Network Attacks

Denial-of-Service & Man-in-the-Middle

Agenda

- Two categories of attacks on networks
  - Denial-of-Service
  - Man-in-the-Middle
- Defence

(D)DoS & MitM

- Denial-of-Service Attacks
  - An attacker sends packets until your server fails
- Distributed Denial-of-Service Attacks
  - Many attackers (and/or bots) send the packets
- Man-in-the-Middle Attacks
  - An attacker places themselves between two parties

Where's the threat?

Denial-of-Service

- Single attacker
- Quite literal
  - Deny access to a service
  - Impair function of a service
- Probably the strongest attack against availability

Security 360

Distributed Denial-of-Service

- Multiple attackers coordinate
  - Geographically separate
  - Usually involves a botnet
- BOTNET
  - Infected hosts (zombies/slaves) unwillingly and unknowingly participate in the attack

Mirai

- Largest botnet at the time (2016)
  - > 1Tbps & 600,000 affected devices
- nmap scans for open ports 23/22 (Telnet/SSH)
  - Try a simple list (~10) of common username/passwords
  - Targets IoT devices with default credentials
- Drop bot code on the device
  - Bot connects to command & control
  - C&C orders the attack when many bots are connected

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J.A., Invernizzi, L., Kallitsis, M. and Kumar, D., 2017. Understanding the mirai botnet. In *26th {USENIX} Security Symposium ({USENIX} Security 17)* (pp. 1093-1110).

Motivations

for launching a denial-of-service

- Public & popular websites
  - To make a point
  - Political, environmental, socio-economic
- Company websites & servers
  - To make a point / €€€
  - To draw attention away from another simultaneous attack

The rise of hacktivsm

Security 360

The Electrum DDoS Attack

- Electrum
  - Enhanced Bitcoin Wallet
  - Adds some enhanced functionality
  - Checks when transactions are verified

- Users should connect to Electrum servers
- Attackers create malicious servers
- DDoS the real servers
- Users get forced onto malicious servers

Security 360

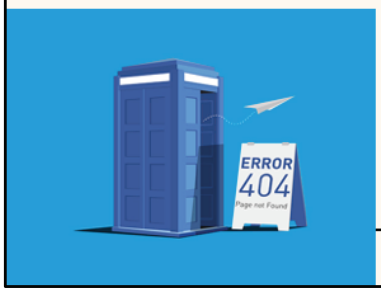
Measuring Attacks

91% UK businesses affected by Denial-of-Service

£140 000 cost of the average attack

£1 000 000 000 total cost to UK businesses

NETSCOUT report 2018



Measuring Uptime

- Service Level Agreement (SLA)
  - A uptime promise from a service provider

99.99% (~4m downtime per month)	
99.9% (~43m downtime per month)	Google Cloud credits 10%
99% (~7hrs downtime per month)	Google Cloud credits 25%
95% (~36hrs downtime per month)	Google Cloud credits 50%

Common (D)DoS Attacks

- SYN Flood
- UDP Flood
- HTTP Flood
- ICMP Flood
- Ping of Death
- Smurf Attack
- Fraggle Attack
- Slowloris

Security 360

Floods (resource exhaustion)

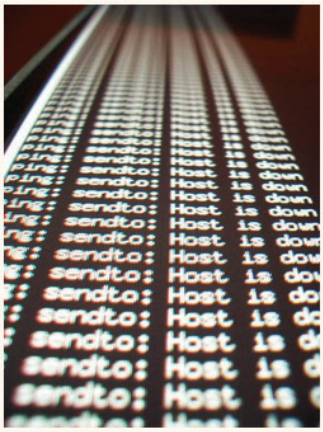
- SYN Flood (remember the 3-way handshake?)
  - Attacker sends SYN packets to all victim ports
  - Never responds with ACK, victim waits patiently
  - Holding all the open connections == DoS
- UDP Flood
  - Attacker sends lots of UDP packets to victim
  - When UDP hits a port without a service, it responds to tell the attacker it failed
  - Responding to all the attacker packets == DoS

HTTP Floods

- Attacker sends HTTP requests
  - GET requests
    - Requests generate info
    - Return to user
  - POST requests
    - Requests take info
    - Send to database/backend
- Server unable to handle them
- Insufficient resources == DoS

ICMP Flood, Ping of Death

- PING! An echo request
  - Alice says hi, Bob says hi
  - Protocol: ICMP (in an IP packet)
- ICMP Flood – A flood of pings
- Ping of Death (patched)
  - Send an IPv4 packet which is too big
  - Attacker receives it, system crashes
  - Returned in 2012 with IPv6! (patched)



Flood Barriers

- **SYN** Flood Defence
  - Firewall limiting connections over time
- **UDP** Flood Defence
  - Firewall closing/limiting UDP ports
- **ICMP** Flood Defence
  - Firewall disabling ICMP requests

Smurf Attack

- An ICMP Flood, in reverse
- Attacker spoofs victim IP
- Attacker pings a special network address
  - **Broadcast Address** - forwards packet to entire network
  - (patched)
- Entire network responds to the ping (@victim IP)
- Victim resources overwhelmed == DoS

Security 360

Slowloris

- Send HTTP requests to victim
  - But slowly this time
- Connections open...
- Connections still open...
- ...just before connection timeout
  - Send another HTTP header!
- And repeat

Affects threaded servers (Apache, Flask)

Security 360

Defending Slow Attacks

- Web server configuration
  - Adjusting the timeout rate
  - Limiting connections per IP
  - Server firewall alerts
- OS Firewall configuration
  - Limiting concurrent connections

Security 360

Man-in-the-Middle

- An attacker places themselves between two legitimately communicating parties
- Receives the packet, and forwards it on

Introducing Mallory

Being in the middle

- You sniff all the traffic between parties
  - No longer limited by switches/MAC addressing
- **tcpkill** – end the connection with an **RST** packet
- **mailSnarf**/**fileSnarf** – view victim emails/files
- **ssldump** – dump victim HTTPS packets
  - Later, find the key and decrypt! (< TLSv1.3*)

Security 360

Suites: dsniff / cain & abel

RSA in <=TLSv1.2 has no “forward secrecy”, so if we get the key later, we can decrypt the data
DHE (Diffie-Hellman Ephemeral) in TLSv1.3 uses a new key for each communication, so is safe (provides forward secrecy)

Getting in the middle

- ARP Cache Poisoning
- DNS Cache Poisoning
- Session/Cookie Hijacking
- SSL Hijacking
- Pineapples

Security 360

ARP Poisoning

- Address Resolution Protocol (L3)
  - Matches IPv4 with MAC Address
  - Sends an ARP request to network
    - *who-has 192.168.1.1 ?*
  - Stores the reply in the ARP Cache
    - Avoids performing the lookup each time
- Mallory sends fake ARP messages
  - Associates own MAC with victim/server IP
  - Cache updated with incorrect addresses
  - Traffic passes through the attacker

Security 360

DNS Spoofing/Poisoning

- Altering DNS queries/entries to point to a malicious server

1. As a follow-up to ARP poisoning
   - DNS queries pass through the attacker now
   - Attacker sends back a malicious DNS response
2. By compromising the DNS server itself
   - Injecting fake DNS entries into the DNS server

Antidotes

- ARP
  - Static ARP entries
    - Fixed MAC - IP resolution
  - Tools: ArpON
- DNS
  - Trusted, secure DNS servers
  - DNSSEC
    - Cryptographically signed DNS responses

Ipv6 is affected by neighbour discovery spoofing

Session Hijacking
Cookie Hijacking

1. Follow-up another MitM (side jacking)
   - Sniff & steal the cookie as it passes the attacker

2. Attacker sends a malicious link (fixation)
   - URL to the trusted site
   - Which defines a specific **session ID**
     - The attacker creates their own cookie with this session ID

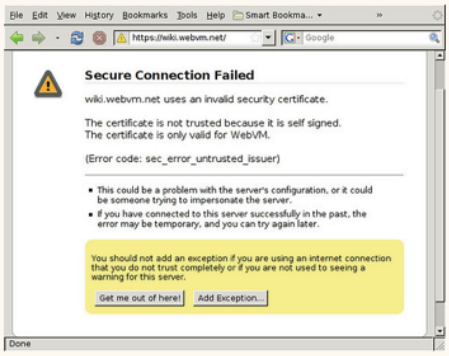
   https://www.myspace.com/HStwbis/login.php?sessionid=10359

SSL Hijacking

Getting in the middle of HTTPS

- Follow-up to other general MitM attacks

1. Downgrade the victim to HTTP
   - sslstrip
2. Generate our own certificates
   - sslsplit / mitmproxy



SSL Hijack Defence

- Modern, updated browsers will warn the victim
  - Whether or not they choose to listen...
- All about culture, awareness
  - Be security-smart!

Rogue Access Points

- Malicious Wireless Access Points
  - Managed by an attacker
- Pineapple WiFi
  - Can impersonate real APs with **Karma**
  - Since wireless NICs look for old APs, Karma just mimics them
- If a victim connects, you're MitM
- Can steal WPA credentials for other networks

A good general defence

- Virtual Private Networks
  - Encrypt all the data

- IPSec VPN
  - Asymmetric DH key exchange, symmetric encryption
  - Network layer (L3), encrypt IP Datagram
- SSL VPN
  - Asymmetric TLS key exchange, symmetric encryption
  - Transport layer (L4), encrypt UDP packet (or TCP)

Network Defence

Firewalls & Intrusion Detection/Prevention

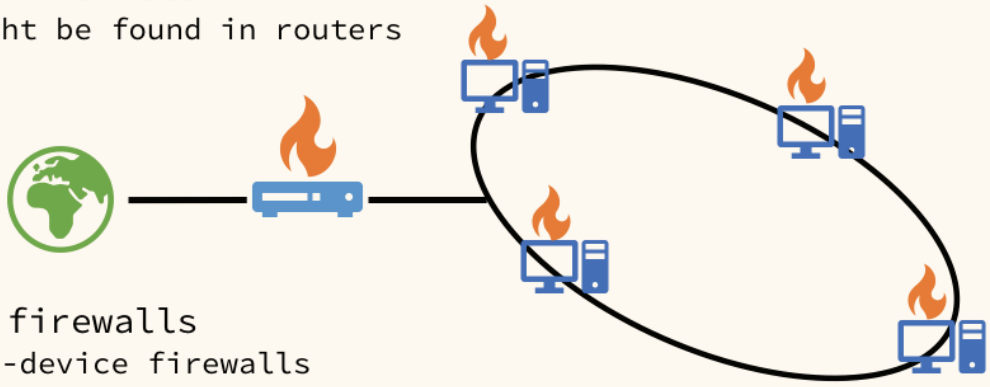
Firewalls

- A security perimeter around a network
  - Which packets can enter
- Hardware vs Software
  - A bit misleading
  - Hardware runs some software
  - Hard firewalls == Routers
  - Soft firewalls == Locally
  - Having both is ideal

Security 360

Firewalls on a Network

- Hard firewalls
  - Might be found in routers



- Soft firewalls
  - Per-device firewalls

Firewall Positioning

- **Perimeter** firewalls prevent unwanted traffic from entering the network
  - A first line of defence

- **Host** firewalls prevent unwanted traffic from hitting the device
  - Defence against attackers on the network

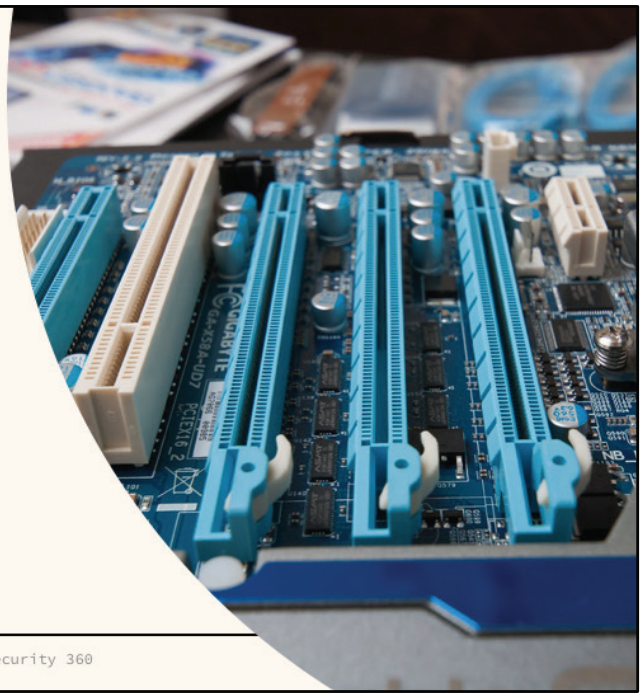
The State of a Firewall

- Firewalls either
  - **ACCEPT** a packet - *connection accepted*
  - **REJECT** a packet - *connection refused*
  - **DROP** a packet - *connection timeout*
- Stateless Firewalls
  - Provide basic **packet filtering**
  - Simple matches, unaware of rest of network
    - Source/destination port, source/destination IP
- Stateful Firewalls
  - Provide **dynamic** packet filtering (stateful inspection)
  - More complex matches based on other network connections

Hard Firewalls

perimeter firewalls

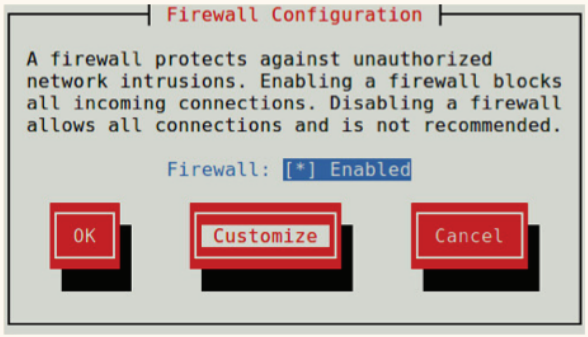
- Buy a Firewall
  - Cisco, Checkpoint
- Build-your-own with pfSense
  - A UNIX distro with firewall & router in one
- Build-your-own with Linux
  - iptables/nftables hook into the Linux kernel



Soft Firewalls

soft

- If you're on Linux
  - Use iptables
- If you're on BSD
  - Use pf
- If you're on Windows
  - Use Windows



Firewall Configuration

An example with iptables

- Three default “chains”
  - INPUT – traffic incoming to host
  - OUTPUT – traffic outgoing from host
  - FORWARD – traffic passing through host
- DROP a ping (ICMP) from a specific IP
  - iptables -A INPUT -p icmp -s 192.168.1.1 -j REJECT
- REJECT outgoing SSH (TCP :22)
  - iptables -A OUTPUT -p tcp --dport 22 -j DROP

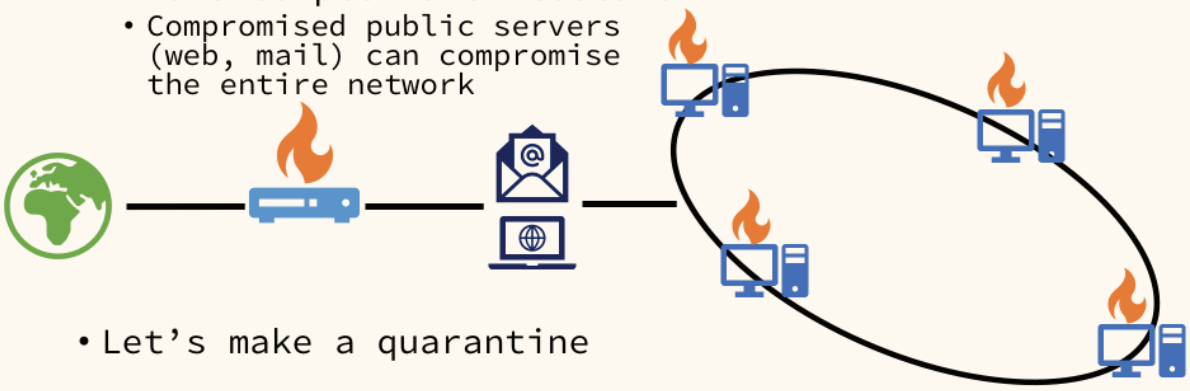
DROP everything first, ACCEPT as needed

Security 360

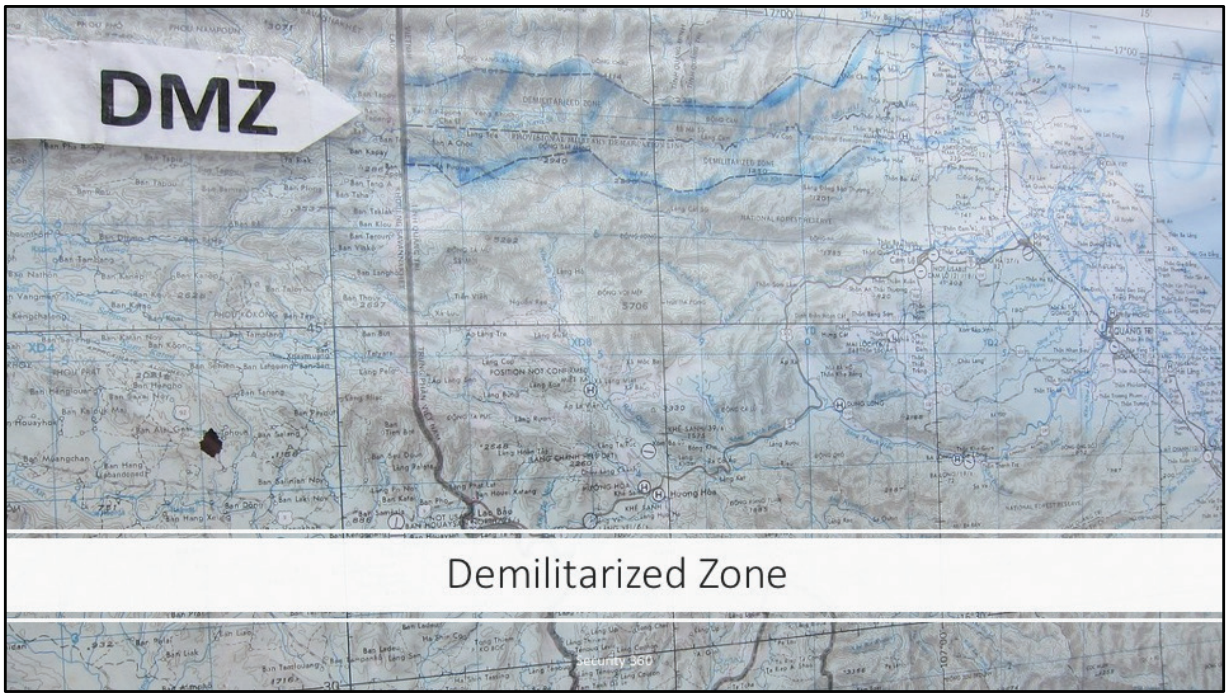
iptables has been superseded by nftables, with an outlook to move to another option - bpfilter - in the future

Securing the Perimeter

- A more complex architecture
  - Compromised public servers (web, mail) can compromise the entire network

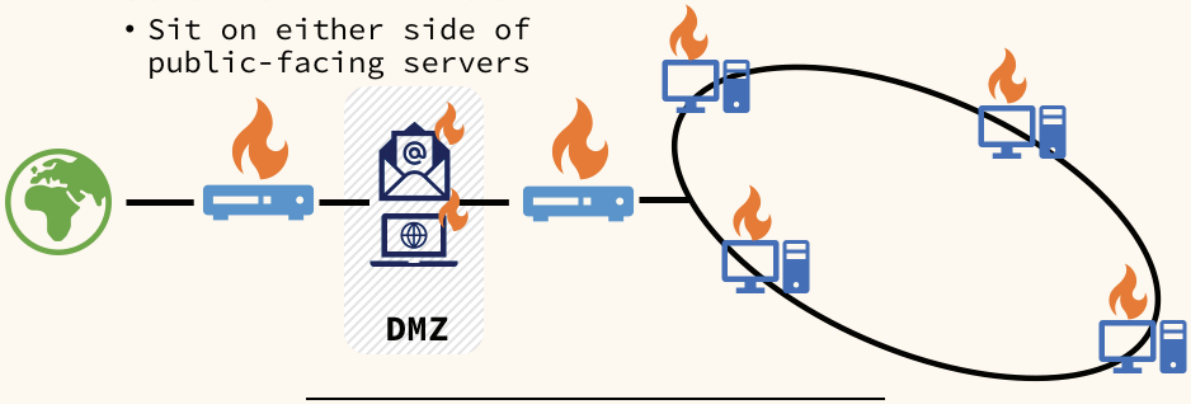


- Let's make a quarantine



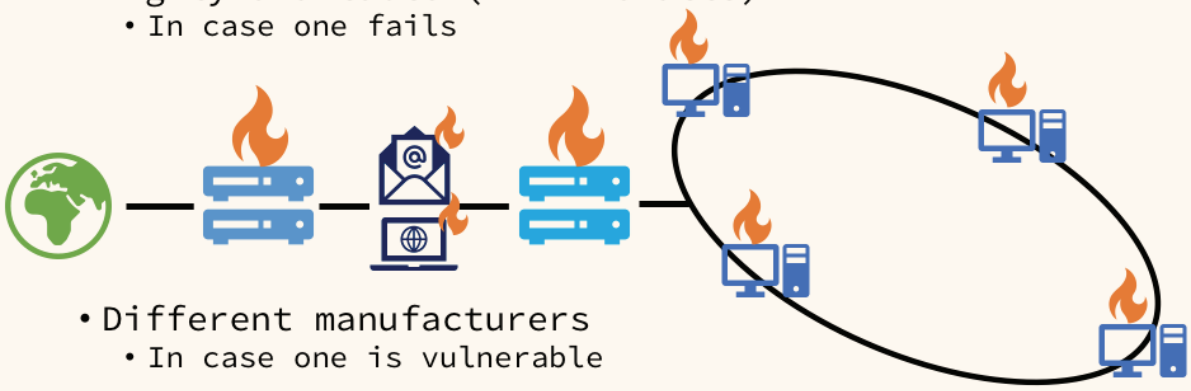
Building the DMZ

- Add another firewall
  - Sit on either side of public-facing servers



Firewall Best Practice

- Highly available (x2 firewalls)
  - In case one fails



- Different manufacturers
  - In case one is vulnerable

L3 vs L7 Firewalls

- L3/L4 Firewalls (Network Firewall)
  - What we've described so far
  - Packet-filter based on IP & Port
- L7 Firewalls (Application Firewall)
  - Group traffic into applications
    - Web browsing
    - Mail
    - Telnet
    - SSH
  - Filter based on groups

Intrusion Detection Systems

- Traditional Network Firewalls
  - Shallow packet inspection –
    decisions made based on headers (IP & TCP)
    - Allowed - or not
- IDS
  - Packet sniffer which can raise alerts/alarms
  - Alerting on top of shallow packet inspection, and...
  - Deep packet inspection –
    decisions made based on the payload

Intrusion Prevention Systems

- IPS
  - An IDS which also works “inline”
  - Can make port filtering decisions based on the alerts generated and drop/reject packets on-the-fly
- Open Source tools
  - Snort
  - Suricata

Next-Generation Firewalls

- AKA UTM Systems
  - Unified Threat Management
- Palo Alto, Fortinet, Cisco

- Built-in
  - Intrusion Detection System
  - Intrusion Prevention System
  - L7 Application
  - Virus/Malware Scanning

Security 360