CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

Common Network Attacks (cont'd)

Chris Samayoa

Week 14 – 1st Lecture
4/19/2022

Course Information

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

- CECS 303
  - Networks and Network Security – 3.0 units
- Class meeting schedule
  - TuTH 5:00PM to 7:15PM
  - Lecture Room: VEC 402
  - Lab Room: ECS 413
- Class communication
  - chris.samayoa@csulb.edu
  - Cell: 562-706-2196
- Office hours
  - Thursdays 4pm-5pm (VEC-404)
  - Other times by appointment only

Objectives

- Common Network Attacks – Overview
  - Man-in-the-Middle Attacks (MitM)
  - DNS Tunneling
- Common Network Defenses

Common Network Attacks

- Malware
  - Malicious software that is used to exploit devices at the expense of victim resources
- Distributed Denial of Service Attack (DDOS)
  - An attack where multiple (typically compromised) systems attack a target with the goal being to overwhelm the resource and make it unavailable for use
- SQL Injection Attacks
  - Attackers can construct a web request that provides unintended access to database resources
  - Can be used to create, modify, delete, or extract data from a database
- Cross-site Scripting (XSS) Attack
  - Attacker injects a malicious script into a trusted website
  - Injected script will then be delivered to a victim's web browser
  - Used to spread malware, steal credentials, or steal user sessions
- Man-in-the-Middle Attack
  - Attacker intercepts communications between two or more parties to intercept data
- DNS Tunneling
  - Command-and-control tactic that uses DNS queries to go undetected
- Email Attacks

Objectives

- Common Network Attacks – Overview
  - Man-in-the-Middle Attacks (MitM)
  - DNS Tunneling
- Common Network Defenses

Man-in-the-Middle (MitM)

- Overview
  - Any attack that seeks to intercept communication between two parties
    - Can be user-to-user or user-to-application
  - Goal can be to spy on communication or to impersonate one of the parties
- Prevalence
  - Malware likely used more often to collect personal information from large groups of victims
  - Still a potentially high risk type of attack that can be used to target more specific types of users
- Potential Impacts
  - Stolen personal information
    - e.g. Credentials or credit card information
  - Identify theft
  - Gather information to use for an APT
  - Financial gain

Common MitM Types

- SSL Stripping
  - Establish HTTPS connection between themselves and the server, but use an unencrypted HTTP connection to the client / victim
- Evil Twin
  - Imitates a legitimate Wi-Fi Access Point
  - Connection can be used to prompt user to access a malicious certificate file
  - Pineapple Attack
    - ➢ Device used to emulate a trusted Wi-Fi network / SSID

Objectives

- Common Network Attacks – Overview
  - Man-in-the-Middle Attacks (MitM)
  - DNS Tunneling
- Common Network Defenses

DNS Tunneling

- Overview
  - Uses DNS protocol to establish persistent communication channel to send data out
    - Could be to command and control server or simply to extract data
  - DNS traffic is often not scanned – so attack can go undetected
- Prevalence
  - Common method to communicate outside of a network once initial compromise has been established
- Potential Impacts
  - Attack can establish persistent access (reverse shell)
  - Sensitive data can be stolen

Objectives

- Common Network Attacks – Overview
  - Man-in-the-Middle Attacks (MitM)
  - DNS Tunneling
- Common Network Defenses

Common Network Defenses

- Anti-virus
  - Signature-based and NGAV
- Firewalls
  - Host-based
  - Network based
    - Including NGFW(e.g. pfSense, OPNSense, NG Firewall)
    - Deep Packet Inspection (DPI)
- Intrusion Detection Systems
  - Can include network monitors
  - e.g. Snort
- Content Delivery Networks
  - Internet edge protection
  - e.g. Akamai (Kona DDoS Defender), Cloudflare

Common Network Defenses

- Large Cloud Providers
  - Amazon Web Services (AWS), Microsoft Azure, Google Cloud
- Network Security Focused Database Development
  - Parameterized database queries
  - Validate user-supplied data
- Software Development Best Practices
  - Dynamic Testing
  - Fuzzing
- Wireless Protection Best Practices
  - Strong passwords
  - VPNs
  - PKI

NGAV

- Overview
  - Anti-virus software that does more than detect virus/attack signatures
  - Typically marketed as using AI
  - Attempts to stop zero-day attacks
- “Artificial intelligence”
  - Buzzword used by many companies in this arena
  - Typically means the use of machine learning
- Typical Features
  - Detect file-less attacks
    - Macros
    - In-memory execution
  - Behavioral detection
  - Use of cloud-based systems
    - Useful for pattern recognition to find indicators of compromise
    - Centralized administration console
  - Ransomware protection
  - Endpoint Detection and Response (EDR)

NGAV (cont'd)

- Managed Endpoint Detection and Response (MEDR)
  - Monitoring can be offloaded to a third-party
- Major competitors
  - Crowdstrike – Falcon
  - Cybereason
  - Carbon Black
  - Sentinel One

NGFW

- Overview
  - Firewalls that provide more advanced protection features than IP, protocol, and port blocking
  - Attempts to stop zero-day attacks
  - Processor intensive features
- Typical Features
  - Deep Packet Inspection (DPI)
  - Behavioral detection
  - Use of cloud-based threat intelligence
  - Application-level inspection
  - Intrusion prevention

DPI

- What is it?
  - Process of analyzing network packets to detect and prevent potential threats and analyze user behavior
- Why is it useful?
  - Can look for signatures and patterns of malware and other types of attacks
    - Detection occurs at a network level
    - Can stop malicious activity before it reaches endpoint devices
  - Prevent data exfiltration
  - Can be used to enforce lawful interception of data by law enforcement
- What about SSL/TLS?
  - Agents can be deployed to individual workstations
  - Certificate signed by organization can be deployed to clients and installed via GPO
    - Often signed by Active Directory Domain's Certificate Authority (CA)

Application-Level Inspection

- What is it?
  - Uses information known about a particular application to determine what “normal” behavior is
  - Typically works in conjunction with DPI
- Why is it useful?
  - Can readily protect against certain attacks on common network protocols
    - e.g. HTTP, HTTPS, SMTP, or FTP
  - Acts as a proxy device between subject / user and application
    - Protections can be added at this layer if necessary
  - Additional rules can be added for custom / unknown applications as needed to be detected at a network level

IDS

- Overview
  - System that monitors network traffic for suspicious or anomalous activity and issues alerts to administrators
  - Should be configured to reflect network policy
    - Often generate false alarms
    - Required fine-tuning to be used effectively
  - Can be signature or anomaly based
  - Custom rules can be created
    - e.g. Snort rules

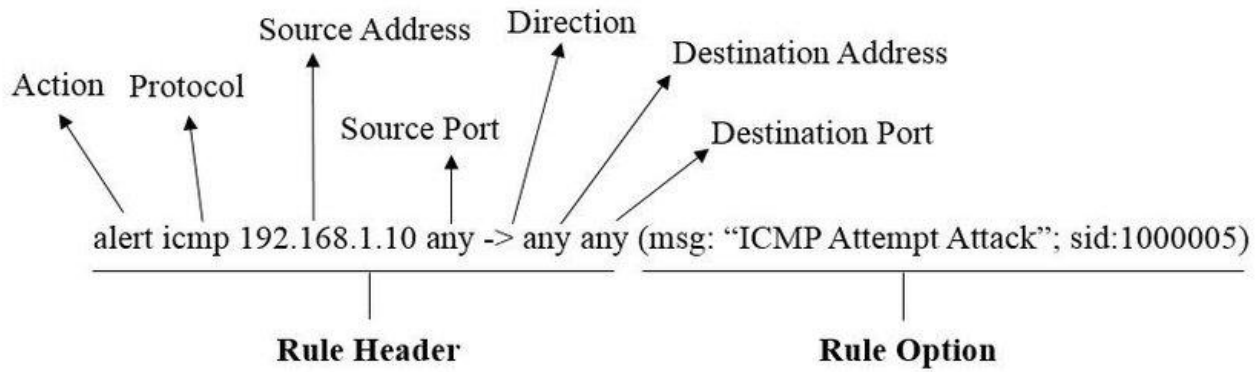
Source: https://www.geeksforgeeks.org/intrusion-detection-system-ids/

IDS (cont'd)

- Types of IDS
  - Network Intrusion Detection System (NIDS)
    - Monitors whole subnet(s) for known attacks or anomalous activity
  - Host Intrusion Detection System (HIDS)
    - Scans inbound/outbound traffic from single host
    - Can takes snapshots of existing system files and compare them with previous snapshots to detect unexpected changes
  - Protocol-based Intrusion Detection System (PIDS)
    - Can be used to monitor a specific protocol such as HTTPS on a server
    - Can scan traffic as its unencrypted, but before it is processed by the web application
  - Application Protocol-based Intrusion Detection System (APIDS)
    - Can monitor system used by a group of servers
    - e.g. Monitor SQL server middleware from web servers watching for database interactions
  - Hybrid Intrusion Detection System (e.g. NIDS + HID)

Source: https://www.geeksforgeeks.org/intrusion-detection-system-ids/

Snort IDS Rule Examples



*local.rules ×

```
#alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:1000001;
rev:1; classtype:icmp-event;)
alert tcp 192.168.132.133 any -> $HOME_NET 21 (msg:"FTP connection
attempt"; sid:1000002; rev:1;)
alert tcp $HOME_NET 21 -> any any (msg:"FTP failed login";
content:"Login or password incorrect"; sid:1000003; rev:1;)
```

Source: https://www.researchgate.net/figure/Example-of-Snort-IDS-Rule-The-rule-options-of-Snort-consist-of-two-parts-a-keyword-and_fig1_281564631
https://resources.infosecinstitute.com/topic/snort-rules-workshop-part-one/

Snort IDS Rule Examples

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

```
edit config
snort -T -i ens33 -c /etc/snort/snort.conf
snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i ens33


rules
reject icmp 10.10.10.2 any <> 10.10.10.1 any (msg:"Blocking ICMP Packet from 10.10.10.2"; sid:1000001; rev:1;)

alert - generate an alert using the selected alert method, and then log the packet

log - log the packet

pass - ignore the packet

drop - block and log the packet

reject - block the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.

sdrop - block the packet but do not log it.

find /etc/snort/rules \( -type d -name .rules -prune \) -o -type f -print0 | xargs -0 sed -i 's/alert/sdrop/g'
```

Source: https://stackoverflow.com/questions/56789379/how-to-create-a-snort-content-rule

Content Delivery Networks

- Overview
  - Initially, a content delivery network (CDN) was used to speed up delivery of web content by caching web pages, images, video, etc.
    - Relieved web congestion by bringing content closer to providers
    - Focus is on distributing content of "origin" servers to local caches
  - Adds resiliency to web applications
    - Content is distributed geographically so that there is not a single point of failure
  - Often used to protect against DDOS attacks
    - Large availability of bandwidth and servers can typically withstand these attacks without affecting the web application
    - Avoids bringing down individual company networks (e.g. internet connections)
  - CDNs carried 56% of all internet traffic in 2017
    - Expected to carry 72% of internet traffic by 2022 according to Cisco

CDNs (cont'd)

- Overview of services
  - Increases performance in serving content by using caches
  - Protects against other common attacks
    - SQL injection
    - Cross-site scripting
  - Provides threat intelligence based on vast networks
    - Data can be used to protect customers from zero-day attacks
  - Attacker can still directly attack an organization's public IP addresses
  - Can be used as a proxy for filtering outbound user traffic for an organization

Cloud Providers

- Overview
  - Major cloud providers offer “built-in” protections against attacks including DDOS and malware
    - Some features are free and some are billed
  - Standard levels of DDOS protection are typically offered for free
    - Massive cloud infrastructures can be leveraged to easily defeat most DDOS attacks
  - Most other types of network protections are also available as additional features
    - Antivirus
    - Host / Network firewalls
    - IDS / Monitoring