Week 9 - Friday

COMP 4290

Last time

- Network basics
- Network threats

Questions?

Project 2

Austin Rheyne Presents

Reconnaissance

Reconnaissance

- A smart attacker learns everything he or she can about the system before attacking it
- Useful methods for reconnaissance of a network include:
  - Port scans
  - Social engineering
  - Dumpster diving
  - OS and application fingerprinting
  - Background research

Port scan

- Many targeted systems include servers that are always listening on various ports, waiting for communication
- A port scanner is a program that tries to connect on many interesting ports to see what kinds of communication is ready to do
- If a server is poorly configured, it might be listening on ports even the administrators don't know about
- Common free port scanners:
  - **`nmap`**
  - **`netcat`**

Social engineering

- **Social engineering** means techniques used to get a human being to unknowingly divulge information to an outsider
- Often this is done by posing as tech support or some kind of contractor
- Attackers can pretend to be someone from another department
- Most employees have been trained to be reluctant to give up their passwords
  - However, they will often reveal their IP address, OS information, and other useful pieces of system information

Gathering more intelligence

- Port scans and social engineering can tell a lot
- **Dumpster diving** or going through trash can tell a lot as well
  - Which pieces of hardware have been bought, by their packaging
  - Phone lists or organization charts could be in the trash
  - Diagrams, notes, even passwords could be written on scraps of paper
  - Old hard drives with sensitive information could turn up
- For high-level attacks, real spying is possible

OS and application fingerprinting

- Port scanning gives a lot of information
  - For example, port 443 is used for HTTPS
- But you may want to know which OS or application is actually listening at a port
  - Vulnerabilities are often system-dependent
- Some applications will reveal themselves directly
- Others will give more information if you ask for a feature that is unavailable or give a bad command
- You are being fingerprinted when you visit websites
  - Your browser identifies which browser it is
  - You can hide this information, but your web pages might look weird

Documentation and hacking tips

- How do you actually do the attack?
- Same as everything else:
  - Google
- Once you know the system you are attacking, you can search the Internet and security blogs and boards for vulnerabilities
- Because networking is often between different kinds of systems running different kinds of software, features are well-documented
  - Most big viruses and worms use publicly known vulnerabilities that haven't been patched

Eavesdropping

Eavesdropping and wiretapping

- **Eavesdropping** means overhearing private information without much effort
  - Administrators periodically need to monitor network traffic
- **Wiretapping** implies that more effort is being used to overhear information
  - **Passive wiretapping** is only listening to information
  - **Active wiretapping** means that you may adding or changing information in the stream

Cable wiretapping

- If you are on the same LAN, you can use a **packet sniffer** to analyze packets
  - Packets are constantly streaming by, and your computer usually only picks up those destined for it
  - Passwords are often sent in the clear
  - Wireshark is a free, popular packet sniffer
- Cable modems are filters that give you only the data you need
  - Sophisticated attackers can tap into a cable network
  - Data is supposed to be encrypted, but many networks don't turn encryption on
- **Inductance** is a property that can allow you to measure the signals inside of a wire without a direct physical connection
- Using inductance or physically connecting to a wire changes its impedance, which can be (but usually is not) measured
- Signals are often **multiplexed**, sharing media with other signals, which can increase the sophistication needed to wiretap

Wireless eavesdropping

- Wireless networks are easy to disrupt, but attackers usually have little to gain by this
- Since they are broadcast, it is not difficult to intercept the signal
  - Special antennas can receive the signal from a longer distance than usual
- Some networks are entirely unencrypted
- WEP is almost completely broken
- WPA and WPA2 have vulnerabilities that can be exploited in some cases

Other media

- Microwave is easy to intercept
  - Long distance phone can use microwaves
  - Cell phones towers can use microwaves
- One difficulty with making use of the intercepted signal is that microwave signals are heavily multiplexed, making it hard to untangle individual signals
- Satellites are similar (unsecure but heavily multiplexed)
- Optical fiber is very difficult to tap
  - Cutting a single fiber means recalibrating the network
  - Repeaters and taps that connect the fiber are the best places to attack

Impersonation

- Rather than wiretapping, attackers will more often try to impersonate a legitimate user
- Different approaches:
  - Guess the identity and authentication information
  - Use other communications or wiretapping to gain such information
  - Circumvent the authentication mechanism
  - Use a target that will not be authenticated
  - Use a target with known authentication data

Authentication issues

- Passwords are often easy to guess
  - Because we're bad at picking passwords
  - Because the user may not have realized that the machine would be exposed to network attacks
- Passwords are sent in the clear
- Bad hashes can give information about the password
- Sometimes buffer overflows can crash the authentication system
- Sometimes authentication is not needed
  - **`.rhosts`** and **`.rlogin`** files in Unix
  - Guest accounts
- Default passwords on routers and other devices that never get changed

Authentication attacks

- **Spoofing** is when an attacker carries out one end of a networked exchange
- A **masquerade** is spoofing where a host pretends to be another host
  - URL confusion: someone types **`hotmale.com`** (don't go there!) or **`gogle.com`**
- **Phishing** is a form of masquerading
- **Session hijacking** (or **sidejacking**) is carrying on a session started by someone else
  - Login is encrypted, the rest of the data isn't always (though it increasingly is, through HTTPS)
  - Firesheep was a browser plugin that allowed you to log on to other people's Facebook and Twitter accounts in, say, the same coffeeshop (but it no longer works)
- **Man-in-the-middle** attacks

Confidentiality threats

- Misdelivery
  - Data can have bad addresses, occasionally because of computer error
  - Human error (e.g. James Hughes (student) instead of James Hughes (professor)) is more common)
- Exposure of data can happen because of wiretapping or unsecure systems anywhere along the network
- Traffic flow analysis
  - Data might be encrypted
  - Even so, it is very hard to hide where the data is going to and where it is coming from
  - Tor and other anonymization networks try to fix this

Integrity threats

- Attackers can falsify some or all of a message, using attacks we've talked about
  - Parts of messages can be combined
  - Messages can be redirected or deleted
  - Old messages can also be replayed
- Noise can degrade the signals
  - All modern network protocols have error correction built in
- Malformed packets can crash systems
- Protocols often have vulnerabilities

Wireless Network Security

WiFi technology

- WiFi signals are radio signals that anyone in range can pick up
- WiFi is built on a set of protocols defined by the 802.11 standards
  - Most of these protocols communicate in the 2.4 and 5 GHz ranges
  - Older protocols can reach about 300 feet and 802.11n may be able to reach 5,000 feet
- A wireless **access point** communicates with a **network interface card** (NIC)
- MAC addresses are used to identify physical devices

Mechanics

- Management frames are data exchanged by access points and routers to structure communication
  - **Beacon frames** announce the presence of an access point
  - **Authentication frames** allow NICs to request access to an access point
  - **Association frames** allow NICs and access points to agree on how to communicate
- The **Service Set Identifier (SSID)** is a string that identifies an access point

WiFi vulnerabilities

- SSIDs do not need to be broadcast
  - However, when someone joins the access point, the SSID is revealed
- Access points associate a computer with a MAC address
  - But MAC addresses can be spoofed!

WEP

- The original system for encrypting wireless communication was Wired Equivalent Privacy (WEP)
  - WEP is not secure!
- WEP keys are effectively either 40 bits (breakable!) or 104 bits
- Static keys are used
- A flaw in the RC4 algorithm allows even 104-bit keys to be broken in minutes
- WEP does no authentication

WPA

- **WiFi Protected Access** (WPA, WPA2, and WPA3) was created to replace WEP
- WPA uses a different key to encrypt each packet
- Authentication for WPA is better (although still uses a shared secret for home use)
- WPA has a better integrity check than WEP
- WPA2 adds AES for encryption, much stronger than RC4
- WPA3 was supposed to make it harder to collect information and brute force the key
- Although each version improves on earlier weaknesses, there are attacks on WPA, WPA2, and WPA3 that can make it possible to intercept wireless traffic

Weaknesses of WPA

- Man-in-the-middle attack is still possible
  - The attacker convinces the access point that he's the user and convinces the user that he's the access point
  - Requires spoofing MAC addresses
- Brute force attacks
  - WPA allows users to select passphrases
  - Users often select poor passphrases
  - Some practical attacks against integrity exist in WPA (but not WPA2)

Denial of Service

Denial of service

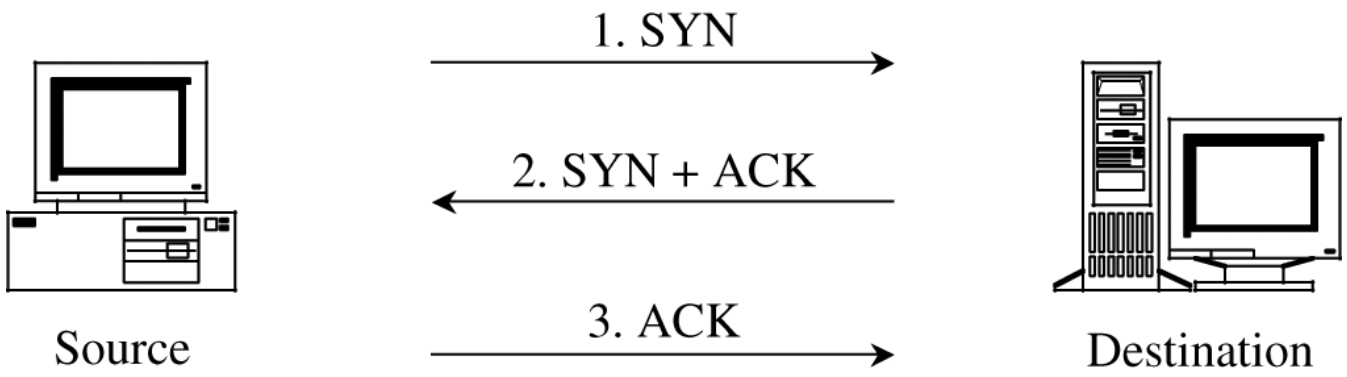
- Networks are one of the best places to launch an attack on availability
- In this setting, these are usually called **denial of service** (DoS) attacks
- DoS attacks are very hard to avoid

Ways to make DoS happen

- Flooding overloads capacity
  - Ask for too many connections
  - Request too many of some other service
- Blocking access
  - Crash an application
  - Interfere with network routing protocols
- Access failure
  - Hardware or software fails

SYN flood

- TCP is built on a three-way handshake
  - Client requests a connection by sending a **SYN** packet
  - The server acknowledges the request by sending a **SYN-ACK** packet back
  - The client responds with an **ACK**, establishing the connection
- An attacker can just keep sending **SYN** packets
- The server will allocate some resources, wait for the **ACK**, and never get it
- A clever attacker will spoof at least his own IP so that the **SYN-ACK** is sent elsewhere
- A more sophisticated attacker will spoof many different IP addresses (or have many bots in a botnet) sending all these **SYN**'s

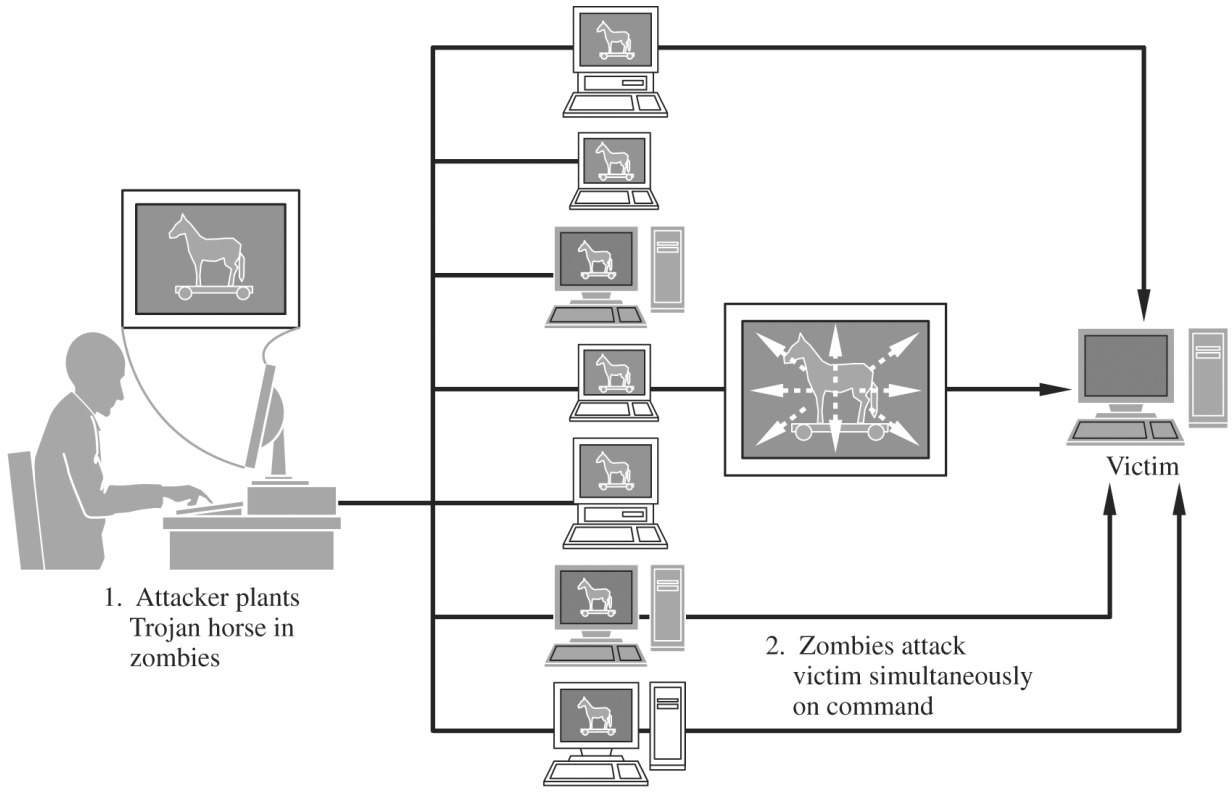


Other denial of service attacks

- Echo-chargen
  - Chargen sets up a stream of packets for testing
  - Echo packets are supposed to be sent back to the sender
  - If you can trick a server into sending echo packets to itself, it will respond to its own packets forever
- Ping of death
  - A ping packet requests a reply
  - If you can send more pings than a server can handle, it goes down
  - Only works if the attacker has more bandwidth than the victim (DDoS helps)
- Smurf
  - A ping packet is broadcast to everyone, with the victim spoofed as the originator
  - All the hosts try to ping the victim
  - The real attacker is hidden
- Teardrop
  - A teardrop attack uses badly formed IP datagrams
  - They claim to correspond to overlapping sequences of bytes in a packet
  - There's no way to put them back together and the system can crash

Distributed denial of service

- **Distributed denial of service** (DDoS) attacks use many machines to perform a DoS attack
- Usually, many targets have been compromised with a Trojan horse making them **zombies** or **bots**
- These zombie machines are controlled by the attacker, performing flooding or other attacks on a victim
  - A network of zombies is called a **botnet**
- The attacker is hard to trace



Stopping DDoS attacks

- The best defense is prevention
  - DDoS attacks are usually mounted by bots that were compromised by known vulnerabilities
  - Patch your stuff!
- Defense against DoS attacks:
  - Tuning: adjusting the number of active servers
  - Load balancing: redirecting traffic to servers that aren't getting used
  - Shunning: reducing service given to certain IP addresses
  - Blacklisting: ignoring traffic from known bad IP addresses

DNS attacks

- The Domain Name System (DNS) uses Domain Name Servers (also DNS) to convert user readable URLs like **`google.com`** to IP addresses
- Taking control of a server means that you get to say where google.com is
  - Called **DNS spoofing**
- For efficiency, servers cache results from other servers if they didn't know the IP
  - **DNS cache poisoning** is when an attacker gives a good server a bad IP address

Summary of vulnerabilities

Target	Vulnerability	Target	Vulnerability
Precursors to attack	• Port scan • Social engineering • Reconnaissance • OS and application fingerprinting	**Confidentiality**	• Protocol flaw • Eavesdropping • Passive wiretap • Misdelivery • Exposure • Traffic flow analysis
Authentication failures	• Impersonation • Guessing • Eavesdropping • Spoofing • Session hijacking • Man in the middle attack	**Integrity**	• Protocol flaw • Active wiretap • Impersonation • Falsification • Noise • Web site defacement • DNS attack
Programming flaws	• Buffer overflow • Addressing errors • Server-side include • Malicious Java or ActiveX • Worms, viruses, Trojan horses	**Availability**	• Protocol flaw • Transmission failure • Flooding • DNS attack • Traffic redirection • DDoS

Ticket out the Door

Upcoming

Next time…

- Network controls
- Colm Oneacre presents

Reminders

- Keep reading Sections 6.6 through 6.9
- Finish Project 2
  - **Due tonight!**