Chapter 1 – Network Security

1.1 Network Security

**Router Functions**
Routers connect networks generally based on network addresses, usually IP network addresses. They create subnets (sub-networks) which isolate broadcast domains (as opposed to collision domains), and to some extent isolate security zones, particularly when access control lists (ACLs) are implemented. Routers can have a manually /statically configured routing table or use routing protocols to dynamically determine the best path.

**Router Security**
Routers should be physical secured in a server room. Default passwords should be changed. Access should be limited to the console port or SSH. TACACS+ or RADIUS is the best method of remote user authentication to a router. ACLs to control allowed traffic should be implemented. ACLs should disallow incoming spoofed addresses, source routing, and broadcasts.

**Switch Functions**
Switches connect hosts on a LAN by MAC address. They reduce or eliminate collisions. VLANs can and should be created on switches. Each VLAN is a broadcast domain and to some extent a security zone. For instance a sniffer on one VLAN cannot see traffic on another VLAN. VLANs are connected by routers or multilayer switches. Although Switches, by design, create collision domains; with the assistance of a router, they can create broadcast domains as well.

**Switch Security**
Client access should be controlled by approved MAC address. This is port security. Unused ports should be disabled. VLANs should be created to isolate broadcast/security domains. Disable Dynamic Trunking Protocol so that an attacker with a sniffer cannot listen to traffic from all VLANs. Change default passwords so an attacker cannot take over a router. To limit attacks, limit remote access and physical access.

**VPN Concentrator**
Virtual Private Networks (VPNs) encrypt traffic passing through the Internet. It follows that VPNs allow secure remote access. A VPN concentrator allows scalable secure remote access by being able to handle the load of multiple heavily utilized VPN connections.
Load Balancer
A load balancer distributes the load among multiple Web servers, increasing performance, and reliability, while eliminating a single point of failure by providing redundancy. Load Balancers can be hardware or software based.

Devices that Inspect Network Packets
Examples of devices that inspect network packets include sniffers, protocol analyzers, NIDS, and NIPS.

Sniffers/Protocol Analyzers
Sniffers capture network packets. They are usually integrated with a protocol analyzers that understand the content of the packets. Examples are Wireshark and Microsoft Network Monitor.

Honeypot and Honeynet
A honeypot is single fake system meant to divert attackers away from a production network and to study hacker tools and techniques. A honeynet emulates a set or network of servers.

NIDs and NIPs
Network based Intrusion detection systems inspect network traffic and do logging and alerting. Network based Intrusion prevention systems take the next step in that they also neutralize attacks.

Types of NIDs & NIPs
Signature based NIDS/NIPS (also HIDS/HIPS) need updates. They are best for known attacks. Anomaly based NIDS/NIPS (also HIDS/HIPS) look for unusual events. They are best for zero day attacks. Behavior based NIDS/NIPS (also HIDS/HIPS) match specifically configured traffic patterns. Heuristic NIDS/NIPS (also HIDS/HIPS) are similar to anomaly based. They use artificial intelligence to detect new attacks.

Filtering Connectivity
To kill connections with an attacker, NIPS do shunning, blocking on attackers, and TCP resets on victims. Firewalls control traffic based on such parameters as ACL, stateful connection inspection, or inspection of the contents of packets at the application layer. A web security gateway / content filter blocks Web sites by URL. A proxy Server caches or stores Web pages for faster client access, while a reverse Proxy can have sophisticated filters. A SPAM filter is typically incorporated in Email. Finally, an all-in-one security appliance integrates many of the above functions.

1.2 Secure Network Administration
Secure Network Administration Elements
Elements of secure network administration include rule-based management, firewall rules, VLAN management, secure router configuration, access control lists, port security, 802.1x, flood guards, loop protection, implicit deny, preventing network bridging by network separation, and log analysis.
Secure Network Administration
Secure network administration includes the setup of firewall and router filtering and access control lists including anti-spoofing rules, aided by an understanding of implicit deny. Implicit deny means that any connection not explicitly allowed is denied by default. Passwords for firewalls, routers, and switches should be changed. Administrators should create VLANs, secure ports by MAC address, disable DTP. Switch trunk ports should be mirrored for NIDS/NIPS so all traffic can be monitored / protected. Remote router authentication should be through SSL or 802.1x. Logs for all network devices should be reviewed. Flood guards should be used to protect against SYN flood attacks, trace the source, generate alerts, and block attack traffic. Loop protection prevents network disruption if both ends of a network cable are connected to different switch ports. Bridging a USB cellular connection to get around a firewall should be disallowed as it may join two networks of different classifications.

1.3 Secure Network Design Elements
Secure Network Design Elements
The following are components of a secure network design: DMZ, subnets, VLANs, NAT, secure Remote Access, hardening of telephony, NAC, virtualization, judicious use of cloud computing including Platform as a Service, Software as a Service, and Infrastructure as a Service. Additional elements are a De-Militarized Zone (DMZ) which is an area between two firewalls. The first firewall protects Web and other public facing servers from threats on the Internet. The second firewall more completely protects the internal network.

Subnetting and VLANs
Subnets and VLANs separate broadcast and to some extent security domains. Subnets are created on routers. VLANs are created on switches. On switches, DTP (Dynamic Trunking Protocol) should be disabled to prevent VLAN jumping, and port spanning/port mirroring should be disabled on trunk ports except for NIDS/NIPS use. DTP provides the ability to automatically negotiate a trunk link between two switches.

Network Address Translation
NAT conserves and hides Private IP addresses from the public internet. Static NAT has a one to one mapping between internal and external addresses. Dynamic NAT allows that mapping to change dynamically. Port Address Translation (PAT) allows multiple hosts to connect at the same time. NAT Transversal (NAT-T) works with IPSEC that also rewrites the IP header. Chances are if you are reading this document ‘on-line’ you are using NAT.

Remote Access
Remote access policy sets rules for remote access. Remote access should use a secure protocol such as SSH (Secure Shell). Finally a VPN concentrator would provide remote access for a large number of users.
Telephony
Telephone switches should be physically secured. Default passwords should be changed. If remote administration is allowed it should be via a secure protocol such as SSH, not Telnet, or SNMP.

Network Access Control (NAC)
NAC would redirect a guest user to the company portal and ask the user to agree to the company’s acceptable use policy. NAC checks out and remediates foreign laptops that attempt to connect to a company network. It also updates patches and antivirus definitions and performs a virus scan before granting access to a corporate network. Finally, NAC provides levels of network access based on predetermined characteristics.

Virtualization
In virtualization, one or more physical servers host multiple virtual servers. This cuts down on the footprint. If you have only one physical server then this is a single point of failure, but if you have multiple physical servers operating as a virtualization farm then availability increases. The specialized operating system that hosts the virtual machines is the hypervisor. The host and guest OSs should all be patched, as virtual machines have the same security requirements as physical servers. In general virtual machines are isolated and are a safe environment to test malware. To prevent reverse engineering, some malware can detect a virtual environment. Memory can be shared between the host virtual machines and could be attacked to harm all of them. Finally escape is the term for an attack that affects more than one virtual machine. The most popular virtualization products would be Hyper-V from Microsoft or ESX from VMware.

Cloud Computing
Cloud computing utilizes hosted services over the Internet. It is sold on demand and is elastic, using virtualization to provision guests on demand. It is also fully managed by the provider, facilitating computing for heavily utilized systems. Security drawbacks of cloud computing are loss of physical control over data, and blended systems and data. Most Cloud Computing environments now use full Virtualization.

Cloud Computing Services
In Platform as a Service (PaaS) developers create applications on the provider’s platform. PaaS is an easy-to-configure OS with on-demand computing. In Software as a Service (SaaS) the vendor supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal. A company would not have to hire additional personnel or servers and could minimize the footprint of their datacenter. In Infrastructure as a Service (IaaS) users can start, stop and configure virtual servers. It would be useful to a company with a lot of sensitive data on unreliable systems.
1.4 Secure and Insecure Network Protocols

**Secure and Insecure Network Protocols**

Network protocols include IPSec, SNMP, SSH, DNS, TLS, SSL, TCP/IP, FTPS, HTTPS, SFTP, SCP, ICMP, as well as IPv4 and IPv6.

**IPSEC**

IPSEC was originally developed for IPv4, but works equally well with IPv6. IPSEC protocols include ESP, AH, and IKE. ESP provides confidentiality through encryption. AH provides message integrity, non-repudiation, authentication, and protection from replay attacks through a hash. ESP is stronger than AH. ESP plus AH is strongest. IKE manages security keys and associations. IPSEC can be used as the encryption piece of a VPN with L2TP (Layer two tunneling protocol) setting up the tunnel, or IPSEC can be the tunneling and encryption piece of a VPN.

**Simple Network Management Protocol**

SNMP is used to manage network devices including printers, servers, routers, and switches. SNMPv1 and SNMPv2 are insecure protocols. SNMPv3 is secure and provides data integrity, authentication, confidentiality, and protection from malicious reordering of the data stream. SNMP can be used to consolidate logging information from various servers and network devices.

**Secure SHell**

SSH is a secure replacement for Telnet and FTP. Slogin replaces Telnet. SCP and SFTP replace FTP. FTPS is another secure version of FTP, but it is not based on SSH.

**Domain Name System**

DNS resolves a host name or Fully Qualified Domain Names to an IP address or IP Addresses. It replaces, but operates alongside a Hosts file. DNS footprinting enumerates the hosts on a network. While DNS kiting reregisters a domain name within the five day grace period. DNS attacks include spoofing and cache poisoning. To detect DNS attacks,

DNS logs should be evaluated for failed zone transfers and attempted zone transfers to an unknown host. NSLookup should not allow a zone transfer.

**HTTP, HTTPS, SSL and TLS**

HTTP transfers Web pages. HTTPS does this securely by using certificates. SSL is the underlying protocol for HTTPS. SSL can also be used in SSTP to set up a VPN that does not require a VPN client setup. TLS is more secure than SSL because it checks that a certificate belongs to the web site, it also can be used to secure traffic between SMTP servers. HTTP uses TCP Port 80, HTTPs uses TCP Port 443.

**TCP/IP**

IP provides addressing and routing. An attacker can forge the source IP address. TCP provides reliability through sequence numbers and acknowledgements. An attacker might monitor a network transmissions predict a sequence number and forge an acceptable response. This is a Man-in-the-Middle attack. Finally, the three-way TCP handshake can be exploited in a SYN Flood attack.
ICMP
ICMP provides network reachability and diagnostics. It supports ping, tracert, and router messages such as source routing. ICMP attacks include Ping of Death, Surf Attack, and bogus source routing updates. Source routing should be disabled. Firewalls should block ping packets and have anti-spoofing rules. Responses to the subnet broadcast address should be disabled.

IPv4 vs. IPv6
IPv4 has a 32 bit address space that is close to being depleted. IPv6 has a 128 bit address, enough for 100 IP addresses for every square foot on the earth. It was designed with security and speed in mind with original support for IPSEC, so it provides secure tunneling services.

1.5 Network Ports
These TCP port numbers should be memorized:

General
FTP 20/21
FTPS 989/990
SSH, SCP, SFTP, SLogin  22
TELNET  23
NetBIOS  139 /445
Radius 1812/1813

Web
HTTP  80
HTTP Admin 8080
HTTPS  443

Email
SMTP  25
POP3   110
IMAP4  143

Networking
DNS 53
DHCP 67/68
RDP 3389

Active Directory
Kerberos 88
LDAP 389/636

VPNs
L2TP 1701
PPTP 1723
IKE 500
IKE Protocol ID 50
1.6 Secure Wireless

Secure Wireless Elements
Elements of secure wireless include WPA (Wi-Fi Protected Access), WPA2, WEP (Wired Equivalent Privacy), EAP (Extensible Authentication Protocol), PEAP, LEAP, MAC filters, disabling the SSID (Service Set Identifier) broadcast, TKIP, CCMP, proper antenna placement, and low power levels.

Securing Wireless Routers
Filter by MAC address. Measures to secure wireless routers include changing the SSID and disabling SSID broadcast. As defenses against war driving, change the default password and only allow secure remote administration. Use the lowest power level that does the job; place the antenna in the center of the building, and use shielding and/or directional antennas.

Wireless Router Encryption
WEP (Wired Equivalent Privacy) is weak. It has a 24 bit initialization vector. It should not be used. WPA is much stronger as it uses EAP (Extensible Authentication Protocol), TKIP, and RC4. WPA2 (Wi-Fi Protected Access version 2) replaces RC4 with AES. 802.11i is better than WPA2 as it replaces TKIP with Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). CCMP changes the whole encryption key on a minute by minute basis, while TKIP changes only part of the encryption key.

PSK vs. Enterprise
In general WPA2 (Wi-Fi Protected Access version 2) is stronger than WPA (Wi-Fi Protected Access). WPA or WPA2 Personal/PSK both use a passphrase/pre-shared key. This is not as secure as WPA or WPA2 Enterprise which uses a longer key or a key that is machine generated and unknown to users. Enterprise also uses 802.1X, so WPA Enterprise is stronger than WPA2 Personal.

EAP, EAP-TLS, PEAP, & LEAP
EAP is Extensible Authentication Protocol. WPA/WPA2 Enterprise use EAP. EAP-TLS uses certificates. PEAP is Protected EAP encapsulates EAP in an encrypted and authenticated TLS tunnel. It also uses certificates and MS-CHAPv2 to perform mutual authentication. LEAP is Lightweight EAP uses MS-CHAPv2 to protect authentication credentials and provide mutual authentication.