CIS4204.01 **Brandon Thompson**
Dr. Ashokkumar Patel

Notes: Ethical Hacking

1 Overview

1.1 Terms and Evolution of Hacking

Hackers / Crackers

- Access to computer system or network without authorization.
  - Breaks the law; can go to prison.

Ethical Hacker

- Performs most of the same activities as a hacker with the owners / company's permission.

Hackers became more prolific and dangerous after the availability of the Internet expanded to include the general public. Originally hacking was the skillful modification of systems. As the Internet began to include more people and technology, there was more of a following for hacking. First for fun or curiosity, then for maliciousness and financial reasons.

1.2 What is Hacking

- Stealing passwords and usernames - "Theft of access"
- Network intrusions - Form of digital trespassing
- Social Engineering - Humans are the weakest point of a computer system.
- Posting / transmitting illegal material - Illegal material can spread very quickly with the use of social media.
- Financial Fraud - Deception of one party to elicit information or system access typically for financial gain to to cause damage.
- Software / data piracy - the possession, duplication / distribution of software in violation of license agreement / act of removing copy protection.

- Dumpster Diving - gathering of material that has been discarded or left in unsecured or unguarded receptacles.
- Creating and Planting Malicious Code - refers to items such as viruses, worms, spyware, adware, rootkits, and other types of malware. (any type of software written to wreak havoc, destruction or disruption.)
- Unauthorized Destruction or Alteration - Modifying, destroying, or tampering of information without permission.
- Data diddling - Unauthorized modification of information to cover up other malicious activity.
- Denial of Service (DoS/DDoS) - Overload a systems resources so it cannot provide the required services to its users.
- Ransomware - encryption of key files on a system for the purpose of extracting payment from the victim.

1.3 Types of Hackers

- Black-Hat Hackers: Bad guys, may or may not have an agenda (Criminal)
- White-Hat Hackers: Good guys, have a code of ethics.
- Gray-Hat Hackers: Could be good or bad (do not trust)
- Suicide Hackers: Trying to prove a point, are not stealthy because they do not care about repercussions.
- Script Kiddies: No or limited training, use prebuilt tools, mainly curious.

1.4 Motives of Hackers

- Monetary - financial gain
- Status - Increased reputation within their communities
- Terrorism - To scare, intimidate, or cause panic to the target group or the victims
- Revenge / Hatred - Disgruntled employees
- Hacktivism - Bring attention to a cause, group, or political ideology.
- Fun - Attacks with no specific goal

1.5 Tasks of Ethical Hackers

- **Penetration Test**
  Perform attacks / exploits on system and network

  1. Attempt to break into a company's network or system or application to find the weakest link.
  2. Report on the attack to company
  3. Company decides how to use the information given by the attack.

- **Vulnerability Assessment / Research**

  1. Tester enumerates all vulnerabilities found in an application or system.
  2. Passively uncovering vulnerabilities or weaknesses.
  3. Correct found vulnerabilities.

- **Security Test**

  1. Analyze company's security policy and procedures.
  2. Security tester must examine best practices, legal issues, and industry regulations.

1.6 Goals of Penetration Tester

Every security minded organization enforces the CIA triad (confidentiality, integrity and availability). Penetration testers work to find the weaknesses in the client's environment that would disrupt the CIA triad. The anti-CIA triad is the DDA (Disclosure, Disruption, Alteration). Blue teams try to maintain CIA and red teams try to do DDA.

1.7 Penetration-Testing Methodologies

- White box model
  "Full information"
  - Tester is told about network topology.
  - Floor plan / network plan
  - Interviews with IT personnel and employees.
  - Information for routers, switches, firewalls, and IDS's.
  - List of OS running on systems.

- Black box model
  "No information"
  - Given to details about technologies used.
  - Tester has to find details themselves.
  - Tests security personnel's ability to detect an attack.
  - Staff does not know about the test.
- Gray box model
  "Some information"
  - Hybrid of white and black box model.

1.8 Pen Testing Process

1. Foot-Printing
2. Scanning
3. Enumeration
4. Hacking (4 phases)
   (a) System Hacking
   (b) Covering Tracks
   (c) Planting Backdoors
   (d) Privilege Escalation

After following this 7-step process the tester should be prepared to present a detailed report of their findings. Depending on the statement of work there could be a presentation of the report, a presentation and recommendations, or a presentation and recommendations with remediation.

1.9 Code of Conduct and Ethics

- Keep private and confidential information gained in your professional work.
- Protect intellectual property
- Provide service in your areas of competence, being forthright about limitations.
- Disclosure to appropriate persons or authorities only.
- Never knowingly use a software or process that is obtained illegally or unethically.

- Ensure good management for any project you lead.
- Conduct yourself in the most ethical and competent manner.
- Do not associate with malicious hackers or engage in malicious activity.

1.10 Before a Pen-Test Answer these questions:

- Why did the client request a pen test?
-

2 System Fundamentals

2.1 Knowing Operating Systems

Operating systems offer common vulnerabilities if not configured properly by the administrator. Quite a few organizations are using OS without configuration or are running old versions that could be susceptible to attackers.

2.1.1 Windows

Windows is a large target because of its large user base. An endless stream of updates are hard for users to keep track of. Default configurations are left in place by many users. Old legacy versions are still in use.

Microsoft Server dominates industry server rooms / farms. Many organizations still use outdated servers that are not secure against modern attacks.

2.1.2 Linux

Linux is an advanced operating system for tech enthusiasts. Also popular with pen testers and a widely used Server OS. Linux distros are open source meaning that the responsibility of maintaining the security of the system is on the administrator.

2.1.3 Mac OS X

Security solutions are lacking compared to other platforms, many of its users do not think they are vulnerable. Features are typically all enabled even if the user is not using them, such as 802.11 wireless and bluetooth connectivity that creates a much larger attack surface.

Apple devices do not work well on Windows domains. Some features work well but others will not.

2.1.4 Android

Android is estimated to be on 80% of smartphones in use today. Designed for touchscreen devices. Android has seen rapid growth because of its flexibility and customization and because it is free to use.

Counterfeit devices are cheap and often contain malware. Has similar issues to Linux were there are many different versions.

2.2 Networks

Networks come in four different sizes, based on the scale of the network.

- Personal Area Network (PAN)
- Local Area Network (LAN)
- Municipal Area Network (MAN)
- Wide Area Network (WAN)

2.2.1 Network Types

- Bus
  - All connecting nodes in a single run.
  - Bus is a common link to all machines.
  - All connectivity is lost if the bus is damaged.
  - No true bus-topology is used today.
- Ring
  - Use the common connector in a loop style.
  - Some layouts use concentric rings for redundancy if one fails.
  - Each node attaches to the ring and delivers packets according to its designated turn or availability of the **token**.
- Star
  - Common because of ease of setup and isolation of connectivity problems.
  - Multiple nodes connect to a central network device.
  - Popular because of its resistance to outages.
- Hybrid
  - Most common layout in use today.
  - Current networks are the offspring of many additions and alterations over many years of expansion or changes.
- Mesh
  - Web of cabling that attaches a group of nodes to each other.
  - Often used for mission-critical services because of its high level of redundancy and resistance to outages.
  - The Internet, is one growing complex mesh network.

2.2.2 OSI Model

Operating System Interconnect (OSI). Defines a common set of rules for vendors of hardware and software.

- Layer 1: Physical
  Physical media and dumb devices (cabling, Category 5e, RJ-45 connectors and hubs).

- Layer 2: Data Link
  Ensures that data transfer is free of errors (Media access control MAC, and link establishment). 802.3 Ethernet and 802.11 Wi-Fi protocols.

- LAyer 3: Network
  Determines the path of data packets based on different factors defined by the protocol used. IP addressing for routing data packets (ICMP is here).

- Layer 4: Transport
  Layer ensures the transport re sending of data is successful, includes error checking operations as well as working to keep data messages in sequence.

- Layer 5: Session
  Identifies session between different network entities. Monitors and controls connections, allowing multiple, separate connections to different resources.

- Layer 6: Presentation
  Translates data that is understandable by the next receiving layer. Traffic flow is presented in a format that can be consumed bt the receiver and can optionally be encrypted vis SSL.

- Layer 7: Application
  User platform in whic the user and the software processes within the system can operate and access network resources. Applications and software suites that we use on a daily basis are in this layer.

2.3 4 Phases of Ethical Hacking

2.3.1 Footprinting

2.3.2 Scanning

2.3.3 Enumeration

2.3.4 System Hacking

3 Scanning

3.1 What is Scanning

Scanning is a process that involves engaging and probing a target network with the intent of revealing useful information of networks and systems. Combined with the information from footprinting, it is possible to get a decent picture of a target organization network-map.

With the rapid growth of networks and turnover of personnel, scanning can sometimes give a better network graph that the client can provide.

3.2 Types of Scanning

- Port Scanning
  Sending packets to a target computer with the intent of learning about the port status.
- Network Scanning
  Locate mostly all live hosts on a network.
- Vulnerability Scanning
  Used to identify weaknesses or vulnerabilities on a target system.

3.3 Port Scanning

Port scanning program / tool report:

- Open Ports
  - Allows access to applications / services and can be vulnerable to attack.
- Closed Ports
  - Does not allow entry or access to a service.
- Filtered Ports
  - Open, but might indicate that a firewall is being used to allow specified traffic into or out of the network, through that port.

Is port scanning legal¿ Some states / countries consider it legal.

3.3.1 Types of port scans

1. Connect Scan (Full-open scan)
    - Utilizes three way handshake
    - Completed handshake indicates open port
    -
2. SYN scan (Half scan)
    - Starts like a full scan but does not complete the final step of the handshake.
    - Lower chance of being logged.
3. FIN scan
4. XMAS Scan
    - All flags enabled, combination of flags is illogical and illegal.
    -
5. NULL Scan
6. ACK scan

3.4 Network Scanning

Network scannign is for checking live hosts.

1. Wardialing is the other forms of scanning in that it simply dials a block of phone number using a standard modem to locate systems that also have a modern attached and accept connections. Modems are still in use so a hacker can use
2. pinging
3. ping sweep

3.5 Vulnerability Scanning

3.6 Banner Grabbing

3.7 Scanning anonymity using proxy

3.8 Mapping the network

3.9 Packet crafting and manipulation