Host/Platform Security

Module 11

Why is Host/Platform Security Necessary?

- Firewalls are not enough
  - All access paths to host may not be firewall protected
  - Permitted traffic may be malicious
  - Outbound traffic is less restricted
    - A person or software may initiate contact to a malicious site or person
    - An established connection tends to be by bidirectional, so although the connection was initiated from the inside, the attacker can take control

Necessity

- Famous Internet security quote related to firewalls:
  - "Hard crunchy shell around a soft chewy center" – William Cheswick
  - The "soft chewy center" refers to the technology and information being protected by the firewall
  - Once passed the firewall, an attacker has an easy time of achieving their objectives

Necessity

- Host/Platform Security attempts to:
- Secure a resource by placing protection as close to it as possible
- Adjusting and maintaining the resource so it is ideally not vulnerable to attacks.
  - Threat x “No Vulnerability” x Impact = No related loss
- When protecting a person, you:
  - Put bodyguards near the protectee
  - Give the protectee body amour if necessary
  - Limit the protectee from risky activities
  - Control access to protectee while at rest

Host/Platform Security

- This topic relates to:
  - Servers – especially those that are located in dangerous portions of the network
  - Portable computers and devices that leave the protection of an IT environment
  - Remote or network related threats are typically of greatest concern for servers
  - Portable equipment has the added challenge of being lost or stolen

Approaches to Host Security

- Computer security is our primary focus
  - Bastion Host – “Passive”
    - Bastion is a term the refers to fortifications of a castle or fort. A bastion host is difficult to breach because it has fewer weaknesses.
  - Endpoint security controls – “Active”
    - Host firewalls
    - Host Intrusion Detection/Host Intrusion Prevention
    - File system integrity monitoring
    - Disk encryption
    - Strong console authentication

Bastion Host

- Requires a narrow well defined operational role
- Will likely be located in hazardous network environments
  - Another possibility, the host handles highly sensitive information or performs critical computations
    - Other defenses may be protecting, however, risk remains high

Bastion Host

- In most non-classified settings:
  - Publically available operating system is used
    - OS is “hardened”
    - Service-software security is implemented
      - Service design is evaluated and possibly adjusted
      - Service configuration is evaluated and possibly adjusted
      - Patches are investigated and applied
- Securing devices
  - Hardening checklists are available for some devices

OS Hardening

- Basic idea
  - Only allow what is absolutely necessary to run or even exist on the system.
  - Secure those applications, services and libraries that will run on the system.
    - Patch vulnerabilities when patches are available
    - Configure every functional element (command line utilities, services, applications) conservatively
      - Conveniences may need to be disabled
      - Limit trust – prepare for malicious change and replacement on system or another system it trusts

OS Hardening

- Side effects:
  - Good: The attack surface has been reduced. There is less for an attacker to exploit.
  - Bad: The system will be harder to manage, which means requiring more time and possibly more people than a less secure system.
  - Bad: Dependency between applications and OS libraries and OS services may may result in broken apps. The supporting features may be too risky to allow.

Services-Software Security

- In-house developed software should follow secure coding best practices
- Limit the complexity of the deployed service if possible
- Limit access to service's dataset and configuration information
- Carefully consider how service is configured and managed

Service-Software Security

- Network services responding to requests may be asked to respond to a malicious requestor.
  - Require authentication when possible
  - Filter request content by removing or modifying requests that may contain attempts to exploit input processing vulnerabilities
  - Patch services when patches are available
  - Limit features available to only those necessary

Ideal Bastion Host

- Host can survive in dangerous environment with no external supplemental protection (e.g. firewalls)
- It is hard to be confident when:
  - Future vulnerabilities are unknowable and potentially some current vulnerabilities are being kept secret

Endpoint Security

- Term traditionally refers to security for user devices, but servers may benefit from this technology
- Types of technology
  - Firewall
  - TCP wrappers for services
  - HIDS/HIPS
  - Anti Virus
  - File system integrity monitor
  - Disk encryption
  - Strong console authentication

Host-Based Firewall

- Host based firewalls
  - Protect TCP/IP stack from connection attempts permitted by network firewall or originating from behind the firewall
    - Another host on LAN may have been compromised
  - Some will limit which processes may use the network
    - Rouge software or malware may attempt to connect out

TCP Wrappers

- Concept: Security services listening on open TCP and UDP ports that allow only authorized IP addresses to connect to a TCP or UDP service.
  - Modular network access control
- Primarily a Unix and Linux security option

HIDS/HIPS

- Host Intrusion Detection System (HIDS)
  - Monitors logs and other vital operating system data looking for malicious activity
  - Alerts administrators if events of concern occur
- Host Intrusion Prevention System (HIPS)
  - Some solutions are policy oriented, and will deny behavior not consistent with policy
  - Some solutions use operating patterns to determine an intrusion and will stop activities

Anti-Virus

- Malware is a significant threat to the environment
  - Primary targets are hosts and devices
- Server oriented anti-virus may be helpful
  - Preventing malware from exploiting server vulnerabilities
  - Cleaning up malware that successfully loaded on the host

File System Integrity Monitor

- Host file systems contain thousands of files in hundreds of directories
- Integrity monitoring checks for content change in files and directories
  - Detected:
    - New files and directories
    - Removed files and directories
    - Changes to files and directories

Disk Encryption

- Encryption of the entire disk
- This technology is most relevant to systems that are anticipated to be moved around
  - Laptops
  - Portable devices
- Once the system successfully starts the encryption is no longer relevant
  - A server's file system is accessible most of the time, because it remains online

Strong Console Authentication

- Password authentication for privileged accounts is inadequate
  - Exposure resulting from unencrypted networking
  - Keystroke logging on remote client and possibly on server
  - Deliberate or accidental credential sharing
  - Password reuse exposes every host configured with same password
  - Password storage can be compromised

Strong Authentication

- Qualities
  - Multi-factor that relies on a combination of:
    - What you know?
    - What you have?
    - What you are?
  - Authenticator is non-reusable or one time use
    - Time based schemes (e.g. Google 2-Step authentication) are subject to reuse
      - Screen scraping trojans can capture entry and enable reuse within time window

Host/Platform Security

- Relies on disabling features
- Modifying configuration details
- Ensuring software is patched
- Adding or enabling additional controls
- Staying informed
  - Vulnerabilities
  - Threats