Chap 6: Types of Hacking

Network Hacking

Network Infrastructure Vulnerability

- **Are foundation** for **all technical security issues** in your information system.

- n/w infrastructure security involves assessing such areas as:
  - Where **firewall or IDS are places on the n/w**
  - What **hackers see when they perform port scans and how they can exploit vulnerabilities in your n/w hosts**
  - Installation **of installed security devices.**
  - **Protocol in use**
  - **Commonly attacked ports** that are unprotected
  - **N/w monitoring and maintenance**

If any of these things exploit then :

- Attack can **take down your internet or even your entire n/w**
- Using n/w analyzer **hacker can steal confidential information in emails and files being transferred.**
- **Back doors** in your n/w can be **set up**

- Always remember these things:
  - **Test your system from both outside in and inside out.**
  - **Obtain permission from partner n/w** that are connected to your n/w to check for vulnerabilities on their ends that can affect your n/w security such as **open ports and lack of firewall or misconfigured router .**

Scanning ports

- A port scanner **is a software tool that basically scans the n/w to see who's there**.
- Port scanner provide basic views of how the n/w is laid out.
- **They can help to identify unauthorized hosts or application and n/w host configuration errors that can cause serious security vulnerabilities.**
- **Executed through the searching of a single host for open ports**

Scanning Ports

Port Scanning means to scan the target system in order to get a list of open ports (i.e. ports listening for connections) and services running on these open ports.

- Port Scanning is normally the first step that an attacker undertakes.
- Is used to get a list of open ports, services and the Operating System running on the target system.
- Can be performed easily by using different methods.

- By port scanning, **one discovers which ports are available** (i.e., being listened to by a service).
- Essentially, **a port scan consists of sending a message to each port, one at a time and examining the response received**.

Ping Sweep

- If you are undetermined about your target and just want a live system, ping sweep is the solution for you.
- **Ping is a system's network-based utility which is used to identify that a host is alive or dead.**
- Though Ping sweep is similar to ping but reduces the time involved in pinging a range of IP addresses.

- **A Ping Sweep is an information gathering technique which is used to identify live hosts by pinging them.**
- **It is executed through the searching of multiple hosts in order to target just one specific open port.**

- **Threat:**
  - Any time there is **open ports** on ones PC **there is potential for the loss of data, the occurrence of a virus and sometimes even complete system compromise.**
  - Therefore **port scanning** is considered a **serious threat** to ones PC as it occurs without producing any outward sign to the owner that anything dangerous is taking place

Countermeasures

- Traffic Restrictions:
  - Enable only the traffic you need to access internal hosts specially from the host you're trying to protect.
  - Can apply these rules in two places:
    - External Router for inbound traffic
    - Firewall for outbound traffic

- **Configure firewalls and IDS** to detect and block probes.
- **Use custom rules** to lock down the network and block unwanted ports.
- **Run port Scanning tools to determine whether the firewall accurately detects the port scanning activities.**
- Security Experts should ensure **the proper configuration of anti-scanners and anti-spoofing(Preventing traffic with spoofed source IP addresses) rules.**
- Security experts of an organization must also ensure that the **IDS, routers, and firewall ,firmware are updated to their latest releases.**

The firmware embedded on the firewall is the software that enables the device to filter traffic and prevent unwanted traffic on the network.

SNMP attack

- **Simple Network Management Protocol** (**SNMP**) is an Internet Standard protocol **for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behaviour.**
- Devices that typically support SNMP include **cable modems, routers, switches, servers, workstations, printers, and more**.

- SNMP is widely **used in network management for network monitoring.**
- SNMP **exposes** management data on the managed systems which describe **the system status and configuration.**
- These variables can then be remotely queried (and, in some circumstances, manipulated) by managing applications.

- **Countermeasures:**
  - Always **disable SNMP** on host if you are not using it
  - **Block the SNMP port** (UDP port 161) at the n/w perimeter.
  - **Change the default SNMP community string** from public to another value that's more difficult to guess .
  - This makes SNMP harder to crack.

Banner Grabbing

- Banner grabbing is essentially **a practice that is used to obtain information about services that are being run on a remote computer or client.**
- **Banners are the welcome screens** that provide **software version numbers** and **other system information on network hosts**, and this makes it an ideal route for malicious hackers to use and obtain information about the services running on the system.

- The technique involves **using** services such as **Telnet**, or **a proprietary program**, to **establish a connection with a remote machine, after which a compromising request is sent.**
- That, in turn, will cause a vulnerable host to respond back with a banner message, which could contain information that the hacker could use to compromise the system further.
- Eg: telnet ipaddress, netcat(grab banner information from routers and other n/w such as Wireless access point or Ethernet switch)

- **Countermeasures:**
  - **If there is no business need for the default banner , then either try to customize banner or disable the banner or remove information from the banner.**

Analyzing n/w data and n/w Analyzer

- A n/w analyzer is **tool that allows you to look into a n/w and analyze data going across the wire for n/w optimization, security and or troubleshooting purpose.**

- **It is just a s/w running on a computer with a n/w card**. It works by placing the n/w card in specific mode which enables the card to see all traffic on the n/w, even the traffic which are not destined to the n/w analyzer host.

- Performs following functions:
  - Captures all n/w traffic
  - Decodes what is found in human readable format
  - Display it all in chronological order.

- To capture all traffic you must have to connect the analyzer to either
  - A hub
  - Monitor/Mirror port of a switch
  - What enters before firewall filters
  - What leaving your n/w after firewall filters

- **Countermeasures:**
  - Ensure that **physical security is in place to prevent a hacker from plugging into your n/w.**
  - **Secure your server room and wiring area**
  - Provide **security to the monitor port on a switch** where a hacker can plug in a n/w analyzer.
  - **Make sure unsupervised and unoccupied desks don't have live connections.**
  - **Use different utilities** to determine whether someone is running an unauthorized n/w analyzer on your n/w.
  - Eg: PromiscDetect, sniffdet etc.

MAC Daddy Attack

- Hackers can **use ARP Protocol** that is running on the network to make their systems seem as your system or another allowed host on your network.
- A too much number of ARP (Address Resolution Protocol) requests can be a sign of an ARP poisoning or spoofing attack on your network.

- Anyone can run a program, such as dsniff tool or Cain & Abel tool, **can modify the ARP tables, which are responsible for saving IP addresses to media access control (MAC) address mappings — on network hosts.**

- That **makes the victim machines to think they require to forward traffic to the hacker's computer rather than to the correct destination machine when communicating on the network.**

- And this is a type of **man-in-the-middle (MITM) attacks**.

- **ARP Spoofing:**
  - ARP spoofing is a type of **attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network.**
  - This results in the linking of an **attacker's MAC address with the IP address** of a legitimate computer or server on the network.
  - Once the **attacker's MAC address is connected** to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address.
  - ARP spoofing **can enable malicious parties to intercept, modify or even stop data in-transit.**
  - ARP spoofing **attacks can only occur on local area networks that utilize the Address Resolution Protocol.**

- **MAC Address Spoofing:**
  - **MAC spoofing** is an unauthorized change of MAC address, **a MAC address falsification** of a network device within a computer network.
  - The **attacker** could use the **fake identification (MAC address) to pass of as your own device and thus be able to, for example, intercept the network communication.**
  - The MAC address falsification can happen in several ways:
    - **change of MAC address**
    - **generating random MAC address etc.**

- **Countermeasures:**
  - Use IDS or stand alone MAC address monitoring utility.
  - Eg: ARP watch : will notify you via mail if there is any change in MAC addresses associated with the IP address.

WLANs

- A WLAN is one in which **a mobile user can connect to a local area network through a wireless connection.**

- **Threats to WLANs:**
  - **Rogue Access Point:** Rogue APs are unauthorized APs in a network .
  - **DOS:**an attempt to deny a particular person from using the service.
  - **Configuration Problem:** Incomplete Configuration/Miss Configuration
  - **Passive Capturing:** an attempts to learn or make use of information from the system but does not affect system resources.
    - The goal of the opponent is to obtain information is being transmitted.

Peer-to-peer Attacks:

- **Devices that are connected to the same access points can be vulnerable to attacks from other devices connected to that access point.**
- Most providers provide for an option such as “Client Isolation” which ensures that clients connected to the access point cannot communicate with eachother, preventing this issue.

Authentication Attacks:

- This is where **the attacker scrapes a frame exchange between a client authenticating with the network,** and then they simply run an offline dictionary attack.
- With this sort of information, and depending on the strength of the password, it could be just a matter of time before they crack the password and gain access.
- Because of this it's important to keep your login credentials as secure as possible.

Man in the Middle Attack:

- It's possible for **hackers to trick communicating devices into sending their transmissions to the attacker's system.**
- Here they can record the traffic to view later (like in packet sniffing) and even change the contents of files.
- Various types of malware can be inserted into these packets, e-mail content could be changed, or the traffic could be dropped so that communication is blocked.

Bluetooth Attacks:

- There are a variety of Bluetooth exploits out there. These range from annoying pop up messages, to full control over the a victims Bluetooth enabled device.

OS Hacking

- What is OS?

Windows OS Vulnerabilities/Linux Vulnerability

- Because of ease, Many well known attacks against Windows/Linux can lead to…
  - **Leakage of confidential information**, including file being copied or credit card details can be stolen
  - **Password being cracked**
  - **System taken completely offline** by DoS attack
  - **Entire database being corrupted or deleted** when insecure Windows based systems are attacked.

- **Auto play** is used w.r.t. removable media then **launches appropriate application again opens door for different attack**

- **Clipboard vulnerability** can allow attacker to get access to the sensitive clipboard data.

Application Hacking

Messaging System

- Are **emails and instant messaging** applications
- These systems are vulnerable because generally **n/w admin forget about securing these s/y's.**

- Hacker attack against messaging systems include:
  - Transmitting malware
  - Crashing server
  - Obtaining remote control of workstations
  - Capturing and modifying confidential information
  - Capturing email in email database on server and workstation
  - Using Instant messages log files on workstation hard drives
  - Try to gather internal n/w configuration information suchas hostname,IP adrees etc

- Different email attacks:
  - Email Bomb
    - Attachment overloading
      - Storage overload
      - Bandwidth blocking
    - Connection attack
    - Auto responder attack

Email Bomb

- Can **crash a server and provide unauthorized admin access**.
- Attack by **creating DoS** condition **against your n/w or internet connection by taking so much storage space or b/w**
- **Act through which massive volume of mails will be send to a specific email address with the goal of overflowing the mailbox**

1.Attachment Overloading

- Send 100 or 1000 of emails with very large attachment
- Impact
  - Storage overload
  - B/w blocking

Storage overload

- * large message quickly fill the total storage
- Not able to work **until and unless automatic deletion of email will be done or manual deletion is require**

b/w Blocking

- **Crash your email service by filling the incoming internet connection with junk.**
- If your s/y discards attachment attack , **the bogus messages eats resources and delay processing of valid messages**

Countermeasures

- **Limit the size of either email or email attachment**
- **Limit each users space on the server**

2.Connection Attack

- A hacker can send a huge amount of email simultaneously **to addressees on your n/w.**
- These connection attacks can **cause the server to give up on servicing any inbound or outbound TCP requests.**
- These causes **complete server lockups or a crash introduces situation where the attacker is allowed admin or root access to the system**

- Carried out as **Spam attacker**

Countermeasures

- Many servers allows you to **limit the number of resources used for inbound connections**.

3.Autoresponder attack

- If auto responder configures
- **Auto responder is automatic email response you often get back from random users when you are subscribing to a mailing list.**
- **Can create DoS**

Countermeasures

- To make policy that **no one sets up an auto responder messages**

Best Practice to minimize email security risk

- Use encrypted messages or messaging systems
- Put your email server behind a firewall
- Disable unused services or protocols on your email server.
- If your server doesn't need any email service then disable them.
- Use proper email monitoring to detect block messages coming from unauthorized user.

- **Use email filtering** so hat it can block certain kind of attachment
- **Verify the URL** attached to email.

Web Application

- Click Here

Database System

- Click Here