HUNTING EXPEDITION IDEAS

There are thousands of opportunities for attack or data-based hunting. In this document I've listed some of my favorites that you can use for the exercises in this class or in your own network. This list isn't close to exhaustive, but it's a great place to start and includes expeditions mentioned in the course. The value of each technique will vary dramatically based on the size and makeup of your network. Not all of these will be prudent or fruitful in every scenario, but they give you a place to start applying the concepts to your network. In almost every case, a single anomaly becomes more suspicious when found alongside the discovery of other anomalies. Therefore, many of these individual techniques can be combined.

SECTION 1: ATTACK-BASED HUNTING

Malicious User Account Creation

- **Evidence Sources**
  - OS Logs
  - Windows EID 4720, 4738, 4732, 4724, 4734
- Anomalies
  - Created not following naming conventions
  - Created with insecure properties
  - Created and added to privileged group
  - Accounts created at unexpected source user activity times
  - Local accounts created on domain members
  - Created by user who's never created one
  - Created from system where one has never been created

Credential Theft

- **Evidence Sources**
  - Authentication Logs
  - Process Execution Logs (EID 4688 / Sysmon 1)
- **Anomalies**
  - Evidence of credential dumping applications
  - Never before seen processes
  - Suspiciously named processes
  - Overly generic processes
  - Suspicious login times
  - Improper login timing
  - Geoinfeasable logins
  - Unexpected logon types (Network, RDP, etc)
  - Unexpected user to host relationships

Malicious Run Key Persistence

- **Evidence Sources**
  - Windows Registry
- **Anomalies**
  - Attempts to mirror legitimate process names
  - Overly generic file names
  - Never before seen file names
  - Unrecognized application names
  - Application path mismatches

Web Shell Usage

- **Evidence Sources**
  - Web Server Logs
  - HTTP Logs (Inbound)
- **Anomalies**
  - Never before seen paths/files
  - Overly generic directory/file names
  - Multiple new files created in a short time
  - Unexpected one-to-many relationship (One user visiting the same page over and over or transferring a lot data)
  - Rarely seen user-agent
  - Odd content formatting in the request/response
  - Unexpected encryption
  - Abnormal PCR (Can present in different ways)

RDP Tunneling

- **Evidence Sources**
  - Windows Host Logs. (EID 4624, 4688, Firewall EID 2005, TerminalServices EID 21/25)
  - Windows Registry
  - PCAP
- **Anomalies**
  - Outbound protocol to never before seen host followed by RDP authentication.
  - RDP auth from a user who doesn't use RDP
  - RDP enabled on a new host by a non IT user
  - Unexpected login times
  - Tunneling application execution
  - RDP cookie observed on non-RDP port

Data Exfiltration

- **Evidence Sources**
  - Network Flows
  - PCAP
- **Anomalies**

- Large upload to unknown external host
- Large upload from host that doesn't normally do that
- PCR deviation for an individual host (useful for staging too)
- Large number of one-to-many (or reverse) connections internally.

HTTP-Based Malware

- **Evidence Sources**
  - HTTP Proxy Logs
  - PCAP
- **Anomalies**
  - Never before seen user agents
  - Uncommon user agents
  - User agent attempts to mirror legitimacy
  - IP addresses in the domain field
  - Unexpected / rare response codes from unknown servers
  - Unsolicited (no referrer) requests leading to rare file type downloads
  - Uncommon file type downloads
  - Domains attempting to mirror legitimacy
  - Domains comprised of high entropy characters

HUNTING EXPEDITION IDEAS

SECTION 2: DATA-BASED HUNTING

HTTP Proxy / Transactions

- **Interesting Fields**
  - Timestamp
  - User Agent
  - Referrer
  - Domain
  - URI
  - Method
  - Response Code
  - Cookie
  - Mime Type
  - HTTP Response Body
- **Anomalies**
  - Never before seen user agents
  - Uncommon user agents
  - User agent attempts to mirror legitimacy
  - IP addresses in the domain field
  - Unexpected / rare response codes from unknown servers
  - Unsolicited (no referrer) requests leading to rare file type downloads
  - Uncommon file type downloads
  - Unexpected encryption/obfuscation
  - Data formatting errors
  - Identical session cookies used by the same host in a short time window
  - Domains attempting to mirror legitimacy
  - Domains comprised of high entropy characters

OS Process Execution Logs

- **Interesting Fields**
  - Timestamp
  - System
  - Account Name
  - New Process Name
  - Process ID
  - Parent Process ID
- **Anomalies**
  - Never before seen files

- File name attempts to mirror legitimacy
- Never before seen command line parameters
- Never before executed by the user
- Unexpected path for file
- High entropy process names
- Unexpected parent/child process relationships
- Improper frequency of occurrence
- Improper execution timing
- Unexpected non-admin use of admin tools
- Unexpected user to application relationship
- Unexpected host to application relationship
- Improper sequence of launch

OS/Application Authentication Logs

- **Interesting Fields**
  - Timestamp
  - Username
  - System/Application
  - Logon Type
  - Group
- **Anomalies**
  - Unexpected one system/user to many relationships
  - Unexpected system/user relationships
  - Abnormal authentication times
  - Usernames that don't follow naming conventions
  - Unexpected logon types for a user
  - Multiple auth failures followed by success
  - Multiple auth failures from one source to many dests

Network Connection/Flow Logs

- **Interesting Fields**
  - Timestamp
  - Source/Dest IP
  - Source/Dest Port
  - Bytes Transferred
- **Anomalies**
  - PCR deviation for an individual host
  - Large upload to unknown external host
  - Large upload from host that doesn't normally do that
  - Large number of one-to-many (or reverse) connections internally
  - Host receiving data on a new/unexpected port
  - Larger than average (> many stdev) bytes transferred for a host
  - Larger than average (> many stdev) number of connections for a host

- Larger than average (> many stdev) duration of connection for a host

User Management Logs (OS or App)

- **Interesting Fields**
  - Timestamp
  - User performing management
  - User being managed
  - Action being taken
  - User account parameters modified
  - Group membership
- **Anomalies**
  - Local user accounts created on domain members
  - Existing user accounts granted elevated privileges
  - New user accounts granted admin privileges
  - User accounts created with no password expiration
  - Account creation by unexpected users
  - Disabled accounts re-enabled
  - User management at odd times
  - Account lock outs

DNS Logs

- **Interesting Fields**
  - Source IP
  - Destination IP
  - Query Type
  - Query
  - Response
- **Anomalies**
  - Queries to unapproved/new DNS servers
  - Domains attempting to mirror legitimacy
  - Domains comprised of high entropy characters
  - Larger than average (> many stdev) number of queries for a host

HTTP Server Logs

- **Interesting Fields**
  - Timestamp
  - Source IP
  - Source Port
  - Request Method
  - URI
  - Response Code
  - HTTP Response Body

- **Anomalies**
  - Never before seen paths/files
  - Overly generic directory/file names
  - Multiple new files created in a short time
  - Data formatting errors
  - Unexpected one-to-many relationship (One user visiting the same page over and over or transferring a lot data)
  - Rarely seen user-agent
  - Odd content formatting in the request/response
  - Unexpected encryption/obfuscation
  - Abnormal PCR

Mail Transaction Logs

- **Interesting Fields**
  - Source IP
  - Sender
  - Recipient
  - Subject
  - Mail Content
  - Content Type
- **Anomalies**
  - Never before seen sender w/ attachment or multiple links
  - One sender to many recipients (possible w/ attachment or link)
  - Either of the above, with special attention to commonly exploited file types (executables, PDFs, flash, office documents).
  - Rarely seen or suspicious content types
  - Overly generic subject lines
  - Outbound e-mails with document attachments containing sensitivity markings
  - Subjects/Content with misspelling of your company name
  - Unexpected encryption/obfuscation
  - Missing expected mail header information
  - Spoofed sources pretending to be from your organization
  - Presence of executable code
  - Any of the above with particular focus on highly visible staff members

Mail Object Access Logs

- **Interesting Fields**
  - Source IP
  - Mailbox
  - Object Accessed
- **Anomalies**
  - Unexpected IP/mailbox relationships

- Unexpected one-to-many (IP to mailbox)
- Larger than average (> many stdev) number of messages opened
- Larger than average (> many stdev) number of older messages read
- Geoinfeasible login or object access

HUNTING EXPEDITION IDEA SOURCES

SECTION 3: OTHER HUNTING IDEA RESOURCES

MITRE Attack (https://attack.mitre.org/): An encyclopedic resource of attacks. Each attack includes links to examples, so this is a fantastic place to look for ABH ideas.

Threat Hunting Project (https://www.threathunting.net/): A small list of threat hunting ideas maintained on Github.

Malware Archaeology (https://www.malwarearchaeology.com/cheat-sheets/): The Windows logging cheat sheets here provide ideas for data-based hunting in Windows logs.

Sigma Rules (https://github.com/Neo23x0/sigma/): Florian Roth's universal signature set. There's a lot of good behavior fodder in here to drive hunting.

Cyb3rWard0g's Threat Hunter's Playbook (https://github.com/Cyb3rWard0g/ThreatHunter-Playbook): A list of hunting techniques and hypotheses from the developer of HELK.

Microsoft Defender ATP Hunting Queries (https://github.com/Microsoft/WindowsDefenderATP-Hunting-Queries): These are specific to the MS product, but can help generate ideas for others.

Atomic Blue (https://eqllib.readthedocs.io/en/latest/atomicblue.html): Hunting queries written in Endgame's EQL syntax.