Security +
Defensive Network Security

Author: Joseph Lee
Email: joseph@ripplesoftware.ca
Mobile: 778-725-3206

General Concepts

Hardening
- The practice of making an operating system or application more secure through configuration

False Positives
- Mis-identification of normal state data as malicious

False Negatives
- Failure to identify malicious data

True Positives / True Negatives
- Correctly identifying threats or regular data as such

Honeypot
- Easily gained network access used to distract potential attackers by diverting their efforts and time with fake network resources

Honeynet
- Group of honeypots in a network configuration

Continuous monitoring
- Performing periodic reviews including threat assessments, vulnerability assessments, and risk assessments

Auditing
- Building an audit trail to reconstruct a sequence of events that happened on the network such as accessing resources, downloading files, etc.

Configuration auditing
- Reviewing appliance, service, workstation and server configurations to ensure best practices, staying current with updates, etc

Usage Auditing
- Reviewing usage metrics, and accounts to ensure that the accounts are limited and sprawl does not occur

Licence auditing

- Reviewing software licences and making sure that all licences are current and documented

Legal compliance auditing
- Reviewing legal and standards to ensure they are being met

Permission Auditing
- Reviews group policy to ensure that the principle of least privilege is enforced
- Helps prevent **privilege creep (permission bloat)** occurs when users are given access to resources for projects or for specific job functions, but those privileges are not revoked post-hoc

Trusted Operating System
- An operating system that provides sufficient support for multilevel security and evidence of correctness to meet a particular set of government requirements
- Meets a set of requirements for authentication and authorization

Common Criteria for Information Technology Security Evaluation (Common Criteria)
- Include requirements for trusted operating systems and assign a score (**Evaluation Assurance Level** or **EAL**) to the product

Master Images

- **Baseline disk-image** of an OS can be used to deploy systems quickly and securely
- Symantec Ghost and many other tools are available for this
- Provide secure starting points
- Reduce costs
- Save time
- Provide security by using a tested baseline configuration

Secure Baseline
- Prevents misconfigured systems and ensures consistency
- Integrity measurements can be compared to baseline for security
- Systems can be quarantined using NAC

Patch Management
- Ensures that systems are up-to-date with most current bug fixed, and security updates
- **Microsoft System Center Configuration Manager (SCCM)** known as **ConfigMgr** does many things including patch management
- **NAC** can identify unpatched systems at they attempt to connection to the network and prevent them from connecting until updates have been installed

Change Management Policy

- Helps to restrain administrators that want to push changes too quickly without testing
- Prevents unintended outages
- Provides accounting structure to document all changes
- Changes are submitted for review and approval or rejection
- If systems fail, change management will document how to change back to pre-failure state

Application Whitelisting and Blacklisting

- Unauthorized software often has malware in it
- Licence compliance can leave the organization with legal problems or downtime
- Software Restriction Policies in Microsoft Group Policy for whitelisting and blacklisting
- **MDM (mobile device management)** applications can be whitelisted or blacklisted

Secure Staging

- Sandboxing is isolating an application, service, or device for testing or development
- Sandboxing can be used for testing antivirus software, patches, software changes, etc.
- VM are good to create environment for sandboxing
- **chroot** linux command can be used for sandboxing a directory before running a command
- Software development can use a four-step approach:
  - Development
    - Choosing a development framework and building components
  - Testing
    - **Unit testing** tests specific functions of the program separately from the whole application
    - **Regression testing** makes sure that any changes have not broken other parts of the software that were previously working properly
    - **Static testing** evaluates the source code directly by reading it
    - **Dynamic testing** evaluates the software while it is running by calculating performance benchmarks and metrics
  - Staging
    - A **simulation of live site** using **real data** from production servers
  - Production
    - Pushing the entire application or patched changes to the live environment

Peripherals also come with a set of security issues

- Wireless keyboards and mouses
- Displays
- External storage
- printers

- USB ports
- Digital cameras
- WiFi enabled MicroSD cards
- MFDs Multi-functional devices

Least Functionality
- Users should only have access to functionality that is required to accomplish the tasks of their job
- Disable / remove unneeded users
- Systems should be configured with only the applications, services, and protocols they need to meet their purpose
- Uninstall unneeded software, disable unneeded services, block unneeded ports

Data Protection

Permissions
- **Linux permissions**
  - Files have owner, group, and others permissions of read (4), write (2), and execute (1)
- **Windows permissions**
  - Read, read and execute, write, and modify

Data Loss Prevention
- **Removable media**
  - Allows files to be quickly exfiltrated from e physical location
  - USB ports are a serious serious concern for malware and auto-run, or keyboard spoofing USB devices
- **Data exfiltration**
  - Is the unauthorized transfer of data outside an organization
- **Network DLP Device**
  - Can monitor sensitive files that are copied and to which devices they are copied to, as well as monitoring emails and attached files, including compressed documents, and detect proprietary encrypted payloads and alert security administrators
  - The network DLP can look for PII such as social security numbers
  - They network DLP can also search for keywords in documents and emails
- **USB Blocking -** Prevents local copies of files from being transferred to USB drives

Firewalls

- Firewalls can be placed in pairs before and after the DMZ as separate devices, or on individual systems

Host based firewall / Personal Firewall
- Monitors traffic going in and out of a single host such as server or

workstation
- Software monitors traffic going through the NIC
- Prevents intrusion into the computer
- Linux uses IPtables, firwalld, ufw, ipv6 tables

Application-based Firewall / Gateway Firewall
- A software application that performs active network traffic filtering

Network-based Firewall
- A hardware appliance with two NICs. Network traffic to flows through the device and is filtered, only allowing authorized traffic to pass through
- Commonly included at the perimeter of the network (DMZ)

Stateless Firewall
- Static ACL rules that are used to filter traffic based on source, destination, port, protocol

State-full Firewall
  - A network wide system configured to **identify and block anomaly network behaviour**
  - This includes fragmented packets and malicious traffic such as cleartext traffic that has no established connection

Web-application Firewall
  - Software designed to protect a web-application
  - It can be a **stand alone appliance** or **software added** to another device

Screened-host Firewalls
  - Combines a **packet-filtering router** with an **application gateway** located on the protected **subnet** side of the router

Screened Subnet Firewalls
- This type of setup is often used by **enterprise systems** that need **additional protection** from outside attacks
- In a screened subnet firewall setup, the network architecture has three components
  - The first is a **public interface** that connects to the **global Internet**
  - The second is a **middle zone**, often called a demilitarized zone, that **acts as a buffer**
  - The third is an **additional subnet** that connects to an **intranet** or other **local architecture**
- The **additional third subnet** helps to **filter attacks** or attract them to a particular network component to further protect the intranet
- Some also claim that a screened subnet firewall can help with throughput and flexibility

Packet-filter Firewalls

- A **firewall** technique used to control network access by monitoring outgoing and incoming **packets** and allowing them to pass or halt based on the source and destination Internet Protocol (IP) addresses, protocols and ports

Proxy-server Firewalls
- Operate at the **application layer** of the firewall
- Both ends of a connection are forced to conduct the session through the proxy
- Runs a process on the firewall that **mirrors a service as if it were running on the end host**
- Essentially turns a two-party session into a four-party session, with the **middle process emulating the two real hosts**
- Can easily **inspect packets** for much more than just source / destination addresses and port numbers
- Nearly all modern firewalls incorporate some form of proxy-server architecture
- Expensive in terms of speed and functionality

Circuit-level Gateway Firewalls
- The connection between the proxy server and the internal client
- Forwards connections on behalf of the internal client
- Filters out personal information
- Forwards the web-server response back to the internal client

IDS (Intrusion Detection System) and IPS (Intrusion Prevention System)

IDS (passive / out-of-band)
- Intrusion Detection System
- Detects and notifications of intrusion attempts

IPS (inline / in-band)
- Intrusion Prevention System
- Reacts to intrusion detection, heals, quarantines, and notifies

HIDS Host based IDS
- Installed on the computer operating system

NIDS Network based IDS
- Installed as an intermediary network component (in DMZ or on network periphery)

HIPS Host based IPS
- Installed on the computer operating system

NIPS Network based IPS
- Installed as an intermediary network component (in DMZ or on network

periphery)

Signature based
- Looks for known vulnerabilities such as attack patterns or file contents

Heuristic / behavioural / anomaly based
- Build a baseline data of normal system operations and detects abnormal usage

Check file Integrity
- Validating the checksum of files that provide checksums before you execute those downloads

DEP Data Execution Prevention / Executable Space Prevention
- **Prevents execution** of code from memory regions marked as **non-executable**
- Relative to buffer-overflows where software allows data to be overwritten from protected write memory to executable memory
- Intel and AMD call this feature **NX-bit (no execute bit)**, and Microsoft calls it **data execution prevention**

Protecting Systems from Malware

Spam filters
- Spam scores generated by applications such as Apache Spam Assassin to filter spam according to desire level of security

Anti-malware software on mail gateways
- Because the email may be coming from a known source or appear to be coming from a known source, all files and links should be scanned for malware

UTM appliances
- Can scan files coming into the network from other sources such as internet downloads and page loads

Anti-virus and Anti-malware
- Scanning software can be installed as the HIPS

Other Software Security Implementations

TCP Wrapper
- Host based ACL
- Uses **host.allow** and **host.deny** to determine if the client should be allowed to use the service
- Similar to a firewall however, operates at the **application level** instead of the **NIC** or **kernel level**

SIEMS Security Information and Event Systems
- Provides centralized solution for collecting, analyzing, and managing

network analytic and log data from multiple sources
- Can be a dedicated appliance / server
- **SEM Security Event Management**
- **NOC Network Operations Center / War-room**
  - A system to display and alert security breaches
- **Aggregation** device / collection of scripts / application that collects log data from multiple sources and combines
- **Correlation engine**
  - Collects and analyzes data from multiple systems within the network
- **Automated alerting**
  - Alerts sys admins of suspicious events
- **Automated triggers**
  - Defines an action in response to an even such as failed login threshold being met
- **Time synchronization**
  - Converting time zones of the log information to a standardized time format such as GMT
- **Even deduplication**
  - Filters logs to remove duplicate instances
- **Logs / WORM Write once read many**
  - Archives logs with write protection

NAC Network Access Controller

- Provides **continuous security monitoring** by inspecting devices and preventing them from accessing the network if they do not pass inspection
- **PNAC port-based Network Access Control**
- **Health** of a client determined by a **NAC and health agent** checks that the client meets the standards up-to-date antivirus, current patches, firewalls enabled and configured properly
- **Host health checks** are done by **health agents** on the **clients** and access is granted by the NAC **health server** in the DMZ
- **Unhealthy** clients are directed to **remediation network** or **quarantine networks** where they can find resources to fix the security issues on the client
- **Agent-based NAC**
  - Uses a software application agent on each device to perform security checks
- **Agent-less NACs**
  - Do not use a software application on each device
- **Permanent agent (persistent NAC)**
  - Installed on the client and remains installed on the client
- **Dissolvable agent**
  - Is downloaded and run on the client when the client logs on remotely
  - These type of agents are often used with mobile devices in a BYOD policy

Log File Management

- **Secure storage**
  - Ensures that log files are **not readable to others**, and thus protect

sensitive information about the network
- **Log backups**
  - Ensure that logs are available in archived format to comply with laws, regulations, etc.
- **Decentralized logs**
  - The norm for small business and small networks
- **Centralized logs**
  - Usually found in in large corporate networks
  - Log automation tools transfer log files to a central server such as a syslog server where administrators can conveniently assess them
- **SIEM Security Information and Event Management**
  - Is an enterprise level technology and infrastructure system that collects logs from all hosts on a network and analyzes the data to look for security and performance issues, in real time
- Common terms for the logs include: **event logs, syslog, security logs, audit logs,** and **audit trails**
- **Log analysis**
  - Enables detection of trends and devices that may affect long term performance and security
- **Security events**
  - Reveal potentially unauthorized activities or data access called **access violations**
- **Trend analysis**
  - Enables network administrators to baseline the traffic on a network to identify security and performance
- **Event anomalies**
  - Are events that fall outside of the baseline

MIB Management Information Base
- A database used for managing the entities in a communication network
- MIBs use **SNMP protocol agents** on each device on a network to relay statistics and information about the device in real-time
- **Traps** are event and threshold **triggers** on devices that relay CPU and memory usage
- The **MIB** can monitor **network health** and functionality of devices on the network
- Push notifications are send to administrators if errors are detected