- Filename: eccouncil-ceh31250-v11-1-7-1-common-adversarial-behaviors.md
- Show Name: CEHv11 (312-50)
- Topic Name: Intro to Ethical Hacking
- Episode Name: Common Adversarial Behaviors

==========

Common Adversarial Behaviors

Objectives:

- Identify and explain specific common behaviors utilized by threat actors

---

- What is the purpose of identifying adversarial behaviors?
    - Predicting attack vectors
        - Better protection against said attack vectors
        - Increased detection rates
- What kind of specific behaviors would an attacker engage in that we should be looking for?
    - Internal Recon
        - Once attacker is inside, they start to enumerate the network...
            - Hosts
            - Services
            - Configs
            - Users
        - Defenders can look for signs of Internal Recon
            - Strange batch files
            - Bash/PowerShell commands
            - Packet capture
- You mentioned the use of Bash or PowerShell. How would an attacker use those tools?
    - Internal Recon
    - Connecting to external resources
    - Data exfiltration
- If they are using built-in tools, how do we detect this activity?
    - It's difficult
    - Logs/Alerts
        - Will most likely contain identifiable information
- Are there other 'built-in' tools or features that could possibly be abused by an attacker?
    - Command Line / Terminal
        - Attacker can...
            - Explore the system
            - Create accounts
            - Change configs
            - Modify data

        - Download/install malware

- Any defense against that?
    - Again, It's difficult
        - Look for odd processes,files,connections
        - Using CLI/Terminal is odd behavior for most users
- What's one of the more sneaky behaviors an attacker may exhibit?
    - Abusing the HTTP User Agent field
        - Communicate with C2
        - Pass certain attacks to the target system
- Defenses?
    - WAF
    - Manual inspection
- What about Web Shells? How do they fit into this conversation?
    - Stealthy method of interacting with compromised web servers
        - Looks like regular web traffic (because it is)
        - Data exfil
        - File upload/download
        - Operating System control
- Defenses? Logging and monitoring?
    - Nailed it!
    - WAF could help automate the process
- Common adversarial behavior wouldn't happen to include the use of Command and Control (C2) now would it?
    - Absolutely!
- Defenses?
    - Block known C2 IPs and Domains
    - https://exchange.xforce.ibmcloud.com/collection/Botnet-Command-and-Control-Servers-7ac6c4578facafa0de50b72e7bf8f8c4
    - Traffic and connection monitoring
    - Anomalous network activity
- What is DNS Tunneling and how do attackers utilize this technique?
    - DNS traffic is crucial to a healthy network
        - Becomes a great way to piggy-back
            - C2 Traffic
            - Data exfiltration
            - Firewall bypass
- Defenses?
    - Logging and monitoring
- Lastly, we have Data Staging. Explain this behavioral element.
    - The collection of data collected by the attacker
        - It is made ready for exfiltration or destruction

- Defenses?
    - File integrity monitoring
    - Backups
    - Logging and monitoring