Information Gathering

Hackers Ethics

Hands On Imperative

“Access to computers and hardware should be complete and total. It is asserted to be a categorical imperative to remove any barriers between people and the use and understanding of any technology, no matter how large, complex, dangerous, labyrinthine, proprietary, or powerful.

Information Wants to Be Free

“ Free might mean without restrictions, control and monetary value

Mistrust Authority.

“Promote decentralization”

No Bogus Criteria

“Hackers should be judged by their hacking, not by "bogus criteria" such as race, age, sex, or position”

You can create truth and beauty on a computer." Hacking is equated with artistry and creativity

Computers can change your life for the better

Hackers Ethics

Above all else, do no harm Do not damage computers or data if at all possible.

Protect Privacy

“ Free might mean without restrictions, control and monetary value

Waste not, want not." Computer resources should not lie idle and wasted

Exceed Limitations Hacking is about the continual transcendence of problem limitations

The Communicational Imperative - People have the right to communicate and associate with their peers freely.

Share! Information increases in value by sharing it with the maximum number of people; don't hoard, don't hide

Self Defense

Hacking Helps Security it is useful and courteous to find security holes, and then tell people how to fix them

Trust, but Test! You must constantly test the integrity of systems and find ways to improve them

Hackers Class

- Black Hat
  - “A person with extraordinary computing skills involved in malicious or destructive activities“
- White Hat
  - “Person possessing hackers skill using them for defensive purpose aka security analyst”
- Gray Hat
  - “Person who plays a role of black hat and white hat at various times”
- Suicide Hackers
  - “A person committed to bring down critical infrastructure without worrying to face punishments”

Hacktivism

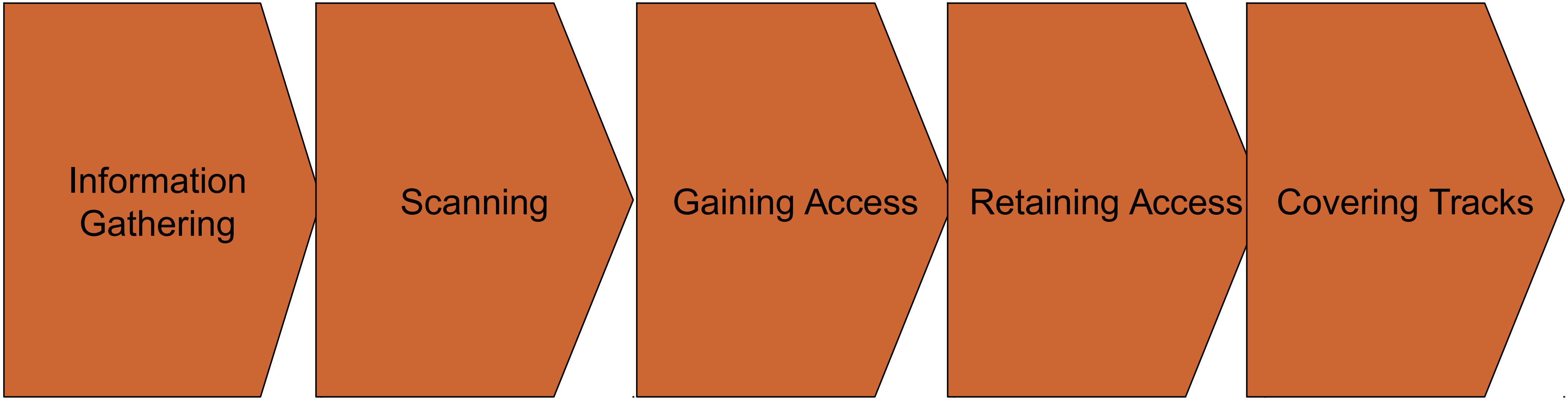
The use of computers and computer networks as a means of protest to promote political ends

hacktivist

The individual who performs an act of hacktivism

Basic Steps Of Hacking

- Information Gathering
- Scanning
- Gaining Access
- Retaining Access
- Covering Tracks



Information Gathering

Scanning

Gaining Access

Retaining Access

Covering Tracks

Information Gathering

Information Gathering

Collects information related to the target

This information can be found on the Organization's website,

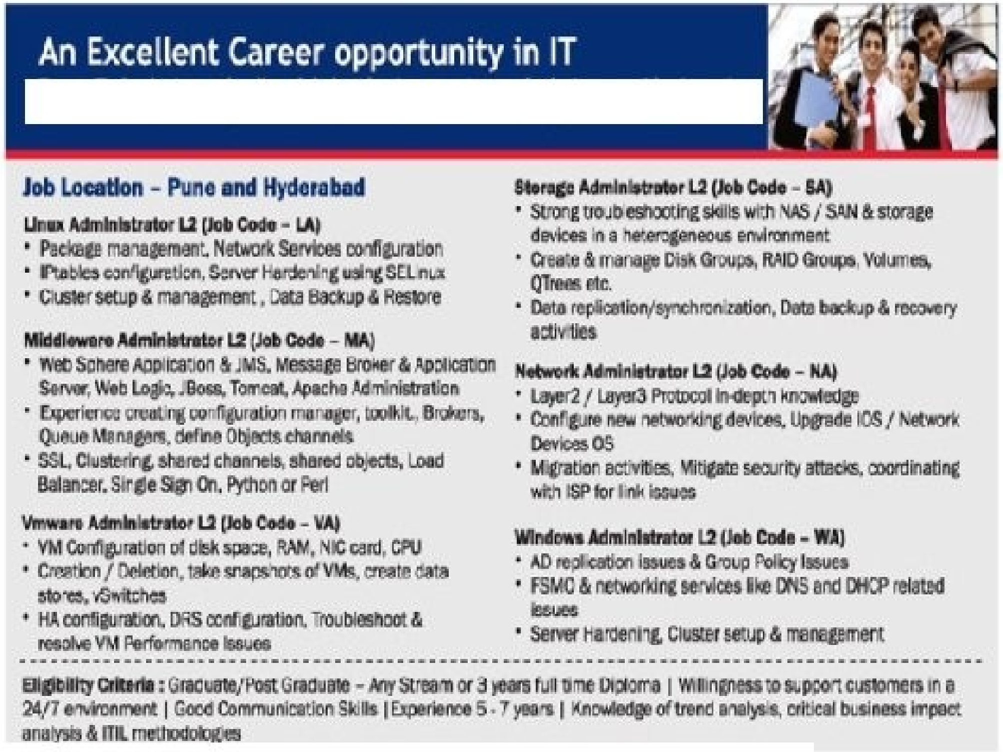
News,

Job Listing

Financial databases,

Employees

Archived Data



An Excellent Career opportunity in IT

Job Location – Pune and Hyderabad

Linux Administrator L2 (Job Code – LA)
- Package management, Network Services configuration
- IPtables configuration, Server Hardening using SELinux
- Cluster setup & management , Data Backup & Restore

Middleware Administrator L2 (Job Code – MA)
- Web Sphere Application & JMS, Message Broker & Application Server, Web Logic, JBoss, Tomcat, Apache Administration
- Experience creating configuration manager, toolkit, Brokers, Queue Managers, define Objects channels
- SSL, Clustering, shared channels, shared objects, Load Balancer, Single Sign On, Python or Perl

Vmware Administrator L2 (Job Code – VA)
- VM Configuration of disk space, RAM, NIC card, CPU
- Creation / Deletion, take snapshots of VMs, create data stores, vSwitches
- HA configuration, DRS configuration, Troubleshoot & resolve VM Performance Issues

Storage Administrator L2 (Job Code – SA)
- Strong troubleshooting skills with NAS / SAN & storage devices in a heterogeneous environment
- Create & manage Disk Groups, RAID Groups, Volumes, QTrees etc.
- Data replication/synchronization, Data backup & recovery activities

Network Administrator L2 (Job Code – NA)
- Layer2 / Layer3 Protocol In-depth knowledge
- Configure new networking devices, Upgrade IOS / Network Devices OS
- Migration activities, Mitigate security attacks, coordinating with ISP for link issues

Windows Administrator L2 (Job Code – WA)
- AD replication issues & Group Policy Issues
- FSMO & networking services like DNS and DHCP related issues
- Server Hardening, Cluster setup & management

Eligibility Criteria : Graduate/Post Graduate – Any Stream or 3 years full time Diploma | Willingness to support customers in a 24/7 environment | Good Communication Skills | Experience 5 - 7 years | Knowledge of trend analysis, critical business impact analysis & ITIL methodologies

Footprinting

Footprinting is the act of gathering information about a computer system and the companies it belongs to

Used to determine organizations' high-value Targets

Helps to minimize the chance of detection

Assessing where to spend the most time and effort.

Reconnaissance

“ military observation of a region to locate an enemy or ascertain strategic features.”

- In Hacking , Reconnaissance is the phase for the attacker to collect and gather as much information as possible about the target of evaluation prior to launching an attack

Reconnaissance

Types of Reconnaissance

Passive

Passive reconnaissance involves acquiring information without directly interacting with the target

eg. search public records, news

Active

Active reconnaissance involves interacting with the target directly by any means

Telephone, email etc.

Tools for Reconnaissance

- DNS
  - nslookup
  - Whois
  - Dig

- Trace route
  - Traceroute
  - Visualroutetrace

  - Google Hacks

Whois

Whois is a query/response protocol that is widely used for querying database in order to determine the registrant or assignee of internet resources, such as a domain name, an IP address block or an autonomus system number.

Whois References

- ARIN: http://ws.arin.net/whois
- RIPE NCC: http://www.ripe.net/whois/
- APNIC: http://whois.apnic.net
- LACNIC: http://whois.lacnic.net
- AfriNIC: http://whois.afrinic.net
- www.whois.org

Traceroute

Traceroute is a network tool which shows the path taken by the packet to reach its destination. It works by using the TTL field of the IP Protocol

- Used for network troubleshooting .
- Used for information gathering of the network architecture.

ping

Program used to verify that a particular IP address exists and can accept requests

Google Hacks

Google hacking is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use.

Google Hacks

Domain Search

site:gov secret
site:bangalore.in
site:in

Directory Listing

intitile:index.of
intitile:index,of name size
site:in

Versioning

intitle:index.of server.at
intitle:index.of server.at site:cdacbangalore.in

Google Hacks

Hacks
inurl:phphotoalbum/upload
inurl:”viewerframe?mode=motion”
inurl:/view.shtml
inurl:axis-cgi/jpg
intitle:”live view/-axis”
filetype:reg intext:”account manager”
filetype:sql ”IDENTIFIED BY”
filetype:inc dbconn

lot of google hacking keywords can be referred from google hacking database (GHDB).

Social Engineering

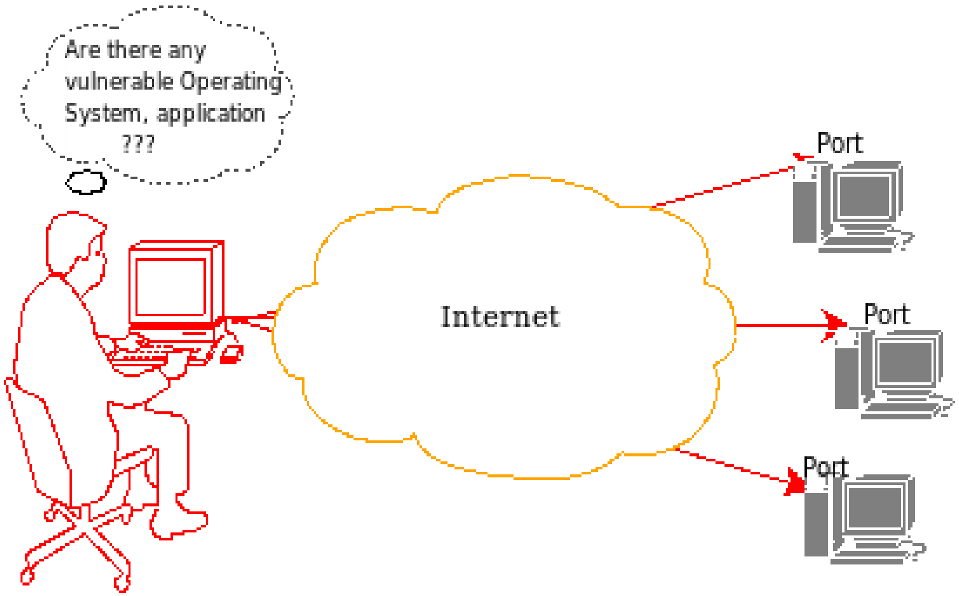
- Victim is tricked to reveal confidential information
- A non technical attack
- Still more dangerous and powerful from most of the complex technical attacks.
- Does not require technical skills

Scanning

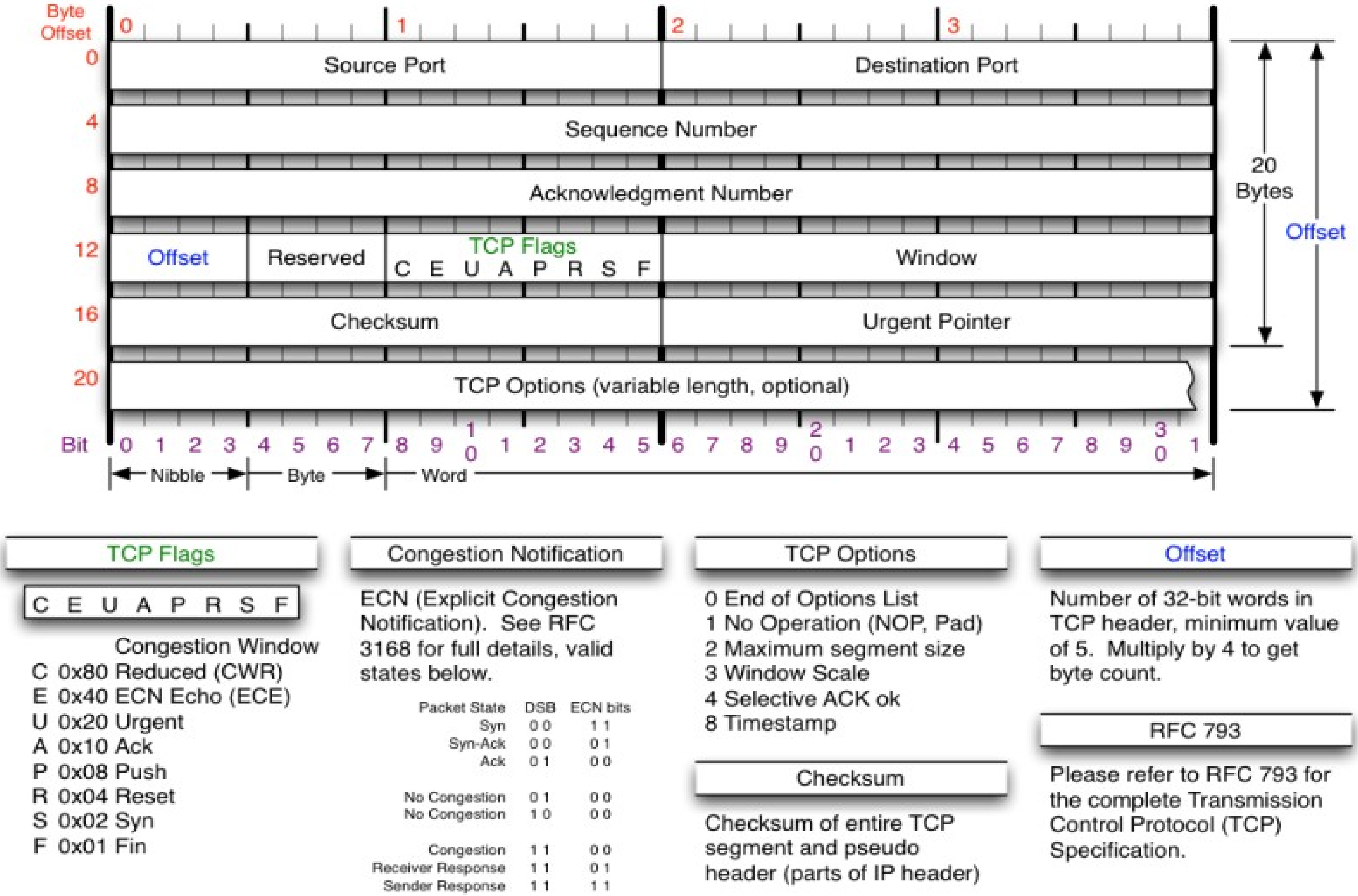
Scanning

- scanning refers to the pre-attack phase when the hacker scans the network for specific information on the basis of information gathered during reconnaissance

- Scanning includes
  - Port scanners
  - Network mapping
  - Vulnerability scanners
  - etc.



TCP Flags



TCP Flags

C E U A P R S F

Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

Offset

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

Types & Tools of Scanning

Once a hacker knows all the services running on your server, he could search for possible vulnerabilities they may have and exploit them to take control of the website

Types & Tools of Scanning

- Port scans
- OS fingerprinting
- Version scans
- Vulnerability scans

Tools

- Nmap
- Nessus / openVAS
- Nikto / w3af

Nmap port scanning states

Open

An application is actively accepting connections this port

- Closed

port is accessible (it receives and responds to probe packets), but there is no application listening on it

- Filtered

cannot determine whether the port is open because packet filtering prevents its probes from reaching the port

Nmap port scanning states

Unfiltered

port is accessible, butunable to determine whether it is open or closed

- open|filtered

  unable to determine whether a port is open or filtered

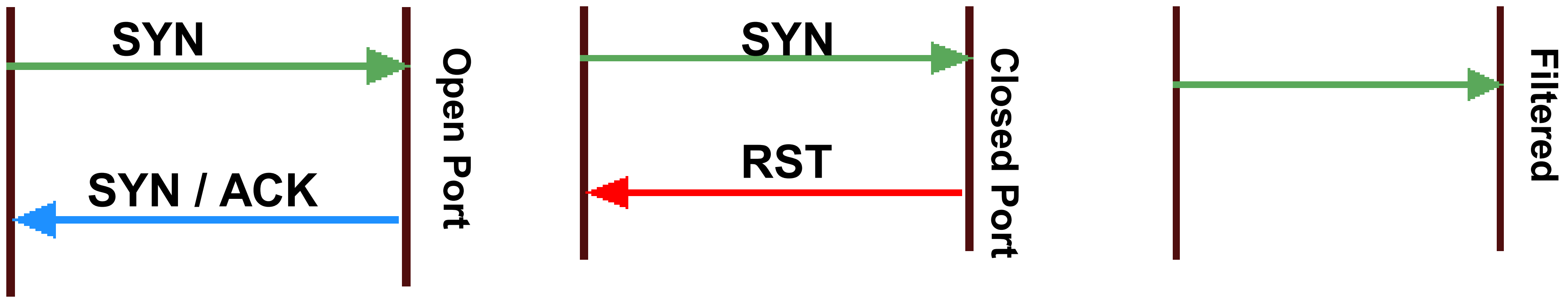
- closed|Filtered

  unable to determine whether a port is closed or filtered

Nmap port scan options

SYN Scan

- half-open scanning
- Works against any compliant TCP stack



Nmap port scan options

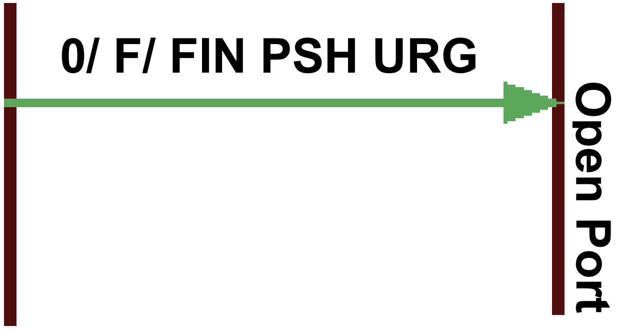
Connect Scan

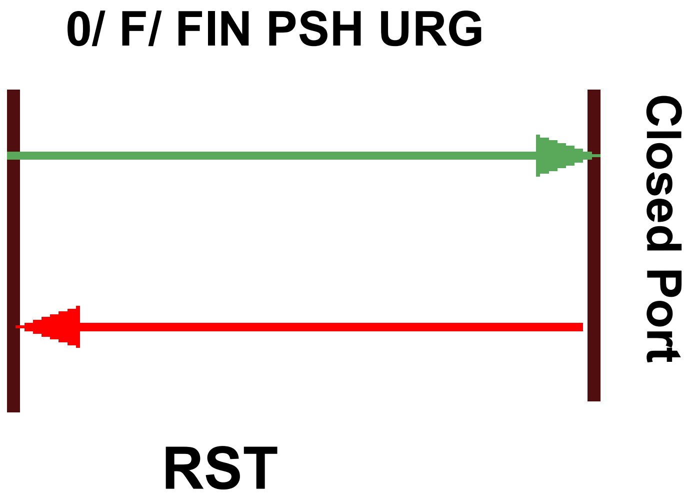
The system call completes connections to open target ports rather than performing the half-open reset that SYN scan does

Nmap port scan options

NULL, FIN, and Xmas scans

- RFC says “if the [destination] port state is CLOSED .... an incoming segment not containing a RST causes a RST to be sent in response”



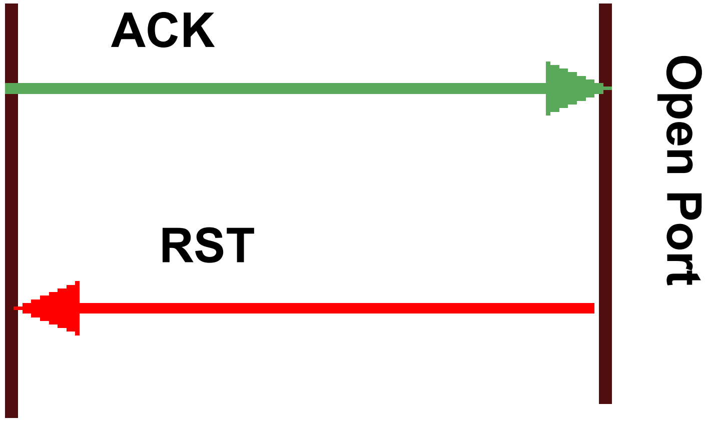


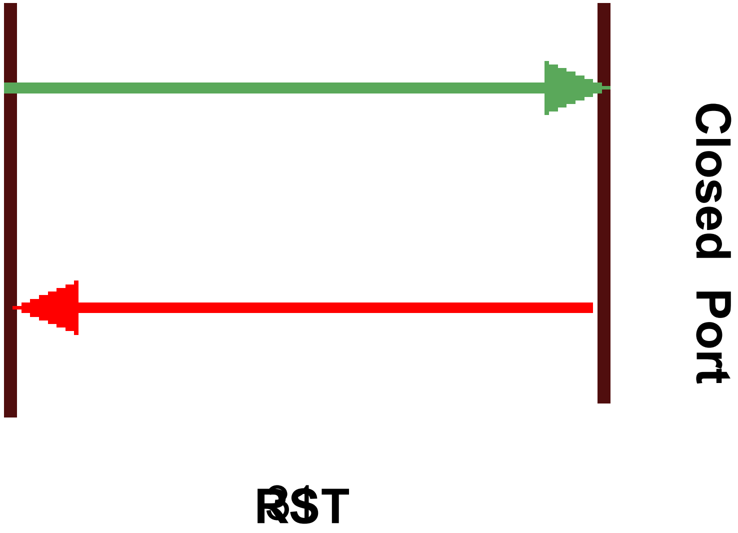
Nmap port scan options

ACK Scan

it never determines open (or even open|filtered) ports.

- used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.



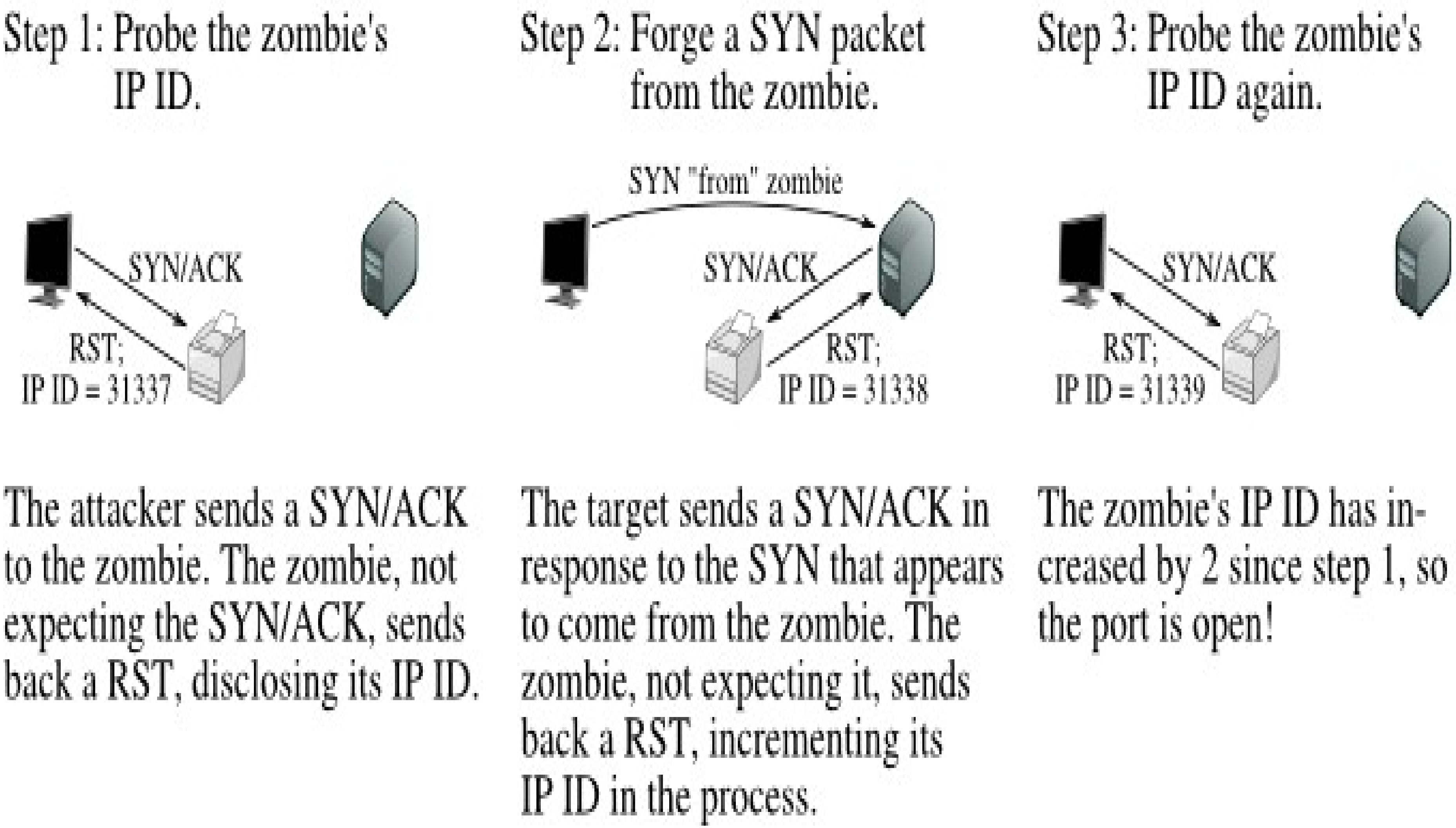


Idle Scan

Attackers can actually scan a target without sending a single packet to the target from their own IP address

- side-channel attack allows for the scan to be bounced off a dumb “zombie host”
- Every IP packet on the Internet has a fragment identification number (IP ID).
- many operating systems simply increment this number for each packet they send, probing for the IPID can tell an attacker how many packets have been sent since the last probe.

Idle Scan – open port



Step 1: Probe the zombie's IP ID.

Step 2: Forge a SYN packet from the zombie.

Step 3: Probe the zombie's IP ID again.

The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID.

The target sends a SYN/ACK in response to the SYN that appears to come from the zombie. The zombie, not expecting it, sends back a RST, incrementing its IP ID in the process.

The zombie's IP ID has increased by 2 since step 1, so the port is open!

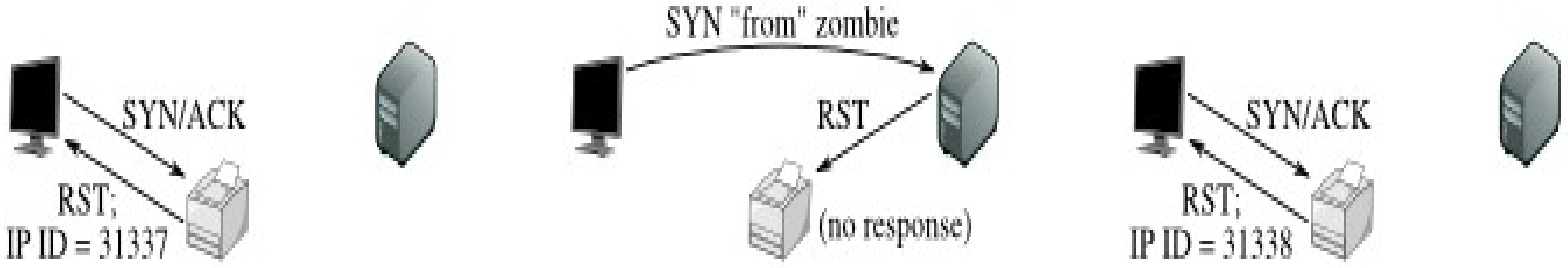
Reference : http://nmap.org

Idle Scan – closed port

Step 1: Probe the zombie's IP ID.

Step 2: Forge a SYN packet from the zombie.

Step 3: Probe the zombie's IP ID again.



The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID. This step is always the same.

The target sends a RST (the port is closed) in response to the SYN that appears to come from the zombie. The zombie ignores the unsolicited RST, leaving its IP ID unchanged.

The zombie's IP ID has increased by only 1 since step 1, so the port is not open.

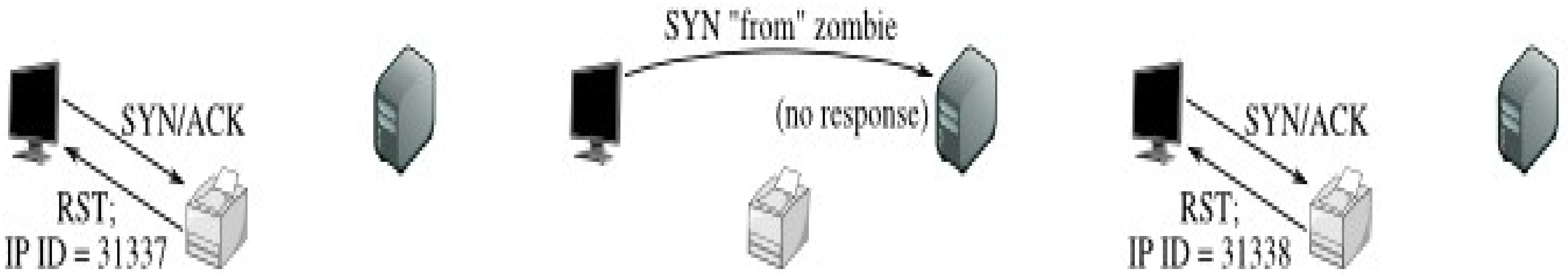
Reference : http://nmap.org

Idle Scan – filtered port

Step 1: Probe the zombie's IP ID.

Step 2: Forge a SYN packet from the zombie.

Step 3: Probe the zombie's IP ID again.



Just as in the other two cases, the attacker sends a SYN/ACK to the zombie. The zombie discloses its IP ID.

The target, obstinately filtering its port, ignores the SYN that appears to come from the zombie. The zombie, unaware that anything has happened, does not increment its IP ID.

The zombie's IP ID has increased by only 1 since step 1, so the port is not open. From the attacker's point of view this filtered port is indistinguishable from a closed port.

Reference : http://nmap.org

Enumeration

The process of probing the identified services for known weaknesses

Provides

- User account names
- Misconfigured shared resources
- Older software version with known vulnerabilities

OS Detection Techniques

Stack Finger Printing

Banner grabing

Stack Fingerprinting

- Vendors uses RFC guidence for implementation

of TCP/IP stacks

- Implementation of the TCP/IP stack varies with vendors
- Probing these differences may reveal OS
- For better accuracy of Stack fingerprinting , at least one listening port is required

Active Stack Fingerprinting

- Types of Probe used are
  - FIN probe to an open port
    - No Response
    - FIN/ACK
  - Initial Sequence Number Sampling
  - Initial Window size
  - ACK value
    - Seq
    - Seq + 1

Passive Stack Fingerprinting

- Passively monitor network traffic to detect the OS
- Parameters
  - TTL
  - Window Size
  - Don't Fragment bit

Banner Grabbing

Banner

- The text that is embedded with a message that is received from a host.
- Usually this text includes signatures of applications that issue the message.

Banner Grabbing is an enumeration technique used to gain information about computer systems on a network and the services running its open ports

Banner Grabbing

Tools used

- Telnet
- Netcat

- Shodan Search engine

Application and Version Identification

Nessus

Banner grabing

Vulnerability Research

- To identify and correct network vulnerabilities.
- To protect the network from being attacked by intruders.
- To get information that help to prevent security problems.
- To know how to recover from network attacks.

Vulnerability Research - CVE

Common Vulnerabilities and Exposures, CVE, is a public dictionary of common identifiers for publicly known information security vulnerabilities.

CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

Vulnerability Research - CVE

- One name for one vulnerability or exposure
- One standardized description for each vulnerability or exposure
- A dictionary rather than a database
- The way to interoperability and better security coverage
- A basis for evaluation among tools and databases
- Free for public download and use

Vulnerability Research - Bugtraq

- Bugtraq is an electronic mailing list dedicated to issues about computer security.
- On-topic issues are new discussions about vulnerabilities, vendor security-related announcements, methods of exploitation, and how to fix them.

Vulnerability Research Web Sites

http://makingsecuritymeasurable.mitre.org/

http://projects.webappsec.org

http://www.exploit-db.com/

- www.securitytracker.com
- www.microsoft.com/security
- www.securiteam.com
- www.packetstormsecurity.com
- www.hackerstrom.com
- www.hackerwatch.org
- www.securityfocus.com
- www.securitymagazine.com