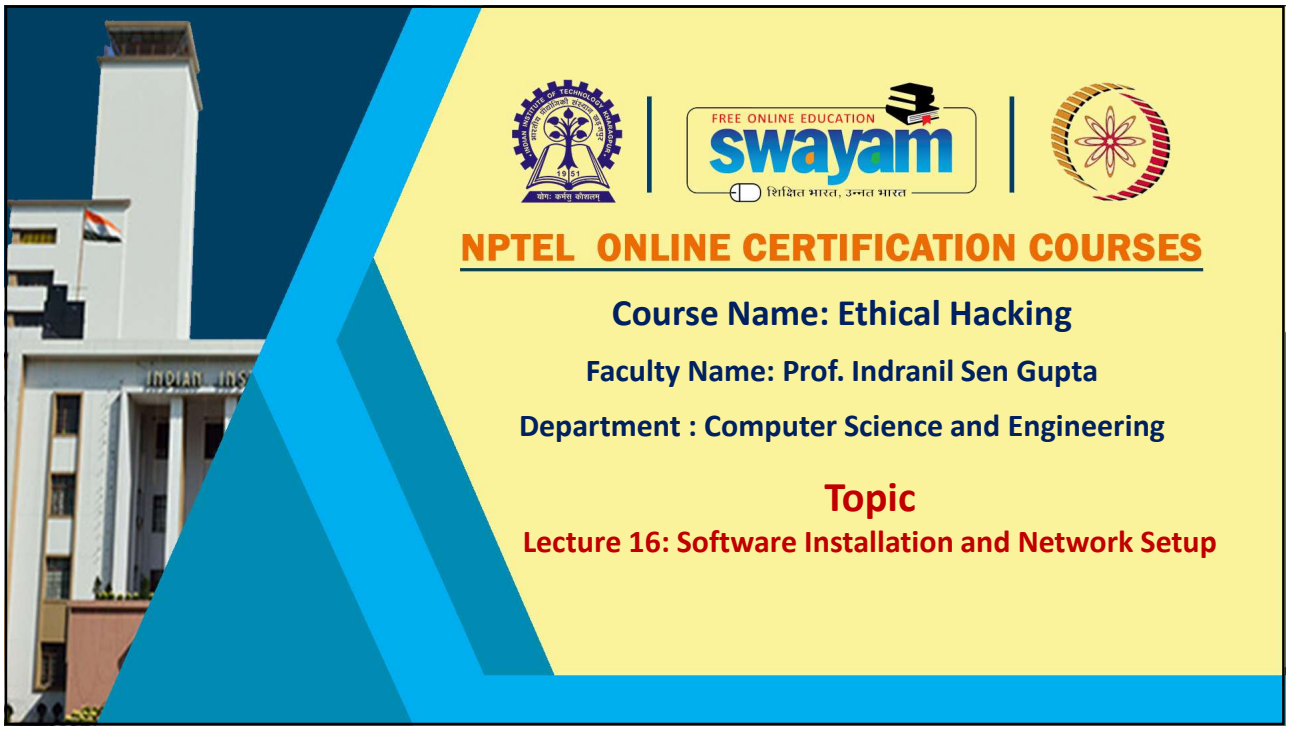
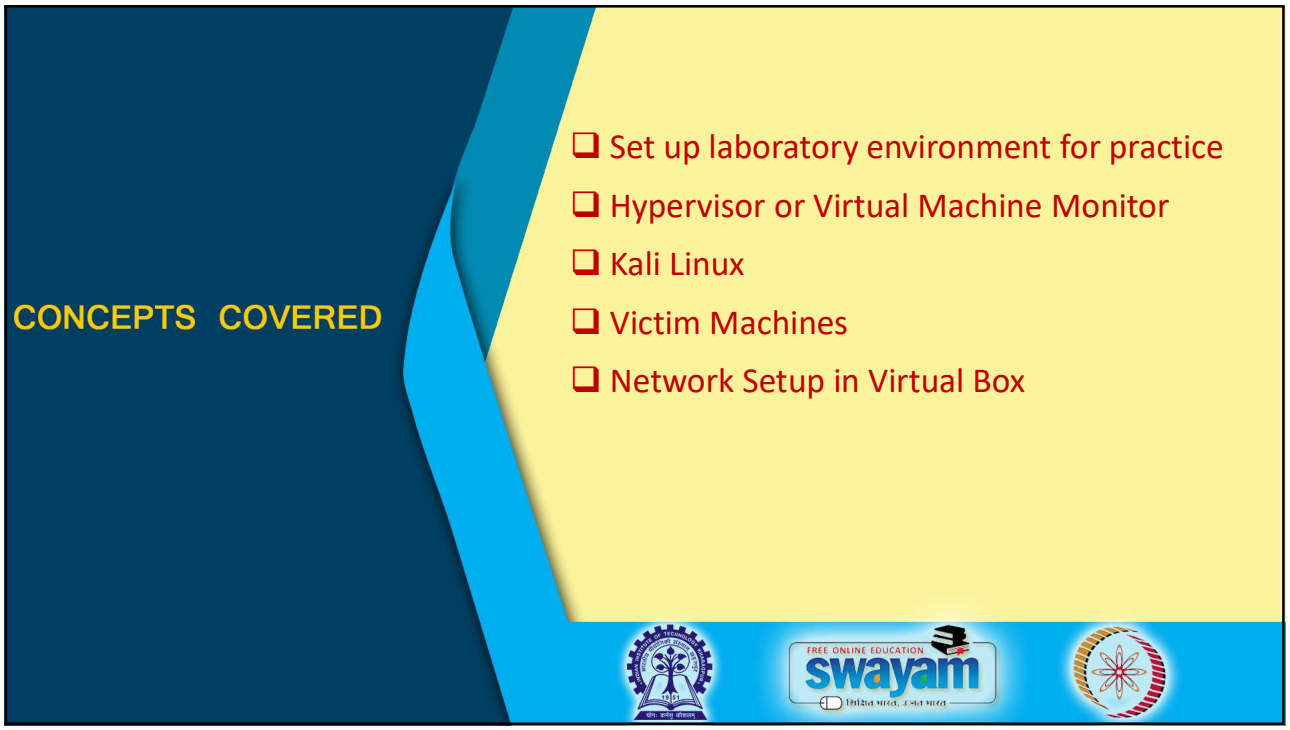

NPTEL ONLINE CERTIFICATION COURSES
Course Name: Ethical Hacking
Faculty Name: Prof. Indranil Sen Gupta
Department : Computer Science and Engineering
Topic
Lecture 16: Software Installation and Network Setup

NPTEL


CONCEPTS COVERED
Set up laboratory environment for practice
Hypervisor or Virtual Machine Monitor
Kali Linux
Victim Machines
Network Setup in Virtual Box

Laboratory Setup For Practice

- **IMPORTANT** – It is illegal to perform any kind of hacking activity on vulnerable machines on the Internet / Intranet that does not belong to you.
  - We shall perform all demonstration on the victim systems installed in virtual machine.
- **DISCLAIMER** – Learners of this course must not use any vulnerable machines available on the internet.
  - If any LEGAL action is taken against them, then NPTEL / IIT KHARAGPUR will not be responsible.
- ***NOTE:*** *Keep your system firewall turned on while practicing.*

3

Requirements for Laboratory Setup

a) **Hypervisor Software**
- VMware, VirtualBox

b) **Attacker System**
- Kali Linux ISO, Parrot Security, Backbox, etc.

c) **Victim System**
- Windows XP, Windows 7
- Metasploitable machines (Metasploitable 2 and Metasploitable 3)

4

(a) Hypervisor or Virtual Machine Monitor

- **Hypervisor** is a software that creates and runs ***virtual machines*** (VMs).
- It allows one host computer to support multiple guest VMs (different operating systems).
  - By virtually sharing its resources, viz. memory, network interface, storage and processing.
- Well-known hypervisor softwares: VMware, VirtualBox.
  - In our demonstration shall use VirtualBox.
- We shall download and install the latest version of virtual box from: https://www.virtualbox.org/wiki/Downloads

5

(b) Kali Linux

- Kali Linux is an open-source, Debian-based Linux distribution.
- It contains thousand of tools that can be used for practicing penetration testing, security research, computer forensics and reverse engineering.
- Some other OS, like Parrot Security, can also be used for same purpose. However for the beginners we recommend to use Kali Linux.
- To install Kali Linux in Virtual box, the disk image file can be downloaded from: https://www.kali.org/get-kali/#kali-bare-metal

6

(c) Victim Machines

- **Metasploitable Machines**: These are intentionally vulnerable (i.e. insecure and hackable) virtual machines designed for training, exploit testing, and general target practice.
  - **Metasploitable 2**: vulnerable Linux based virtual machine.
  - **Metasploitable 3**: vulnerable Windows based virtual machine.
- We can also install some older machines such as Windows XP for practice.

7

Network Setup in Virtual Box

- By default virtual box uses ***Network Address Translation*** (NAT).
- In NAT mode the Virtual OS is separated from outside (i.e., HOST system).
  - The virtual box itself allocates virtual IP's to systems installed inside it.
  - We can check that all OS installed in VM have the same IP address.
  - We can connect to the Internet in this mode.
- To establish connection between host as well as other systems installed inside virtual box, the best option is to enable ***Bridge Adapter*** mode.

8

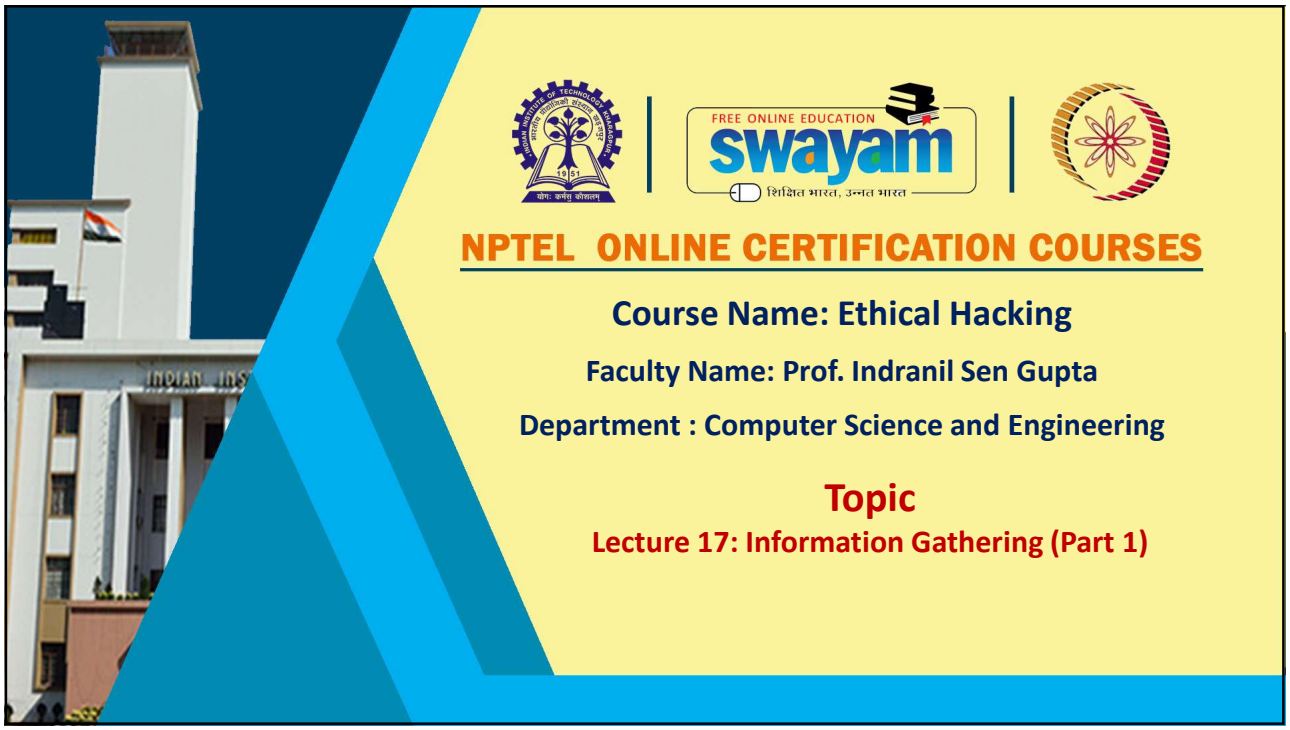
Demonstration: Installation of Attacker and Victim System and Network Setup

Alternatives

- Software setup in virtual box demands high RAM and storage.
  - Minimum 4GB RAM, 30-40 GB storage.
- If we do not have such system, then we can use Live Kali Linux.
  - Kali Linux in flash/pen drive.
- If we do not have windows system, then alternatively we can install tools available in Kali such as NMAP, Metaexploit etc. in Unix/Linux based system.


FREE ONLINE EDUCATION
swayam
NPTEL ONLINE CERTIFICATION COURSES
Thank you!
11

NPTEL


FREE ONLINE EDUCATION
swayam
NPTEL ONLINE CERTIFICATION COURSES
Course Name: Ethical Hacking
Faculty Name: Prof. Indranil Sen Gupta
Department : Computer Science and Engineering
Topic
Lecture 17: Information Gathering (Part 1)

CONCEPTS COVERED

- Reconnaissance or information gathering
- Passive and active reconnaissance
- Demonstration of passive reconnaissance

Reconnaissance (Information Gathering)

- Reconnaissance is the process of collecting as much information as possible about a target network.
  - Required for identifying ways to intrude into an organization's/victim's network system.
  - It is the first step before mounting any attack.
- We collect useful information about target PC.
  - Such as IP address, list of open ports, secure ports, vulnerability, etc.

Objectives of Reconnaissance

- Collect network information:
  - Domain name, IP addresses, internal domain name, services running (TCP, UDP).
- Collect system information:
  - User names, routing tables, system names, system architecture, password, etc.
- Collect organization information:
  - Employee details, organization names, location, contact information, security policies, etc.
- Two types of Reconnaissance:
  a) Passive reconnaissance
  b) Active reconnaissance.

15

Passive Reconnaissance

- In this type of information gathering we collect information about the target indirectly.
  - Without direct communication with the target system.
  - Collection of the data that are publically available for webpage/application.
  - We can collect information using **archive.org**, **Whois**, **Netcraft** and **Harvester** tools.
  - We can also use search engine and search operator available with search engine.

16

Active Reconnaissance

- In this type of information gathering we collect information directly by communicating with victim system.
  - Can provide more detailed information about target machine. But as we are directly communicating with target there is also risk of detection.
  - Can be carried out using Network Mapper (NMAP), Nessus, Metasploit framework, etc.
  - We can also use Mail tracker and DNS enumeration, Email enumeration, etc..

17

(a) Passive Reconnaissance: archive.org

- In **archive.org** website we can get complete history of any website like when it was last updated.
- We can go back to the particular date and observe the webpage.
- We can mirror the website which will load all the files locally, such as HTML codes, images etc. that can be used to observe the directories used.

18

(b) Passive Reconnaissance: Whois

- Whois database lookup allows us to access many useful information about target such as:
  - Registration details
  - IP address
  - Contact number and Email ID
  - Domain owner
  - Name servers
  - Regional Internet Registries

19

(c) Passive Reconnaissance: Netcraft

- Netcraft is an internet service company.
- Through Netcraft we can find the list of subdomains and operating system of the corresponding server.
- This can be useful while exploiting the system.

20

(d) Passive Reconnaissance: Search Engine and Search Operator

- Using search engine we can extract information such as platform used by organization, employee details, login pages.
  - Use various filters to restrict the search.
- We can also extract some information from search engine cache and internet archives.

21

Useful Search Operators

- **site:** We can get result from specific website.
- **cache:** We can find the most recent cache of a specified webpage.
- **intitle:** This is a narrower operator that can help us find more targeted results for specific search phrases.
- **inurl:** Finds pages on a site that has the targeted search term in the URL.
- **filetype:** Finds files that only fall under a specific file type.

22

Useful Search Operators (contd.)

- **@:** If we want the search to be restricted to only social media, then we use @ before the search key.
- **Quotes (“ ”):** Will help to get exact match result.
- Many more search operators are available.
  - We can also combine search operators to get more specific information.
  - Can be helpful for, targeted search, exclude/include specific terms/sites, site index information, etc.

23

Other Ways of Reconnaissance

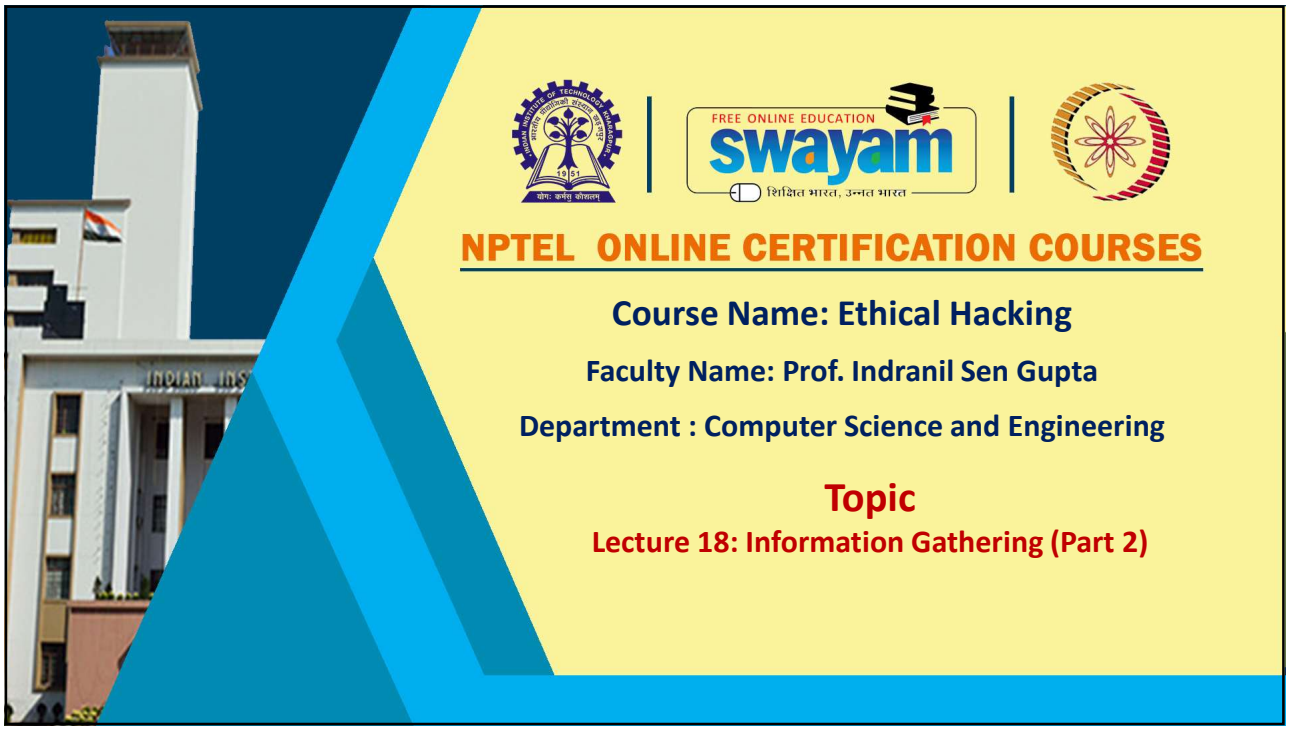
- We can register and opt for alerts to know all updates about a company /organization.
- If we are analyzing social media accounts then we can follow the targeted person / organization to get all new updates.
- We can even look into groups, forums, and blogs.
- Simple browsing of the website can identify the software, database used, etc.

24

Demonstration: Passive Reconnaissance

25

NPTEL


NPTEL ONLINE CERTIFICATION COURSES
Course Name: Ethical Hacking
Faculty Name: Prof. Indranil Sen Gupta
Department : Computer Science and Engineering
Topic
Lecture 18: Information Gathering (Part 2)

NPTEL


CONCEPTS COVERED
Approaches to active reconnaissance
Demonstration of active reconnaissance

(1) Active Reconnaissance: DNS and Mail Server Enumeration

- In the enumeration process, attacker creates active connections to system and performs directed queries to gain more information about the target.
- DNS/Mail Server enumeration is the process of locating all DNS servers and their corresponding records for an organization.
  - Can yield usernames, computer names, and IP addresses of potential target systems.
  - Can reveal the size of the organization that can translate to the potential size of the attack.
- Tools used:
  - **nslookup**, **host**, **dig**, etc.

29

Demonstration: DNS and Mail Server Enumeration

30

(2) Active Reconnaissance: Scanning

- In active reconnaissance scanning tool performs major role.
- Scanning can be used to detect:
  - Live host in a network and network infrastructure
  - Open ports
  - Service running in some particular port
  - Operating system of target machine
  - Vulnerabilities of network/application/OS/target system.
- Tools used:
  - **NMAP**, **ZenMap**, **Nessus**, **Nexpose**, etc.

31

Introduction to Network Mapper (NMAP)

- NMAP is a free, open-source tool for vulnerability scanning and network discovery.
- Generic command to run NMAP on command prompt:

```
nmap [scan types] [options] <host or network ...>
```

- The main feature of NMAP are:
  - **Host Discovery:** Which hosts are alive?
  - **Port Scanning:** What services are available?
  - **Service and Version Detection:** Which version is running?
  - **OS Detection:** Which OS version is running?

32

NMAP: Host Discovery (Live System Discovery)

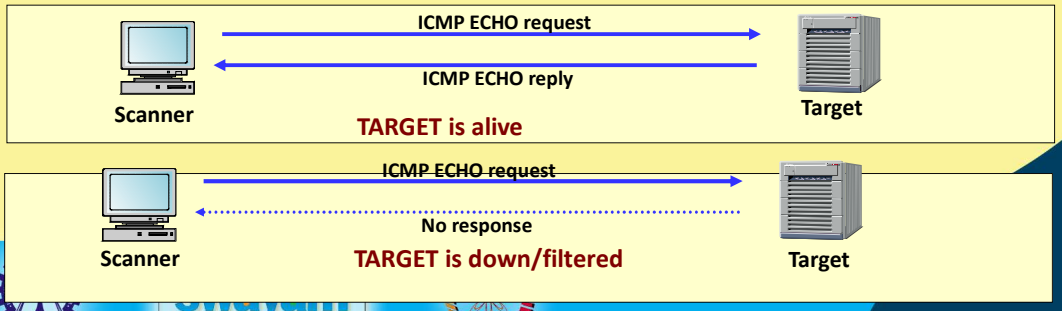
- To detect live host NMAP queries multiple hosts.
  - If it gets reply then the target/host is marked as live.
  - This is known as **ping sweep** operation.
- Various host scan techniques are supported by NMAP:
  a) ICMP sweep
  b) Broadcast ICMP
  c) Non-Echo ICMP
  d) TCP sweep
  e) UDP sweep

33

(a) Host discovery using ICMP Sweep

- How it works?
  - Send out an **ICMP ECHO request** (ICMP type 8)
  - If an **ICMP ECHO reply** (ICMP type 0) is received → ***TARGET IS ALIVE***
  - No response is received → ***TARGET IS DOWN***
  - To perform ICMP echo sweep `-PE` option is used.

- Easy to implement
- Rather slow
- Easy to block



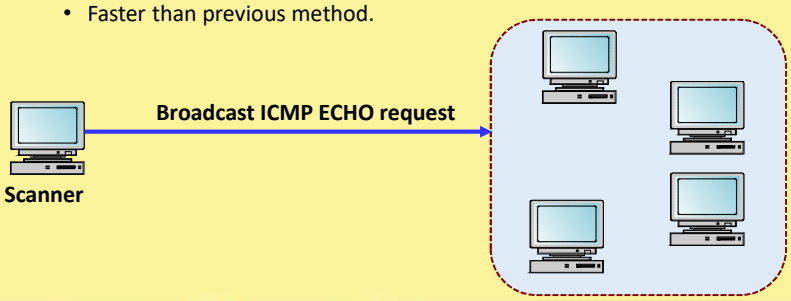
34

Demonstration: ICMP Sweep Scan

(b) Host discovery using Broadcast ICMP

- **Most routers block this.**
- **Windows ignore these requests.**

- How it works?
  - Send out an **ICMP ECHO request** to the network and/or broadcast address.
  - All the hosts in the network will simultaneously send back **ICMP ECHO reply** packets.
    - Faster than previous method.



(c) Host discovery using Non-ECHO ICMP

- How it works?
  - Instead of ICMP ECHO request, the scanner sends out other types of ICMP messages.
    - The target will respond to such messages.
  - **Approach 1**: Send ICMP type 13 messages (***TIMESTAMP***) (-PP option)
    - The scanner queries current time to the target.
  - **Approach 2**: Send ICMP type 17 messages (***ADDRESS MASK REQUEST***) (-PM option)
    - The scanner queries subnet mask to the target (this feature is used by diskless workstations during booting).

37

Demonstration: Non-Echo ICMP Sweep

38

(d) Host discovery using TCP Sweep

- How it works?
  - The scanner sends out **TCP SYN** or **TCP ACK** packet to the target.
  - It also detect open ports.
  - The port number can be suitably selected to prevent blocking by firewall.
    - Typical port numbers used: 21, 22, 23, 25, 80
- TCP sweep can be performed using two options:
  - `-PS` : for TCP SYN sweep
  - `-PA` : for TCP ACK sweep
- TCP sweep is also used by default **port scanning** options.

39

Demonstration: TCP Sweep Scan

40

(e) Host discovery using UDP Sweep

- How it works?
  - The scanner sends a UDP datagram to the target.
  - If no **ICMP PORT UNREACHABLE** message is received → ***TARGET IS ALIVE***
  - If an **ICMP PORT UNREACHABLE** message is received → ***TARGET IS DOWN***
- To perform UDP sweep **-PU** option is used.
- If the UDP port is unreachable then the port will be reported as closed.

> - **Routers can drop UDP packets as they cross the Internet.**
> - **Many UDP services do not respond.**
> - **Firewalls typically drop UDP packets (except DNS).**
> - **Not very reliable**

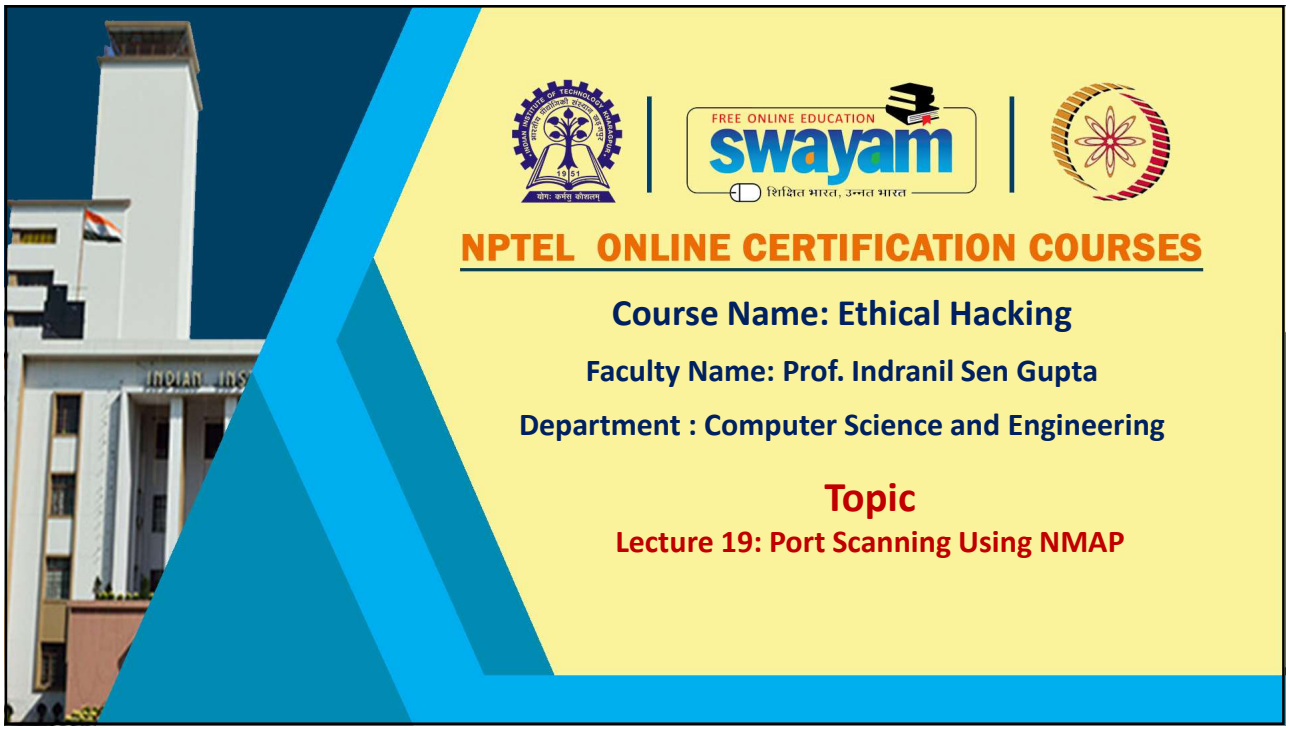
41

Demonstration: UDP Sweep Scan

42


FREE ONLINE EDUCATION
swayam
NPTEL ONLINE CERTIFICATION COURSES
Thank you!
43

NPTEL


FREE ONLINE EDUCATION
swayam
NPTEL ONLINE CERTIFICATION COURSES
Course Name: Ethical Hacking
Faculty Name: Prof. Indranil Sen Gupta
Department : Computer Science and Engineering
Topic
Lecture 19: Port Scanning Using NMAP

CONCEPTS COVERED

- TCP Connect scan
- TCP SYN scan
- TCP Stealth scan
- FTP Bounce scan

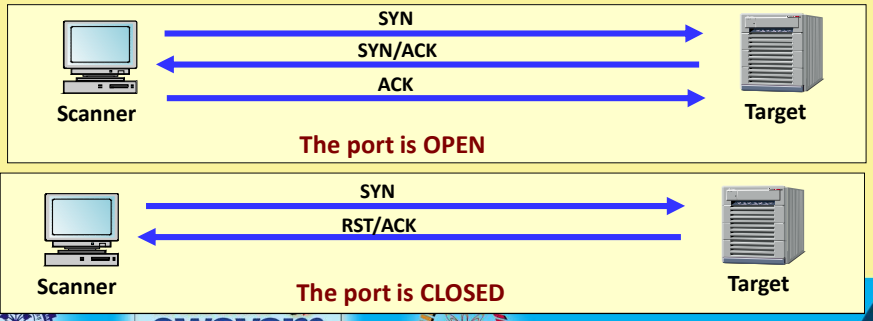
Port Scanning Using NMAP

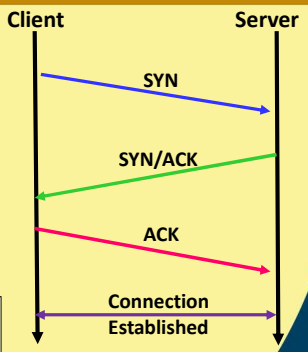
- To determine what services are running or LISTEN-ing.
  - Each running TCP service is associated with a port number, which ***listens*** for incoming connections.
  - Each running UDP service is associated with a port number.
- Various port scanning techniques in NMAP:
  a) TCP Connect scan
  b) TCP SYN scan
  c) TCP Stealth scan
  d) FTP Bounce scan

46

(a) TCP Connect scan

- How it works?
  - Use basic TCP connection establishment mechanism.
  - Complete 3-way handshake.
- Easy to detect by inspecting the system log.





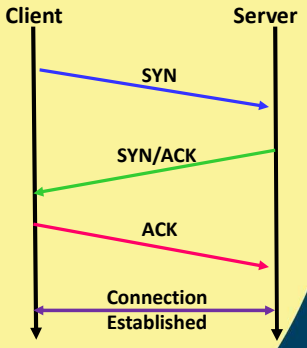
47

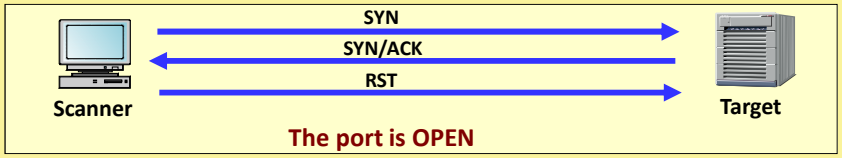
Demonstration: TCP Connect scan

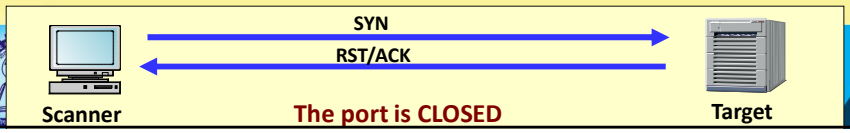
48

(b) TCP SYN scan

- How it works?
  - Do not establish complete connection (half-open scanning).
  - SYN/ACK is received → The port is ***LISTENING***
    - Immediately terminate connection by sending RST.
  - RST/ACK is received → The port is ***NON-LISTENING***
- The `-sT` scan uses both TCP SYN and TCP ACK packets.
  - It also uses ICMP ECHO sweep for checking if host is up or not.







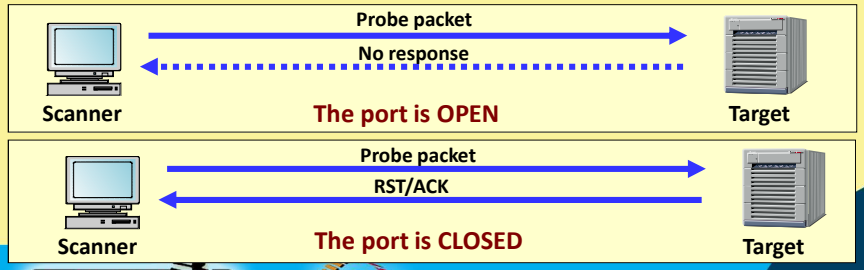
Demonstration: TCP SYN scan

(c) TCP Stealth scan

- Basic idea:
  - Carry out port scanning while avoiding detection.
  - Try to hide themselves among normal network traffic.
  - Not to be logged (stealth).
- How it works?
  - Flag probe packets (also known as *Inverse Mapping*)
    - Response is sent back only by closed port.
    - Intruder determines what services do not exist, and can infer the ones that exist.
  - Slow scan rate
    - Difficult to detect, and needs long history log.

51

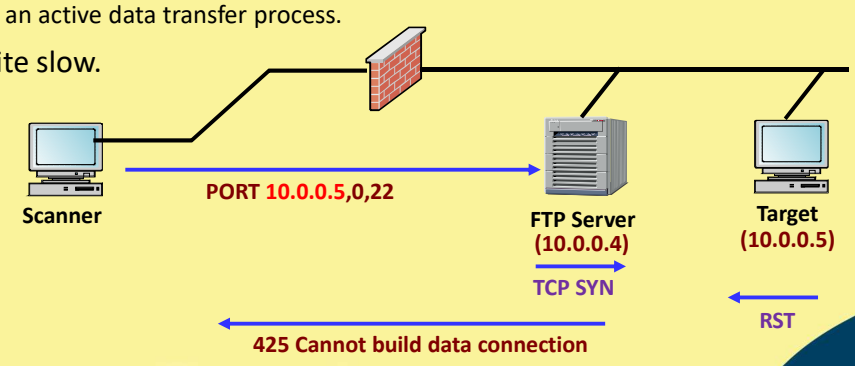
- How it can be done?
  - RFC793 talks about how to handle wrong packets.
    - Closed ports → Reply with a RESET packet
    - Open ports → Ignore any packet in question
  - Various ways:
    - Send a RST scan packet.
    - Send a FIN probe with FIN flag set.
    - Send an XMAS probe with FIN, URG, SYN, RST, PSH flags set.



52

(d) FTP Bounce scan

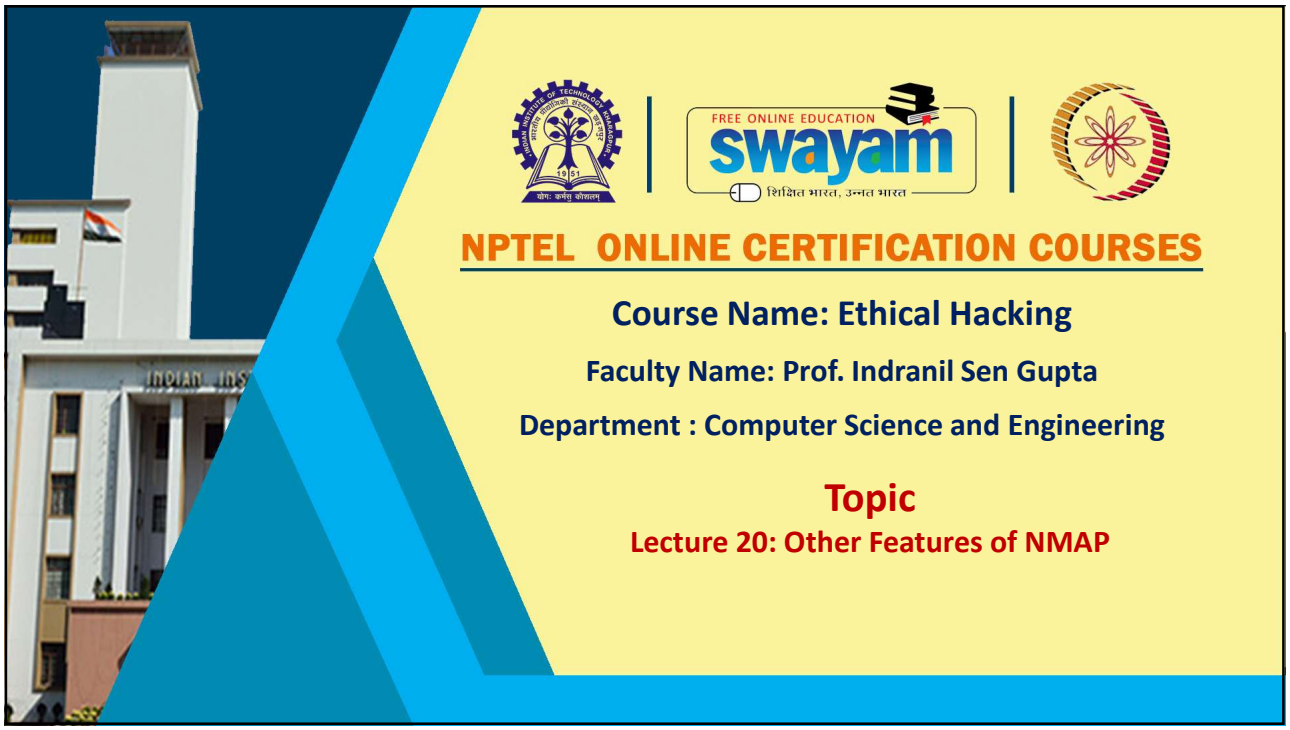
- How it works?
  - Connect to a FTP server, and establish a control connection, and ask the FTP server to initiate an active data transfer process.
- Quite slow.



Demonstration: TCP Stealth and FTP Bounce Scan


FREE ONLINE EDUCATION
swayam
NPTEL ONLINE CERTIFICATION COURSES
Thank you!
55

NPTEL


FREE ONLINE EDUCATION
swayam
NPTEL ONLINE CERTIFICATION COURSES
Course Name: Ethical Hacking
Faculty Name: Prof. Indranil Sen Gupta
Department : Computer Science and Engineering
Topic
Lecture 20: Other Features of NMAP

CONCEPTS COVERED

- Service version and OS detection
- NMAP command options for host discovery
- Some countermeasures for reconnaissance

Service Version and OS Detection

- Some OS responds with specific messages in response to certain requests.
  - Helps in identification of its type.
- TCP/IP fingerprinting (IP stack implementation will respond differently).
  - FIN probe, Bogus Flag probe
  - TCP initial sequence number sampling, TCP initial window, ACK value
  - ICMP error quenching, message quoting, ICMP echo integrity
  - IP: DF, TOS, Fragmentation

58

Some Specific Examples

- **ACK**: sending ***FIN|PSH|URG*** to a closed port
  - Most OS → ACK with the same sequence number.
  - Windows → ACK with sequence number + 1
- **Type of Service**: Probing with ***ICMP_PORT_UNREACHABLE*** message
  - Most OS → Returns with TOS = 0.
  - Linux → Returns with TOS = 0xC0.
- For detecting OS and version –o and – sV options are used.

59

More on Host Detection

- By default NMAP uses all types of sweep operations in common scanning options such that it can get better details about any system.
- Commands that use all types (except UDP sweep) are **`-sP`**, **`-sn`**, **`-sl`**, **`-Pn`**, etc.
- We will show example of **`-sP`** command.
  - This is used to print whether all or specific hosts are up and running.

60

NMAP Command Options for Host Discovery in Brief

- **sL:** List Scan - simply list targets to scan
- **-sP:** Ping Scan - go no further than determining if host is online
- **-PN:** Treat all hosts as online - skip host discovery
- **-PS/PA/PU [portlist]:** TCP SYN/ACK or UDP discovery to given ports
- **-PE/PP/PM:** ICMP echo, timestamp, and netmask request discovery probes
- **-PO [protocol list]:** IP Protocol Ping
- **-n/-R:** Never do DNS resolution/Always resolve [default: sometimes]
- **--dns-servers** <serv1[,serv2],...>: Specify custom DNS servers
- **--system-dns:** Use OS's DNS resolver
- **-sU:** UDP Scan

61

More NMAP Options for Port Scanning

- **Scan Techniques:**
  - -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  - -sN/sF/sX: TCP Null, FIN, and Xmas scans
  - -b <FTP relay host>: FTP bounce scan
- **Port specification and Scan Order:**
  - -p <port ranges>: Only scan specified ports
    - Examples: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
  - -F: Fast mode - Scan fewer ports than the default scan
  - -r: Scan ports consecutively - don't randomize
  - --top-ports <number>: Scan <number> most common ports

62

More NMAP Options for OS Detection

- **Service / Version Detection:**
  - -sV: Probe open ports to determine service/version info
  - --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  - --version-light: Limit to most likely probes (intensity 2)
  - --version-all: Try every single probe (intensity 9)
  - --version-trace: Show detailed version scan activity (for debugging)
- **OS Detection:**
  - -O: Enables OS detection
  - --osscan-limit: Limit OS detection to promising targets
  - --osscan-guess: Guess OS more aggressively

63

Demonstration: OS and Version Detection

64

Demonstration: Some more options of NMAP

Reconnaissance Countermeasures

- Some steps can be taken to prevent reconnaissance such as:
  - Do not release critical info publically.
  - Use footprint techniques to discover and remove sensitive information.
  - Use split DNS, and restrict zone transfer.
  - Disable directory listing.
  - Educate employee about various social engineering attacks.
  - Encrypt password and sensitive information
  - Keep your system updated.
  - Use server mask

Reconnaissance Countermeasures (contd.)

- Use different file extension such as use .htm instead of .asp
- Examine logs for suspicious packets
- Identify connections not properly terminated
- Analyze ports usage

67