COMMON INSECURE SERVICES, PORTS, & PROTOCOLS

PCI DSS Requirement 1.1.6 v3.2.1: "Documentation of business justification and approval for use of all services, protocols, and ports allowed, **including documentation of security features implemented for those protocols considered to the insecure.**"

PCI DSS Requirement 1.2.6 v4.0: "**Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.**"

This cheat sheet is designed to help you identify the common insecure ports and protocols and the services that run on them. If your organization uses insecure services, you must have security features defined and implemented. This is not an exhaustive list of every insecure service, port, & protocol.

INSECURE SERVICE	PROTOCOL	PORT
TELNET Telnet is an unencrypted protocol that transmits login credentials in plain text, making it easy for attackers to intercept and steal this information. **To secure telnet, use SSH instead, which provides encrypted communication and secure remote access.**	TCP	23
FTP: FTP transmits data in clear text, making it vulnerable to interception and tampering. **To secure FTP, use FTPS or SFTP, which encrypts the data in transit.**	TCP	21
HTTP HTTP is an unencrypted protocol used for web browsing and web server communication. **To secure HTTP use HTTPS, which provides encryption and integrity protection.**	TCP	80
SNMP Simple Network Management Protocol (SNMP) is used for network management and monitoring. SNMPv1 and SNMPv2c use plain text passwords, which can be easily intercepted. **To secure SNMP, use SNMPv3, which provides authentication and encryption.**	UDP	161

COMMON INSECURE SERVICES, PORTS, & PROTOCOLS

PCI DSS Requirement 1.1.6 v3.2.1: "Documentation of business justification and approval for use of all services, protocols, and ports allowed, **including documentation of security features implemented for those protocols considered to the insecure.**"

PCI DSS Requirement 1.2.6 v4.0: "**Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.**"

This cheat sheet is designed to help you identify the common insecure ports and protocols and the services that run on them. If your organization uses insecure services, you must have security features defined and implemented. This is not an exhaustive list of every insecure service, port, & protocol.

INSECURE SERVICE	PROTOCOL	PORT
SMB: Server Message Block (SMB) is used for file and printer sharing in Windows environments. SMBv1 and SMBv2 are vulnerable to exploitation and attacks, so it's recommended to disable these versions and **use SMBv3, which provides encryption and improved security features.**	TCP	445
RDP: RDP is a protocol used for remote desktop access to Windows systems. To secure RDP, **use Remote Desktop Gateway (RDG), which provides encrypted communication and access control features.**	TCP	3398
DNS: Domain Name System (DNS) is used for translating domain names into IP addresses. DNS traffic can be manipulated by attackers, leading to DNS spoofing and other attacks. **To secure DNS, use DNSSEC, which provides cryptographic authentication of DNS data.**	UDP	53