Holes in the Fence

Prevention of Security System breaches of networked Edge Devices

Presented By:

- Dave Engebretson, Contributing Technology writer, *SDM* Magazine
- Industry Instructor in Fiber and Networking

CompTIA Network+™ Certified

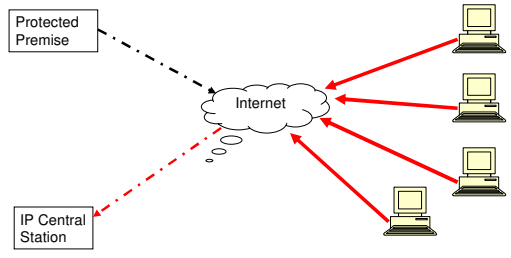
Agenda

- Why Network Security is important
- Goals of Proper Network Security
- Types of Threats
- Types of Attackers
- Why Networks are Vulnerable
- Attack Techniques
- Attack Tools & Methods
- Options for Securing Networks

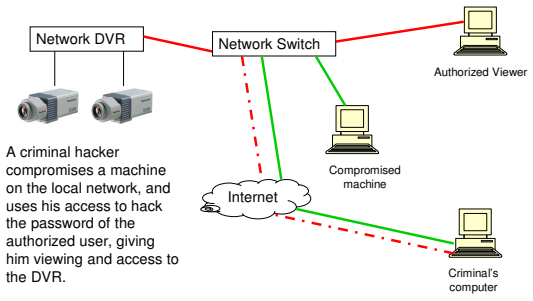
Why Network Security is Important

- Putting Cameras, DVRs, Access and Alarm Transmitters onto networks creates opportunities for inside and outside hackers

DDos Attack



IPCCTV Attack



A criminal hacker compromises a machine on the local network, and uses his access to hack the password of the authorized user, giving him viewing and access to the DVR.

- Physical Security Integrators need to understand the threats and how to protect against them

Goals of a Secured Network

- Confidentiality – Secrecy and Privacy of information transfers
- Integrity – Information is correct and unaltered
- Availability – Authorized users can access information and applications when needed

Types of Threats

- Unauthorized access
- Stolen/damaged/modified data
- Disclosure of confidential information
- Hacker attacks
- Cyber Terrorism/Extortion
- Viruses and malware
- Denial of service

Types of Attackers

- Script Kiddies – Young hackers who download programs from the Internet, hack into random targets
- Disgruntled (former) Employees – Hacks specific target for revenge
- Cyber Criminals – Hacks for payoff/extortion
- System Crackers – Highly skilled, very knowledgeable about operating system vulnerabilities

Why Networks are Vulnerable

- Basic network technologies are “open” – all machines talk to each other, protocols are common knowledge
- Internet connections exposes 1000’s of networks on the grid
- Poor network management and planning – Lack of firewalls, poor password management

Why Networks are Vulnerable

- Physical Security Issues – Control of access to machines & network connections
- Volume of network traffic
- Any door will do – If a hacker can get into a single machine on a network, they can use that machine to hack into another on that network

IP Packet Problems

- IP packet information can be manipulated
- Software programs readily available that can change any aspect of a packet
- Packets can be manipulated to probe networks or shut down servers or devices

Operating System Fingerprints

- Network machines use an “OS” (operating system) program to perform underlying and basic functions
- Linux and Windows are the most common OS in use
- All OS have vulnerabilities that hackers can exploit
- Each OS handles specific packets and communications differently – identifies the OS of a server when probed by a hacker

IP Header Structure

Version	IHL	Type of Service	Total Length
Identification	Flags	Fragment Offset	
Time to Live	Protocol	Header Checksum	
Source Address			
Destination Address			
Options			Padding

Any aspect/setting of an IP packet can be manipulated.

Modified packets are called “raw.”

General Attack Methods

- Reconnaissance
- Scanning
- Gaining Access
- Escalating Privileges
- Exploiting Access
- Covering Tracks & Maintaining Access

Reconnaissance

- Passive Surveillance
- Web sites, company literature
- Sitting in parking lot
- Dumpster diving

Reconnaissance

- Social Engineering – Acting like you’re someone else (on the phone, fax, email or in person) to gather information to help attack a network – passwords, modem dial in numbers, server IP addresses, etc.
- Rogue Access Point – Placing a Wi-Fi device in or near a building to fool wireless devices

Google Hacking

- Search: allinurl:tsweb/default.htm

Reconnaissance

- Determining Network Range
- Dnsstuff.com demo

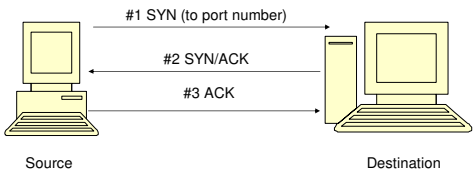
Scanning

- Where and What – Gathering the IP addresses of devices on the network, and what OS they're using
- Hackers scan networks with a variety of tools
- Ping – Some networks turn off "ping" (ICMP) responses

Scanning

- TCP 3 Way Handshake
- Hackers can send modified and/or out of sequence packets to gather responses from target machines

TCP Three-Way Handshake



Either side can send a "RST" flagged packet to end the communication.

Scanning

- TCP/IP Ports – specific ports must be open to provide connections/communications
- 65,535 available ports
- Common Ports – services like DNS, FTP, HTTP, often use specific port numbers

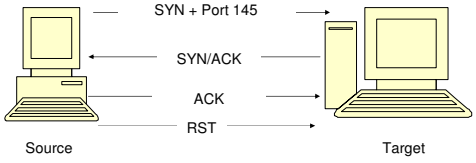
Scanning

- Hackers scan for port status:
- Closed – responds to scan, not available for communications
- Open – services available, will communicate
- Stealth – doesn't respond to scan, status unknown
- Filtered – Behind firewall which restricts access

Scanning

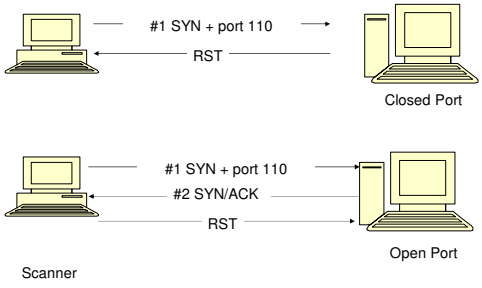
- Port Scan Options

TCP Connect Scan

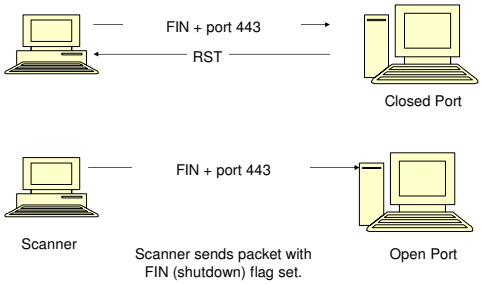


This scan attempts to establish full connections with each port on the target machine.

TCP SYN Scan

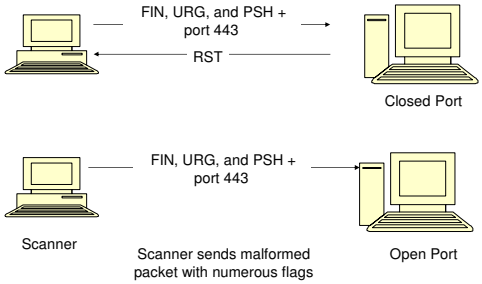


TCP FIN Scan



Scanner sends packet with FIN (shutdown) flag set.

TCP XMAS Scan



Scanner sends malformed packet with numerous flags set.

Scanning

- Why different port scans?
- Different scans for different OS
- Security settings/firewalls can make one scan work better than another

Scanning

- OS Fingerprinting – Different OS manipulate packets in distinct ways
- IP TTL
- TCP Window Size
- Fragmentation Handling
- IP type of Service Flag

Scanning

- OS need security patching
- Version of OS will indicate level of security patching
- Known vulnerabilities can be exploited

Gaining Access

- Buffer Overflow
- Password Cracking
- Social Engineering
- Hacker doesn't have to access primary attack – get onto another machine, gain access, install sniffer, figure out how to gain access to main target

Gaining Access

Buffer Overflow – Entering illicit command data into an available input on a server

Gaining Access

- Password Cracking/Theft
- 60% of unauthorized network usage comes from manipulation of passwords
- Brute force attack

Escalation of Privileges

- Hacker wants “administrator” or “root” passwords – allows complete control of network and/or devices

Exploiting Access

- Install sniffers to gather packets – email out or dump to internal file
- Steal other passwords
- Observe network activity
- Install rootkits – software that attaches to OS, allows hacker access, hides hacker activities

Covering Tracks & Maintaining Access

- Erase/change log files
- Add users/passwords
- Fix original vulnerability that let the hacker into the network
- Open TCP/IP ports
- Install Keystroke loggers

Attack Tools & Methods

- Nmap – multi-tool network scanner software
- DEMO

Attack Tools & Methods

- Ethereal – Packet sniffer and protocol analyzer
- DEMO

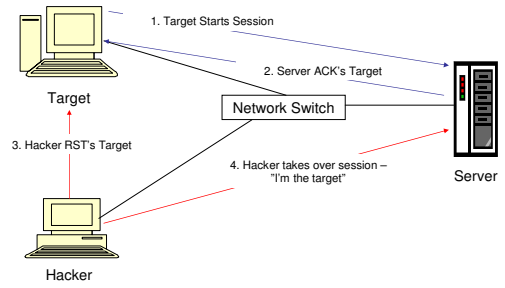
Attack Tools & Methods

- Etherflood – Floods switch with random MAC addresses – can force switch to broadcast all packets
- DEMO

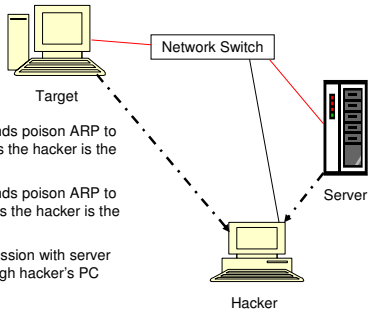
Attack Tools & Methods

- SMAC – MAC address disguises
- DEMO

Session Hi Jacking



Man in the Middle Attack

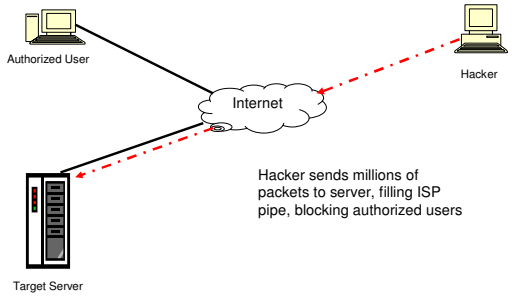


1. Hacker sends poison ARP to target, says the hacker is the server
2. Hacker sends poison ARP to server, says the hacker is the target
3. Target's session with server flows through hacker's PC

Attack Tools & Methods

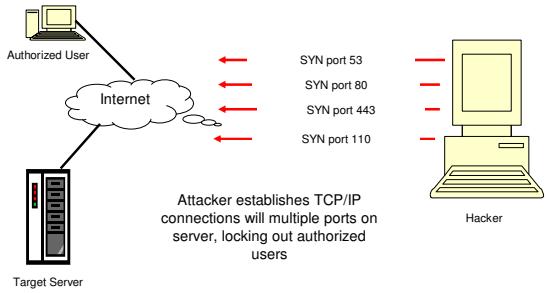
- Denial of Service Attacks
- Stop a network or service from operating
- Cut the phone lines, or attack over the network

Bandwidth Consumption DoS Attack



Hacker sends millions of packets to server, filling ISP pipe, blocking authorized users

SYN Flood DoS Attack

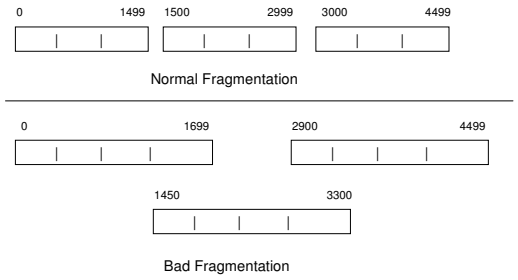


Attacker establishes TCP/IP connections will multiple ports on server, locking out authorized users

Attack Tools & Methods

- Bad Fragmentation DoS
- Large files are transmitted as “fragmented” packets, with start and stop bit flags set
- “Bad” fragmentation can lock up some OS

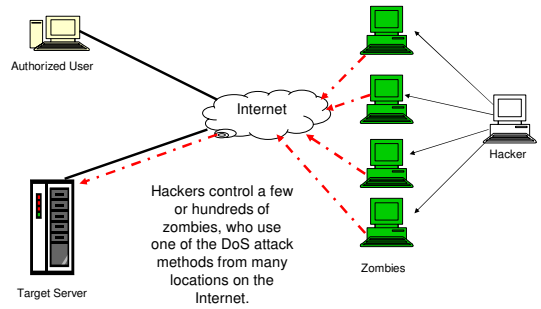
Bad Fragmentation DoS Attack



Attack Tools & Methods

- Ping of Death DoS
- Attacker sends huge “Ping” packets at target, larger than 65,536 bytes
- Receiving server locks up when attempting to reassemble the packets

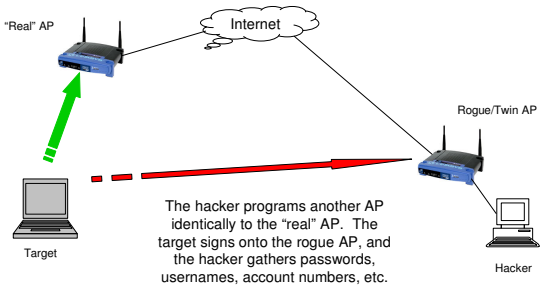
Distributed DoS Attack



Attack Tools & Methods

- Wi-Fi Attacks
- WEP vulnerabilities
- Airsnort Demo
- Evil Twin AP attack

Rogue/Evil Twin AP



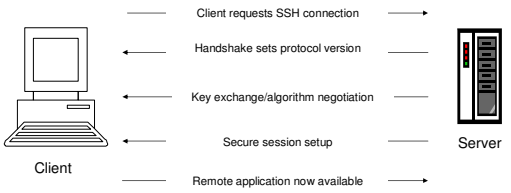
Options for Securing Networks

- Strong Passwords
- Passwords need to be at least eight characters, letters, numbers, symbols, capitals and lower-case letters
- Passwords need to be changed regularly

Options for Securing Networks

- Data Encryption
- SSH – Secure Shell
- SSL – Secure Socket Layer

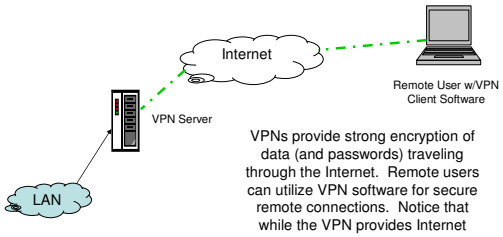
SSH Negotiations



Options for Securing Networks

- SSL – Provides encrypted communications over the Internet
- Uses port 443 as a default
- Passwords and data are encrypted
- DEMO- file

Virtual Private Network



VPNs provide strong encryption of data (and passwords) traveling through the Internet. Remote users can utilize VPN software for secure remote connections. Notice that while the VPN provides Internet encryption, its likely that the data in the LAN is cleartext.

Options for Securing Networks

- Network Intrusion Detection systems
- Devices placed at ingress/egress points of network that detect unusual network traffic

Options for Securing Networks

- Firewall types
- Packet Filtering – each packet entering network is compared to an set of rules (access control list – ACL).
- Options include: IP address to/from, source/destination port, TCP flags, protocols, direction in/out

Options for Securing Networks

- Firewall types
- Stateful Inspection – maintains a "state table" and allows or denies packets based on the state of the connection – keeps track of TCP three-way handshakes

Options for Securing Networks

- Deny All doctrine
- Close off all ports, protocols, IP addresses that are not needed for communications

Options for Securing Networks

- Egress Filtering
- What goes out of a network can be more important that packets coming in. Firewalls can be configured to watch for suspicious packets leaving the network.

Options for Securing Networks

- Patch Maintenance
- Security vulnerabilities will be found. Security contractors need to consider their devices and ask these questions:
- Can the device be patched?
- How will patches be installed?
- Who will do the patches at a remote location?

Options for Securing Networks

- Connection Security
- Turn off unused switch ports
- Physical security of telecom closets
- Periodically check for rogue access points
- Require regular password changes
- Increase employee awareness of social engineering schemes

Options for Securing Networks

- Understand the threat
- Security Patch maintenance
- Scan networks for vulnerabilities and fix'em

Reference Sources

- *Certified Ethical Hacker*, Michael Gregg, Que Publishing
- *Security+ ExamCram2*, Kirk Hausman, Que Publishing
- *Secrets and Lies*, Bruce Schneier, Wiley Publishing