Implement Configuration Changes to Existing Controls to Improve Security

Chapter 12

Episode 12.01

Permissions

Objective 3.2 Given a scenario, implement configuration changes to existing controls to improve security.

- Permissions
- Whitelisting
- Blacklisting

Permissions

- Identify:
  - Users
  - Groups
- Set permissions for:
  - Files
  - Resources

Permissions Demo

- Windows
  - Users/Groups
  - Local Group Policy Editor
- Linux
  - Users/Groups
  - permissions

Permissions

- Blacklist
  - Deny specific traffic or applications
- Whitelist
  - Can use Windows Group Policy Editor
  - Disable everything except those explicitly listed

Episode 12.02

Firewalls

Objective: 3.1 Given a scenario, analyze data as part of security monitoring activities.
• Log review
- Web application firewall (WAF)

Objective: 3.2 Given a scenario, implement configuration changes to existing controls to improve security.
• Firewall

Firewalls

- Operating systems come with firewall built in
  - Includes default rules
- Simple firewalls
  - Look at protocol, port, source, destination
  - Decide if a rule is allowed

Firewall Rules

- Define higher level rules
  - Then exception comes after
- Defines:
  - Source, destination, port, protocol, action (accept/reject)

Firewalls

- Web proxies
  - Sit between Web servers and Web clients
- Web application firewalls
  - Used for Web traffic
- Operating system firewalls
  - OS level, runs on individual machine
- Device-oriented firewall
  - Example: Cisco firewall

Episode 12.03

Intrusion Prevention Rules

Objective: 3.2 Given a scenario, implement configuration changes to existing controls to improve security.

- Intrusion prevention system (IPS) rules

IDS/IPS

- Intrusion detection system (IDS)
- Intrusion prevention system (IPS)
  - Like firewalls that take an action against threats
  - Filters traffic, compares to rules, then acts
  - Example: Snort

Snort Rule Building

- Syntax
  - Snort action
  - Protocol
  - Source IP address
  - Source port
  - Direction
- Example 1
  - alert tcp any any -> any 80 (msg:"A web connection was made!";flow: stateless; rev:1;)

Snort Rule Building

- Example 2
  - alert udp $HOME_NET any -> any 53 (msg:"Suspicious DNS requests for a .buzz domain"; flow:to_server; byte_test:1,!&,0xF8,2; content:"|02|buzz|00|"; reference:url,www.spamhaus.org/statistics/tlds; sid:12345; rev:1;)

IPS Rules

- Zeek logs
  - Logs events based on rules
  - Runs scripts to analyze events
  - Looks for anomalies and correlates data
- Suricata
  - Free, open-source threat detection engine
  - IDS, IPS, and network monitoring tool

Episode 12.04

DLP and Endpoint Detection

Objective: 3.2 Given a scenario, implement configuration changes to existing controls to improve security.

- Data loss prevention (DLP)
- Endpoint detection and response (EDR)

Data Loss Prevention

- Similar to IDS
- Inspects traffic of data movement
- Goal is to limit data leakage
- Some SaaS solutions provide DLP options
  - Microsoft 365
  - Google G Suite

Endpoint Detection and Response (EDR)

- Part of full-scale security solution
- Endpoints can be laptops, workstations, smart phones, etc. that connect to your network
- If endpoints get compromised, it can lead to internal compromise
- Structured extension to traditional malware detection

Endpoint Detection and Response (EDR)

- Primary capabilities
  - Monitor
  - Detect
  - Respond
    - Main difference from standard antimalware approach

Episode 12.05

Frustration and Attrition

Objective: 3.2 Given a scenario, implement configuration changes to existing controls to improve security.

- Network access control (NAC)
- Sinkholing
- Port security

Defending Your Network - Honeypots

- Specially configured servers
- Reside on a real network
- Lure attackers away from a production network
- Track latest techniques, tactics, and procedures (TTPs) of an attacker

Honeypots

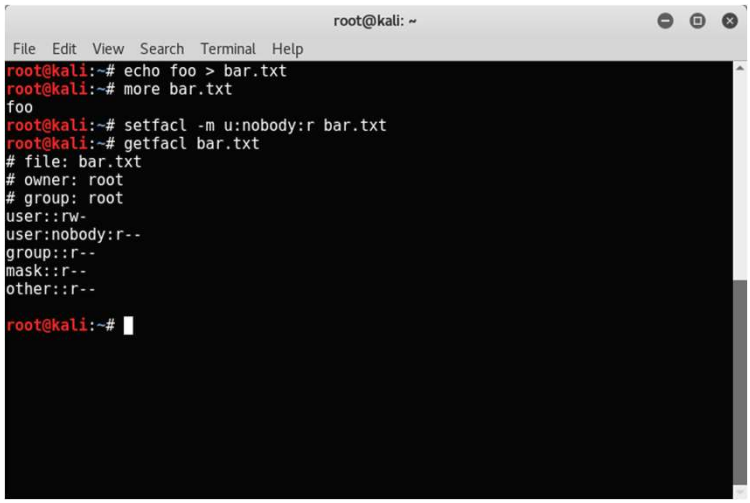
- Two types
  - Production
    - Reside on real networks with possible sensitive information
    - Designed to take the attention away from the production network
  - Research
    - Measure how attackers circumvent technical measures
    - Designed to look real to trick attackers
    - Inform network defenders to improve best practices

Defending Your Network

- ACLs
  - Tables with objects' permissions
    - Objects: network resources or files
    - ACLs define access level & permissions by users/groups
  - Very powerful
  - Requires a lot of up-front setup

Access Controls

- Filesystem ACLs
- Linux demo



Defending Your Network

- Network ACLs
  - List of access permissions to network resources
  - Reside on several layers of OSI model

More Trickery

- Black holes
- Cloaking
- DNS sinkholing

Security Models - Access Controls

- Discretionary Access Control
  - Content owner's discretion
- Mandatory Access Control
  - Need-to-know
- Role-Based Access Control
  - It's all about the job

Compensating Controls

- Origin in the financial industry
  - One person does accounting, another signs the check
- Security sector
  - Use strong encryption in areas where you don't have strong physical controls
- Ideally combines controls from different levels and types

Defending Your Network - Ports

- Ports
  - In the Internet Protocol Suite, ports are endpoints for communication between TCP & UDP at Transport layer
  - 0-65535
  - 0-1023 are well-known ports
  - Above 1023 are ephemeral ports
- Well-know ports
- Reducing your attack surface

Patch!

- Continues to be an Achilles Heel
- Wannacry example

https://www.sophos.com/en-us/lp/wanna-ransomware-outbreak-how-to-stay-protected.aspx