THE NETWORK PROTOCOL CHEATSHEET

Riddhi Suryavanshi

[1]*University of Delhi,* [2]*Lucideus Technologies*

riddhisuryavanshi11@gmail.com

I. INTRODUCTION

This document is intended for students and security professionals as a quick reference for networking protocols. It covers 50 protocols classified according to the OSI Layer they operate on. The corresponding RFC has been provided to further check for parameters/commands of a particular protocol. From security perspective, the corresponding attacks/vulnerabilities are also included in this cheatsheet.

II. KEY TERMS

Protocol, Port, RFC, OSI Layer, Attack, Vulnerability

III. DEFINITIONS

[1] Protocol- A protocol is a standard set of rules that allow electronic devices to communicate with each other.
[2] Port- A logical construct that identifies a specific process or a type of network service.
[3] RFC- A formal document from the Internet Engineering Task Force that is the result of committee drafting and subsequent review by interested parties.
[4] OSI Layer- One of the seven layers of the Open Systems Interconnection Model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
[5] Attack: An information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission.
[6] Vulnerability: A flaw in a system that can leave it open to attack.

IV. ABBREVIATIONS

DoS	Denial of Service
MitM	Man in the Middle
b/w	between
MAC	Media Access Control
VPN	Virtual Private Network
N/W	Network
VoIP	Voice over IP
Aka	Also known as
DROWN	Decrypting RSA using Obsolete and Weakened Encryption
DDoS	Distributed Denial of Service

S No.	PROTOCOL	PORT(s)	TCP/UDP port	RFC	OSI LAYER	DESCRIPTION	ATTACKS/ VULNERABILITES
1	**IEEE 802.11**	-	-	-	Physical	• Specifies MAC & physical layer protocols for implementing WLAN Wi-Fi.	• DoS by MAC address spoofing
2	**PPTP** (Point-to-Point Tunneling Protocol)	1723	Both	2637	Data Link	• Implements VPN • Uses TCP control channel and Generic Routing Encapsulation(GRE)	• MitM • Bit flipping
3	**L2TP** (Layer 2 Tunneling Protocol)	1701	Both	2661, 3931	Data Link	• Extension of PPP • Uses UDP to avoid TCP meltdown problem.	• DoS
4	**PPP (**Point to Point Protocol)	-	-	1661	Data Link	• Provides communication b/w 2 routers directly without any host or networking. • Provides connection authentication, transmission encryption & compression.	• Format string attack
5	**ARP** (Address Resolution Protocol)	-	-	826	Layer 2.5	• Discovers the MAC address. • Creates a communication in internal N/W.	• ARP cache poisoning
6	**RARP** (Reverse Address Resolution Protocol)	-	-	903	Layer 2.5	• Resolves MAC address to an IP address.	• ARP Poisoning
7	**ICMP** (Internet Control Message Protocol)	-	-	792	Network	• Used by ping & traceroute utility to report info. about network connectivity. • Uses a data packet with 8-byte header. • Each packet has a Type & Code. • No port used as N/W software itself interprets all ICMP messages.	• Ping sweep • Ping flood • ICMP tunneling • Forged ICMP redirects
8	**IGMP** (Internet Group Management Protocol)	-	-	3376	Network	• Used by TCP/IP suite to achieve dynamic multicasting. • Class D IP addresses are used.	• DoS
9	**OSPF** (Open Shortest Path First)	-	-	2328, 2740	Network	• Routing protocol for IP networks. • Uses link state routing algorithm. • Part of interior gateway protocols (IGPs).	• DoS • Local authentication bypass
10	**NAT** (Network Address Translation)	-	-	3022	Network	• Maps one IP address space to another. • Modifies network address in IP header of packets. • Helps to conserve global address space.	• DoS • Interception of internal & external traffic due to improper configuration.

						• Requires 1-to-1 relationship.	
11	**PAT** (Port Address Translation)	-	-	-	Network	• Aka NAT overloading. • Permits multiple devices on a LAN to be mapped to a single public IP address. • Provides many-to-one relationship.	• Discovery of intranet IP addresses.
12	**IP** (Internet Protocol)	-	-	791, 2460	Network	• Provides the functions necessary to deliver a datagram from a source to a destination over an interconnected system of networks. • No reliability, flow control & sequencing.	• IP Spoofing
13	**RIP** (Routing Information Protocol)	520	UDP	1058, 2080, 2453	Network	• Dynamic routing protocol. • Uses hop count to find the best path b/w source & destination.	• DDoS reflection attacks.
14	**IPSEC** (IP Security)	1293	Both	2407	Network	• Provides data authentication, integrity, and confidentiality. • 3 components: Encapsulating Security Payload, Authentication Header & Internet Key Exchange.	• Bleichenbacher attack
15	**TCP** (Transmission Control Protocol)	0-65535	TCP	793	Transport	• Connection oriented. • Error checks & reporting. • Acknowledgement. • 20 byte header.	• SYN flooding • TCP Reset • TCP Session hijacking
16	**UDP** (User Datagram Protocol)	0-65535	UDP	768	Transport	• Connectionless. • Error checks but no reporting. • No acknowledgement. • 8 byte header.	• UDP flood attack.
17	**NETBIOS** (N/W Basic Input Output System)	137,138	Both	1001, 1002, 1088	Session	• Allows applications on separate computers to communicate over a local area network. • Relies on API.	• Information disclosure • Connection using null sessions
18	**RPC** (Remote Procedure Call)	530	Both	1057	Session	• Used for interprocess communication in client-server based applications.	• XML-RPC attacks.
19	**SMB** (Server Message Block)	139,445	Both	-	Session	• Enables user to access file on a server, or other application. • CIFS was its early version.	• Eternal Blue attack • Gives remote access • WannaCry & Petya.
20	**SOCKS** (Socket Secure)	1080	Both	1928	Session	• Exchanges network packets between a client and server through a proxy server. • No compatibility issues unlike HTTP proxy.	• Arbitrary command execution. • DoS

21	**RTP** (Real-time Transport Protocol) , **SRTP**	16384-32767	Both	3550, 3711	Session	• VoIP protocol. • Delivers audio & video over IP networks.	• RTP flooding attack • RTP bleed
22	**SSL** (Secure Sockets Layer)	-	-	6101	Presentation	• Establishes encrypted communication b/w client & server. • Created by Netscape.	• BEAST • SSL Renegotiation
23	**TLS** (Transport Layer Security)	-	-	2246	Presentation	• Establishes encrypted communication b/w client & server. • Created by IETF.	• DROWN • ROBOT • POODLE • Heartbleed
24	**Kerberos**	88	Both	1964	Presentation	• Provides security & authentication. • Uses symmetric key distribution using symmetric encryption to access file server. • Helps nodes to prove their identity to one another.	• DoS • Arbitrary code execution. • Buffer Overflow.
25	**WPA** (Wi-Fi Protected Access)	-	-	-	Presentation	• Security standard that provides better encryption & authentication than WPA.	• KRACK
26	**MIME** (Multipurpose Internet Mail Extensions)	-	-	1521, 1522	Presentation	• Supports text in multiple character sets; as well as attachments of audio, video, apps & images.	• XSS using MIME Sniffing
27	**ECHO**	7	Both	862	Application	• Used for testing & measurement of round trip timings in IP networks. • Server sends back identical copy of the data it received.	• Can perform DoS
28	**DHCP** (Dynamic Host Configuration Protocol)	67	UDP	2131, 3315	Application	• A network management protocol used to automate the process of configuring devices on IP networks.	• Remote code execution • Bogus DHCP client & server
29	**BOOTP** (Bootstrap Protocol)	67,68	Both	951	Application	• Older version of DHCP. • Automatically assigns IP address to network devices from a configuration server.	• BootpD • BOOTP server impersonation
30	**HTTP** (Hyper Text Transfer Protocol)	80	Both	1945	Application	• Used for communication over World Wide Web.	• MitM attack
31	**HTTPS** (Hyper Text Transfer Protocol Secure)	443	Both	-	Application	• HTTPS with SSL for security.	• SSL Stripping • DROWN attack
32	**FTP** (File Transfer Protocol)	20,21	Both	959, 2228	Application	• File transfer • Uses TCP, hence file delivery is guaranteed.	• Brute force attack • Packet capture • Anonymous authentication • Directory traversal attack

33	**FTPS** (FTP with SSL)	989,990	Both	4217	Application	• Uses command channel & opens new connections for data transfer. • Requires a certificate.	• MitM
34	**SFTP** (SSH File Transfer Protocol)	22	Both	913	Application	• Uses encrypted credentials to authenticate. • SSH keys can also be used to authenticate.	• Brute force attack
35	**POP3** (Post Office Protocol)	110,995	Both	937, 1939	Application	• Store-and-forward client/server protocol. • Deletes mail on server as soon as user has downloaded it.	• Buffer overflow in POP3 servers can cause DoS.
36	**SSH** (Secure Shell)	22	Both	4251	Application	• Cryptographic network protocol for operating network services securely over an unsecured network.	• Static SSH keys • Embedded SSH keys can provide backdoor.
37	**Telnet** (TELecommunication NETwork)	23	Both	15, 854, 855	Application	• Allows to connect to remote computers over a TCP/IP network.	• Brute force attack • Stealing credentials by sniffing. • SSH and SMTP banner grabbing.
38	**NTP** (Network Time Protocol)	123	Both	1059, 1119, 1305	Application	• Synchronizes clock among devices.	• NTP Amplification DDoS attack.
39	**IMAP/S** (Internet Message Access Protocol)	143; 993	Both	1176, 1730	Application	• Allows user to create folders & assign messages to folders. • User can obtain just the message header (useful in low-bandwidth connection).	• Password spraying attacks.
40	**DNS** (Domain Name System)	53	Both	1034, 1035	Application	• Resolute names in TCP/IP network.	• Typosquatting • DNS Poisoning.
41	**SOAP** (Simple Object Access Protocol)	80	Both	-	Application	• XML based messaging protocol to exchange info. • Characteristics: extensibility, neutrality & independence.	• SOAP injection • Unauthenticated romote access
42	**SNMP/S** (Simple Network Management Protocol)	161; 162	Both	1157, 1441, 2570	Application	• Allows network manager to monitor networking equipment & remotely modify settings & configuration.	• Sniffing of plain text password. • Modification of packet header.
43	**SMTP/S** (Simple Mail Transfer Protocol)	25; 465	Both; TCP	5321	Application	• Transfers mail from sender's mail server to recipient's mail server.	• Account enumeration. • E-mail header disclosures. • Helps find internal IPs.
44	**SNTP** (Simple Network Time Protocol)	123		2030, 4330	Application	• Used when full implementation of NTP is not needed. • Synchronizes a computer's system time with a server that has already been	• DoS via a crafted NTP packet.

						synchronized by a source such as a radio, satellite receiver or modem. • Supports unicast, multicast and anycast operating modes.	
45	**RFB** (Remote Frame Buffer)	5900	Both	6143	Application	• Used by VNC (Virtual N/W computing) [only TCP port used] • Graphical desktop sharing system. • Used in technical support.	• Stack buffer overflow. • Information disclosure.
46	**RDP** (Remote Desktop Protocol)	3389	Both	-	Application	• Provides GUI to connect to another computer.	• Reverse RDP attack. • Sabotage sandboxes.
47	**TFTP** (Trivial File Transfer Protocol)	69	Both	1350	Application	• A lockstep FTP. • Allows a client to get a file from or put a file onto a remote host. • Simpler than FTP.	• No encryption & authentication. • TFTP server spoofing.
48	**NFS** (Network File System)	2049	Both	3530	Application	• Allows a user to access files over a computer network much like local storage is accessed.	• Elevation of privilege. • Arbitrary code execution.
49	**SIP/S** (Session Initiation Protocol)	5060; 5061	Both; TCP	3261	Application	• Used for initiating, maintaining & terminating real-time sessions. • VoIP protocol.	• Registration hijacking. • Message tampering.
50	**LDAP/S** (Lightweight Directory Access Protocol)	389; 636	Both	1777, 2253	Application	• An open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an IP network.	• LDAP injection • DoS • NULL Base querying

REFERENCES

[1] https://www.cvedetails.com/
[2] https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
[3] https://www.rfc-editor.org/
[4] https://resources.infosecinstitute.com/nat-pmp-vulnerability/#gref
[5] https://cve.mitre.org/
[6] https://www.f5.com/services/resources/white-papers/the-myth-of-network-address-translation-as-security
[7] https://www.infoworld.com/article/2942749/obsolete-internet-protocol-once-again-becomes-an-attack-vector.html
[8] https://www.geeksforgeeks.org/ip-security-ipsec/
[9] https://www.sciencedaily.com/releases/2018/08/180814134201.htm
[10] http://www.cis.syr.edu/~wedu/seed/Book/book_sample_tcp.pdf
[11] https://en.wikipedia.org/wiki/UDP_flood_attack
[12] https://www.techrepublic.com/blog/it-security/the-problem-with-netbios/
[13] https://www.netsparker.com/blog/web-security/xml-rpc-protocol-ip-disclosure-attacks/
[14] https://www.synopsys.com/blogs/software-security/attacks-on-tls-vulnerabilities/
[15] http://riseandhack.blogspot.com/2015/02/xml-injection-soap-injection-notes.html
[16] https://nvd.nist.gov/vuln/detail/CVE-2019-1660#vulnCurrentDescriptionTitle
[17] https://www.techopedia.com/definition/4539/simple-network-time-protocol-sntp
[18] https://beyondsecurity.com/scan-pentest-network-vulnerabilities-ldap-null-directory-bases.html?cn-reloaded=1