Anatomy of an Attack

Cyber security notes 2023-01-03

Types of Hackers

- White Hat: Hack with permission; stay within scope and legal bounds.
- Grey Hat: Their hacking can be outside legal bounds; "ends justify the means"
- Black hat: their hacking is outside legal bounds
- Script Kiddies: Hackers without knowledge; use tools & attampt to hack
- Hacktivist: Hackers for a cause; they typically do not care if caught

Phases of an attack

There are five phases of an attack testing a network.

1. Reconnaissance: The attacker gathers information about the target.
2. Scanning and enumeration: The attacker scans the target to find vulnerabilities.
3. Gaining access: The attacker exploits the vulnerabilities to gain access to the target.
4. Maintaining access: The attacker maintains access to the target.
5. Covering tracks: The attacker covers their tracks to avoid detection.

Reconnaissance

First step, collect as much data on the target as possible. Also called `Footprinting`. There are two types of Footprinting: - Passive: Collecting data without interacting with the target. - Active: Interacting with the target to collect data.

For example, by interacting with a target (a company for example), you can find out when they make breaks, when they have meetings, anything that could give you an advantage.

Remember, the biggest security vulnerability are the employees.

Purpose of footprinting

- Gather Orgagnizational Information
  - Names, numbers, history, technology, etc.®
- Gather Network Information
  - IP, IP range, DNS, Server Names, Hosting Information
- Gather System information
  - Locations, username algorithms, passwords, OS information
- Reduce the Focus
  - Attackers have a target in mind. Efficiency is important to going unnoticed.

Passive Footprinting:

- More difficult to detect as it often looks like normal traffic or goes unnoticed on site.
- This method Footprinting falls within legal parameters and is rarely capable of prosecution.
- If an attacker is caught this phase can be discovered through digital forensics investigation.

The focus of this phase is OSINT or Open Source Intelligence without "touching" the target.

Some activities include:

- Dumpster diving
- Advanced Internet searches harvesting personal information
- Social engineering
- Examining the target's website history
- Using job site searches to discover network

Some of the tools used may be: - Netcraft - Netcat - DNS Recon - Maps / geolocation - Whois - Wget (slowed wwith wait)

Active Footprinting:

Could include actually physically breaking into the building where target is located. Activities are more detectable. The attacker tries to identify systems and network infrastructure.

Some activities include: - Ping sweeps - Httrack - Sniffing with Wireshark - Talking to employees

Scanning and Enumeration

Scanning: Discover host, ports, services, OS systems, wbe-apps, etc.

Enumeration: Gathering more details about systems. The phase is considered active as it involves interacting with the target.

Gaining access

"Pwning" a system. - Pwned means owned or dominated - Used by hackers to mean owning a system

Once a system is owned, that system will be used to furhter exploit other systems. This is called Pivotting. - The goal of this stage is to target and own a system. steal the data needed, and pivot as needed. - A lot goes into this stage including vulnerability scanning, sniffing, exploit building, explotation, and post exploitation. - This phase will be revisited in detaul throughout the course.

Some tools that may be used: - Metaspoit Framework - Nessus - OpenVas - Searchsploit - CVE Lookup - Password cracking tools - CANVAS Framework - Use of Trojans

Maintaining access

- The attacker takes steps to gain access for as long as needed.
  - includes installing malware such as root kits and trojans
- This phase can be as asimple as adding a user with admin rights who looks like a legimate user and opening the right ports to gain access with a program lke netcat
- The attacker has to know the envronoment well.
- There are some devices taht detect changes and will alert administrators.

Clearing Tracks

- The attacker will remove all evidence that can be used to trace their activity.
  - All accounts created, malware installed, firewalls turned off, ports opened, etc. will be returned to their original state.
- If all goes well for the attacker, noone wil ever known they were there.
- This state is why its said that msot organizations have been hacked, but do not know they have been hacked.
  - Attackers obtain the information and move on.
  - For example, if credit card numbers are stolen and used slowly over over a year, often times the owners have no idea how their information was stolen.

Attack Vectors

- The path by which an attacker gains access to a system
- Not an exploit, but a way to get information necessary
- With the exeption of the Hacktivist, most attackers want the quitest avenue.
  - For example, when someone tries to rob you, they wait for you to be out of town / not at home.
- Stealth is the key to success.
  - Many attackers take time to stury their victims and plan their attack to determine the best attack vector.

Overt Channel - Legitimate way for programs to access systems or network resources.

Covert Channel - Secretly accessing a system without permission that took a path that was intended for communication by unauthorized programs.

Common Attack Vectors: - Unnecessary open ports - Design flaws - OS flaws - Zero day exploits - Buffer overflows - Default passwords - Physical access to a system

Threats

Malware is the general term used to describe software that is attempting to harm or covertly access a system.

Type of Threats:

- Botnets
- Phishing Scams
- Command Injection
- Spyware
- Cross-Site Scripting
- SQL Injection
- Ransomware
- Rootkits

Excersise tasks: Task 1: Full Disclosure Research Task 2: Discovering Whitepapers Task 3: