Network Device Forensics

Digital Forensics

Focus

- Network device forensics is focused on determining if the integrity of a network device has been compromised
- The operating software is a target
- The configuration files are targets
- Data stored on the devices is a target
- The location of the device in the network can be a target

Risks

- Most data created, stored, and used by users is kept in files on computers running end user oriented operating systems like Windows, MacOSX, and Linux
- Some network devices are crucial to the operation of the rest of the network, so an attack on them can be either debilitating to the device or allow an attacker to view, exfiltrate, or compromise data passing over the network without any end user seeing that happen
- A compromised device on the network can become a LAN-based attacker which opens a much wider range of attacks than could be attempted from outside the network, as well as offering the attacker a wide range of spoofing opportunities
- Some network devices also store end user credentials in their configurations, offer file sharing (NAS devices), or host data (proxies, caches, etc.) for streaming protocols and they can be compromised or used to hold inappropriate files

Network Device Management

- Network devices are not directly accessed by normal users so unless you are actively monitoring them, you don't know if they are functioning as intended
- Enterprise-grade hardware includes many options for monitoring and managing network devices such as switches, routers, access points, surveillance systems, industrial control equipment, etc.
- Consumer-grade hardware provides little visibility and usually has less engineering effort spent on security, leading to higher vulnerability
- Managed hardware is actively configured and upgraded, unmanaged hardware remains susceptible to discovered vulnerabilities

Typical Response Measurement

- Devices in the network often have predictable workloads and performance characteristics
- Monitoring systems can be your first alert mechanism to unusual situations, and log analysis tools can also bring network device behaviours that are unexpected to your attention
- When the situation isn't typical, the first step is to identify specifically what is affected, which may be more than one device or service
- Triangulating those impacts may help locate which devices to examine

Device Examination

- Look for access changes (e.g. passwords no longer working)
- Look for services no longer running, or giving incorrect or slow responses
- Compare configuration settings to expected settings
- Use any on-board tools available to view logs or history on the device
- Use on-board tools to examine what is running and compare to what is observed passing through the device
- Actively examine by doing scanning and response testing, scripts can be helpful with this

Device Information Sources

- Logging, logging, logging
- Enable event tracking for things like dhcp transactions, port up/down, route up/down, login access success/failure, service access success/failure, port scans, etc.
- Enable remote logging, consider limiting or removing logs in device memory to reduce data available to an attacker who compromises a device
- Take memory dump if the device supports it for deeper analysis of compromised device operating systems when compromise is suspected or observed
- Balance how much you track with your logging capabilities, losing log entries is not good

Challenges

- Since every device has its own operating system, you will require resources from the manufacturer to fully examine them
- To provide more extensive access or privileges, some devices have backdoors which the manufacturer does not publish
- Device software is not generally published so security problems are normally not made public until fixes are ready which increases the length of time devices remain vulnerable
- A compromised device may not run all commands, or run them properly, or present complete and legitimate output
- A compromise may have altered the device functions and hidden that alteration (rootkit installed, firmware modified), so it can be very difficult to obtain trustworthy data from such a device

Configuration Checks

- Many simple network devices do not give you much help with forensic examination
- Often your only realistic approach is to examine the configuration for signs of compromise
- Check for additional users, modified authentication methods, ssh or telnet access, modified or disabled firewall, vpn services that should not be there, logging changes or disabling, extra certificates, dns overrides that should not be there, proxies configured, mac address changes, remote logging

External Checks

- Use monitoring software to watch for unusual traffic patterns
- Use firewalls to mitigate attempts to open or use back doors
- Configure firewall to log unusual traffic
- Disable or block UPNP
- Install a transparent proxy to catch and control traffic
- Install an IDS or IPS

Tools

- Release and patch management is essential; you cannot know if a configuration has changed if you don't know what it is supposed to be
- Sometimes the easiest way to check a config is to take a backup of it and do a text diff of the backup and a known good backup
- Cisco Information Retrieval tool (https://www.blackhat.com/presentations/bh-dc-08/FX/Whitepaper/bh-dc-08-fx-WP.pdf)
- Network Appliance Forensic Toolkit (https://blog.didierstevens.com/programs/network-appliance-forensic-toolkit/)
- Shodan IoT search engine (https://www.shodan.io/search?query=%22default+password%22)