Network Equipments

D) Management Protocols

Weaknesses in the protocols commonly used for the remote management of devices.

Telnet :

* Port No - 23
* OSI Layer - Layer 7 (Application Layer)

Clear text vulnerable to password sniffing (cain using ARP spoofing)

Vulnerbility in Telnet

* Default password
* Brute force for Password
* Telnet Exploit scripts

Ex: Sun Solaris 10 (sparc + x86) Telnet Remote Authentication Bypass Vulnerability

Solaris (<=8 sparc + x86) TTYPROMPT Telnet Vulnerability

Web based Protocol

* Clear text for HTTP
* Default passwords
* Brute force attack against password with default user accounts (hydra)

SSH

* Port NO - 22
* OSI Layer - Layer 7 (Application Layer)

Fingerprint SSH Service using Telnet, ncat, nc

Vulnerabilities in SSH.

* Brutiforce Attacks
* SSH1 CRC32 Compensation Exploit

SSH-1 has inherit flaw, which is vulnerable (man-in-middle attacks)

Avoid by explicitly disabling fallback to SSH-1

SNMP (Covering network information enumeration and common attacks against Cisco Configurations)

* Port NO - UDP (161)
* OSI Layer - Layer 7 (Application Layer)

Vulnerabilities in SNMP:

* Default SNMP community string (Public, Private)
* Clear text protocol so community string can be easily sniffed from the network (wireshark or cain)
* Brute force SNMP Community Strings
* Information enumeration (snmpwalk, snmpnetstat)
* Cisco snmp 'write' community string TFTP Config retrieval.
* Assend snmp 'write' community string TFTP config retrieval
* With Config you can crack [Cisco Type 7 passwords (+) Vigenere cipher

TFTP :-

* Port NO - 69 (UDP)
* OSI Layer - Layer 7 (Application Layer)

TFTP client requests the "dir.txt" file, the server will generate and send a file that lists the content of the base directory

Vulnerabilities in TFTP :-

* No authentication. file can be retrieved if you know the file name

* TFTP bruteforce

Cisco Reverse Telnet

* Cisco reverse Telnet is specialized application of telnet. where the server side of the connections read and writes data to TTY line (RS-232 serial port).

* To do reverse Telnet aux port of the router must be connected to the Console of the device.

NTP :- (Network Time Protocol)

* Port No - 123 (UDP)

* OSI Layer - Trasport Layer

* It is used for Synchronizing the clocks of Computer Systems over a Network

Vulnerabilities in NTP :-

* RH 7 ntpd Remote Buffer Overflow

D2) Network Traffic Analysis

It is a method of monitoring network availability and activity to identify anomalies including security and operational issues

D2a) Techniques for local network traffic Analysis

Tools : Wireshark

Linux CLI : tcpdump

D2b) Analysis of network traffic stored in Pcap file

* Load the file into wireshark
* tcpdump -r <capturefile>

D3) Networking Protocols

Security issues relating to the networking protocols.

ARP : Address Resolution Protocol

ARP Spoofing enables sniffing traffic on a switch LAN and performing man-in-the-middle attack.

Tools : Cain, Ettercap.

DHCP : Dynamic Host Configuration Protocol

Port : DHCP Server - 67, DHCP Client - 68

OSI Layer: Network

DHCP is a network management protocol used to automate the process of configuring devices on IP networks.

CDP : Cisco Discovery Protocol

Port :

OSI Layer : Data Link Layer

* Information disclosure from CDP such as devices, OS version, IP address and VLAN ID by sniffing network traffic.

* DOS via CDP flooding :

Tools : yersinia

HSRP : Host Standby Routing Protocol

HSRP allows you to configure two or more routers and only a single router as active router at a time.

Tools : Yersinia

VRRP :- Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol is a computer networking protocol that provides for automatic assignment of available internet protocol routers to participating hosts

VTP :- VLan Trunking Protocols:-

This protocol manages the addition, deletion and renaming of virtual Local Area Network on a network-wide basis.

Tods :- Yasinia

STP :- (Spanning Tree Protocol)

Port Number :- 128

OSI Layer :- Data Link Layer

* The Spanning Tree Protocol is a network protocol that builds a loop free logical topology for Ethernet networks.

* The basic function of STP is to prevent bridge loops and the broadcast radiations that results from them

* Disabling the STP root switch will also result in a network DOS.

Tools: Yersinia

TACACS+:

TACACS(+) - Terminal Access Controller Access-Control System Plus

Port Number: 49

* This protocol which provides access control for routers, network access servers and other networked computed devices via one or more centralized servers.
* TACACS(+) provides separate authentication, authorization and accounting services.
* TACACS(+) uses TCP port 49,
* The Packet body is encrypted, but the header is not.

P4) IPSec

Enumeration and fingerprinting of devices running IPsec Services.

ISAKMP - Security Association and key Management Protocol

*ISAKMP is accessible through port 500 and provides Internet Key Exchange (IKE) support of IPsec VPN tunnels.

*IKE is used as the authentication mechanism when establishing an IP connection

Main mode :-

Main mode authenticates both parties to each other. This process first establishes a secure channel in which authentication information is then exchanged securely between two parties

Aggressive mode :-

* Aggressive mode does the same thing that main mode does but in faster. Aggressive mode does not provide secure channel to protect authentication information.

Enumeration Commands

nmap -sU -p 500 target :- Port Scan

ike-scan -M target :- Identifies IPsec VPN devices

ike-scan -M --showbackoff :- analysis ike-scan

ike-scan -A -M target - Aggresive mode

D5) VoIP :-

D5a) Enumeration and fingerprinting of devices running VoIP services.

Port Number : 5060

OSI layer :- Transport Layer

Voice Over Internet Protocol, also called IP Telephony is a method and group of technologies for the delivery of voice communications and multimedia sessions over Internet protocol networks

Enumerate SIP devices :-

svmap.py target - map SIP services

svwar.pl ipaddress - Identify extensions

svcrack.pl <IP> -u <ext> -d pass.txt - crack password for <ext>

D6) Wireless

D6a) Enumeration and fingerprinting devices running wireless (802.11) services.

* Netstumbler.exe - Windows GUI
* Kismet - Linux tool

D6b) Knowledge of various options for encryption and authentication and the relative methods of each.

WEP: Wired Equivalent Privacy

Key Size : 40 bits

Types of Authentication : i) Open System Authentication
ii) Shared Key Authentication

* In Open System Authentication, the WLAN client does not provide its credentials to the Access point during the authentication
* In shared key authentication, the WEP key is used for authentication in a four-step challenge response handshake. The client sends an authentication request to Access point:

TKIP : Temporal Key Integrity Protocol

key size : 128 bits

* TKIP is vulnerable to MIC Key Recovery attack that, if successfully executed.

* It allows an attacker to transmit and decrypt arbitary packets on the network being attacked.

WPA | WPA2 : Wi-fi Protected Access

key Size : 256 bits

* WPA/WPA2 - Enterprise integrate the use of

*EAP to perform 802.1x authentication via a remote authentication server and 802.1x enabled clients

EAP:- Extensible Authentication Protocol.

only "EAP-TLS" was certified by the Wi-Fi Alliance

EAP Types

* EAP-TLS
* EAP-TTLS / $MSCHAP_{v_2}$
* $PEAP_{v_0}$ / EAP-$MSCHAP_{v_2}$
* $PEAP_{v_1}$ / EAP-GTC
* EAP-SIM

LEAP - Lightweight Extensible Authentication Protocol

* LEAP is a Cisco propriety Protocol.

* Important feature of LEAP are dynamic keys and mutual Authentication (between a wireless client and a RADIUS Server.

PEAP : Protected Extensible Authentication Protocol

* It is vulnerable to man-in-the-middle attack if the client doesn't validate the servers certificate.

D7) Configuration Analysis

Analysing configuration files from the following types of cisco equipments.

i) Routers : same as switch

nipper -ios-router -input = <config file>
--output = report.html

ii) Switch : (use nipper)

nipper -ios-switch -input = <config file> --output = report.ht

D7a) Interpreting the Configuration of other manufacturers

--ios-switch - IOS-based switch
--ios-router - IOS-based router
--ios-catalyst - IOS-based catalyst