ETHICAL HACKING

(USCS607)

Smitha Renny

UNIT - III

- **Ethical Hacking: Enterprise Security**
- **Phases : Gaining and Maintaining Access : Systems hacking** – Windows and Linux – Metasploit and Kali Linux, Keylogging, Buffer Overflows, Privilege Escalation, Network hacking - ARP Poisoning, Password Cracking, WEP Vulnerabilities, MAC Spoofing, MAC Flooding, IPSpoofing, SYN Flooding, Smurf attack,
- **Applications hacking** : SMTP/Email-based attacks, VOIP vulnerabilities, Directory traversal, Input Manipulation, Brute force attack, Unsecured login mechanisms, SQL injection, XSS, Mobile apps security
- **Malware analysis** : Netcat Trojan, wrapping definition, reverse engineering
- **Phases :** Covering your tracks : Steganography, Event Logs alteration
- **Additional Security Mechanisms** : IDS/IPS, Honeypots and evasion techniques, Secure Code Reviews (Fortify tool, OWASP Secure Coding Guidelines)

SELF STUDY - ASSIGNMENT

ETHICAL HACKING – I (ENTERPRISE SECURITY)

PHASES : GAINING AND MAINTAINING ACCESS :

Systems hacking Windows and Linux – Metasploit(computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.) and Kali Linux(Debian-derived Linux distribution designed for digital forensics and penetration testing.)

- **Metasploit** is one of the most powerful exploit tools. Most of its resources can be found at: https://www.metasploit.com. It comes in two versions – **commercial** and **free edition**. There are no major differences in the two versions.
- As an Ethical Hacker, you will be using "Kali Distribution" which has the Metasploit community version(free) embedded in it along with other ethical hacking tools.
    - The hardware requirements to install Metasploit are –
        - 2 GHz+ processor
        - 1 GB RAM available
        - 1 GB+ available disk space

METASPLOIT FRAMEWORK

- The Metasploit framework is a freeware tool used to test or hack operating systems or web server software. Exploits can be used as plug-ins, and testing can be performed from a Windows or Unix platform. Metasploit was originally a command-line utility, but it now has a web browser interface. Using Metasploit, hackers can write their own exploits as well as utilizing standard exploits.
- Three terms to keep in mind:
  - **Vulnerability** – A vulnerability is a weakness of the system which allows the attacker to exploit the system
  - **Exploit** – An exploit is an attack on a system, especially one that takes advantage of a particular vulnerability of the system.
  - **Payload** – A payload is a piece of code that executes in the vulnerable system after exploitation of the system

METASPLOIT PAYLOADS

- Payloads, are simple scripts that the hackers utilize to interact with a hacked system. Using payloads, they can transfer data to a victim system.
- Metasploit payloads can be of three types –
- **Singles** – Singles are very small and designed to create some kind of communication, then move to the next stage. For example, just creating a user. These kinds of payloads are self-contained, so they can be caught with non-metasploit handlers such as netcat.
- **Stagers** – It is a payload that an attacker can use to upload a bigger file onto a victim system.
- **Stages** – Stages are payload components that are downloaded by Stagers modules. The various payload stages provide advanced features with no size limits such as Meterpreter and VNC Injection.

KEYLOGGERS

- Keylogger is a spyware or surveillance software which tracks all the activities of the user.
- It can record key strokes , take screenshots, and also record history(advanced keyloggers).
- It can be installed on
    - Windows
    - Linux
    - MAC
    - Android
- The concept of a keylogger breaks down into two definitions:
- **Keystroke logging**: Record-keeping for every key pressed on your keyboard.
- **Keylogger tools:** Devices or programs used to log your keystrokes.

HOW KEYSTROKE LOGGING WORKS

- Keystroke logging is an act of tracking and recording every keystroke entry made on a computer, often without the permission or knowledge of the user. A "keystroke" is just any interaction you make with a button on your keyboard.
- Keystrokes are how you "speak" to your computers. Each keystroke transmits a signal that tells your computer programs what you want them to do.
- These commands may include:
- Length of the keypress
- Time of keypress
- Velocity of keypress
- Name of the key used

BUFFER OVERFLOWS

- A buffer overflow arises when a program tries to store more data in a temporary data storage area (buffer) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information can overflow into adjacent buffers, thus corrupting the valid data held in them.
- *Buffer overflows* are exploits that hackers use against an operating system or application; like SQL injection attacks, they're usually targeted at user input fields.
- A buffer overflow exploit causes a system to fail by overloading memory or executing a command shell or arbitrary code on the target system.
- A buffer-overflow vulnerability is caused by a lack of bounds checking or a lack of input-validation sanitization in a variable field (such as on a web form).
- If the application doesn't check or validate the size or format of a variable before sending it to be stored in memory, an overflow vulnerability exits.

- The two types of buffer overflows are stack-based and heap-based.
- The *stack* and the *heap* are storage locations for user-supplied variables within a running program.
- Variables are stored in the stack or heap until the program needs them.
- Stacks are static locations of memory address space, whereas heaps are dynamic memory address spaces that occur while a program is running.
- A heap-based buffer overflow occurs in the lower part of the memory and overwrites other dynamic variables.
- As a consequence, a program can open a shell or command prompt or stop the execution of a program.
- To detect program buffer overflow vulnerabilities that result from poorly written source code, a hacker sends large amounts of data to the application via a form field and sees what the program does as a result.

Overview of Stack-Based Buffer Overflows

The following are the steps a hacker uses to execute a stack-based buffer overflow:

1. Enter a variable into the buffer to exhaust the amount of memory in the stack.
2. Enter more data than the buffer has allocated in memory for that variable, which causes the memory to overflow or run into the memory space for the next process. Then, add another variable, and overwrite the return pointer that tells the program where to return to after executing the variable.
3. A program executes this malicious code variable and then uses the return pointer to get back to the next line of executable code. If the hacker successfully overwrites the pointer, then the program executes the hacker's code instead of the program code.

Most hackers don't need to be this familiar with the details of buffer overflows. Pre-written exploits can be found on the Internet and are exchanged between hacker groups.

PRIVILEGE ESCALATION ATTACK

- A privilege escalation attack is a type of network intrusion that takes advantage of programming errors or design flaws to grant the attacker elevated access to the network and its associated data and applications.
- Not every system hack will initially provide an unauthorized user with full access to the targeted system. In those circumstances privilege escalation is required. There are two kinds of privilege escalation: vertical and horizontal.

- **Vertical privilege** escalation requires the attacker to grant himself higher privileges. This is typically achieved by performing kernel-level operations that allow the attacker to run unauthorized code.

- **Horizontal privilege** escalation requires the attacker to use the same level of privileges he already has been granted, but assume the identity of another user with similar privileges. For example, someone gaining access to another person's online banking account would constitute horizontal privilege escalation.

Smitha Renny

NETWORK HACKING - ARP POISONING

- ARP allows the network to translate IP addresses into MAC addresses.
- When one host using TCP/IP on a LAN tries to contact another, it needs the MAC address or hardware address of the host it's trying to reach.
- It first looks in its ARP cache to see if it already has the MAC address; if it doesn't, it broadcasts an ARP request asking, "Who has the IP address I'm looking for?" If the host that has that IP address hears the ARP query, it responds with its own MAC address, and a conversation can begin using TCP/IP.

- *ARP poisoning* is a technique that's used to attack an Ethernet network and that may let an attacker sniff data frames on a switched LAN or stop the traffic altogether.
- ARP poisoning utilizes ARP spoofing where the purpose is to send fake, or spoofed, ARP messages to an Ethernet LAN.
- These frames contain false MAC addresses that confuse network devices such as network switches.
- As a result, frames intended for one machine can be mistakenly sent to another (allowing the packets to be sniffed) or to an unreachable host (a Denial of Service [DoS] attack).
- ARP spoofing can also be used in a man-in-the-middle attack in which all traffic is forwarded through a host by means of ARP spoofing and analyzed for passwords and other information.

PASSWORD CRACKING

- Many hacking attempts start with attempting to crack passwords.
- Passwords are the key piece of information needed to access a system. Users, when creating passwords, often select passwords that are prone to being cracked.
- Many reuse passwords or choose one that's simple—such as a pet's name—to help them remember it.
- Because of this human factor, most password cracking is successful; it can be the launching point for escalating privileges, executing applications, hiding files, and covering tracks.
- Passwords may be cracked manually or with automated tools such as a dictionary or brute-force method.

- Manual password cracking involves attempting to log on with different passwords. The hacker follows these steps:

1. Find a valid user account (such as Administrator or Guest).
2. Create a list of possible passwords.
3. Rank the passwords from high to low probability.
4. Key in each password.
5. Try again until a successful password is found.

- A hacker can also create a script file that tries each password in a list. This is still considered manual cracking, but it's time consuming and not usually effective.

- A more efficient way of cracking a password is to gain access to the password file on a system. Most systems *hash* (one-way encrypt) a password for storage on a system.
- During the logon process, the password entered by the user is hashed using the same algorithm and then compared to the hashed passwords stored in the file.
- A hacker can attempt to gain access to the hashing algorithm stored on the server instead of trying to guess or otherwise identify the password.
- If the hacker is successful, they can decrypt the passwords stored on the server.

PASSWORD-CRACKING COUNTERMEASURES

- The strongest passwords possible should be implemented to protect against password cracking.
- Systems should enforce 8–12 character alphanumeric passwords.
- To protect against cracking of the hashing algorithm for passwords stored on the server, we must take care to physically isolate and protect the server.
- The systems administrator can use the SYSKEY utility in Windows to further protect hashes stored on the server hard disk.
- The server logs should also be monitored for brute-force attacks on user accounts.
- A systems administrator can implement the following security precautions to decrease the
- effectiveness of a brute-force password-cracking attempt:

1. Never leave a default password.
2. Never use a password that can be found in a dictionary.
3. Never use a password related to the host name, domain name, or anything else that can be found with whois.
4. Never use a password related to your hobbies, pets, relatives, or date of birth.

WEP (WIRED EQUIVALENT PRIVACY) VULNERABILITIES

- Wireless networks add another entry point into a network for hackers.
- Due to the broadcast nature of Radio Frequency (RF) wireless networks and the rapid adoption of wireless technologies for home and business networks, many vulnerabilities and exploits exist.
- Two methods exist for authenticating wireless LAN clients to an access point: open system or shared key authentication.
- Open system does not provide any security mechanisms. It requests to make a connection to the network.
- Shared key authentication has the wireless client hash a string of challenge text with the WEP key to authenticate to the network.

WEP WORKING

- Wired Equivalent Privacy (WEP) was the first security option for 802.11 WLANs.
- WEP is used to encrypt data on the WLAN and can optionally be paired with shared key authentication to authenticate WLAN clients.
- WEP uses an RC4 64-bit or 128-bit encryption key to encrypt the layer 2 data payload.
- This WEP key comprises a 40-bit or 104-bit user-defined key combined with a 24-bit Initialization Vector (IV), making the WEP key either 64- or 128-bit.
- The process by which RC4 uses IVs is the real weakness of WEP: It allows a hacker to crack the WEP key.
- The method, knows as the *FMS(Fluhrer, Mantin, Shamir) attack,* uses encrypted output bytes to determine the most probable key bytes.
- Although a hacker can attempt to crack WEP by brute force, the most common technique is the FMS attack.

MAC FLOODING

- A packet sniffer on a switched network can't capture all traffic as it can on a hub network; instead, it captures either traffic coming from or traffic going to the system.
- It's necessary to use an additional tool to capture all traffic on a switched network.
- There are essentially two ways to perform active sniffing and make the switch send traffic to the system running the sniffer: ARP spoofing and flooding.
- ARP spoofing involves taking on the MAC address of the network gateway and consequently receiving all traffic intended for the gateway on the sniffer system.
- A hacker can also *flood* a switch with so much traffic that it stops operating as a switch and instead reverts to acting as a hub, sending all traffic to all ports.
- This active sniffing attack allows the system with the sniffer to capture all traffic on the network.

- A **media access control attack** or **MAC flooding** is a technique employed to compromise the security of network switches.
- The attack works by forcing legitimate MAC table contents out of the switch and forcing a unicast flooding behavior potentially sending sensitive information to portions of the network where it is not normally intended to go.

WHAT IS MAC FLOODING?

- The MAC Flooding is an attacking method intended to compromise the security of the network switches. Usually, the switches maintain a table structure called MAC Table.
- This MAC Table consists of individual MAC addresses of the host computers on the network which are connected to ports of the switch.
- This table allows the switches to direct the data out of the ports where the recipient is located.
- The hubs broadcast the data to the entire network allowing the data to reach all hosts on the network but switches send the data to the specific machine(s) which the data is intended to be sent. This goal is achieved by the use of MAC tables
- The aim of the MAC Flooding is to takedown this MAC Table. In a typical MAC Flooding attack, the attacker sends Ethernet Frames in a huge number. When sending many Ethernet Frames to the switch, these frames will have various sender addresses. The intention of the attacker is consuming the memory of the switch that is used to store the MAC address table. The MAC addresses of legitimate users will be pushed out of the MAC Table. Now the switch cannot deliver the incoming data to the destination system. So considerable number of incoming frames will be flooded at all ports.
- MAC Address Table is full and it is unable to save new MAC addresses. It will lead the switch to enter into a fail-open mode and the switch will now behave same as a network hub. It will forward the incoming data to all ports like a broadcasting.

ETHERNET FRAME

- A network switch is a computer networking device that connects devices together on a computer network.
- The switches work very similar to the Network hubs but there are differences.
- The switches have computers inside a network connected to it with physical ports. Thus switches form a network.
- When incoming data arrives a switch, it will forward the data to one or more ports – computers – where the data is intended to reach.
- A hub is less advanced and they will broadcast the incoming data to all the ports.
- An Ethernet frame is a physical layer communication transmission, comprised of 6 fields which are assembled to transmit any higher layer protocol over an Ethernet Fabric.

BENEFITS OF THE ATTACKER WITH MAC FLOODING ATTACK

- As the attacker is a part of the network, the attacker will also get the data packets intended for the victim machine.
- So that the attacker will be able to steal sensitive data from the communication of the victim and other computers. Usually a packet analyzer is used to capture these sensitive data.
- After launching a MAC Flood attack successfully, the attacker can also follow up with an ARP spoofing attack.
- This will help the attacker retaining access to the privileged data even after the attacked switches recover from the MAC Flooding attack.

HOW TO PREVENT THE MAC FLOODING ATTACK?

We can prevent the MAC Flooding attack with various methods. The following are some of these methods.

1. Port Security
2. Authentication with AAA server
3. Security measures to prevent ARP Spoofing or IP Spoofing
4. Implement IEEE 802.1X suites

MAC SPOOFING

- **MAC spoofing** is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device.
- The MAC address that is hard-coded on a network interface controller (NIC) cannot be changed.
- However, many drivers allow the MAC address to be changed. Additionally, there are tools which can make an operating system believe that the NIC has the MAC address of a user's choosing.
- The process of masking a MAC address is known as MAC spoofing. So, MAC spoofing involves changing a computer's identity.
- So MAC Spoofing is an unauthorized change of MAC address, a MAC address falsification of a network device within a computer network.

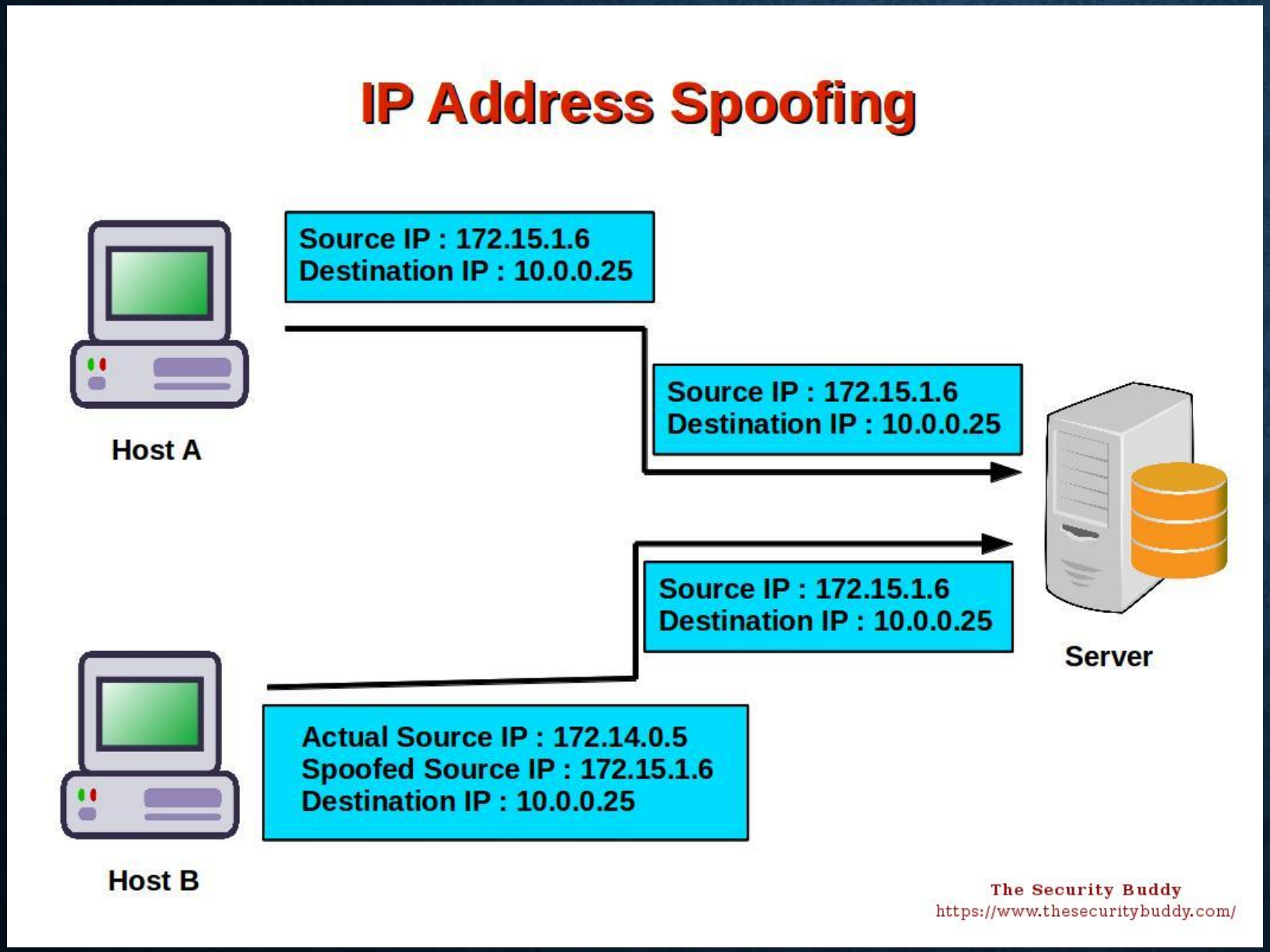
The MAC address falsification can happen in several ways:

1. change of MAC address
2. generating random MAC address
3. setting up a MAC address of a different manufacturer
4. setting up a MAC address without changing the manufacturer and subsequent automatic activation of the new MAC address

PROTECTING DEVICE AGAINST MAC SPOOFING

- To combat this technique and protect your network, both **protection** and **active detection** (network monitoring and analysis) are required.
- A restricted access to the network connection (wifi) should be reserved to the visitors (This is because a big portion of the MAC spoofing attacks take place from within an **internal network**.)
- The company should also make sure that there are no unauthorized persons in the company's premises and that visitors are never left alone. This is to avoid the risk of unauthorized people connecting to or manipulating the internal network by means of, for example, bypassing the wifi protection by connecting directly to the (ethernet) using a cable.

IPSPOOFING



IPSpoofing / IP Address Spoofing is the creation of IP packets with a forged source IP address.

This is done for the purpose of concealing the identity of the sender or impersonating another computer system.

HOW IS IPSPOOFING DONE?

- Each IP packet contains a source IP address and a destination IP address in its header.
- By forging the header one can change the source IP address so that the packet will appear to come form a different IP address.
- The machine that gets the spoofed IP packets will send response to the forged source address

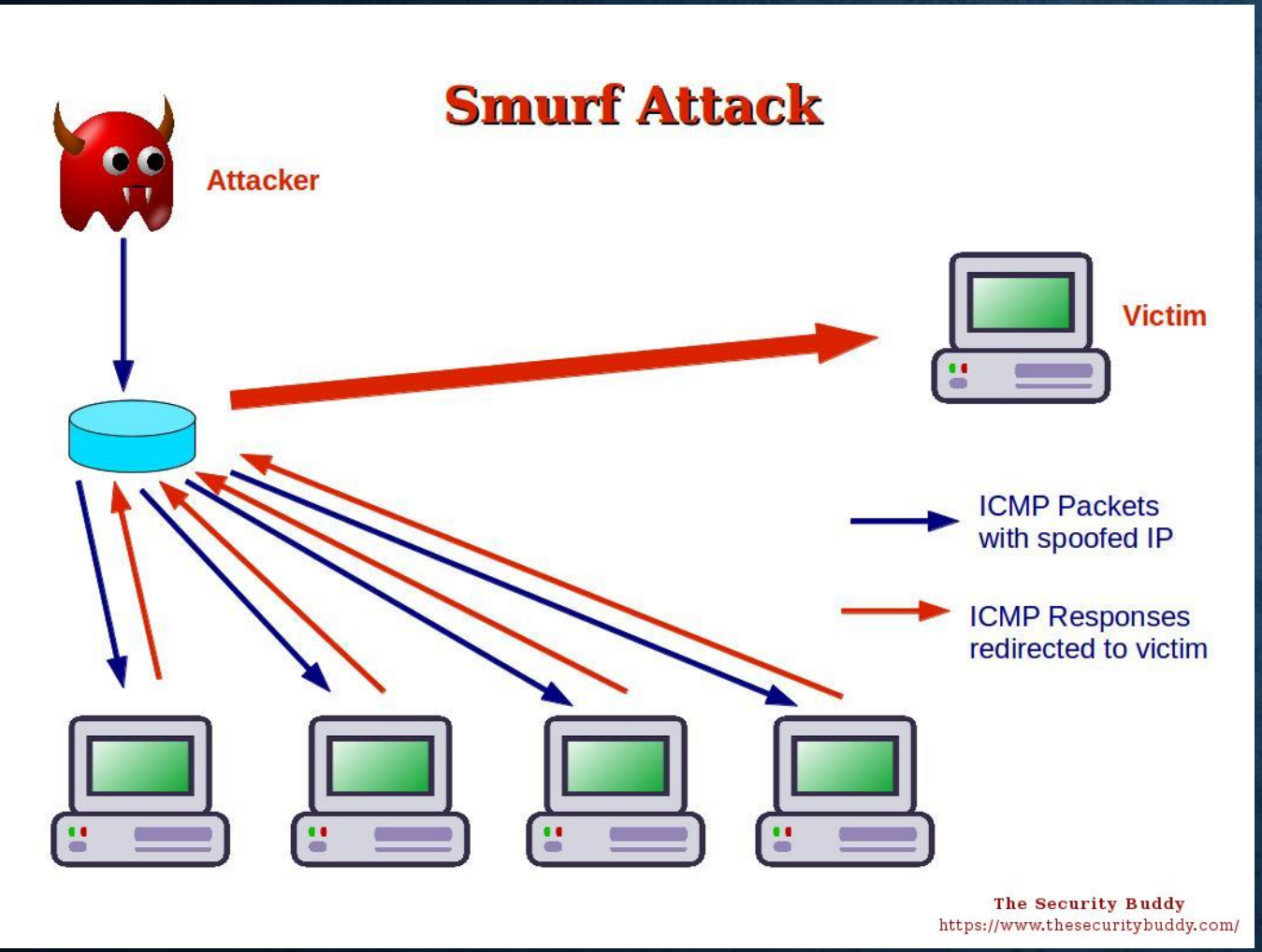
WHY IS IP SPOOFING DONE?

- IP Spoofing is done by attackers mainly incase of denial of service attacks..
- The attackers send a large number of IP packets to a machine forging the source address and do not care about the responses of the sent packets.
- They normally select different IP addresses as source addresses and it becomes difficult to filter out those packets.
- As a result the target machine gets overburdened with network traffic.

HOW TO PREVENT IP SPOOFING

- Packet filtering is one way of defending against the IP spoofing attacks.
- The gateway should block all the packets that come from outside the network, but has a source address internal to the network.

SMURF ATTACK



- A smurf attack is a Denial of Service attack (DoS) which is commonly perpetrated and can turn down a system completely.
- In smurf attack, an attacker creates lots of ICMP packets with the intended victim's IP address as source IP and broadcasts those packets in a network using IP Broadcast address
- As a result most devices of the network respond by sending reply to the victim's IP address.

If the number of devices in the network is very large and most of the devices send reply, the victim's machine floods with network traffic.
This can slow down the victim's computer to such an extent that it will become impossible to work on it…resulting in a Denial of Service Attack

HOW TO PREVENT A SMURF ATTACK

There are mainly three ways a Smurf Attack can be handled:

1. Configure individual hosts and routers in the network not to respond to ICMP requests or broadcasts
2. Configure routers not to forward packets directed to broadcast addresses.
3. Ingress Filtering: (ingress filtering is a technique used to ensure that incoming packets are actually from the networks from which they claim to originate) block the packets in the network which come from outside the network and have a source address which belongs to the network

SYN FLOODING

- SYN flooding is an attack vector for conducting a denial-of-service (DoS) attack on a computer server.
- The attack involves having a client repeatedly send SYN (synchronization) packets to every port on a server, using fake IP addresses. When an attack begins, the server sees the equivalent of multiple attempts to establish communications. The server responds to each attempt with a SYN/ACK (synchronization acknowledged) packet from each open port, and with a RST (reset) packet from each closed port.
- In a normal three-way handshake, the client would return an ACK (acknowledged) packet to confirm that the server's SYN/ACK packet was received, and communications would then commence. However, in a SYN flood, the ACK packet is never sent back by the hostile client. Instead, the client program sends repeated SYN requests to all the server's ports. A hostile client always knows a port is open when the server responds with a SYN/ACK packet.

- The hostile client makes the SYN requests all appear valid, but because the IP addresses are fake ones, it is impossible for the server to close down the connection by sending RST packets back to the client. Instead, the connection stays open. Before time-out can occur, another SYN packet arrives from the hostile client.
- A connection of this type is called a half-open connection. Under these conditions, the server becomes completely or almost completely busy with the hostile client and communications with legitimate clients is difficult or impossible. For this reason, SYN floods are also known as half-open attacks.
- The transmission by a hostile client of SYN packets for the purpose of finding open ports and hacking into one or more of them, is called SYN scanning.

APPLICATIONS HACKING : SMTP/EMAIL-BASED ATTACKS

- **Browser attacks**
- Browser based attacks are the most common network attack shown in the data. They try to trick internet surfers into downloading malware that is disguised as a software application or an update.
- **Brute force attacks**
- Pay attention to your passwords! A brute force attack is when a hacker tries to decode a password or pin number through trial and error
- **Denial of service attacks**
- A Denial of Service (DOS) attack prevents legitimate users from accessing services or information. It succeeds when an attacker overloads a server with more requests than the server can process.
- Distributed Denial of Service (DDoS), is when an attacker takes control of computers and uses them to flood a particular email with messages, or a website with enormous blocks of data

- **SSL attacks**
- Secure Sockets Layer (SSL) establishes an encrypted link between a website and a browser, or a mail server and a mail client. It is a standard security technology that enables secure information to be safely delivered. A website secured by SSL begins with https.
- **Scans**
- Port scans are hostile searches on the internet for open ports through which attackers can gain access to a computer. They are not really true types of network attacks, but they are typically reconnaissance activities and can be seen as potential precursors to attack.

- **DNS attacks**
- Domain name servers (DNS) maintains a directory of domain names, and translates them into IP addresses.
- DNS spoofing is when data is introduced into the domain name system cache, causing the name server to return an incorrect IP address, which redirects traffic to an alternate computer selected by the attacker. DNS queries come through Port 53, which traditional firewalls leave open.
- DNS hijacking is a type of network attack that redirects users to a bogus website when they are trying to access a legitimate one. Many companies do not protect DNS because they don't realize it is a threat vector.
- To prevent your Business sensitive information from leaking and attacked by outside threats, you should use an **SMTP Server** with higher security. Eg. Mailcot Smtp Service.

EMAIL ATTACKS

- **Identity Theft**
- Many organizations these days are either using Microsoft Office 365, G Suite, Zoho or similar services to manage their email systems. Other than hosting emails, services like these offer a suite of useful business tools to manage information in one place. Some apps in the suite include added cloud storage space, project management and collaboration tools, Office suite and much more.
- Since they are all part of the same suite as the email service, end users do not need a separate set of login credentials to access them. Regardless of whether a company uses the above-mentioned services or their own proprietary service, they all tend to face the same consequences when a hacker manages to get hold of a user's identity (i.e. login credentials).
- Employees usually use the suite to store confidential data which will, in a short period of time, be exposed if an attacker gains a handle on the employee's email account. Today, email identity theft can have much bigger consequences than it did a few years ago.

- Phishing Attacks
- Phishing is one of the fastest growing attack vectors. For hackers, it is a tried and tested method that has been successfully working for more than a decade. In fact, it has been more than two decades since the first reported phishing attack in 1995.
- As the internet grew, so did the number of users having a minimum of two email accounts. Hackers now have far wider reach than ever before. According to a recent report, there were 9,576 phishing incidents recorded in 2015, with 916 of them reporting a breach of data.
- Phishing employs several different techniques. Each type of attack has its own target audience and purpose.

- **Pharming**
- In an attack called **Pharming**, the hacker changes IP address associated with the website. This redirects the user to the malicious website despite entering a correct domain name in the URL. **Deceptive phishing** scams the user by posing as a legitimate website and scares them into paying money. **Spear phishing** uses the same technique as deceptive phishing, except that this attack makes the user hand over their personal data. According to a report by Symantec, spear-phishing campaigns targeting employees increased 55% in 2015.

- **Virus**
- Attacking with a virus through email is another form using email as a vector. Creating a virus and implementing it requires a meticulous amount of planning, an activity more likely to be conceived and executed by a group rather than an individual.
- A targeted virus can have one specific or multiple purposes. Regardless of that, email itself is rarely a target, merely the first stage of the attack. If the attack is successful, the virus could quickly spread across the network in a short time and can even have the ability to shut down the complete network.
- Even the simplest virus will attempt to lure the end user into downloading an attachment. Masquerading as documents, they are in fact files which if executed could either take control over the host or even lead to the consequence mentioned above.
- In a 2015 report , Kaspersky Lab's web antivirus detected 121,262,075 unique malicious objects: scripts, exploits, executable files, etc.

- **Spam**
- Spam is the most commonly known form of email attack. Perhaps the reason is because we all have a "spam" folder within our email accounts where we receive unwanted emails or emails we didn't subscribe to.
- Spam emails saw a rise in the last couple of years because of the growth of social media and e-commerce websites. Companies, usually broadcast their "latest news" or announcements over email to large numbers of people who are a part of an opt-in list.
- With the right kind of planned attack, spamming could prove to be fatal for companies if not the users. If a hacker is somehow able to gain control of an organization's email, they can send unsolicited emails to even larger numbers of people.
- Worse, since the emails are going out from legitimate email addresses, hackers could take advantage of the situation and send emails with a phishing attack or by attaching a virus within an email, hence infecting large amount of users simultaneously.

VOIP VULNERABILITIES

- **VoIP is vulnerable** to similar types of attacks that Web connection and emails are prone to. VoIP attractiveness, because of its low fixed cost and numerous features, come with some risks that are well known to the developers and are constantly being addressed.
- **Remote eavesdropping**
- Unencrypted connections lead to communication and security breaches. Hackers/trackers can eavesdrop on important or private conversations and extract valuable data.
- The overheard conversations might be sold to or used by competing businesses.
- The gathered intelligence can also be used as blackmail for personal gain.

- **Network attacks**
- Attacks to the user network, or internet provider can disrupt or even cut the connection.
- Since VOIP is highly dependent on our internet connection, direct attacks on the internet connection, or provider, are highly effective way of attack.
- This kind of attacks are targeting office telephony, since mobile internet is harder to interrupt.
- Also mobile applications not relying on internet connection to make VOIP calls. are immune to such attacks.

- **Default security settings**
- Hardphones (a.k.a. VoIP phone) are smart devices, they are more a computer than a phone, and as such they need to be well configured. The Chinese manufacturers, in some cases are using default passwords for each of the manufactured devices leading to vulnerabilities.
- **VOIP over WiFi**
- VoIP even while VoIP is relatively secure in 2017, it still needs a source of internet, which in most cases is WIFI network. And while a home/office WIFI can be relatively secure, using public or shared networks will further compromise the connection.

DIRECTORY TRAVERSAL

- Directory traversal or Path Traversal is an HTTP attack which allows attackers to access restricted directories and execute commands outside of the web server's root directory.
- Web servers provide two main levels of security mechanisms
  - **Access Control Lists (ACLs)** – An Access Control List is a list which the web server's administrator uses to indicate which users or groups are able to access, modify or execute particular files on the server, as well as other access rights
  - **Root directory** – The root directory is a specific directory on the server file system in which the users are confined. Users are not able to access anything above this root.

- **What an attacker can do if the website is vulnerable**
- With a system vulnerable to directory traversal, an attacker can make use of this vulnerability to step out of the root directory and access other parts of the file system. This might give the attacker the ability to view restricted files, which could provide the attacker with more information required to further compromise the system.
- Depending on how the website access is set up, the attacker will execute commands by impersonating himself as the user which is associated with “the website”. Therefore it all depends on what the website user has been given access to in the system.

INPUT MANIPULATION

- **Input manipulation** is where employees alter data that is **input** in the computer. For example altering payroll time cards, creating fictitious data **inputs**, and entering data without proper source documents.
- Program **manipulation** occurs when a program is altered in some way to commit fraud.
- ***Input manipulation*** involves the manipulation of input, usually through the intentional entry of false data, like credits for merchandise returns that did not actually occur. A fraudster needs no specialized knowledge or expertise — just access during the input phase of operations. Input manipulation is easy to do and difficult to detect.

BRUTE FORCE ATTACK

- In the world of Cyber crimes, brute force attack is an activity which involves repetitive successive attempts of trying various password combinations to break into any website.
- This attempt is carried out vigorously by the hackers who also make use of bots they have installed maliciously in other computers to boost the computing power required to run such type of attacks.
- There are many tools available for securing different applications which will deny a user after a predefined number of attempts.
- For example, for SSH we can use Fail2ban or Deny hosts. These programs will deny the IP address after a few wrong attempts.

How to prevent it!

- Password Length.
- Password Complexity.
- Limit Login Attempts.
- Modifying .htaccess file. (server configuration file which specifies how to redirect users, password protect admin area or directories)
- Using Captcha.
- Two Factor Authentication.

UNSECURED LOGIN MECHANISMS

- Many websites require users to log in before they can do anything with the application. (Surprisingly,)these can be a great help to hackers.
- These login mechanisms often don't handle incorrect user IDs or passwords gracefully.
- They often divulge too much information that an attacker can use to gather valid user IDs and passwords.
- To test for unsecured login mechanisms, browse to your application and log in
- Using an invalid user ID with a valid password
- Using a valid user ID with an invalid password
- Using an invalid user ID and invalid password

- After you enter this information, the web application will probably respond with a message similar to Your user ID is invalid or Your password is invalid. The web application might return a generic error message, such as Your user ID and password combination is invalid and, at the same time, return different error codes in the URL for invalid user IDs and invalid passwords.
- In either case, this is bad news because the application is telling you not only which parameter is invalid, but also which one is valid. This means that malicious attackers now know a good username or password — their workload has been cut in half! If they know the username, they can simply write a script to automate the password-cracking process, and vice versa.

MOBILE APPS SECURITY

- Mobile app security is the extent of protection that mobile device applications have from malware and the activities of crackers and other criminals. The term can also refer to various technologies and production practices that minimize the risk of exploits to mobile devices through their apps.
- A mobile device has numerous components, all of them vulnerable to security weaknesses.
- The parts are made, distributed, and used by multiple players, each of whom plays a crucial role the security of a device.
- Each player should incorporate security measures into mobile devices as they are designed and built, and into mobile apps as they are conceived and written, but these tasks are not always adequately carried out.
- Common vulnerabilities for mobile devices include architectural flaws, device loss or theft, platform weakness, isolation and permission problems and application weakness.

Smitha Renny

SELF STUDY / ASSIGNMENTS

- **Malware analysis** : Netcat Trojan, wrapping definition, reverse engineering
- **Phases :** Covering your tracks : Steganography, Event Logs alteration
- **Additional Security Mechanisms** : IDS/IPS, Honeypots and evasion techniques, Secure Code Reviews (Fortify tool, OWASP Secure Coding Guidelines)

Thank You