Security Monitoring Challenges

Brian Olliff

Defensive Engineering Instructor

Key Concepts

+ Infrastructure monitoring challenges
+ Challenges from attackers

MAJOR TOPICS

- Encryption
- Network monitoring
- Evasion
- Traffic manipulation

LEARNING OUTCOMES

- Understand challenges that encryption brings to security monitoring
- Be familiar with different types of challenges when monitoring network traffic
- Understand common attacker tactics for evasion, data exfiltration, and pivoting

PREREQUISITES

+ Basic understanding of cybersecurity

Let’s Get Started!

Security Monitoring Challenges

+ Aligned with Cisco CyberOps Associate certification & material

Encryption

Encryption

- Many types and uses
  - Data encryption (at rest, in transit)
  - Network traffic encryption (SSH, HTTPS, etc)
- Useful for protection information and privacy
- Multiple challenges
  - Monitoring more difficult
  - Attacker usage
- Many security products can decrypt, analyze, and re-encrypt
  - Some privacy concerns
- Metadata can still be used for analysis

Attacker Use of Encryption

- Remote tunnels (VPNs, etc)
  - Remote access
  - Data exfiltration
    - Encrypt data for exfiltration to evade detection
- Malware
  - Encrypt organization data and demand payment (ransomware)
  - Bypass detection and obfuscate activity/code
    - Effective with normally encrypted traffic (HTTPS)

Network Monitoring Challenges

NAT

- Network Address Translation
- Hides internal range of address from unprotected networks
- IPs in logs may appear as translated address
  - With PAT - many hosts could appear as same translated address

- Many security products on perimeter of network can assist
- Cisco Stealthwatch
  - *NAT stitching* - feature that maps translated to real in logs

Tor

- Heavily used by attackers for communication and illegal activities
  - Also used for legitimate privacy reasons
- Traffic encrypted and sent through multiple nodes (Tor relays)
  - Encrypted multiple times (layers)
  - Each relay decrypts single layer
- Exit node
  - Last node where encrypted traffic exits to public Internet
  - Can be targeted to monitor traffic (if known)
- Recommended to block Tor exit nodes on network

P2P

- Distributed architecture that shares resources of connected devices
  - Does not require a centralized server
- Often used for illegal file sharing
  - Movies, music, software
- Many legitimate uses
  - Spotify previously used
  - Several universities use for sharing data
- Attackers often take advantage
  - Malware embedded in otherwise “legitimate” files
  - Can have numerous software vulnerabilities

Network Time

- Important to keep time synchronized across all endpoints
  - Authentication and authorization may require
  - Logging timestamps
- Log data is almost useless if timestamps are incorrect
  - Nearly impossible to correlate events and build timeline
- Network Time Protocol (NTP)
  - Server on network synchronizes time with authority server
    - Public Internet time servers (NIST, NTP Pool Project, Google, etc)
  - Endpoints on network sync time with time server

Evasion & Exfiltration

Detection Evasion

- Several methods attackers use (always changing & discovering new)
- Numerous encryption methods
- Remote access/vpn tunnels
- Network traffic manipulation techniques
  - Traffic fragmentation
  - Protocol misuse
  - Timing attacks
- Vulnerability exploits
- Exploiting weaknesses in security controls
  - IPS/IDS (network or host), endpoint protection, logging systems, etc

Tunnels

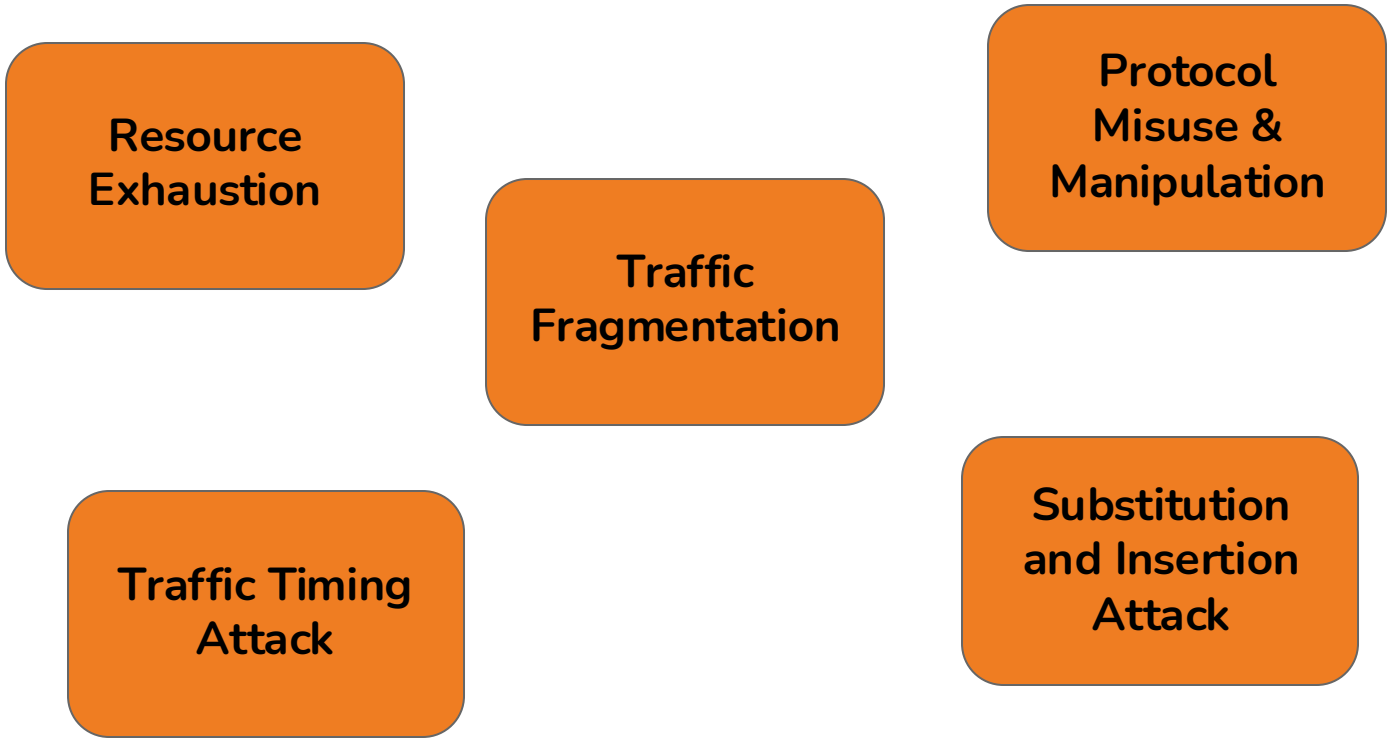
- Attackers can use in many ways
  - Data exfil, evade detection, remote access
- Several protocols
  - SSH (most common), HTTPS, DNS
- Methods
  - Run software on endpoint to initiate connection to attacker infrastructure
  - Exploit vulnerable/compromised remote access system
  - Hardware device to initiate
    - Can be more difficult to detect

Data Exfiltration

- Theft of confidential data from organization
  - Often paired with encryption
  - Typically demand ransom to not sell/release data
- Often the end goal of attackers
- DNS tunneling
  - One of many methods of obfuscated tunneling/data exfil
    - Using protocol not normally used for data transfer
  - Encoding techniques frequently used to obfuscate contents
    - Base64, binary, hex, etc
  - Traffic appears to be normal DNS traffic
    - Deeper analysis can often detect malicious activity

Network Traffic Manipulation

Traffic Manipulation



Resource Exhaustion

- Consuming resources otherwise needed for system workload
  - Type of DoS attack, also used to evade detection
- Very effective against security controls that fail open
  - Security features/functions stop to ensure traffic still flows upon failure
- Systems with monitoring/logging/tracking functionality
  - Monitoring resources exhausted - attacker can act without being tracked
  - Logging systems stop accepting or generating logs
    - Results in less data & evidence for investigation and forensics
- Many modern systems have protections against
  - Can recognize attack and block
  - Throttling to slow down attack and keep resources available

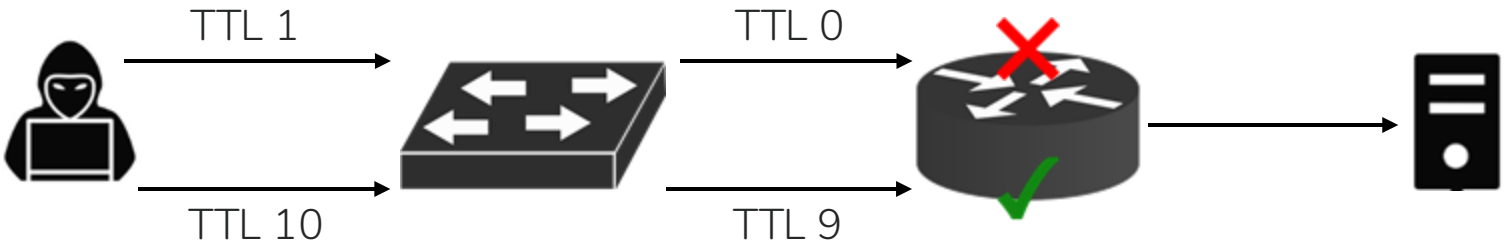
Traffic Fragmentation

- Network traffic designed to function in specific ways
- Fragmentation
  - Breaking up single IP datagram into multiple, smaller packets
- Designed to attempt to bypass filtering & monitoring
- Most modern controls have protections against
  - Reassemble packets for examination and analysis
  - Most systems that operate as a full proxy are not susceptible
- Methods to bypass protection
  - Attacker can reorder segmented traffic to confuse IPS
  - Overlapping fragments

Protocol Misuse & Manipulation

- Data structures that define how traffic is exchanged over a network
- Many ways to manipulate many different protocols
  - Protocol being used
  - Developer configuration of receiving systems
    - defenses, limitations on accepted traffic, validation methods, etc
  - Actions system takes when it encounters manipulation
- TCP checksum manipulation
- TTL abuse
  - Altering TTL values of traffic to trick security controls
- Most modern security products can detect and block

TTL Manipulation Attack



Traffic Timing, Substitution, & Insertion

- Timing attack
  - Attempt to evade detection by performing actions slower than normal
  - Example:
    - Sending packets slower than detection system tuned to detect
    - System does not tie packets together
- Substitution and insertion attack
  - Substituting payload data with data in different format, with same meaning
  - Goal is to not be recognized by security control due to format
  - Most controls can decode substituted data
    - Often requires flaw in decoding process

Pivoting

Pivoting

- Moving from one endpoint to another, or one segment to another
  - Can also be called *island hopping*
- Attacks start with gaining a foothold in environment
  - Weak guest wireless
  - Vulnerable system in DMZ
- Next action for attacker is to move to another system with greater access
  - Normally administrative or root access
  - Pivoting with privilege escalation
  - Moving to other network segments with greater access
- Can also move across systems with equal access/permissions
  - Lateral movement

Defenses

- Effective network segmentation with access control between segments
  - Limit what systems and network segments can access
- Proper access controls on hosts
- Endpoint security controls
- Effective patch management
- Network traffic monitoring
  - NetFlow
- Cisco ISE
  - Authentication and authorization mechanisms
  - Device profiling
  - Network permissions granted based on multiple factors

Security Monitoring Challenges - Summary

Key Concepts - Recap

+ Infrastructure monitoring challenges
+ Challenges from attackers

Learning Outcomes Recap

+ Understand challenges that encryption brings to security monitoring
+ Be familiar with different types of challenges when monitoring network traffic
+ Understand common attacker tactics for evasion, data exfiltration, and pivoting

Next Steps

- Review any needed courses or material from CyberOps Associate Learning Path
- Continue studying (if not complete)
- Explore additional courses for security monitoring and analysis at INE

Thank you!

Security Monitoring Challenges

+ Aligned with Cisco CyberOps Associate
+ Thank you for your time!

EXPERTS AT MAKING YOU AN EXPERT