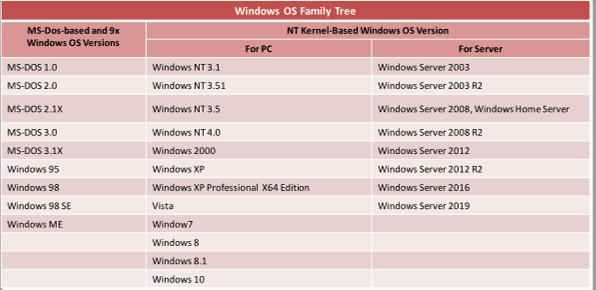
**Module : Appendix**

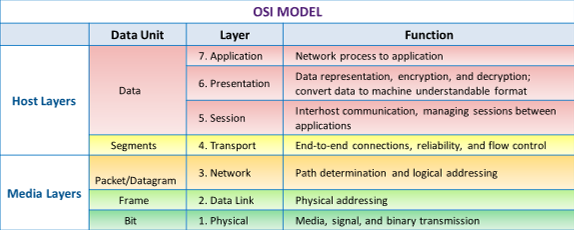
**Operating System**

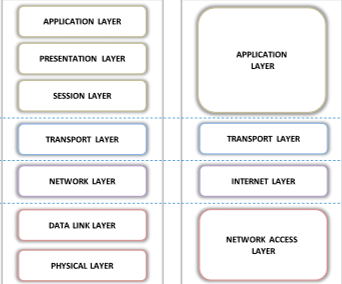
* **Windows OS family Tree** 
* The processors of the Windows system works in two different modes: **User mode**, **Kernel Mode:**
* **Windows Command**
  + **ipconfig**
  + **netstat:** Display all active network connections and ports
  + **nslookup:** Display info that we can use to diagnose DNS infrastructure
  + **ping**
  + **chdir:** Show the current dir name or change the current folder
  + **dir**
  + **echo**
  + **format:** Format the disk
  + **help**
  + **label**
  + **mkdir**
  + **nbtstat:** Display protocol statistics and current TCP/IP connections
  + **systeminfo:** Display comprehensive configuration info about a computer and its OS
* **UNIX OS**
  + **Three main components**
    - **Kernel:** Allocate time and memory to programs. Handle file store and communicates with system calls
    - **Shell**
    - **Programs**
  + **Command**
    - ls
    - cd
    - mkdir
    - rmdir
    - cp
    - rm
    - mv
    - passwd
    - grep
    - diff
    - head
    - ispell
    - pr
    - pwd
    - id
* **MAC OS X OS**
  + Layers of MAC OS X
    - Cocoa Application layer
    - Media layer
    - Core Services layer
    - Core OS layer
    - Kernel and Device Driver layer

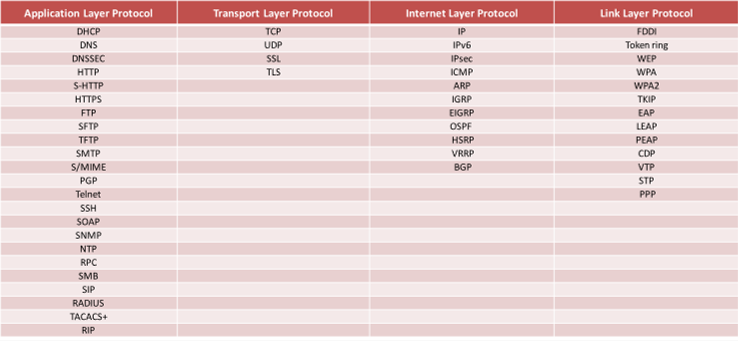
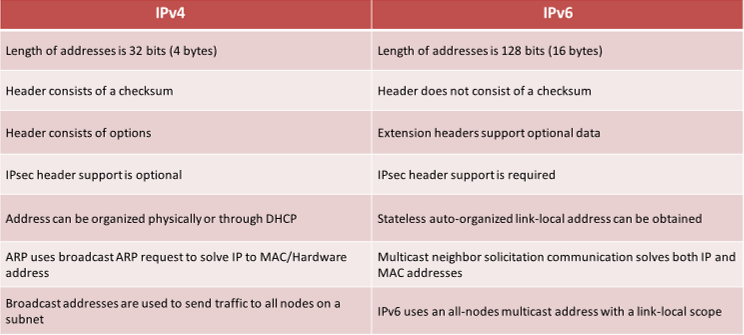
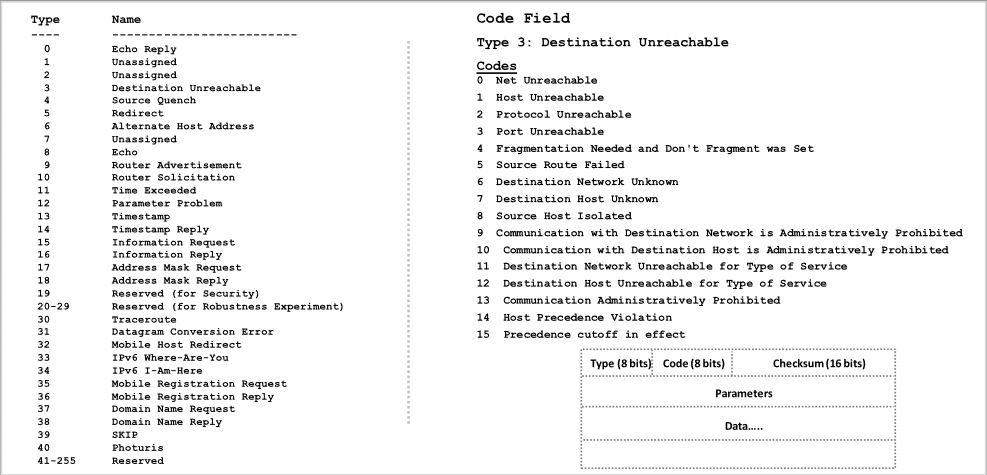
**File System**

* Major file systems include **FAT, NTFS, HFS, HFS+, APFS, Ext2, Ext3, Ext4**, among others
* Windows File System
  + EFS: Encrypting File System
  + Sparse Files
* Linux File System
  + FHS: Filesystem Hierarchy Standard
  + EXT: Extended File System
* Mac OS X File System
  + HFS: Hierarchical File System
  + HFS Plus
  + UFS: UNIX File System

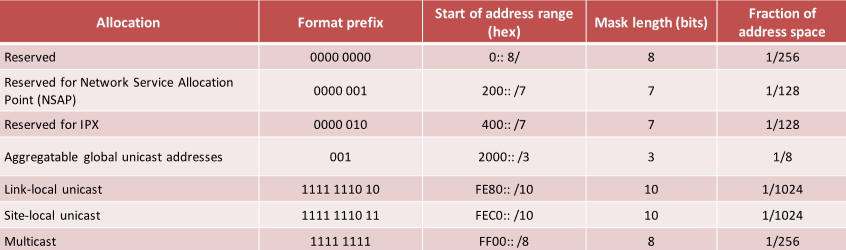
**Computer Network**

* **OSI Model** 
* **Comparing OSI and TCP/IP**



* Types of Networks: **LAN, WAN, MAN, PAN, CAN, GAN**
* Wireless technologies
  + WIMAX
  + Microwave Transmission
  + Optical Wireless communication
  + 2G
  + 3G
  + 4G
  + Tetra
  + Bluetooth:
    - Cover distances of **up to 10m**
    - Transfer data at **less than 1Mbps**
    - Come under **IEEE 802.15**
    - Use a radio technology called **Frequency-hopping spread spectrum**
* **Network Topologies**
  + **Bus topology**
  + **Star topogoly**
  + **Ring topology**
  + **Mesh topology**
  + **Tree topology**
  + **Hybird topology:** Star-bus or Star-ring are widely used
* **TCP/IP Protocol Suite** 
* DNS Hierarchy: **Root->Top-level domains->Second level domains->sub-domains**
* **DNSSEC: (Application layer)**
  + A suite of the IETF (Internet Engineering Task Force)
  + Shield Internet users from **artifical DNS data**
  + Secure certain types of info provided by **DNS**
  + Work by digitally signing records for **DNS lookup** using public-key crypto
  + Guarantee: **Authenticity, Integrity, The non-existence of a domain name or type**
  + Do not guarantee: **Confidentiality, Protect against DoS**
* **HTTP**
* **S-HTTP:** The alternate for the HTTPS (SSL) protocol
* **HTTPS:**
  + Against **MITM**
  + Be vulnerable to **DROWN** (Decrypting RSA with Obsolete and Weakened eNcryption)
* **FTP**
  + Active mode
  + Passive mode
* **SFTP**
  + A secure version of FTP and an extension of SSH2 protocol
* **TFTP**
  + **A lockstep communication protocol**
  + Both direction
  + Generally used only with **LAN**
  + Vulnerable to DoS
  + Vulnerable to Dir traversal vulnerability
* **SMTP**
* **S/MIME**
  + Use RSA for its digital signature and DES for message encryption
* **PGP**
  + An application layer protocol provides **crypto privacy** and authentication for…
  + Encrypt and decrypt email communication and authenticates message with **digital signatures** and encrypts stored files
* **Telnet**
  + Vulnerable to DoS, Packet sniffing
  + Used on a LAN
* **SSH**
* **SOAP (Simple Object Access Protocol)**
  + Equivalent to **RPC**
  + Disad: Stateless, reliance on HTTP, Slower than CORBA
* **SNMP**
  + Vulnerable to DDoS, Remote Code Execution
* **NTP**
* **RPC**
  + Allow inter-process communication between two programs
* **SMB (Server Message Block)**
  + **Application layer** network protocol
  + Provide an authenticated inter-process communication mechanism
  + The transport layer protocol that **Microsoft SMB Protocol,** is most often used with is **NetBIOS over TCP/IP (NBT)**
* **SIP (Session Initiation Protocol)**
* **RADIUS**
* **TACACS+**
  + **Client server** model
  + No integrity checking
  + Vulnerable to **replay a**ttacks
  + Accounting info is sent in plain text
  + Weak encryption
* **RIP**
  + **Distance Vector routing protocol**, used for **smaller** networks
* **TCP (Transport layer)**
* **UDP**
* **SSL**
  + Use **RSA encryption**
  + Provide a secure authentication mechanism between two…
* **TLS**
  + Use a **symmetric key** for **bulk encryption**, an **asymmetric key** for **authentication** and **key exchange**, and **MAC** for **message integrity**
  + Use RSA with 1024-and 2048-bit strengths
* **IP (Internet layer)**
* **IPv6**
  + Store a larger address space
  + Have more security features built into its foundation
  + VS 
* **IPsec**
* **ICMP**
  + Unreliable method for the delivery of network data
  + Format of an ICMP message 
* **ARP**
  + A stateless procotol
* **IGRP (Interior Gateway Routing Protocol)**
  + Distance-Vector protocol
* **EIGRP (Enchanced Interior Gateway Routing protocol)**
  + Hybrid routing protocol
* **OSPF**
  + An interior gateway protocol
  + Link-state routing protocol
* **HSRP (Hot standby router protocol)**
* **VRRP (Virtual router redundancy protocol)**
* **BGP**
* **FDDI (Link layer protocol)**
* **Token Ring**
* **CDP ( Cisco discovery protocol)**
* **VTP (VLAN Trunking protocol)**
* **STP (Spanning Tree protocol)**
  + Vulnerable to: MITM, DoS, DNS Spoofing, Session hijacking…
* **PPP (Point to point)**

**IP Addressing and Port numbers**

* **IANA (Internet assigned number authority)**
  + Responsible for the global coordination of DNS Root, IP addressing, and …
  + Well-known ports are assigned by IANA, **0-1023**
* **IPv6** 

**Network Terminology**

* **Routing**
  + Static routing
  + Dynamic routing
* **NAT**
* **PAT**
* **VLAN**
* **Shared media network**
* **Switched Media Network**

**Network Troubleshooting**

* **Tools**
  + ping
  + Tracert/traceroute
  + ipconfig/ifconfig
  + nslookup
  + netstat: **display both the incoming and outgoing TCP/IP traffic**
  + PuTTY/Tera Term
  + Subnet and IP calculator
  + Speedtest.net
  + Pathping/mtr
  + Route

**Virtualization**

* **Characteristics of virtualization**
  + partitioning
  + isolcation
  + encapsulation
* **Virtual firewall**
* **Virtual OS**
* **Virtual Database**

**NFS (Network File System)**

* A distributed file system protocol
* IP-based networks
* Methods of securing access controls in NFS
  + Root squashing
  + nosuid
  + noexec

**Web Markup and Programming Languages**

* HTML
* XML
* Java
* .Net
* C#
* JSP
* ASP
* PHP
* Perl
* JS
* Bash scripting
* PowerShell: **Object-orirented** command line shell and scripting language
* C
* C++
* CGI (Common Gateway Interface)
  + The standard way for a web server to connect to external applications

**Application Development Frameworks and Their Vulnerabilities**

* .NET
  + Remote code execution
  + DoS
  + Feature Bypass
  + Modifying the framework Core
* J2EE
  + XSS
  + Execute arbitrary programs
  + DoS
  + Sensitive info disclosure
* Cold Fusion
  + Dir traversal
  + DoS
  + CSRF
  + Unvalidated browser input
* Ruby On Rails
  + Remote code execution
  + Authentication bypass
  + DoS
  + Dir Traversal
  + XSS
* AJAX
  + XSS
  + CSRF
  + SQL injection
  + XPATH injection

**Web Subcompoinents**

* Thin and Thick clients
* Applet: A java program that is embedded in a webpage
* Servlet
* ActiveX
* Flash Application

**Info Security Controls**

* **EISA** (Enterprise info security architecture)
  + A set of requirements, processes, principles, and models that determines the structure and behavior of an org’s info systems
* **Administrative Security Controls:**
  + Administrative acess controls implemented by …
* **Regulatory Framework Compliance**
  + Complying with regulatory frameworks is a **collaborative effort** between governments and private bodies to encourage voluntary **improvements** to cybersecurity
* **Info security policies**
  + The foundation of **security infrastructure**
  + Define the basic security requirements and rules to be implemented in order to protect and **secure an organization’s information systems**
  + Types
    - **Promiscuous policy:** No restrictions
    - **Permissive policy:** Begin wide open and only known dangerous srvs, attacks, and behaviors are blocked
    - **Prudent policy:** Block all srvs and only safe or necessary srvs are individually enbaled, everything is logged
    - **Paranoid policy:** Forbid everything
* Privacy policies at the workplace
* HR or Legal Implication of Security Policy Enforcement
* Security Awareneess and Training
* Employee Awareness and Training: Physical Security
* Social Engineering
* Data classification
* Separation of Duties (SoD)
* Least Privileges (POLP)
* Physical Security Contorl
  + Lock
  + Fences
  + Badge systems
  + Security guards
  + Mantrap door
  + Biometric systems
  + Lighting
  + Motion detectors
  + Closed-circuit TVs
  + Alarms
* Types of Physical Security Controls
  + Preventive Controls: **Door lock, security guard, etc.**
  + Detective Controls: **Motion detectors, alarm systems, video surveillance**…
  + Deterrent Controls: **Warning signs**
  + Recovery Controls: **Disaster recovery, business continuity plans, backup systems…**
  + Compensating Controls: **Hot sites, backup power systems…**
* Access control
  + DAC (Discretionary access control)
  + MAC (Mandatory access control)
  + Role-based Access
* IAM (Identity and Access management)
* Types of authentication
  + Password
  + 2FA
  + Biometric
    - Fingerprinting
    - Retinal scanning: **Layer of blood vessels at the back of their eyes**
    - Iris scanning: **Colored part of the eye**
    - Vein Structure recognition
    - Face recognition
    - Voice recognition
  + Smart Card
    - **Crypto-based** authentication, stronger than password authentication
    - Insert smart card and type PIN
  + SSO
* Accounting

**Network Security Solution**

* SIEM (Security Incident and Event Management)
* UBA (User behavior analytics)
* UTM (Unified Threat Management)
* Load Balancer
* NAC (Network access control)
* VPN
  + Components
    - Vpn client
    - Tunnel terminating device
    - NAS (Network access server)
    - VPN protocol
  + **VPN Concentrators**
    - A network device used to create secure VPN connections
    - Act as a VPN router which is generally used to create a remote access or site-to-site VPN
  + Functions
    - Encrypt and decrypt data
    - Authenticate users
    - Manage data transfer across the tunnel
    - Negotiate tunnel parameter
    - Manage security key
    - Establish tunnels
    - Assign user address
    - Manage inbound and outbound data transfer as a tunnel endpoint or router
* Data Leakage
  + **DLP (Data loss prevention)**
* Data backup
  + **RAID (Redundant array of independent disks)**: A method of combining multiple hard drives into a single unit and writing data across several disk drives that offers fault tolerance
  + Method
    - Hot backup (online)
    - Cold backup (offline)
    - Warm backup (nearline): a combination of a hot and cold backup
* Data recovery

**Risk Management**

* ERM (Enterprise risk management framework)
* NIST risk management framework
* COSO ERM framework
* COBIT framework
* Enterprise network risk management policy
* Risk mitigation
* Control the risks
* Risk calculation formulas
  + **Asset Value (AV):** The value you have determined an asset to be worth
  + **Exposure Factor (EF):** The **estimated percentage** of damage or impact that a realized threat would have on the asset
  + **Single Loss Expectancy (SLE):** The projected loss of a single event on an asset
  + **Annual Rate if Occurrence (ARO):** The estimated number of times over a period the threat is likely to occur
  + **Annualized Loss Expectancy (ALE):** The projected loss to the asset based on an annual estimate
  + Qualitative risk: A subjective assessment
  + Quantitative Risk: A numeric assessment, **ARO\*SLE=ALE**

**Business Continuity and Disaster Recovery**

* BC (Business continuity)
* DC (Disaster Recovery)
* BIA (Business Impact Analysis)
* RTO (Recovery Time Objective)
* RPO (Recovery Point Objective)
* BCP (Business Continuity Plan)
* DCP (Disaster Recovery Plan)

**Cyber Threat Intelligence**

* CIF (Collective Intelligence Framework)
* Threat intelligence data collection
* Threat intelligence sources
  + OSINT (Open-source intelligence): Publicly available sources
  + HUMINT (Human intelligence): Interpersonal contacts
  + SIGINT (Signals intelligence): Intercepting signals
  + …
* Collect IoCs (Indicator of compromise)

**Penetration Testing**

* **Security audit:** Check **whether the org is following a set of standard**…
* **Vulnerability assessment: Discover the vulnerabilities** in the info system, but **do not indicate** whether the system can be exploited successfully
* **Penetration testing:** Encompass the security audit and vulnerability assessment and demonstrate if the vulnerabilities in the system can be successfully exploited
* **Blue Team**
* **Red Team**
* Black box
* White box
* Grey box: Limited knowledge of the infrastructure to be tested
* Phases of penetration testing
  + Pre-attack
  + Attack
  + Post-attack
* Security testing methodology
  + OWASP
  + OSSTMM
  + ISSAF
  + EC-Council LPT Methodology
* ROE (Role of engagement)

**Software Development Security**

* **N-tier Application Architecture**
  + Presentation tier
  + Logic tier
  + Data tier
* **3-Tier Application Architecture**
  + Presentation tier
  + Application tier
  + Database tier