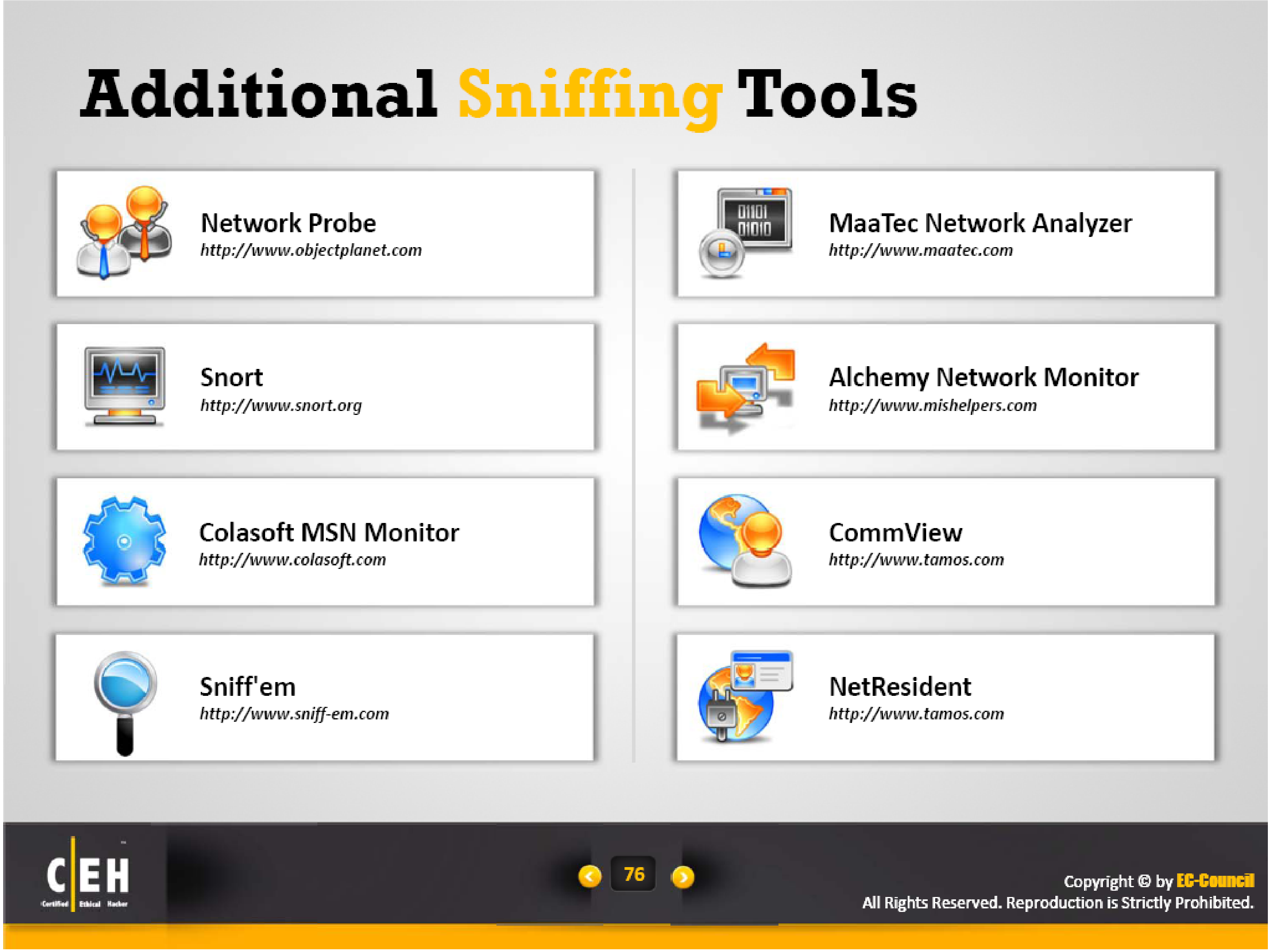
No.	Delta Time	Source	Destination
1	0.100000	00:00:00...	FF:FF:FF:FF:FF:F
2	0.100000	00:00:00...	FF:FF:FF:FF:FF:F
3	0.100000	0.0.0.0	0.0.0.0
4	0.100000	0.0.0.0:0	0.0.0.0:0

http://www.colasoft.com



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*

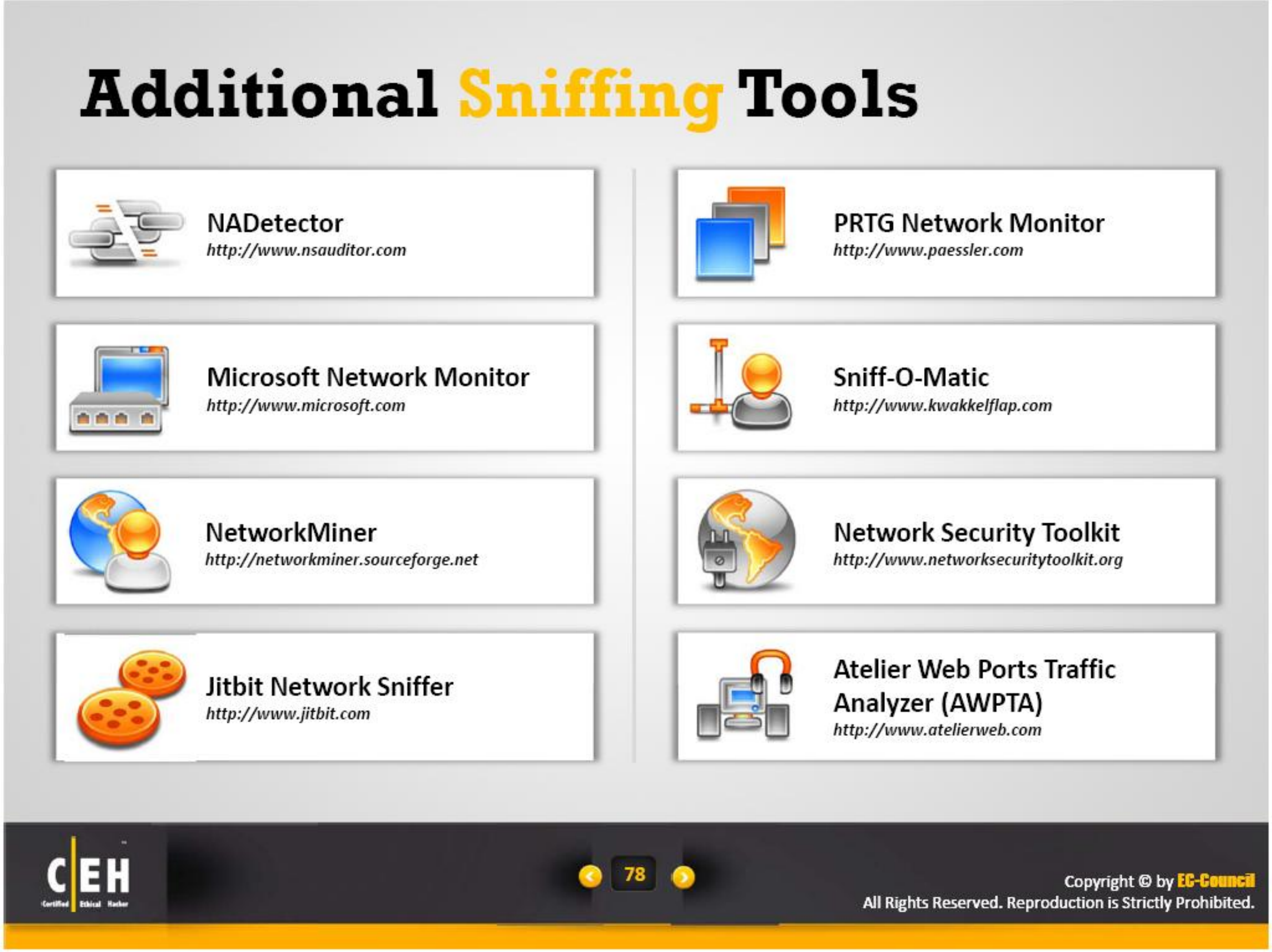


Additional Sniffing Tools

Network Probe *http://www.objectplanet.com*	**MaaTec Network Analyzer** *http://www.maatec.com*
Snort *http://www.snort.org*	**Alchemy Network Monitor** *http://www.mishelpers.com*
Colasoft MSN Monitor *http://www.colasoft.com*	**CommView** *http://www.tamos.com*
Sniff'em *http://www.sniff-em.com*	**NetResident** *http://www.tamos.com*

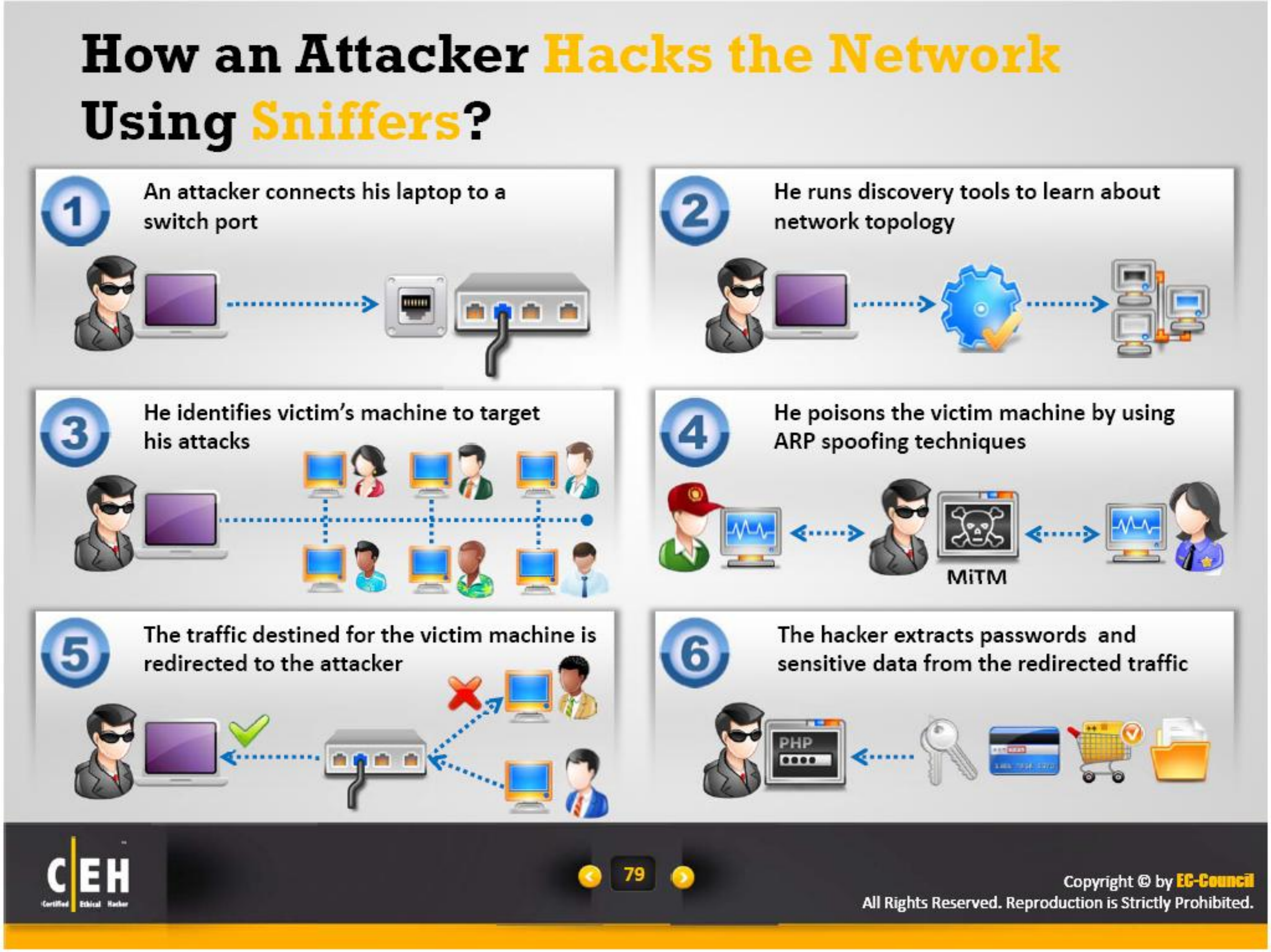
Additional Sniffing Tools

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 *http://erwan.l.free.fr*	EtherScan Analyzer *http://www.etherscan.com*



Additional Sniffing Tools

NADetector *http://www.nsauditor.com*	PRTG Network Monitor *http://www.paessler.com*
Microsoft Network Monitor *http://www.microsoft.com*	Sniff-O-Matic *http://www.kwakkelflap.com*
NetworkMiner *http://networkminer.sourceforge.net*	Network Security Toolkit *http://www.networksecuritytoolkit.org*
Jitbit Network Sniffer *http://www.jitbit.com*	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

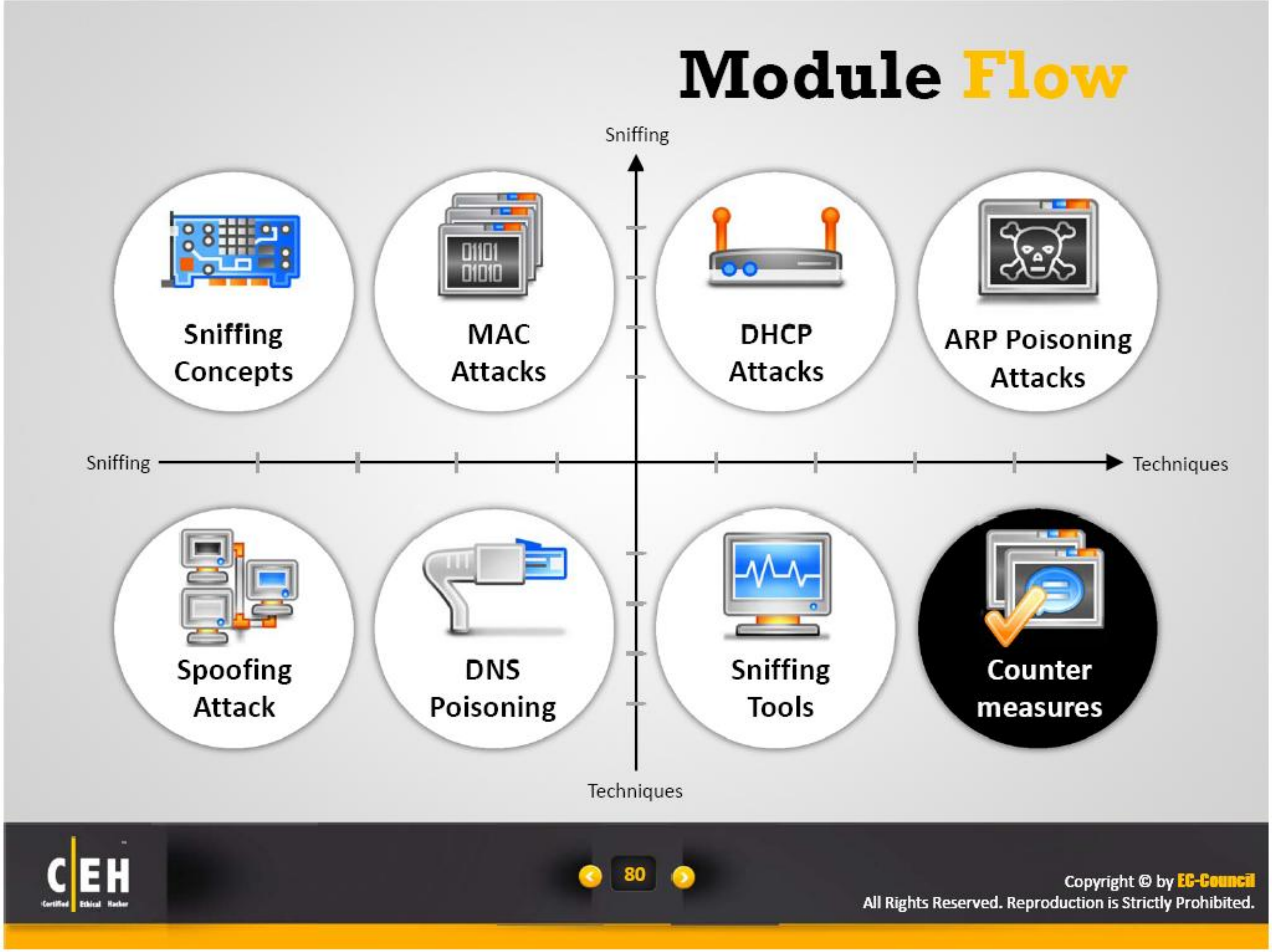
2. He runs discovery tools to learn about network topology

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



Module Flow

Sniffing

Sniffing

Techniques

Techniques

Sniffing Concepts

MAC Attacks

DHCP Attacks

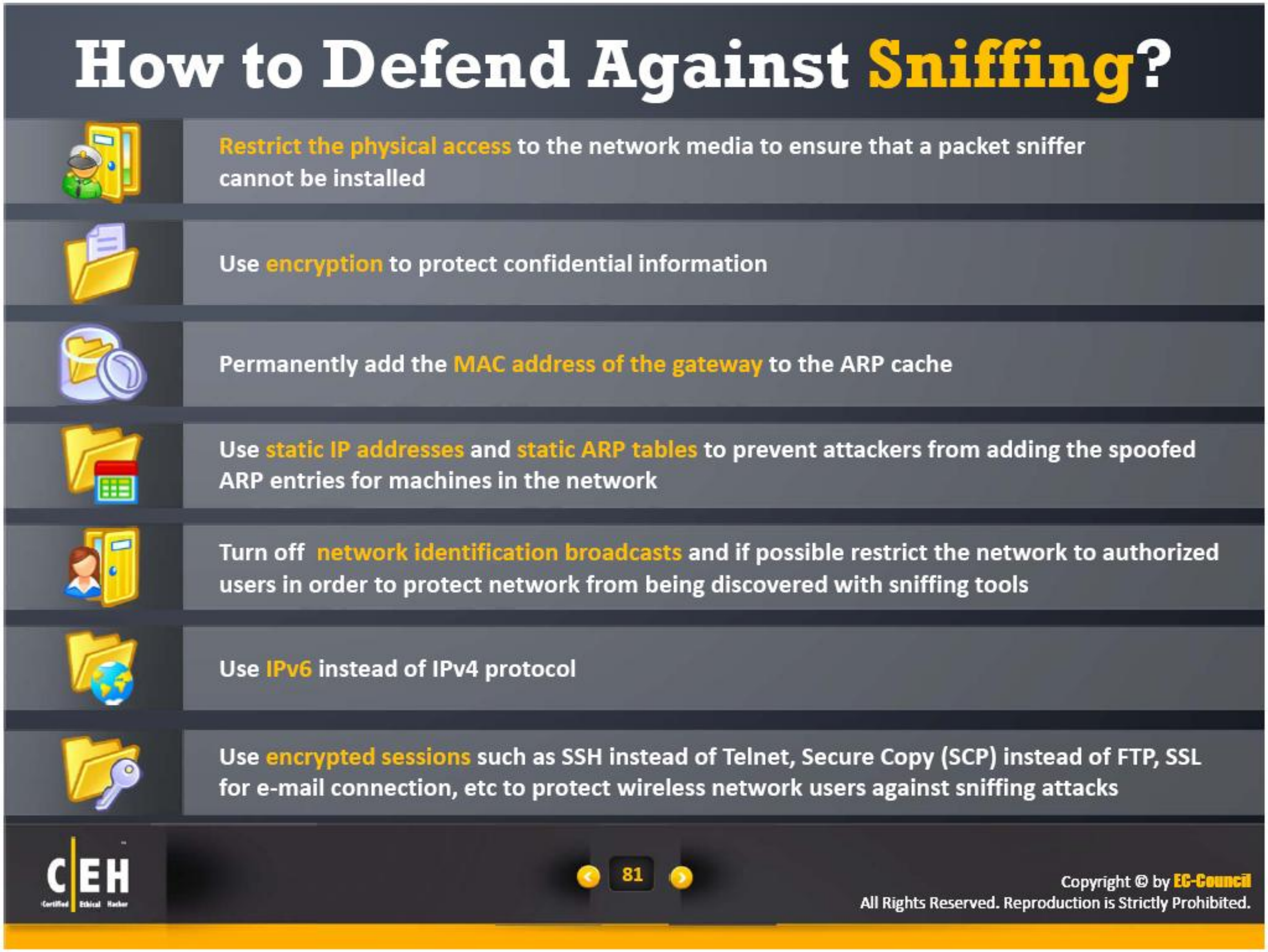
ARP Poisoning Attacks

Spoofing Attack

DNS Poisoning

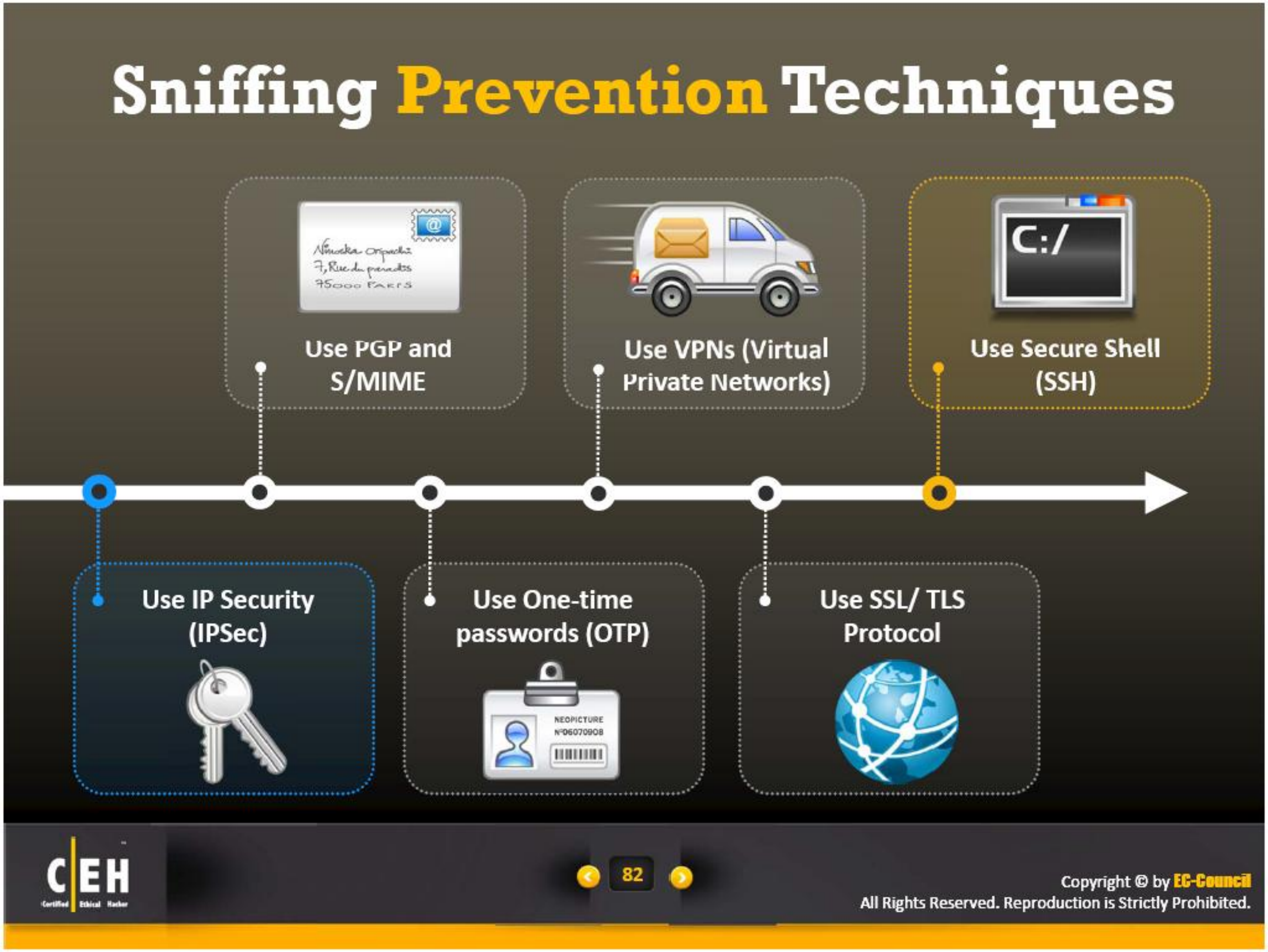
Sniffing Tools

Counter measures



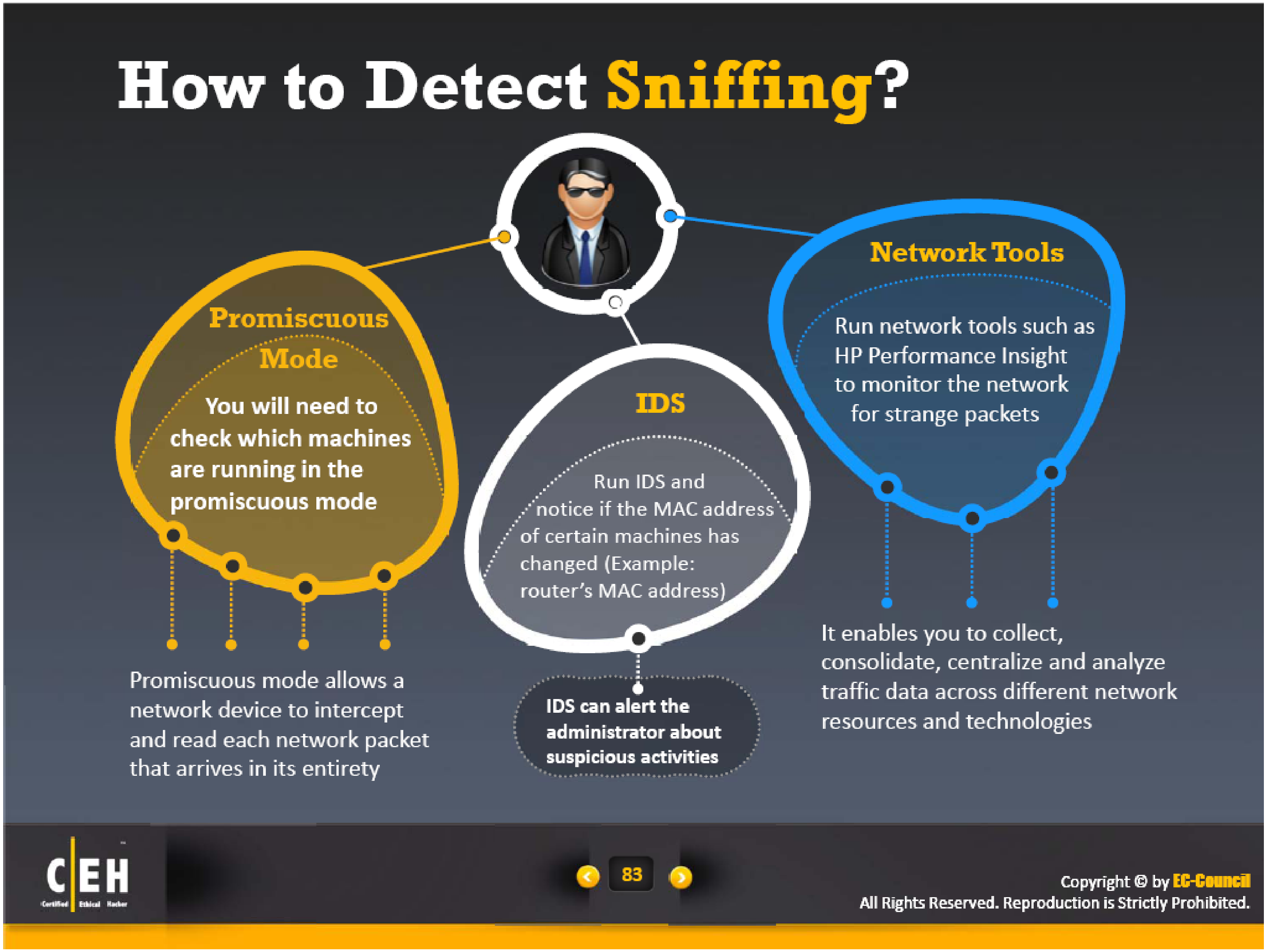
How to Defend Against Sniffing?

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



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

IDS

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

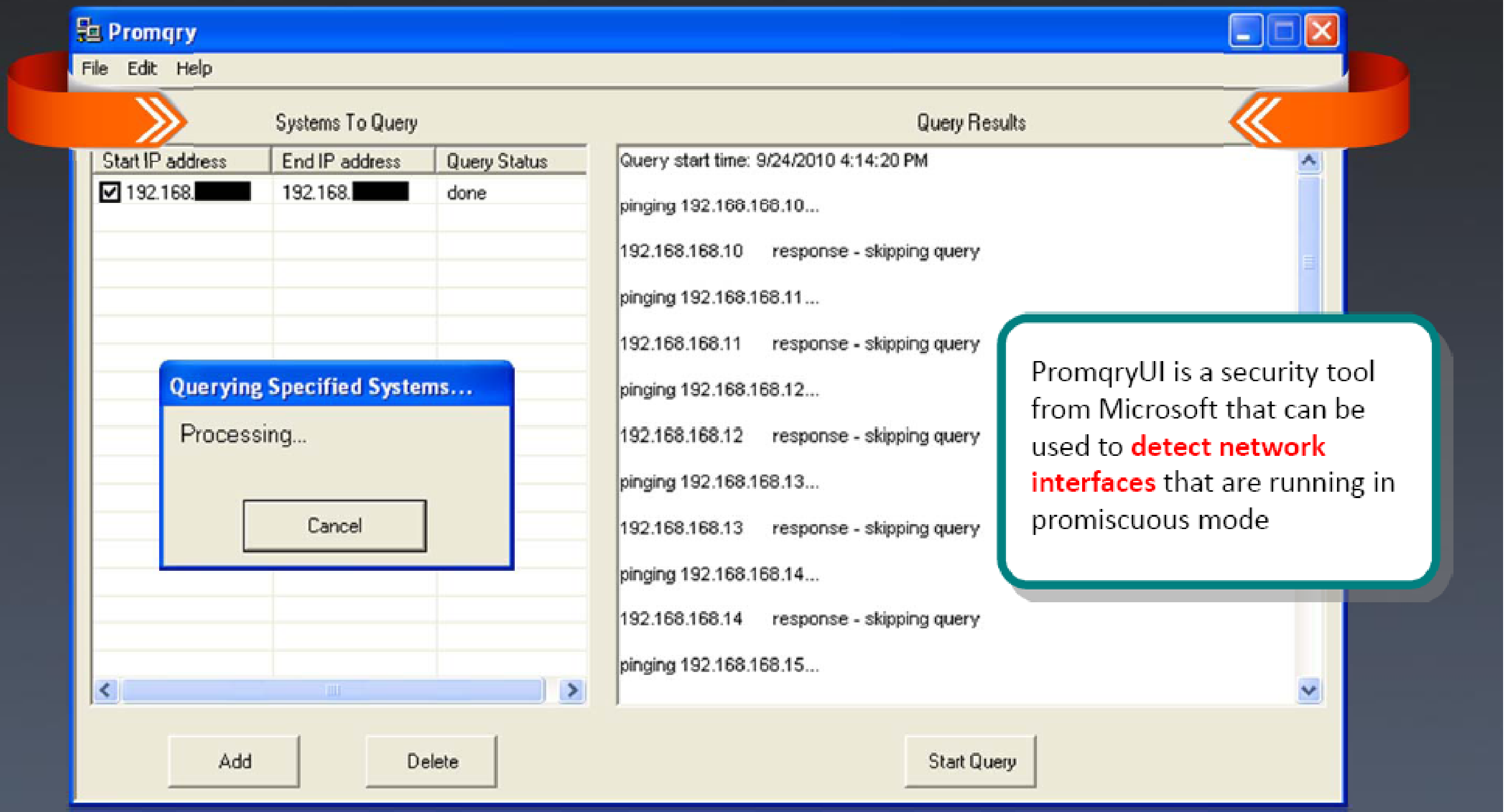
IDS can alert the administrator about suspicious activities

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

Promiscuous Detection Tool: PromqryUI



Start IP address	End IP address	Query Status
☑ 192.168.[redacted]	192.168.[redacted]	done

```
Query start time: 9/24/2010 4:14:20 PM

pinging 192.168.168.10...

192.168.168.10     response - skipping query

pinging 192.168.168.11...

192.168.168.11     response - skipping query

pinging 192.168.168.12...

192.168.168.12     response - skipping query

pinging 192.168.168.13...

192.168.168.13     response - skipping query

pinging 192.168.168.14...

192.168.168.14     response - skipping query

pinging 192.168.168.15...
```

Querying Specified Systems...

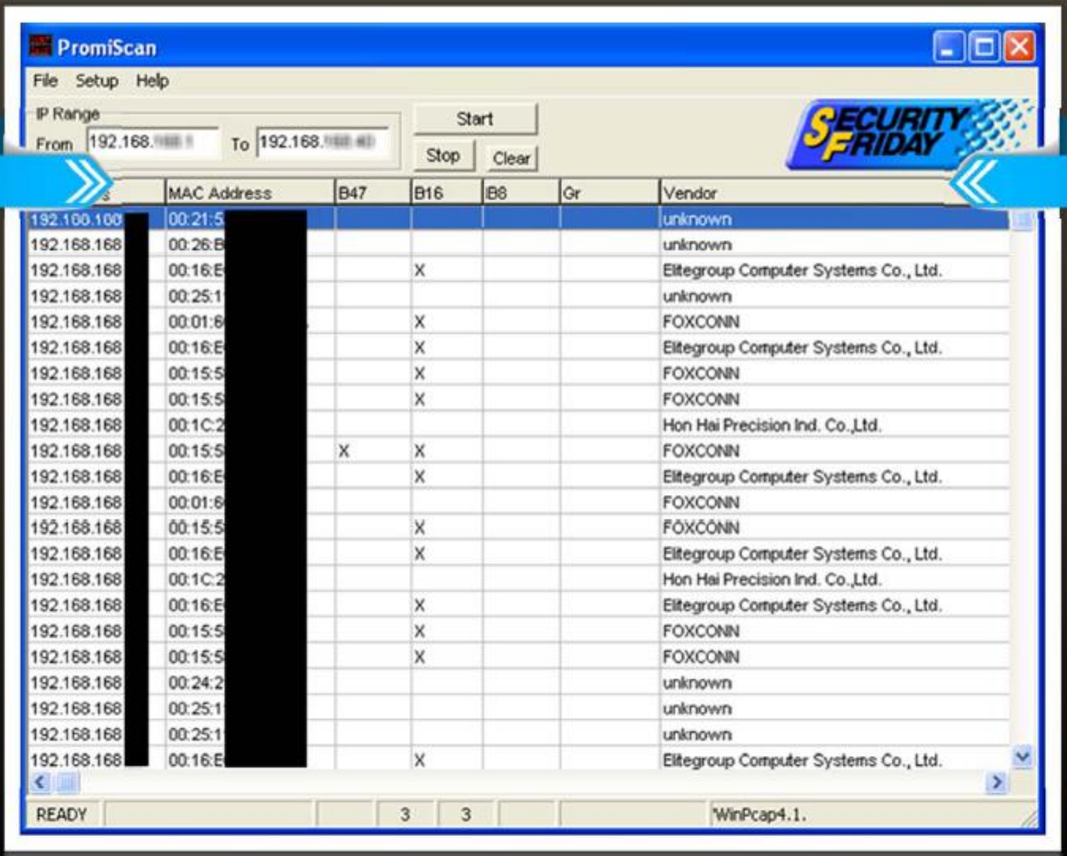
Processing...

Cancel

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



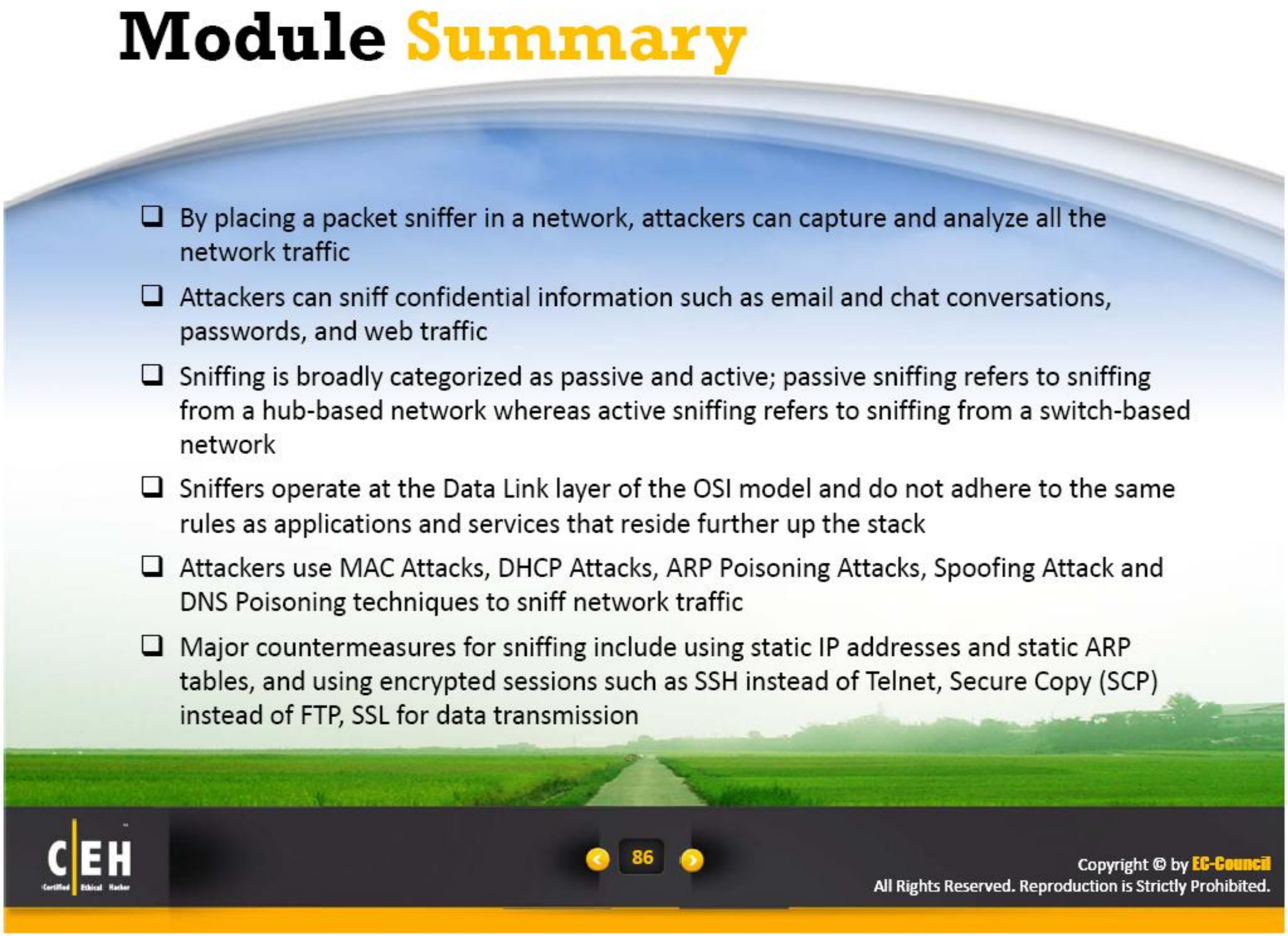
IP Range

From 192.168.[redacted] To 192.168.[redacted]

s	MAC Address	B47	B16	B8	Gr	Vendor
192.100.100 [redacted]	00:21:5 [redacted]					unknown
192.168.168 [redacted]	00:26:B [redacted]					unknown
192.168.168 [redacted]	00:16:E [redacted]		X			Elitegroup Computer Systems Co., Ltd.
192.168.168 [redacted]	00:25:1 [redacted]					unknown
192.168.168 [redacted]	00:01:6 [redacted]		X			FOXCONN
192.168.168 [redacted]	00:16:E [redacted]		X			Elitegroup Computer Systems Co., Ltd.
192.168.168 [redacted]	00:15:5 [redacted]		X			FOXCONN
192.168.168 [redacted]	00:15:5 [redacted]		X			FOXCONN
192.168.168 [redacted]	00:1C:2 [redacted]					Hon Hai Precision Ind. Co.,Ltd.
192.168.168 [redacted]	00:15:5 [redacted]	X	X			FOXCONN
192.168.168 [redacted]	00:16:E [redacted]		X			Elitegroup Computer Systems Co., Ltd.
192.168.168 [redacted]	00:01:6 [redacted]					FOXCONN
192.168.168 [redacted]	00:15:5 [redacted]		X			FOXCONN
192.168.168 [redacted]	00:16:E [redacted]		X			Elitegroup Computer Systems Co., Ltd.
192.168.168 [redacted]	00:1C:2 [redacted]					Hon Hai Precision Ind. Co.,Ltd.
192.168.168 [redacted]	00:16:E [redacted]		X			Elitegroup Computer Systems Co., Ltd.
192.168.168 [redacted]	00:15:5 [redacted]		X			FOXCONN
192.168.168 [redacted]	00:15:5 [redacted]		X			FOXCONN
192.168.168 [redacted]	00:24:2 [redacted]					unknown
192.168.168 [redacted]	00:25:1 [redacted]					unknown
192.168.168 [redacted]	00:25:1 [redacted]					unknown
192.168.168 [redacted]	00:16:E [redacted]		X			Elitegroup Computer Systems Co., Ltd.

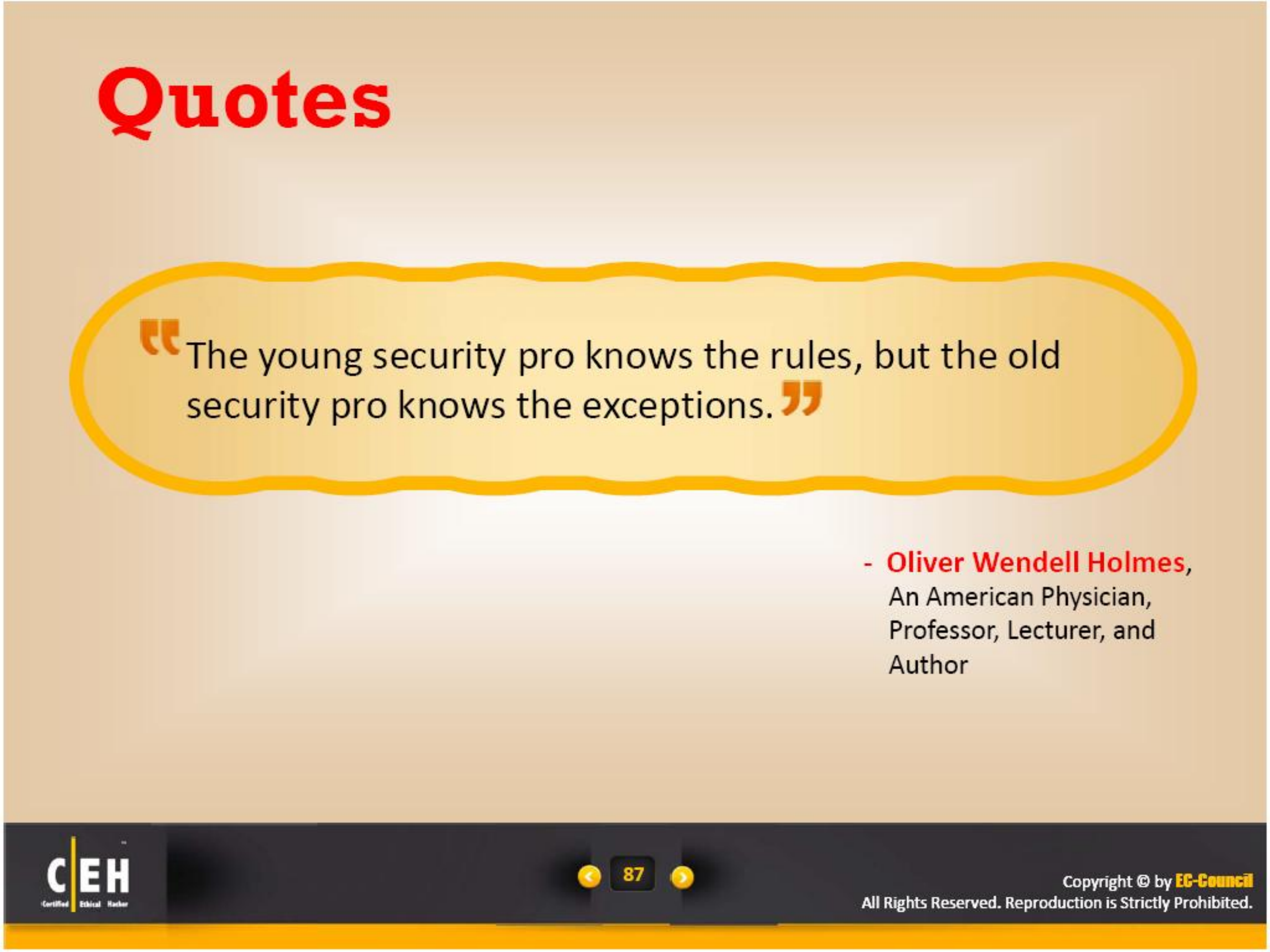
READY | 3 | 3 | WinPcap4.1.

http://www.securityfriday.com



Module Summary

- □ 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



Quotes

> “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