CMSC 426
Principles of Computer Security

Network Attacks

Last Class We Covered

- Intro to TCP/IP model

- Link layer
- Internet layer
- Transport layer
- Application layer

Any Questions from Last Time?

Today's Topics

- Network attacks on the different layers
  - Link layer
  - Internet layer
  - Transport layer
  - Application layer

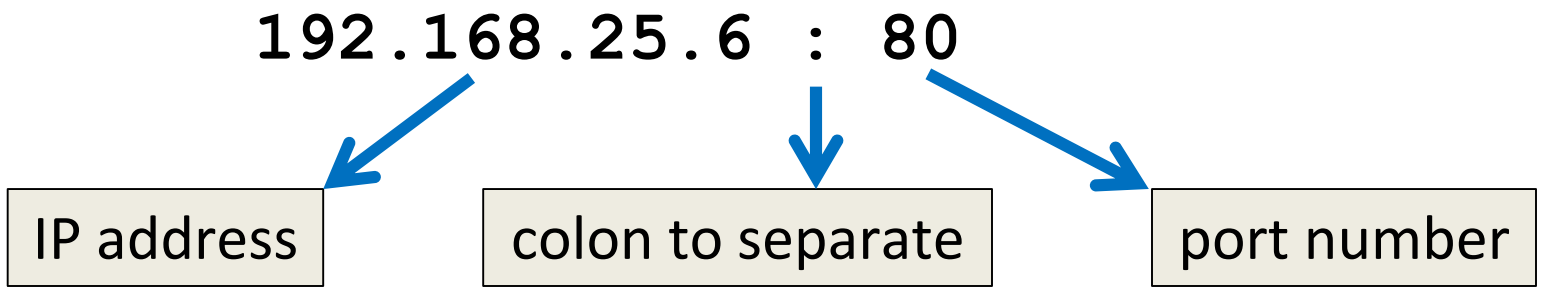
- Network Security

Quick Info: Ports

- IP addresses are used to identify individual machines
  - Information is accepted via different ports

- Some ports are associated with specific application layer services
  - HTTP uses 80, SSH uses port 22, SMTP uses 25, FTP uses 21, etc.

- If you've heard the term "socket," that's an IP address and a port



Link Layer Attacks

Link Layer Attacks: ARP

- Address Resolution Protocol, used to convert between MAC address and IP address

- ARP spoofing
  - Attacker spoofs ARP messages to the local network, linking the victim's IP address to the MAC address of the attacker
  - Causes all of the victim's traffic to be redirected to the attacker
  - Attacker may simply "sniff" the traffic and send it on to the victim, or they may selectively allow some/none of the traffic through
  - Can be the start of other attacks (MITM, denial-of-service, etc.)

Link Layer Attacks: ARP (cont)

- ARP poisoning
  - Attacker sends spoofed ARP messages to the victim, “poisoning” their ARP table, causing messages they send out to possibly be routed to the incorrect MAC address for the given IP address

- ARP man in the middle (MITM)
  - Attacker spoofs two machines (two different IP addresses, one MAC address “M”), and conveys to Alice that Bob’s IP address matches with M, and to Bob that Alice’s IP address matches with M
  - All traffic between Alice and Bob now flows through the attacker’s machine, located at MAC address “M”

Internet Layer Attacks

Internet Layer Attacks: IP Spoofing

- IP address spoofing
  - Source address in an IP packet is spoofed
  - Attacker will not receive any returned messages

- Multiple uses (some are even legitimate)
  - Use a trusted IP address to authenticate to a network
  - Use different IP addresses in a denial-of-service attack to make it difficult for the victim to filter the messages based on IP address
    - A similar tactic is used when a network, website, or service is having a performance test run on it

Transport Layer Attacks

Transport Layer Attacks: Prediction

- In TCP's three-way handshake, there is a sequence number, used to assure that the packets were transmitted chronologically
  - Client: SYN → seqX
  - Server: SYN ACK → seqX + 1 and seqY
  - Client: ACK → seqX + 1 and seqY + 1
- One number is updated, the other is the one expected

- To take advantage of this, need to correctly predict the numbers
  - If working blindly, the chances are small (one in billions)
  - Better solution would be a MITM attack

Transport Layer Attacks: Hijacking

- On an unencrypted connection, an attacker can observe every packet being passed between client and server
  - This means attacker can also see the SYN-ACK sequence numbers

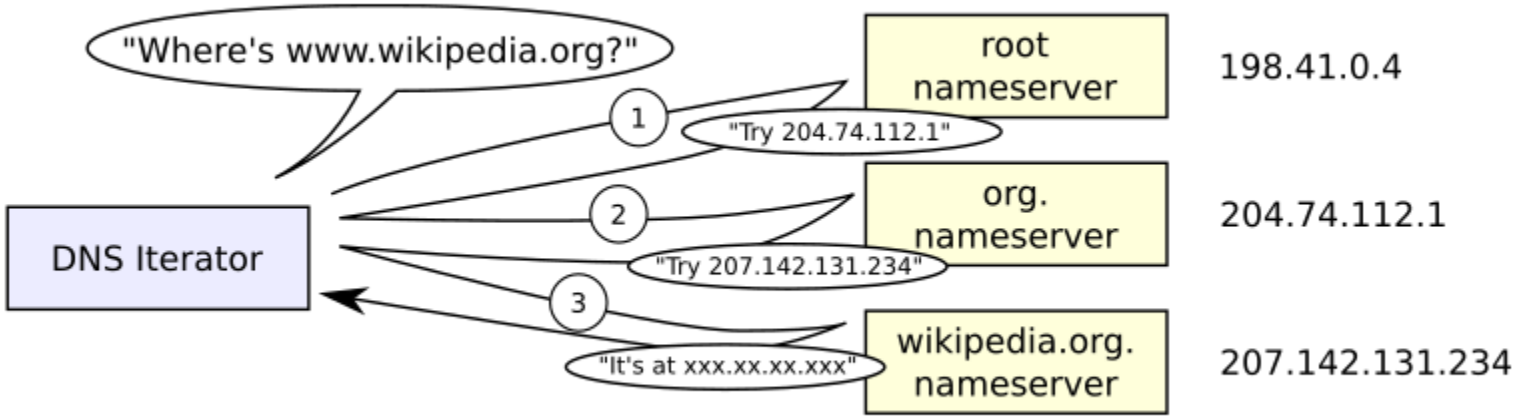
- Attacker can create a new message, using the observed source and dest. IP, sequence number, etc. and send it to the server
  - Server will accept the message and increment the sequence number
  - Now when the victim sends a legitimate message, the server will think that the sequence number is “outdated” and drop the connection

Application Layer Attacks

Quick Note: More Information on DNS

- Domain Name System, resolves domain names to IP addresses
  - System is hierarchical, and uses caching for further speed-ups
  - Root name servers store addresses of authoritative name servers for their subdomains, which in turn store addresses of host in their domain

- DNS is usually sent in UDP, not in TCP
  - Why?
  - Speed!



App Layer Attacks: DNS

- DNS cache poisoning
  - Specific DNS servers are set to cache DNS query results to reduce the strain on the overall DNS system and to improve performance
  - DNS cache servers will pull information from each other as well

- Cache poisoning involves creating false entries in the DNS cache of a local name server
  - Because cache servers pull from each other, it's possible for the "poison" to spread

Cache Poisoning

- The “Great Firewall of China” uses deliberate cache poisoning
  - The domain name servers return invalid IP addresses for sites that are blocked (along with other methods)

- In 2010, at least one ISP began fetching DNS information from a root DNS server based in China
  - The deliberate cache poisoning spread outside of China
  - Users could not access Facebook, YouTube, or Twitter
  - This affected people in the United States and Chile

Information from https://www.computerworld.com/article/2516831/security0/china-s-great-firewall-spreads-overseas.html

DDoS Attacks

- Distributed Denial-of-Service

- Large-scale DoS attack using hundreds or thousands (or more) unique IP addresses to overwhelm a system
  - Difficult to distinguish legitimate traffic from the attack
  - Attack cannot be thwarted by blocking a few IP addresses

- Often carried out via botnets, as a single machine (even one spoofing unique IP addresses) is still not capable of pushing out hundreds of GBs of traffic and requests per second

Network Security

Firewalls: Host-Based vs Network-Based

- Host-based firewalls are installed on each individual device
  - Different users may have different configurations, either due to knowledge or preference
- Network-based firewalls filter the data as it travels into or out of the network as a whole
  - Single set of rules for all connected devices
  - Someone who knows what they're doing configures it (we hope!)
- Ideally use both, if only to make an attacker's job more difficult if they make it through the network-based firewall

Information from https://www.wideband.net.au/blog/host-based-vs-network-based-firewalls/

Firewall Types

- Packet filters
  - Monitor incoming and outgoing packets, and filter based on criteria
  - Criteria include source and destination addresses, as well as protocol
- Stateful filters
  - Tracks the state and characteristic of network connections made
  - Allows packets only if they are from a known accepted connection
- Application layer
  - Firewall policy can control traffic on specific applications or services
  - Can “understand” things like FTP and DNS, and detect if protocols are unwanted, being used on a non-standard port, etc.

Internet Layer Attacks: IP Fragmentation

- Fragmentation is exactly what it sounds like: breaking up IP packets into multiple smaller packets
  - Happens when a single IP packet exceeds the maximum size allowed

- Fragmented packets means the TCP header is also fragmented
  - A fragmented header is difficult for a firewall to read and parse
  - Some firewalls only inspect the first fragment, and let the rest of the fragments go through uninspected
  - This means it is possible to get a payload into a system by splitting it among fragments (although they still must follow certain rules in order to be re-assembled at the end)

Ingress and Egress Filtering

- Each has different criteria and scenarios they wish to prevent
- Ingress means scanning incoming packets
  - Check packet header for origin, and ensure it matches as expected
  - Also prevent incoming packets from certain addresses
  - Can be thwarted by IP address spoofing
- Egress means scanning outgoing packets
  - Ensure that disallowed or malicious traffic does not leave the network
  - *e.g.*, not spreading malware, blocking certain sites or applications

IDS and IPS

- Intrusion Detection System
- Intrusion Prevention System
  - Both monitor networks and systems for malicious activities
  - Look for known signatures, and sometimes anomalous behavior

- IDS only detects, followed by notifying and logging
- Often an extension of IDS, IPS can perform more actions
  - *e.g.*, dropping malicious packets, blocking “bad” IP addresses, etc.

Virtual Private Network (VPN)

- "Extends" a private network across a public network
  - Uses IP tunneling, in which the data portion of a packet carries the actual packets being transmitted, encapsulating them
  - Traffic is thus "repackaged" using encryption, hiding the nature and details of the traffic from anyone listening in (not even the ISP)

- Using a VPN can protect from a number of attacks
  - Including DNS poisoning, as many have their own name servers

Information from https://www.pcmag.com/article2/0,2817,2403388,00.asp

Tor (The Onion Router)

- Software that enables anonymous communication
- Directs a user's internet traffic via onion routing
  - Multiple "hops" are used to get the user to their desired destination, with encryption used at each step to hide the path and information

- Encryption occurs in the application layer
  - Multiple layers of encryption, like layers of an onion

How Tor Works

- Tor encrypts the data multiple times
  - Including the next node destination IP address
  - Sends it through a virtual circuit of successive, random Tor relays
- Each relay decrypts a layer of encryption to reveal the next relay in the circuit to pass the remaining encrypted data on to
  - Final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing or knowing the source IP address
- Routing is (partly) concealed at every hop in the Tor circuit
  - Eliminates any single point of failure

Information from https://en.wikipedia.org/wiki/Tor_(anonymity_network)

Announcements

- Dr. Gibson's OH for this coming Monday are cancelled
- Lab 4 will be released this week
  - Total VM size will be large (~20 GBs) so prepare your machine
- Homework 4 will be released next week
- Final exam is Thursday, December 13th at 3:30 PM

Image Sources

- DNS resolution
  - https://en.wikipedia.org/wiki/File:Example_of_an_iterative_DNS_resolver.svg