NPTEL ONLINE CERTIFICATION COURSES

# Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering



## Topic

## Lecture 41: Packet Sniffing (Part 1)

# CONCEPTS COVERED

- Network analysis and sniffing
- Wireshark packet analysis tool

# What is Sniffing?

- What is network analysis or Sniffing?
  - It is a process of analyzing network activity by capturing network traffic.
  - Sniffer is a program that monitors the data travelling around the network.
  - **Example tools**: Wireshark, Solarwinds, Kismet, burpsuit, and many others.
- Features of a network analyzer or sniffer:
  a) Support for multiple protocols
  b) Graphical user interface
  c) Statistical report generation

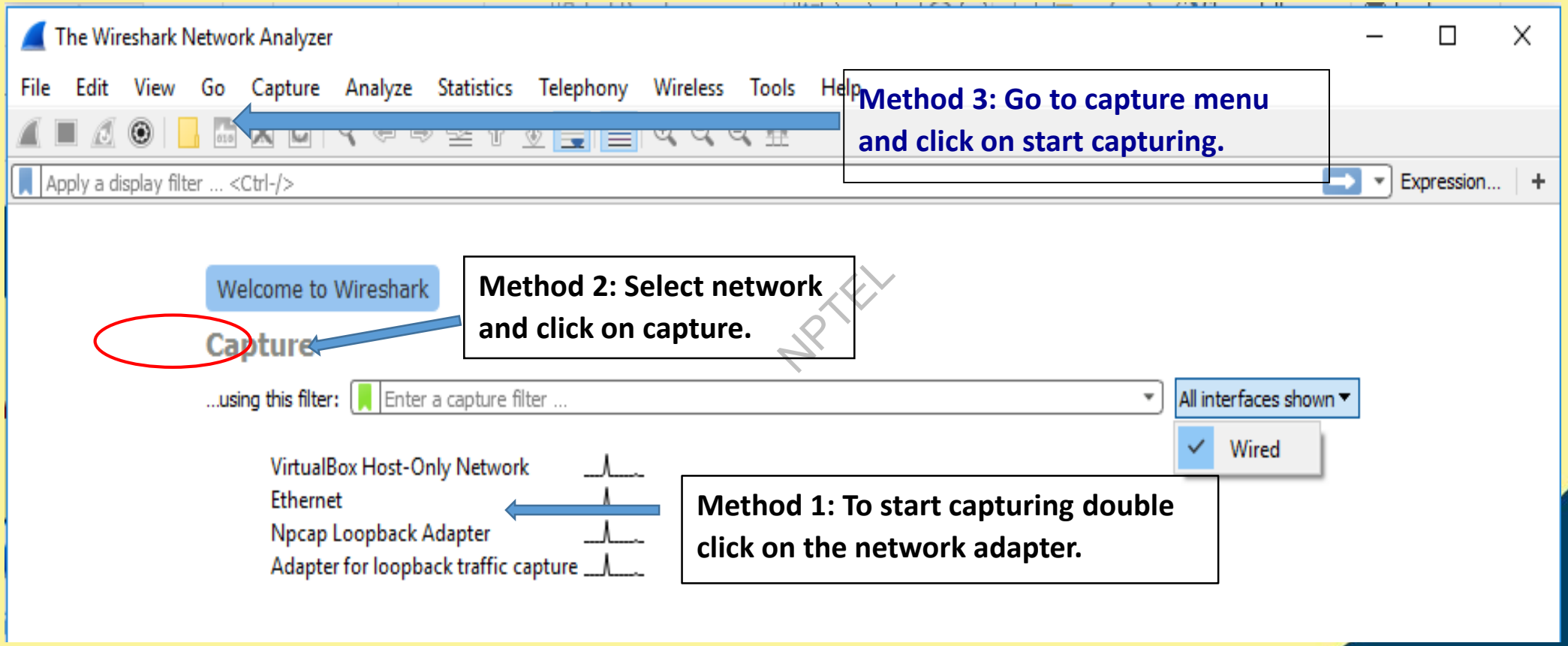
# What is Wireshark?

- It is an open source tool for profiling network traffic and analyzing packets.
  - Often referred to as a network analyzer, network protocol analyzer or sniffer.
  - Can be downloaded from: **http://www.wireshark.org**
- What is does really?
  - Captures network data and displays them in a readable format.
  - Log network traffic for forensics and evidence.
  - Analyze network traffic generated by various applications.

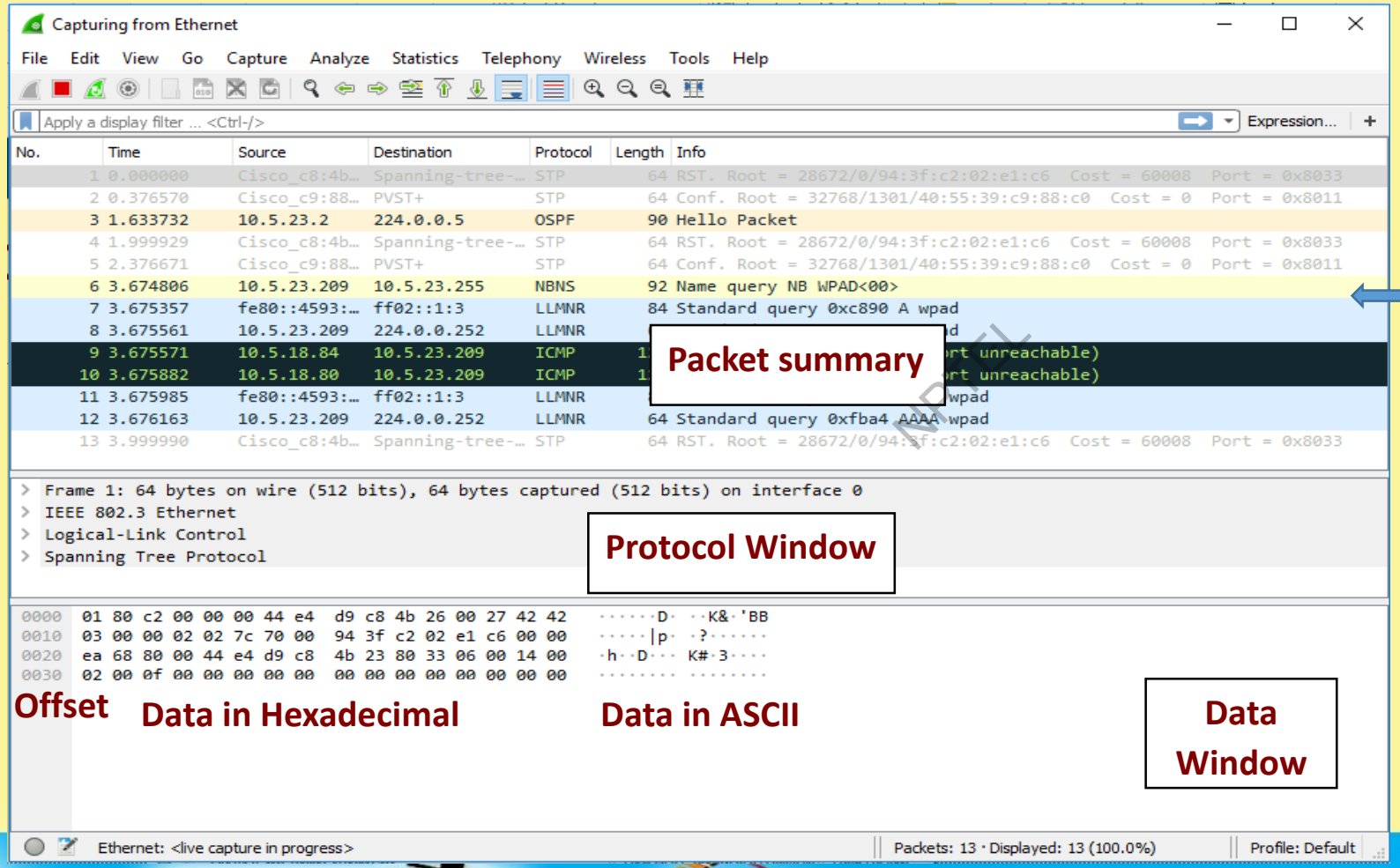
# How Packet Sniffer works?

- Ethernet is the most widely used protocol used in a LAN.
  - At the data-link layer level.
- While running Wireshark the machine's network interface card (NIC) is put in ***promiscuous mode***.
  - In this mode, the sniffer can read all traffic on the network segment to which the NIC is connected (irrespective of the sender and the receiver).
  - Requires root privilege to set the NIC to promiscuous mode.
  - If the LAN uses a switch, then packets from other network segments cannot be captured.

# Packet Capture using Wireshark



# Packet Capturing Starts




**Packet Information**

**No:** Frame number

**Time:** Time in second

**Source:** source address

**Destination:** Destination address

**Protocol:** Protocol that is used for communication

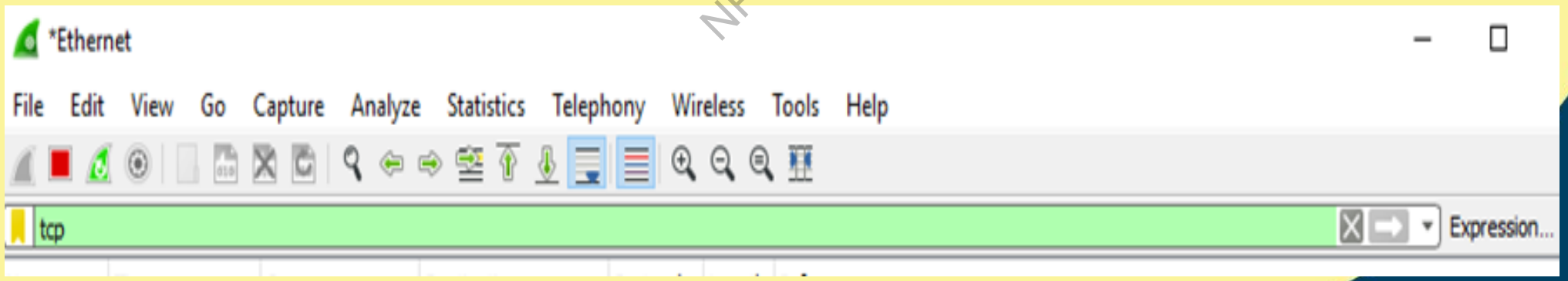
**Length:** Length of packet in bytes

**Info:** Info of the packet (Type version etc.)

# Filtering different type of packets

- To filter packets put filter name in filter bar and press <enter> or the arrow.
  - Restrict the packets that are displayed in summary window.
  - For correct filter, bar will convert from white to green and for wrong filter it will be shown as red.





# Demonstration: Wireshark

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

# Thank you!

NPTEL ONLINE CERTIFICATION COURSES

# Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering



## Topic

## Lecture 42: Packet Sniffing (Part 2)

# CONCEPTS COVERED

- Packet capturing demo using Wireshark
- Sniffing countermeasures
- Sniffing detection

# Demonstration: Password Capture

# Sniffing Countermeasure

- Restrict the physical access to the network media to ensure that a packet sniffer cannot be installed.
- Use encryption to protect confidential information.
- Permanently add the MAC address of the gateway to the ARP cache.
- Use static IP addresses and static ARP tables to prevent attackers from adding the spoofed ARP entries for machines in the network.
- Use IPv6 instead of IPv4 protocol.

# Sniffing Countermeasure (contd.)

- Use encrypted sessions such as SSH instead of Telnet, Secure Copy (SCP) instead of FTP, SSL for email connection, etc. to protect wireless network users against sniffing attacks.
- Use HTTPS instead of HTTP to protect user names and passwords.
- Use switch instead of hub as switch delivers data only to the intended recipient.
- Use SFTP, instead of FTP for secure transfer of files.
- Use PGP and S/MIPE, VPN, IPSec, SSL/TLS, Secure Shell (SSH) and One-time passwords (OTP).

# Sniffing Detection

- Nmap's NSE script allows us to check if a target on a local Ethernet has its network card in promiscuous mode.
- Command to detect NIC in promiscuous mode:

  **nmap --script=sniffer-detect [Target IP Address/Range of IP add]**

# Demonstration: Sniffing Detection

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

# Thank you!

NPTEL ONLINE CERTIFICATION COURSES

# Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering



## Topic

## Lecture 43: Packet Sniffing (Part 3)

# CONCEPTS COVERED

- Sniffing with Ettercap and Burpsuite
- HTTPS and DNS Sniffing

# Ettercap Sniffing Tools

- Ettercap is a free and open source network security tool for man-in-the-middle attacks on LAN.
- It can be used for computer network protocol analysis and security auditing. It runs on various Unix-like operating systems including Linux, Mac OS X, BSD and Solaris, and on Microsoft Windows.
- It is capable of intercepting traffic on a network segment, capturing passwords, and conducting active eavesdropping against a number of common protocols.
- Ettercap has plugin support so that the features can be extended by adding new plugins.

# Features of Ettercap

- IP-based Filtering: We can filter packets based on IP source and destination.
- MAC-based Filtering: packets can be filtered based on MAC address, useful for sniffing connections through a gateway.
- Character injection into an established connection: characters can be injected into a server (emulating commands) or to a client (emulating replies) while maintaining a live connection.
- SSH1 support: the sniffing of a username and password, and even the data of an SSH1 connection. Ettercap is the first software capable of sniffing an SSH connection in full duplex.

# Features of Ettercap

- HTTPS support: the sniffing of HTTP SSL secured data—even when the connection is made through a proxy.
- Plug-in support: creation of custom plugins using Ettercap's API.
- Packet filtering/dropping: setting up a filter that searches for a particular string (or hexadecimal sequence) in the TCP or UDP payload and replaces it with a custom string/sequence of choice, or drops the entire packet.
- TCP/IP stack fingerprinting: determine the OS of the victim host and its network adapter.
- And many more features available.

# BurpSuite Sniffing Tools

- Burpsuit is an integrated platform for performing security testing of web applications.
- The tool is written in Java and developed by PortSwigger Security.
- It can be used for computer network protocol analysis and security auditing. It has two versions free version and a professional version.

# Various Modules of BurpSuite

- Target: The target tool gives an overview of target applications content and functionality.
- Proxy: Gives direct view of how target applications works by working as proxy server or as a man-in-the-middle between you and your server such that you can intercept, inspect and modify the raw traffic.
- Spider: Used for automotive crawling web applications.
- Scanner: Used for finding vulnerabilities in web applications.
- Intruder: it is used for automating customized attacks against web applications.
- Repeater: Is used for manipulating and reissuing HTTP requests and analyzing application response.

# Demonstration: Sniffing using Burpsuit

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

# Thank you!

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

# Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering



## Topic

## Lecture 44: Social Engineering Attack

# CONCEPTS COVERED

- Social engineering attacks
- Types of social engineering attacks
- Social engineering countermeasures

# Social Engineering Attack

- Social engineering is the art of convincing people to reveal confidential information.
  - Social engineers lure targets to provide information by promising something for nothing (greediness).
- Common targets of social engineering:
  - Help desk personnel
  - Technical support executives
  - System administrators
  - Frustrated employees etc.

# Phases in a Social Engineering Attack

a) Research on Target Company:
   - Dumpster diving, websites, employees, tour company, etc.

b) Select Victim:
   - Select most vulnerable victim such as greedy employee.

c) Develop Relationship:
   - Develop relationship with the selected victim.

d) Exploit the Relationship:
   - Collect sensitive information such as financial information, current technologies etc.

# Types of Social Engineering Attack

a) Human-based Social Engineering:
   - Collect sensitive information by direct interaction with victims.

b) Computer-based Social Engineering:
   - Social engineering is carried out with the help of computers.

c) Mobile-based Social Engineering:
   - Social engineering is carried out with the help of mobile applications.

# (a) Human Based Social Engineering

- **Impersonation:**
  - The attacker pretends to be someone legitimate or authorized person – most common.
- **Reverse Social Engineering:**
  - A situation in which an attacker presents himself as an authority and the target seeks his advice offering the information that he needs.
- **Piggybacking:**
  - An authorized person allows (intentionally or unintentionally) an unauthorized person to pass through a secure door. *"I forgot my ID badge at home. Please help me"*

# (a) Human Based Social Engineering (contd.)

- **Tailgating:**
  - An unauthorized person, wearing a fake ID badge, enters a secured area by closely following an authorized person through a door requiring key access.
- **Eavesdropping:**
  - Interception of audio, video, or written communication. It can be done using communication channels such as telephone lines, email, instant messaging, etc.
- **Shoulder Surfing:**
  - Uses direct observation techniques such as looking over someone's shoulder to get information such as passwords, PINs, account numbers, etc.

# (b) Computer-based Social Engineering

- **Pop-up Windows:**
  - Windows that suddenly appears while surfing the Internet and ask for users' information to login or sign-in or for providing help.
- **Chain Letters:**
  - Chain letters are emails that offer free gifts such as money and software on the condition that the user has to forward the mail to the said number of persons.
- **Instant Chat Messenger:**
  - Gathering personal information by chatting with a selected online user to get information such as birth dates, maiden names, emails, contact information etc.

# (b) Computer-based Social Engineering (contd.)

- **Phishing:**
  - An illegitimate email falsely claiming to be from a legitimate site attempts to acquire the user's personal or account information. Phishing emails or pop-ups redirect users to fake webpages of mimicking trustworthy sites that ask them to submit their personal information.
- **Spear Phishing:**
  - A direct, targeted phishing attack aimed at specific individuals within an organization. Attackers send a message with specialized, social engineering content directed at a specific person or a small group of people.

# (c) Mobile-based Social Engineering

- **Publishing Malicious Apps, Fake Security Applications:**
  - Attackers create malicious apps with attractive features and similar names to that of popular apps, and publish them on major app stores. Unaware users download these apps and get infected by malware that sends credentials to attackers.
- **Using SMS:**
  - Send messages which looks like very important message from bank/company etc and need urgent call in the given number.
  - Victim calls to check account then attacker asks for information such as credit/debit card numbers etc.

# Demonstration: Phishing using SEToolkit

# Social Engineering Countermeasures

- Good policies and procedures are ineffective if they are not taught and reinforced by the employees.
- **Password Policies:**
  - Periodic password change, Avoiding guessable passwords, Account blocking after failed attempts.
- **Physical Security Policies:**
  - Identification of employees by issuing ID cards, uniforms, etc. Escorting the visitors, Access area restrictions.

# Social Engineering Countermeasures (contd.)

- **Training:**
  - Include all security policies and methods to increase awareness on social engineering.
- **Access privileges:**
  - There should be administrator, user, and guest accounts with proper authorization.
- **Classification of Information:**
  - Categorize the information as top secret, proprietary, for internal use, for public use, etc.
- **Background Check and Proper Termination Process:**
  - Insiders with a criminal background and terminated employees are easy targets.

# Social Engineering Countermeasures (contd.)

- **Anti-Virus/Anti-Phishing Defenses:**
  - Use multiple layers of anti-virus defenses at end-user and mail gateway levels to minimize social engineering attacks.
- **Two-Factor Authentication:**
  - Instead of fixed passwords, use two-factor authentication for high-risk network services such as VPNs and modem pools.

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

# Thank you!

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

# Course Name: Ethical Hacking

Faculty Name: Prof. Indranil Sen Gupta

Department : Computer Science and Engineering



## Topic

## Lecture 45: Denial of Service Attack

## CONCEPTS COVERED

- Denial of service attack
- Various attack tools

# Denial-of-Service Attack

- It is an attack on a computer or network that reduces, restricts or prevents accessibility of system resources to its legitimate users.
  - In a DoS attack, attackers flood a victim system with non-legitimate service requests or traffic to overload its resources.
  - It leads to unavailability of a particular website and show network performance.
- A distributed denial-of-service (DDoS) attack involves a multitude of compromised systems attacking a single target, thereby causing denial of service for users of the targeted system.

# DoS / DDoS Attack Techniques

- **Bandwidth Attacks:**
  - Overwhelm network equipment.
  - It cannot be done using single system, an attacker uses several computers to flood a victim.
- **SYN Attack:**
  - The attacker sends a large number of SYN request to victim server with fake source IP addresses.
  - The target machine sends back a SYN/ACK in response to the request and waits for the ACK to complete the session setup.
  - The target machine does not get the response because the source address is fake.

# DoS / DDoS Attack Techniques (contd.)

- **SYN Flooding:**
  - Takes advantage of a flaw in how most hosts implement the TCP three-way handshake.
  - When Host B receives the SYN request from A, it must keep track of the partially-opened connection in a "listen queue" for at least 75 seconds.
  - A malicious host can exploit the small size of the listen queue by sending multiple SYN requests the a host, but never replying to the SYN/ACK.
- **ICMP Flood Attack:**
  - The attacker send a large number of ICMP packets directly or through reflection networks to victims causing it to be overwhelmed and subsequently stop responding to legitimate TCP/IP requests.

# DoS/DDoS Attack Techniques (cont.)

- **Application-Level Flood Attacks:**
  - This results in the loss of services of a particular network, such as emails, network resources, the temporary ceasing of applications and services, and more.
  - The attackers exploit weaknesses in programming source code to prevent the application from processing legitimate requests.
  - Using application-level flood attacks, attackers attempts to: (a) Flood web applications to legitimate user traffic, (b) Disrupt service to a specific system or person, for example, blocking a user's access by repeating invalid login attempts.

# Botnets

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

# DoS / DDoS Attack Tools: Slowloris

- This is the most effective tool for DDoS attack. It works by opening thousands of connections to the targeted web server and holding them open for a long time.
- This is achieved by sending partial HTTP requests, and none of them will be completed ever. It requires minimal bandwidth to target web server and no after effects.

# DoS / DDoS Attack Tools: Low Orbit Ion Cannon (LOIC)

- It is an open source network stress testing and DoS attack software written in C#.
  - This tool performs a DOS attack by sending UDP, TCP, or HTTP on the target with the intention of disrupting its services
  - It is mainly used for DoS attack on small servers. It is available on Linux, Windows, and Android as well.
- LOIC basically turns computer's network connection into a firehose of garbage requests, directed towards a target web server.

# DoS / DDoS Attack Tools: RUDY (R U Dead Yet ?)

- R.U.D.Y. is a popular low and slow attack tool that is designed to crash a web server by submitting long form fields.
  - The attack browses the target website and detects embedded web forms. Once the forms are identified, it sends a legitimate HTTP POST request with an abnormally long ‘content-length’ header field and then it starts injecting the form with information, one byte-sized packet at a time.
- Many more tools are available.

# Demonstration: DoS using “Slowloris script”

# Demonstration: LOIC Tool

# Demonstration: Ping of Death

# Countermeasures

- Shut down all the services until the attack has subsided.
- Install anti-virus and anti-Trojan software and keep these up-to-date.
- Increase awareness of security issues and prevention techniques.
- Disable unnecessary services, uninstall unused applications, and scan all the files received from external sources.
- Increase bandwidth on critical connections to absorb additional traffic generated by an attack.
- Replicate servers to provide additional failsafe protection.

FREE ONLINE EDUCATION
swayam
शिक्षित भारत, उन्नत भारत

NPTEL ONLINE CERTIFICATION COURSES

# Thank you!