**Module 2 Technologies & Tools**

**2.4 Security Technologies**

**Host Technologies – Firewalls**

* Firewalls

1. Windows – type *wf.mac* in cmd
2. Linux Uncomplicated Firewall (*ufw*)/*iptables*

* Firewall Configuration

1. End users shouldn’t be allowed to disable firewall
2. Monitor both incoming & outgoing network traffic

* Output depends on firewall app & OS

1. Windows Event Viewer
2. Linux Logging */var/log*

**Host Technologies – HIDS/HIPS**

* Sensors on each host relay to centralised management console

1. Compiles data to identify distributed friends

* May be included with Host Firewall or Antivirus solution
* Consult documentation
* Issues

1. False positives – legit traffic labelled as attack
2. False negatives – attacks labelled as legit traffic
3. Matching traffic identified as attack with actual network traffic

* NIST SP 800-94 – Guide to Intrusion Detection & Prevention Systems (IDPS)

**Antivirus/Antimalware**

* End-user Pop-up Warning
* Centralised management
* Console warning
* Quarantine vs. Removal
* Issues

1. Antivirus not updated/outdated signatures
2. False positives
3. Ignored/unseen
4. Incorrect decision
5. Malware may still be present

* Solutions

1. Auto-update (need network connectivity)
2. Detach system from network
3. Use multiple Antivirus products Eg. Malwarebytes
4. Manual removal – hunting malware with Windows Sysinternals
5. Reimage system

**File Integrity Checker**

* Computes cryptographic hash (Eg. SHA-1/MD5) for all selected files & creates database of hashes
* Hashes are periodically recalculated & compared to hashes in database to check for modification
* Output to centralised server
* For alerts, determine what changed & why

**Application Whitelisting**

* Organisation approves/permits software apps – all others not allowed
* Windows AppLocker – based on conditions

1. Publisher, for digitally signed files
2. Path, which identifies app by its location
3. File hash, which uses system-computed cryptographic hash

**Data Loss Prevention**

* Prevent sensitive information from physically/logically leaving corporate systems
* Designed to detect & prevent unauthorised use & transmission of confidential information
* Should include corporate data stored in cloud
* Network – Content Filtering (Proxy)
* System – Application White-Listing
* Hardware – USB Blocking

**Removable Media Control**

* Detects/prevents use of removable media (Eg. Hard drives, USB thumb drives etc.)
* Local/network
* Set by corporate policy
* Exception handling
* Use only corporate owned/secured devices
* Scan removable media on each use
* Encryption

**Patch Management**

* Automatic updates when possible
* Patching process

1. Vendor notification
2. Testing
3. Staged deployment
4. Reporting

* Alerting on failed patches
* Patching all apps/systems

**Patch Management Services**

* Microsoft System Centre Configuration Manager (SCCM) formerly Systems Management Server (SMS)
* Linux RPM (Red Hat Package Manager)

**Unified Threat Management (UTM) Next Generation Firewall (NGFW)**

* All-in-one firewall appliance/single interface/single vendor
* Management console
* Network IDS/IPS
* URL filtering – block websites based on category/URL
* Content inspection – application aware
* Malware inspection

**Web Application Firewalls (WAF)**

* Controls input, output &/or access from/to/by app/service based on categories/rules/heuristics
* Deep packet inspection
* Function at Layer 7 (Application) of OSI model
* WAF protects web apps from known attacks (Injection, Buffer Overflows etc.)
* Often included in other firewall types (proxy, IDS/IPS)

**Data Execution Prevention (DEP)**

* Hardware/software
* Prevents malware from executing in memory space reserved for OS system processes
* Both Advanced Micro Devices (AMD) & Intel platforms have DEP hardware capabilities
* Available on Windows 10