Hacking

ICT 3156

Basics

- What is hacking?
- Classification of Hackers
- Types of hacking
- Ethical Hacking
- Common Security Vulnerabilities
- Various Types of Hacking attacks

What is Hacking?

- Hacking is the practice of modifying the features of a system, in order to accomplish a goal outside of the creator's original purpose.
- Hacking is simply finding an alternative or unintended use of computer hardware or software, so as to enhance their applications and solve problems.
- Hacking is using the technology available in new and counterintuitive ways in order to solve problems that conventional techniques cannot.
- In the current digital age, hacking has become synonymous with bypassing security, illegally accessing another person’s computer, and wrecking havoc.

History of Hacking

- When did hacking start?
- 1870s: Bell Telephone Company switchboard operators.
- 1950s: Term was coined by MIT model train enthusiasts.
- 1970s: Phreakers
- 1980s:Malign purpose.

Classifications of Hacker

- White Hat Hacker
- Black Hat Hacker
- Grey Hat Hacker
- Blue Hat Hacker
- Elite Hacker
- Script kiddie
- Neophyte “newbie”
- Hacktivist
- Nation state
- Organized criminal gangs
- Bots

Classifications of Hacker

- **White Hat Hacker**
  - An ethical hacker, or a computer security expert, is one who specializes in penetration testing and in other testing methodologies to ensure the security of an organization's information systems.
  - They hack into a system with prior permission to find out vulnerabilities so that they can be fixed before a person with malicious intent finds them.
  - White-hat hackers are also called penetration tester, sneakers, red teams, or tiger teams.
- The general view is that, while hackers build things, crackers break things.

Classifications of Hacker

- **Black Hat Hacker**
  - An individual with extensive computer knowledge whose purpose is to breach or bypass internet security. Also known as crackers or dark-side hackers.
  - They are computer security hackers that break into computers and networks or also create computer viruses. Black hat hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network.
  - They choose their targets using a two-pronged process known as the "pre-hacking stage".
  - Step 1: Targeting
  - Step 2: Research and Information Gathering
  - Step 3: Finishing the Attack

Classifications of Hacker

- **Grey Hat Hacker**
  - A grey hat hacker is a combination of a black hat and a white hat hacker. It may relate to whether they sometimes arguably act illegally, though in good will, or to show how they disclose vulnerabilities.
  - They usually do not hack for personal gain or have malicious intentions but may be prepared to technically commit crimes during their technological exploits in order to achieve better security.
- **Blue Hat Hacker**
  - A blue hat hacker is someone outside computer security consulting firms who is used to bug test a system prior to its launch, looking for exploits so they can be closed.
  - Microsoft also uses the term Blue Hat to represent a series of security briefing events.

Classifications of Hacker

- **Elite Hacker**
  - Used to describe the most skilled. Newly discovered activities will circulate among these hackers
- **Script kiddie**
  - A script kiddie (or skiddie) is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept.
- **Neophyte “newbie”**
  - A neophyte, "noob", or "newbie" is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology, and hacking.

Classifications of Hacker

- **Hacktivist**
  - A hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks.
- **Nation state**
  - Refers to Intelligence agencies and cyber warfare operatives of nation states.
- **Organized criminal gangs**
  - Criminal activity carried on for profit.
- **Bots**
  - Automated software tools, some freeware, available for the use of any type of hacker.

Different Types of Hacking

- Website Hacking

  Taking unauthorized control over a web server and its associated software such as databases and other interfaces.

- Network Hacking

  Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.

Different Types of Hacking

- Email Hacking

  This includes gaining unauthorized access to an Email account and using it without taking the consent of its owner for sending out spam links, third-party threats, and other such harmful activities.

- Password Hacking

  This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.

- Computer Hacking

  This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

Ethical Hacking

- Computer experts are often hired by companies to hack into their system to find vulnerabilities and weak endpoints so that they can be fixed.
- This is done as a precautionary measure against legitimate hackers who have malicious intent.
- Such people, who hack into a system **with permission**, without any malicious intent, are known as **ethical hackers** and the process is known as **ethical hacking.**

Phases of Ethical Hacking

Reconnaissance

- The process of information gathering.
- In this phase, the hacker gathers relevant information regarding the target system.

  These include detecting services, operating systems, packet-hops to reach the system, IP configuration etc.
- Various tools are used for reconnaissance purposes

Scanning

- In the scanning phase, the hacker begins to actively probe the target machine or network for vulnerabilities that can be exploited.
- Tools are widely used by hackers in this process.

Gaining Access

- In this phase, the vulnerability located during scanning is exploited using various methods and the hacker tries to enter the target system without raising any alarms.
- The primary tool that is used in this process is Metasploit.

Phases of Ethical Hacking

Maintaining Access

- This is one of the most integral phases.
- In this phase, the hacker installs various backdoors and payloads onto the target system
- Backdoors help the hacker gaining quicker access onto the target system in the future.

Clearing Tracks

- This process is an unethical activity.
- It has to do with the deletion of logs of all the activities that take place during the hacking process.

Do Ethical Hackers need to perform this? Why?

Reporting

- Here the Ethical Hacker compiles a report with findings and the job that was done such as the tools used, the success rate, vulnerabilities found, and the exploit processes.

Common Security Vulnerabilities

- Some of the most common security vulnerabilities that ethical hackers will have to work with and eventually keep an eye on:
  - Network Infrastructure Attacks
  - Non-Technical Attacks
  - Attacks on an Operating System
  - Attacks on Applications

Network Infrastructure Attacks

- Refer to hacks that break into local networks as well as on the Internet.
- One way to hack into a network is to connect a modem to a local network. The modem should be connected to a computer that is behind the network's firewall.
- Another method of breaking into a network is via NetBIOS, TCP/IP, and other transport mechanisms within a network. Some tricks include creating a denial of service by flooding the network with a huge load of requests.
- Network analyzers capture data packets that travel across a network. The information they capture is then analyzed and the information in them is revealed.
- Another example of a common network infrastructure hack is when people piggyback on WiFi networks that aren't secured.

Non-Technical Attacks

- Non-technical attacks basically involve manipulating people into divulging their passwords, willingly or not. **Social Engineering**
- Simply walking into another person's room where the computer is, booting the computer, and then gathering all the information that you need.

Attacks on an Operating System

- Operating system attacks are one of the more frequent hacks performed per quota.
- There are a lot of loopholes in many operating systems – even the newest ones around still have a few bugs that can be exploited.
- One of the avenues for operating system attacks is password hacking or hacking into encryption mechanisms.

Attacks on Applications

- Apps, especially the ones online and the ones that deal with connectivity, get a lot of attacks.
- Spam mail can carry pretty much anything that can hack into your computer system.
- Malware or malicious software is also another tool in the hands of a hacker when they try to attack pretty much everything, especially apps.
- Another set of applications that get attacked frequently are SMTP applications and HTTP applications.

Various Types of Hacking **Attacks**

- Active attacks

  An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.

- Passive attacks

  A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target.

Types of Active attacks

- Masquerade Attack

  The intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized for.

  A masquerade may be attempted using stolen login IDs and passwords, through finding security gaps in programs or through bypassing the authentication mechanism.

- Session Replay Attack

  A hacker steals an authorized user's log in information by stealing the session ID. The intruder gains access and the ability to do anything the authorized user can do on the website.

Types of Active attacks

- Message Modification Attack

  An intruder alters packet header addresses to direct a message to a different destination or modify the data on a target machine.

- Denial of Service (DoS) attack

  Users are deprived of access to a network or web resource. This is generally accomplished by overwhelming the target with more traffic than it can handle.

- Distributed Denial-of-Service (DDoS) exploit

  Large numbers of compromised systems (sometimes called a botnet or zombie army) attack a single target.

Passive Attacks

- Passive attacks include active reconnaissance and passive reconnaissance.
- In passive reconnaissance, an intruder monitors systems for vulnerabilities without interaction, through methods like session capture.
- In active reconnaissance, the intruder engages with the target system through methods like port scans.

Methods of passive attacks

- War driving
  - Detects vulnerable Wi-Fi networks by scanning them from nearby locations with a portable antenna.
  - The attack is typically carried out from a moving vehicle, sometimes with GPS systems that hackers use to plot out areas with vulnerabilities on a map.
  - Can be done just to steal an Internet connection or as a preliminary activity for a future attack.
- Dumpster diving
  - Intruders look for information stored on discarded computers and other devices or even passwords in trash bins.
  - The intruders can then use this information to facilitate covert entry to a network or system.
- An intruder might masquerade as an authorized network user and spy without interaction. With that access, an intruder might monitor network traffic by setting the network adapter to promiscuous mode.

Phishing

- Phishing is a method of trying to gather personal information using deceptive e-mails and websites.
- Typically, the messages appear to come from well-known and trustworthy Web sites. Web sites that are frequently spoofed by phishers include PayPal, eBay, MSN, Yahoo, BestBuy, and America Online.
- What really distinguishes phishing is the form the message takes: the attackers masquerade as a trusted entity of some kind.
- Nearly a third of all breaches in the past year involved phishing, according to the 2019 Verizon Data Breach Investigations Report. For cyber-espionage attacks, that number jumps to 78%.

Purpose of Phishing

- Hand over sensitive information.
- Download malware.
  - Often the messages are "soft targeted" .

Phishing Types

- Spear phishing
  - When attackers try to craft a message to appeal to a specific individual, that's called spear phishing.
- Whaling
  - Whale phishing, or whaling, is a form of spear phishing aimed at the very big fish.
- Vishing
- Clone phishing
- DNS-Based Phishing/ Pharming
- Search Engine Phishing
- And many more.

Signs you May have Received a Phishing Email

- Unofficial "From" address
- Urgent action required
- Generic greeting
- Link to a fake web site
- Legitimate links mixed with fake links

Points of caution

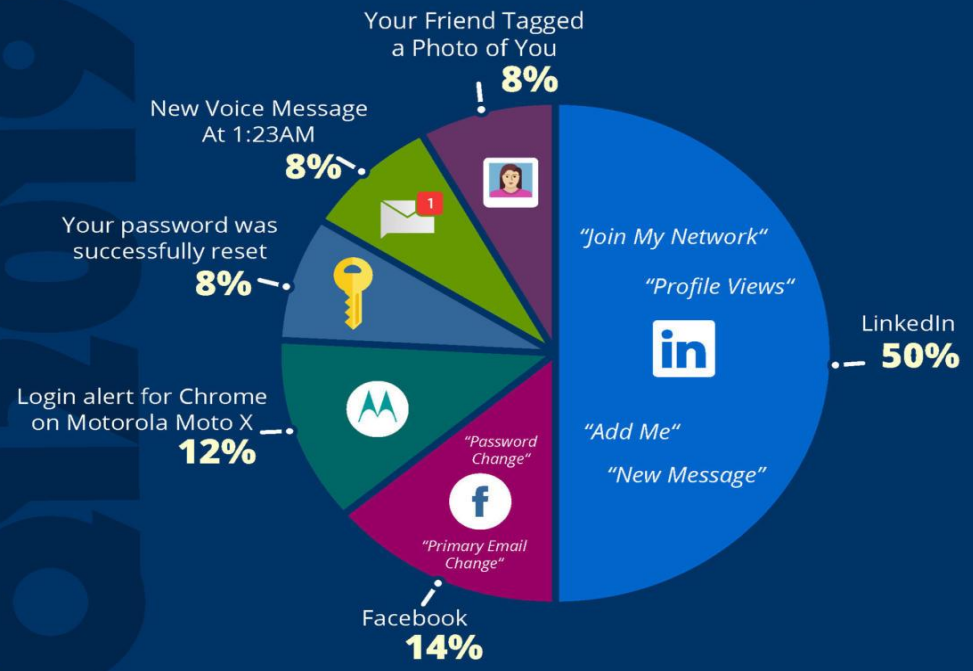
- Check the Web address: spelling and URL redirects.
- Be cautious of pop-ups.
- Give a fake password.
- Use a Web browser with anti-phishing detection.
- Be wary of other methods to identify a legitimate site.
- If you receive an email from a source you know but it seems suspicious, contact that source with a new email, rather than just hitting reply.
- Don't post personal data, like your birthday, vacation plans, or your address or phone number, publicly on social media.

Phishing Webinar by Cyren

KnowBe4
Human error. Conquered.

TOP-CLICKED PHISHING TESTS

TOP SOCIAL MEDIA EMAIL SUBJECTS



KEY TAKEAWAY

LinkedIn messages continue to dominate the top social media email subjects, with several variations of messages such as "new message" or "add me." Other alerts containing security-related warnings come unexpectedly and can cause feelings of alarm. Messages such as new message or a friend tagged a photo of you can make someone feel special and entice them to click.

TOP 10 GENERAL EMAIL SUBJECTS

De-activation of [[email]] in Process	20%
A Delivery Attempt was made	13%
You Have A New Voicemail	11%
Failed Delivery for Package #5357343	9%
Staff Review 2018	8%
Revised Vacation & Sick Time Policy	8%
APD Notification	8%
Your Order with Amazon.com	8%
Re: w-2	8%
Scanned image from MX2310U@[[domain]]	7%

KEY TAKEAWAY

Hackers are playing into employees' emotions, causing them to panic when they see a de-activation of [email] in process. Their curiosity is piqued with delivery attempt messages and orders from Amazon. And who can resist HR-related messages that could potentially affect the daily work of employees?

COMMON *"IN THE WILD"* ATTACKS

- Wells Fargo: You have a new secure mail
- Undelivered Mail
- Etrade: Action Required!
- Microsoft Teams: Rick sent a message
- Microsoft/Office 365: Action required: Update your payment information now
- Stripe: Just now someone logged in to your account
- HR: Your Action Required
- Amazon: Refund Notification
- OneDrive: Your OneDrive is out of storage space
- HR: Download your W2 now

KEY TAKEAWAY

The common theme we see here is the push for action required. One message even has an exclamation point, which emphasizes the urgency of the message. These types of attacks are effective because they cause a person to react before thinking logically about the legitimacy of the email.

KnowBe4 Human error. Conquered. SECURITY AWARENESS TRAINING | www.KNOWBE4.com

Brute Force Attack

- A brute force attack involves ‘guessing’ username and passwords to gain unauthorized access to a system.
- Brute force is a simple attack method and has a high success rate.
- Some attackers use applications and scripts as brute force tools.
- In other cases, attackers try to access web applications by searching for the right session ID.

Types of Brute Force Attacks

- Simple brute force attack
- Hybrid brute force attacks
  - Starts from external logic to determine which password variation may be most likely to succeed, and then continues with the simple approach to try many possible variations.
- Dictionary attacks
- Rainbow table attacks
- Reverse brute force attack
  - Uses a common password or collection of passwords against many possible usernames. Targets a network of users for which the attackers have previously obtained data.
- Credential stuffing
  - Uses previously-known password-username pairs, trying them against multiple websites. Exploits the fact that many users have the same username and password across different systems.

How to Prevent Brute Force Password Hacking

- **Very strong passwords!!**
- Two-factor authentication
- Lockout policy
- Progressive delays
- Captcha
- Defensive Tools: Php-Brute-Force-Attack Detector

Denial of Service

- Denial-of-Service, or DoS, attack is an attempt to defeat availability, the third of **the three basic properties** to be preserved in computer security.
- Confidentiality and integrity tend to be binary. Availability?
- How can DOS be inconvenient or dangerous?
- The source of a denial-of-service attack is typically difficult or impossible to determine with certainty.

How Service Is Denied?

- DOS can occur from excessive volume, a failed application, a severed link, or hardware or software failure.
- The three root threats to availability:
    - Insufficient capacity; overload.
    - Blocked access.
    - Unresponsive component.

Flooding attack

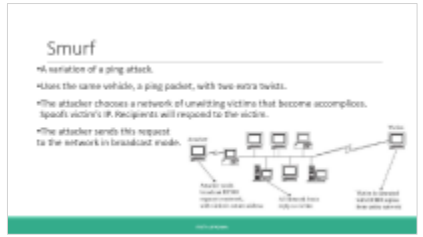
- The most common malicious denial-of-service attack type is flooding.
- Either overwhelm a victim with prodigious resources; or write a few lines of code from one computer that can bring down a seemingly more powerful network entity.
- How flooding attacks are assembled:
    - Insufficient Resources
    - Insufficient Capacity

Denial of Service Attack Methods

- Network Flooding Caused by Malicious Code
- Network Flooding by Resource Exhaustion
- Denial of Service by Addressing Failures
- Traffic Redirection
- DNS Attacks
- Physical Disconnection

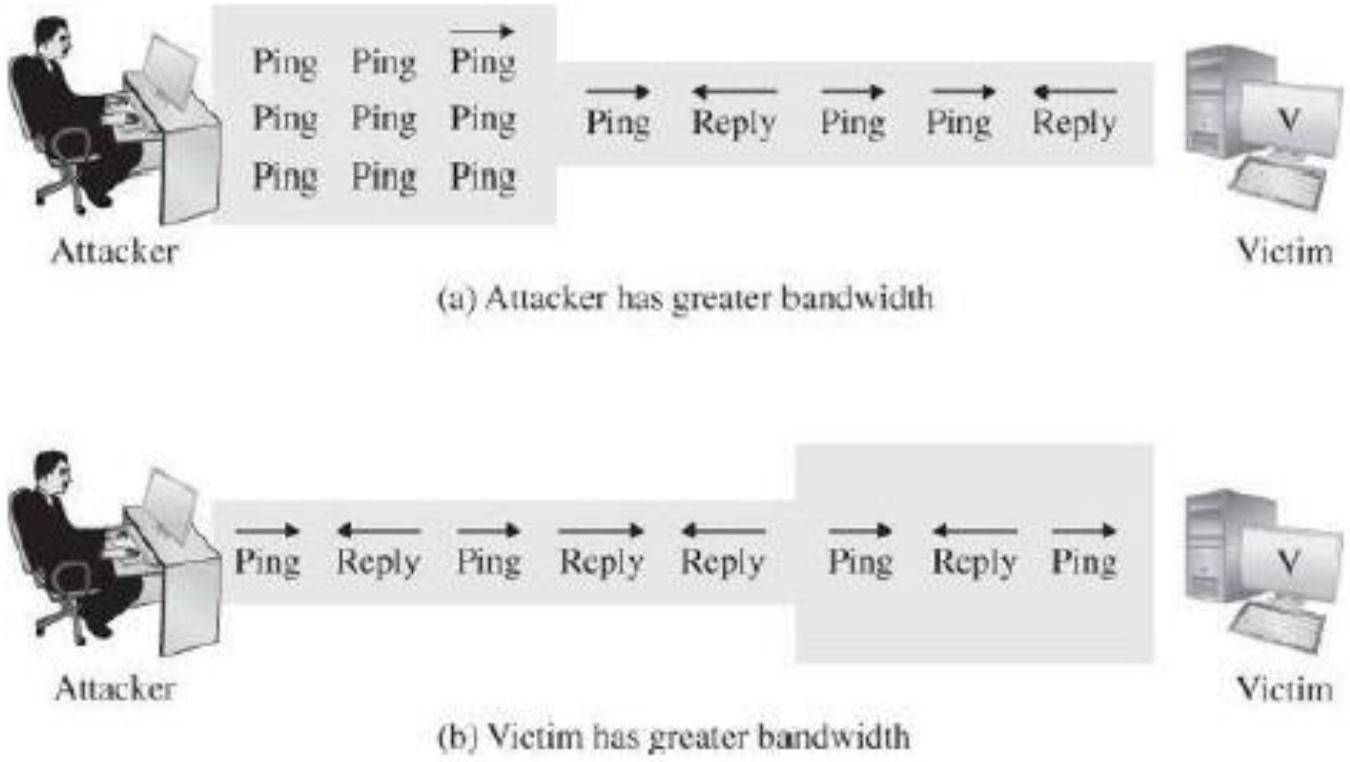
Network Flooding Caused by Malicious Code

- The most primitive denial-of-service attack is flooding a connection.
- More sophisticated attacks use or misuse elements of Internet protocols. TCP, UDP, ICMP.
- **ICMP**: ping, echo, destination unreachable, source quench.
- Peculiarities or oversights in the protocols or their implementations can open the way for an attacker to exploit a weakness to overwhelm the code supporting the protocol function.
  - Ping of Death
  - Smurf
  - Echo–Chargen
  - SYN Flood



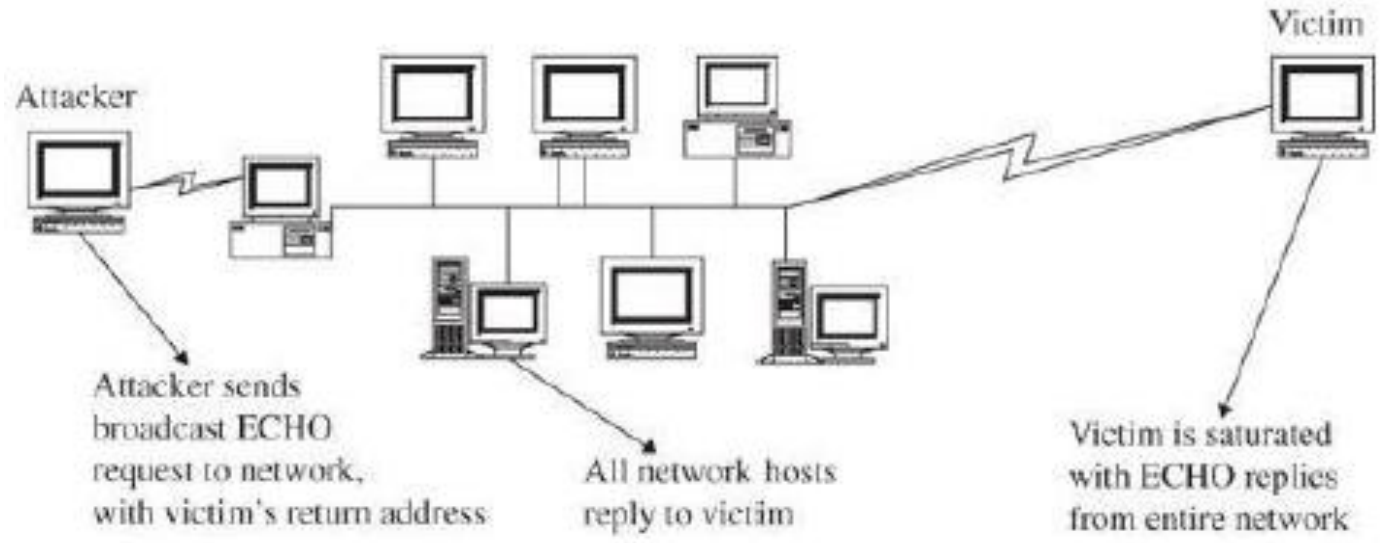
Ping of Death

- Uses ping command.
- Since ping requires the recipient to respond to the packet, all the attacker needs to do is send a flood of pings to the intended victim.
- The attack is limited by the smallest bandwidth on the attack route.



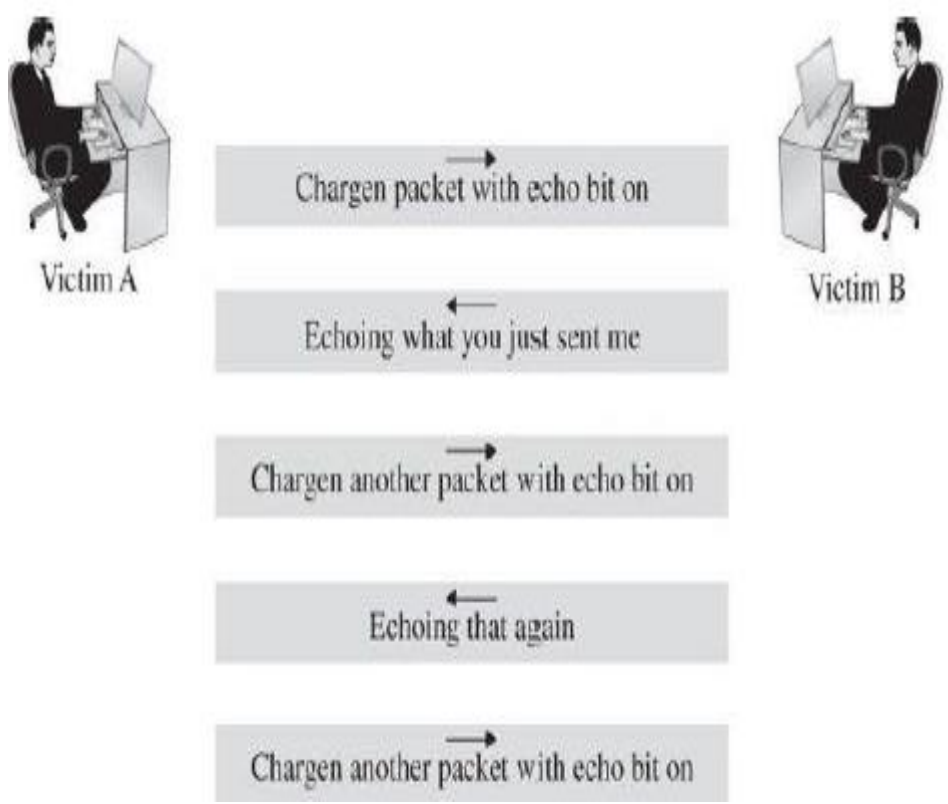
Smurf

- A variation of a ping attack.
- Uses the same vehicle, a ping packet, with two extra twists.
- The attacker chooses a network of unwitting victims that become accomplices. Spoofs victim's IP. Recipients will respond to the victim.
- The attacker sends this request to the network in broadcast mode.



Echo-Chargen

- The echo–chargen attack works between two hosts.
- Chargen is an ICMP protocol that generates a stream of packets to test the network's capacity.
- The attacker picks two victims, A and B, and then sets up a chargen process on host A that generates its packets as echo packets with a destination of host B. Thus, A floods B with echo packets.
- But because these packets request the recipient to echo them back to the sender, host B replies by returning them to host A.

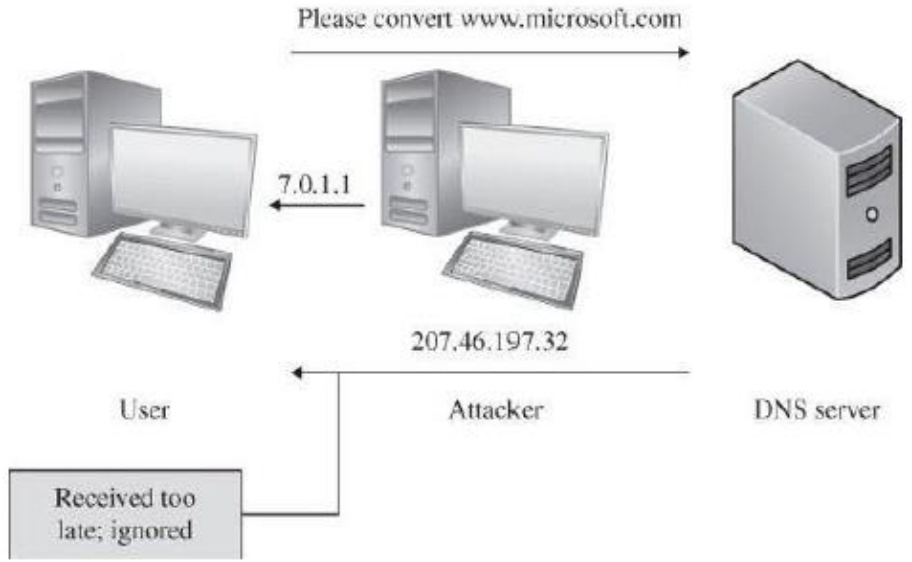


Network Flooding by Resource Exhaustion

- Context Switching and Thrashing. Which resource is exhausted here?
- Buffer space: Email buffer, Logging, and so on.
- Even identification and authentication can become vulnerable in an exhaustion attack. Lockout Policy.
- **IP Fragmentation: Teardrop attack**.
- The **teardrop** attack misuses a feature ironically intended to improve network communication.
- Fragments overlap, so they cannot be reassembled properly.
- In an extreme case, the operating system locks up with these partial data units it cannot reassemble, thus leading to denial of service.

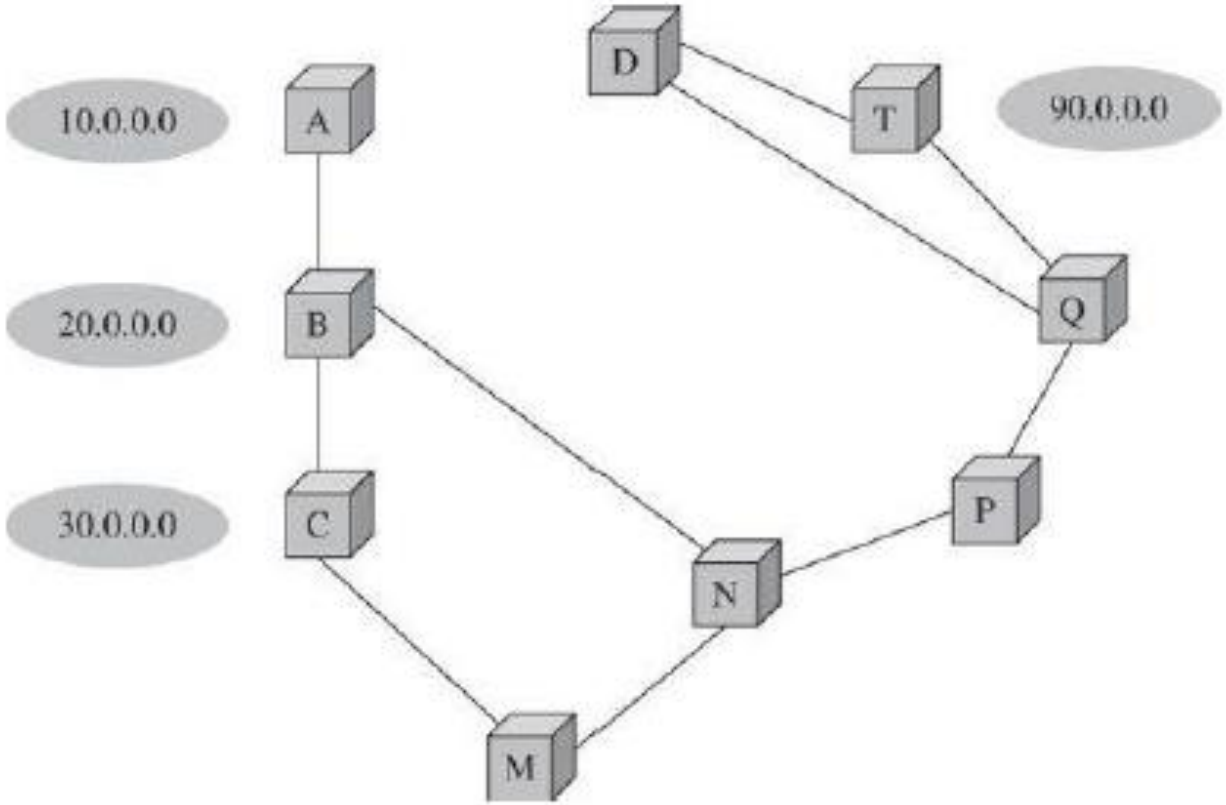
Denial of Service by Addressing Failures

- DNS Spoofing
- Router Takes Over a Network: BGP.



Denial of Service by Addressing Failures

- DNS Spoofing
- Router Takes Over a Network: BGP.
- Rerouting Routing
  - How routers exchange information?
  - What if A is a rogue router?
  - Can be non-malicious or malicious.



Traffic Redirection

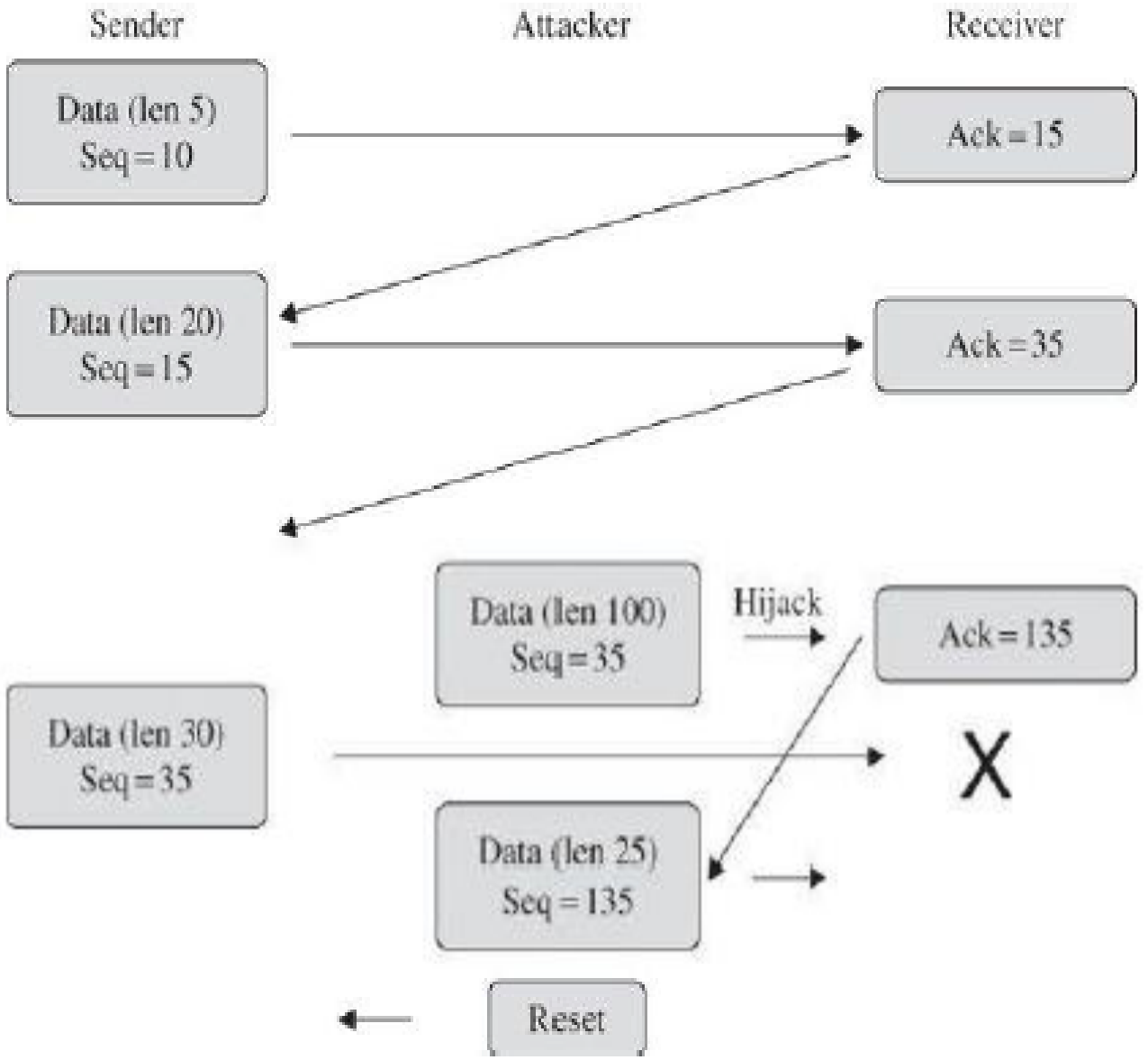
- If an attacker can corrupt the routing, traffic can disappear.
- Routers use complex algorithms to decide how to route traffic. Each router advises its neighbors about how well it can reach other network addresses. This characteristic allows an attacker to disrupt the network.
- Suppose a router advertises to its neighbors that it has the best path to every other address in the whole network. Soon all routers will direct all traffic to that one router.
- Routers trust each other! A standard countermeasure to exclude impostors is **identification and authentication.**
- For efficiency, router communication protocols were designed without authentication. Only now are authenticating steps being added to router protocols.

DNS Attacks

- Name Server Application Software Flaws
  - Name servers use software which may have flaws.
  - By overtaking a name server or causing it to cache spurious entries, an attacker can redirect the routing of any traffic, with an obvious implication for denial of service.
- Top-Level Domain Attacks
  - 2002 TLD attacks. 2007 root server attacks.
  - Make it distributed!

DNS Attacks

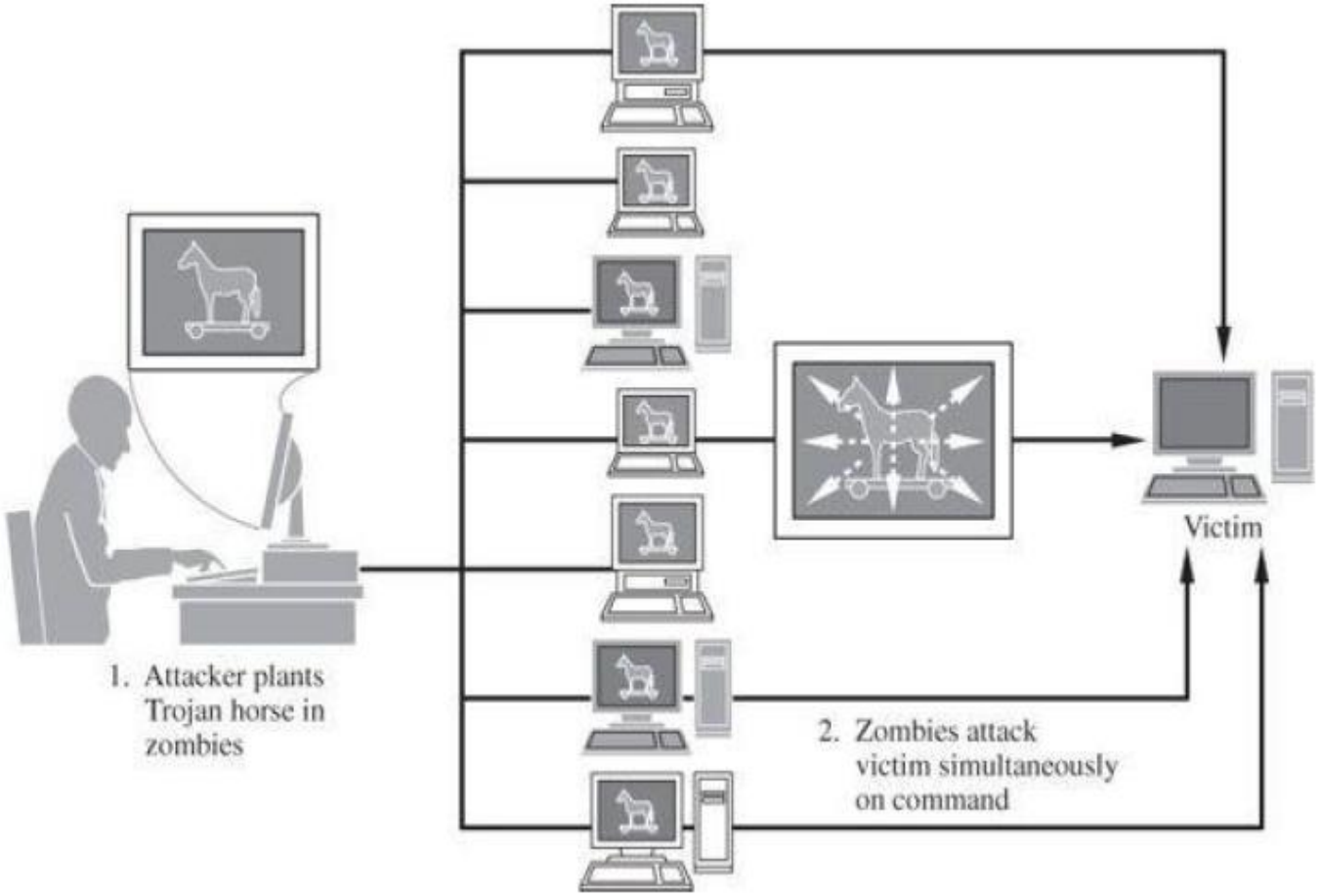
- Session Hijacking
- In a session hijack attack, the attacker allows an interchange to begin between two parties but then diverts the communication, much as would a man in the middle.
- Session hijacking is facilitated by elements of the TCP/IP protocol design.



Distributed DoS (DDoS)

- Distributed denial-of-service attacks change the balance between adversary and victim by marshalling many forces on the attack side.
- To mount a DDoS attack, an attacker does two things.

1. The attacker conscripts an army of compromised machines to attack a victim. **Zombie** formation.
2. The attacker chooses a victim and sends a signal to all the zombies to launch the attack.



Scripted Denial-of-Service Attacks

- DDoS attacks are a serious problem. Why?
  - Their tremendous multiplying effect.
  - They are easily launched from scripts.
- Given a collection of denial-of-service attacks and a propagation method, one can easily write a procedure to plant a Trojan horse that can launch any or all of the denial-of-service attacks.
- DDoS tools also include: code to turn a compromised system into a zombie.
- Zombie selection has been largely random; it means that no organization or accessible host is safe from attack.
- Compromised zombies to augment an attack are located by scanning random computers for unpatched vulnerabilities.

Bots

- Zombies or **bots** are machines running pieces of malicious code under remote control.
- These code objects are **Trojan horses** that are distributed to large numbers of victims' machines.
- Because they may not interfere with or harm a user's computer (other than consuming computing and network resources), **they are often undetected.**

Botnets

- A network of compromised machines ready, willing, and able to assist with the attack.
- Neither the machines nor their owners are aware they are part of an attack.
- Botnets, networks of bots, are used for massive denial-of-service attacks, implemented from many sites **working in parallel against a victim**.

Botnets

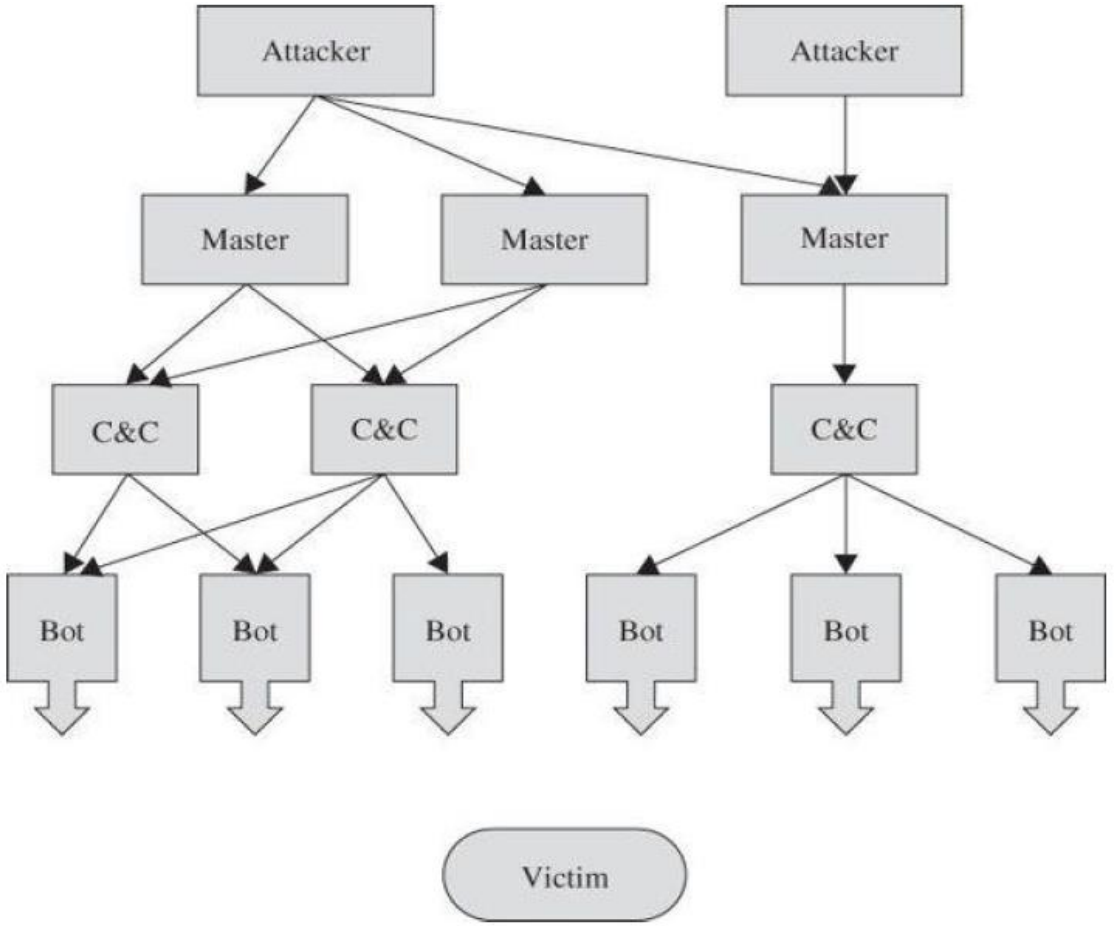
- Botnets tend to be multinational entities with pieces in many countries. Implications?
- Complicates prosecution because of different laws, standards of evidence, investigative practices, and judicial structures.
- The key elements of botnets use crime-friendly hosting services that protect their clients from abuse complaints and takedown requests.
- Thus, both law enforcement officials and network security administrators have difficulty taking action against major botnets.

Botnet Command and Control Update

- A network of bots requires a command hierarchy; the bots require someone to tell them **when** to attack, against **whom**, and **with what** weapon.
- The bot headquarters is called a **command-and-control center**.
- The mastermind wants to be isolated from the actual configuration, to reduce the likelihood of detection.
- In case part of the army is isolated and taken down, the attacker wants redundancy to be able to regroup, so the attacker builds in redundancy.
- The attacker controls one or more master controllers that establish command-and-control centers.

Botnet Command and Control Update

- Command-and-control centers control the individual bots, telling them when to start and stop an attack against which victim.
- **Communication** from the command-and-control center to the bots can be either **pushed** or **pulled**.
- To avoid detection, masters change command-and-control centers often, for which the push model is more effective. Why?
- The individual bots do not have to be informed of the address of the new command-and-control computer.
- Structured as a loosely coordinated web, a botnet is **not subject to failure** of any one bot or group of bots, and with multiple channels for communication and coordination, they are **highly resilient**.



Rent-A-Bot

- People who infect machines to turn them into bots are called **botmasters**.
- A botmaster may own (in the sense of control) hundreds or thousands of bots.
- Because the infected machines belong to unsuspecting users who do use them for real computing, these bots are not always available.
- Botmasters also sometimes rent out their botnets to others. Why?
- DoS activity tends to be targeted, not random, so one botmaster is unlikely to have an unlimited number of victims against which to direct the bots.
- Thus, to bring in a little income, botmasters also sometimes rent out their botnets to others.

Opt-In Botnets

- Join with a group of like-minded individuals to launch a distributed denial-of-service attack against any outrage.
- Download and install an attack script and show up at the specified time to protest by pointing your attacking computer at the victim.
- Join in and drop out when you want.

Penetration Testing

- Penetration testing is the process of attempting to gain access to resources without knowledge of usernames, passwords and other normal means of access.
- If the focus is on computer resources, then examples of a successful penetration would be obtaining or subverting confidential documents, pricelists, databases and other protected information.
- The main thing that separates a penetration tester from an attacker is **permission**. The penetration tester will have permission from the owner of the computing resources that are being tested and will be responsible to provide a report.

Goals of Penetration Testing

- To **increase the security of the computing resources** being tested.
- In many cases, a penetration tester will be given user-level access.
- In those cases, the goal would be to elevate the status of the account or user; other means to gain access to additional information that a user of that level should not have access to.
- Some penetration testers are contracted to find one vulnerability, but in many cases, they are expected to keep looking past the first one so that additional vulnerabilities can be identified and fixed.
- It is important for the pen-tester to keep detailed notes about how the tests were done so that the results can be verified and so that any issues that were uncovered can be resolved.

Penetration Testing versus Vulnerability Assessment

Penetration testing has more of an **emphasis on gaining as much access as possible.**

While

Vulnerability testing places the **emphasis on identifying areas that are vulnerable to a computer attack**.

- An automated vulnerability scanner will often identify possible vulnerabilities based on service banners or other network responses that are not in fact what they seem. Any Penetration Test is a sampling of the environment.
- A vulnerability assessor will **stop just before compromising a system**, whereas a penetration tester will **go as far as they can** within the scope of the contract.
- A penetration test is like any other test in the sense that it is a sampling of all possible systems and configurations. Unless the contractor is hired to test only a single system, they will be unable to identify and penetrate all possible systems using all possible vulnerabilities.

How Vulnerabilities Are Identified?

- Vulnerabilities need to be identified by both the penetration tester and the vulnerability scanner.
- The steps are similar for the security tester and an unauthorized attacker.

1. Reconnaissance.
2. Verification.
3. Testing.
4. Attack.

How Vulnerabilities Are Identified?

1. Reconnaissance.

   - This is where the tester attempts to learn as much as possible about the target network as possible.
   - This normally starts with **identifying publicly accessible services** such as mail and web servers from their service banners.
   - Many servers will report the Operating System they are running on, the version of software they are running, patches and modules that have been enabled, the current time, and perhaps even some internal information like an internal server name or IP address.

How Vulnerabilities Are Identified?

2. Verification.
   - Once the tester has an idea what software might be running on the target computers, that information needs to be verified.
   - The tester really doesn't KNOW what is running but may have a pretty good idea.
3. Testing.
   - The information that the tester has can be combined and then compared with known vulnerabilities, and then those vulnerabilities can be tested to see if the results support or contradict the prior information.
4. Attack.

Why Perform Penetration Testing?

- Security breaches and service interruptions are costly.
  - Security breaches and any related interruptions in the performance of services or applications, can result in direct financial losses, threaten organizations' reputations, erode customer loyalties, attract negative press, and trigger significant fines and penalties.
- It is impossible to safeguard all information, all the time.
  - New vulnerabilities are discovered each day, and attacks constantly evolve in terms of their technical and social sophistication, as well as in their overall automation.
- Penetration testing identifies and prioritizes security risks.
  - Test results validate the risk posed by specific security vulnerabilities or flawed processes, enabling IT management and security professionals to prioritize remediation efforts.

Penetration Testing Strategies

- Targeted testing
- External testing
- Internal testing
- Blind testing
- Double blind testing

Penetration Testing Strategies

- Targeted testing
  - Performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights-turned-on" approach because everyone can see the test being carried out.
- External testing
  - This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.
- Internal testing
  - This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

Penetration Testing Strategies

- Blind testing
  - A blind test strategy simulates the actions and procedures of a real attacker by **severely limiting the information** given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company.
  - Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.
- Double blind testing
  - In this type of test, only one or two people within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.