






FINAL PROJECT EPICODE W12 D4

TECHNICAL REPORT FROM NESSUS WITH

This document gives a technical analysis of all the vulnerabilities found during an automatic advanced scan with a vulnerability assessment tool (Nessus). The vulnerabilities have been listed in order of severity and they have been sorted in a table containing: severity level, title, protocol, CVSS score, a brief description and the number of times the same vulnerability has been found by Nessus.

N° VULNERABILITIES DISCOVERED :

-  CRITICAL : 56 (CVSS 9.0 – 10.0)
-  HIGH : 4 (CVSS 7.0 – 8.9)
-  MEDIUM : 25 (CVSS 4.0 – 6.9)
-  LOW : 8 (CVSS 0.1 – 3.9)
-  INFO : 127 (CVSS 0.1 – 3.9)

[Summary list of all vulnerabilities](#)

Gravity	Vulnerability	Service	Protocol	CVSS	Port	Description	N° rep.
CRITICAL	Apache Log4Shell CVE-2021-45046 Bypass Remote Code Execution	RPC	TCP	10.0	111(RPC BIND)	Remote code execution vulnerability exists in Apache Log4j < 2.16.0 due to insufficient protections on message lookup substitutions when dealing with user controlled input	1
CRITICAL	Apache Log4Shell RCE detection via Path Enumeration	Apache HTTP Server	TCP	10.0	80(HTTP)	Log4j RCE vulnerability detected via HTTP path enumeration. Server may log crafted URLs, allowing remote code execution through JNDI injection.	1

CRITICAL	Apache Log4Shell RCE detection via Raw Socket Logging	Apache HTTP Server	TCP	10.0	80 (HTTP)	A remote, unauthenticated attacker can exploit this, via a web request to execute arbitrary code with the permission level of the running Java process.	25
CRITICAL	Apache Log4Shell RCE detection via callback correlation (Direct Check DNS)	Apache HTTP Server	TCP	10.0	80 (HTTP)	Log4j RCE detected via DNS callback from HTTP requests. Indicates vulnerable backend logging behavior.	1
CRITICAL	Apache Log4Shell RCE detection via callback correlation (Direct Check FTP)	FTP (vsFTPD)	TCP	10.0	21	Log4j RCE triggered via FTP input. DNS callback confirms vulnerable backend logging.	1
CRITICAL	Apache Log4Shell RCE detection via callback correlation (Direct Check HTTP)	Apache HTTP Server(TCP)	TCP	10.0	80 (HTTP)	Log4j RCE triggered via HTTP request. DNS callback confirms backend vulnerability.	1
CRITICAL	Apache Log4Shell RCE detection via callback correlation (Direct Check MSRPC)	MSRPC	TCP	10.0	135	Log4Shell RCE attempt detected by correlating callback on MSRPC traffic. Confirms backend vulnerability through direct callback monitoring.	1
CRITICAL	Apache Log4Shell RCE detection via callback correlation (Direct Check NetBIOS)	NetBIOS	TCP	10.0	139	By sending a special NetBIOS query, the server could potentially be affected remote code execution vulnerability.	1

CRITICAL	Apache Log4Shell RCE detection via callback correlation (Direct Check RPCBIND)	RPCBIND	TCP / UDP	10.0	111(RPC BIND)	The version of Apache Log4j used on the remote server is affected by a remote code execution vulnerability.	3
CRITICAL	Apache Log4Shell RCE detection via callback correlation (Direct Check SMB)	SMB	TCP	10.0	445	Log4Shell RCE attempt detected by correlating callback on SMB traffic. Confirms backend vulnerability through direct callback monitoring.	1
CRITICAL	Apache Log4Shell RCE detection via callback correlation (Direct Check SMTP)	SMTP	TCP	10.0	25	Remote Code Execution vulnerability in Apache Log4j exploited via crafted input causing malicious callbacks over SSH service, enabling attacker to execute arbitrary code on the server.	1
CRITICAL	Apache Log4Shell RCE detection via callback correlation (Direct Check SSH)	SSH	TCP	10.0	22	The remote host appears to be running SSH. SSH itself is not vulnerable to Log4Shell; however, the SSH server could potentially be affected if it attempts to log data via a vulnerable log4j library.	1
CRITICAL	Apache Log4Shell RCE detection via callback correlation (Direct Check Telnet)	Telnet	TCP	10.0	23	Remote Code Execution vulnerability in Apache Log4j exploited via crafted input transmitted over Telnet, triggering outbound callbacks and allowing arbitrary code execution on vulnerable systems.	1
CRITICAL	Apache Tomcat AJP Connector Request Injection (Ghostcat)	AJP (Apache JServ protocol)	TCP	10.0	8009	Request injection vulnerability in Apache Tomcat AJP connector (CVE-2020-1938) allows attackers to read or include arbitrary files from the server (Ghostcat flaw).	1

CRITICAL	Bind Shell Backdoor Detection	Bind Shell Backdoor Detection	TCP	10.0	Variable (common 4444, 5555, etc..)	A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.	1
CRITICAL	Canonical Ubuntu Linux SEoL (8.04.x)	Canonical Ubuntu Linux SEoL (8.04.x)	TCP	10.0	Depends on what type of active service	Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.	1
CRITICAL	Debian OpenSSH/ OpenSSL Package Random Number Generator Weakness	SSH	TCP	10.0	22	Cryptographic weakness in Debian-based OpenSSL package (2006–2008) causes predictable SSH keys, allowing attackers to brute-force authentication.	1
CRITICAL	Debian OpenSSH/ OpenSSL Package Random Number Generator Weakness (SSL check)	SSL/TLS	TCP	10.0	443	Vulnerable Debian OpenSSL package generates predictable SSL keys, exposing HTTPS services to key recovery and man-in-the-middle attacks.	1
CRITICAL	SSL Version 2 and 3 Protocol Detection	SSL/TLS	TCP	10.0	443(SSL PORTS)	The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: Attacks like POODLE, should be disabled. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.	1
CRITICAL	VNC Server 'password' Password	VNC	TCP	10.0	5900	VNC server is accessible using the weak default password "password," allowing unauthorized remote desktop access and potential system compromise.	1
HIGH	ISC BIND Service Downgrade / Reflected DoS	DNS	UDP / TCP	7.0	53	Instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities.	1
HIGH	NFS Shares World Readable	NFS	UDP / TCP	7.6	2049	The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).	1

HIGH	NodeJS System Information Library Command Injection (CVE-2021-21315)	HTTP	TCP	7.5	80 /443	The remote host contains a web application framework library that is affected by a command injection vulnerability.	1
HIGH	SSL Medium Strength Cipher Suites Supported (SWEET32)	HTTPS/ SSL Service	TCP	7.5	443(SSL PORTS)	The remote service supports the use of medium strength SSL ciphers. Allows attackers to recover sensitive data from long-lived SSL sessions using 64-bit block ciphers vulnerable to SWEET32 birthday attacks.	1
MEDIUM	Samba Badlock Vulnerability	Samba (SMB/ CIFS)	TCP	5.9	53	Man-in-the-middle attackers can downgrade authentication protocols in Samba, allowing impersonation of users and unauthorized access to sensitive data.	1
MEDIUM	DNS Server Cache Snooping Remote Information Disclosure	DNS	UDP	5.0	53	The remote DNS server is vulnerable to cache snooping attacks. This can reveal internal systems' activity or monitored communications, potentially aiding further targeted attacks.	1
MEDIUM	DNS Server Zone Transfer Information Disclosure (AXFR)	TCP	TCP	5.0	53	The remote name server allows DNS zone transfers to be performed. A zone transfer lets a remote attacker instantly populate a list of potential targets.	1
MEDIUM	HTTP TRACE / TRACK Methods Allowed	HTTP / HTTPS	TCP	4.3	80/443	The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. TRACE or TRACK methods enabled on the web server can expose session data via Cross-Site Tracing (XST) attacks.	1
MEDIUM	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS	DNS (BIND)	TCP	5.0	53	Due to an assertion failure when attempting to verify a truncated response to a TSIG-signed request. An authenticated, remote attacker can exploit this issue by sending a truncated response to a TSIG-signed request to trigger an assertion failure, causing the server to exit.	1

MEDIUM	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	DNS	TCP	5.0	53	The remote DNS resolver does not use random ports when making queries to third-party DNS servers. An unauthenticated, remote attacker can exploit this to poison the remote DNS server, allowing the attacker to divert legitimate traffic to arbitrary sites.	1
MEDIUM	SMB Signing not required	SMB- TCP	TCP	5.0	445	Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.	1
MEDIUM	SMTP Service STARTTLS Plaintext Command Injection	SMTP	TCP	6.4	25	The remote SMTP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase.	1
MEDIUM	SSH Weak Algorithms Supported	SSH	TCP	5.0	22	The SSH server supports weak cryptographic algorithms, making encrypted sessions vulnerable to cryptanalysis and potential interception by attackers.	1
MEDIUM	SSL Anonymous Cipher Suites Supported	SSL/TLS	TCP	5.0	443(SSL PORTS)	The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.	1
MEDIUM	SSL Certificate Cannot Be Trusted	SSL/TLS	TCP	5.0	443(SSL PORTS)	If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.	1
MEDIUM	SSL Certificate Expiry	SSL/TLS	TCP	4.3	443(SSL PORTS)	The SSL certificate has expired, potentially causing trust issues and exposing users to man-in-the-middle attacks due to invalid certificate validation.	1
MEDIUM	SSL Certificate with Wrong Hostname	SSL/TLS	TCP	4.3	443(SSL PORTS)	The SSL certificate's hostname does not match the server's actual hostname, potentially enabling man-in-the-middle attacks due to trust misconfiguration.	1

MEDIUM	SSL DROWN Attack Vulnerability	SSL/TLS	TCP	4.3	443(SSL PORTS)	The remote host may be affected by a vulnerability that allows a remote attacker to potentially decrypt captured TLS traffic.	1
MEDIUM	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	SSL/TLS	TCP	4.3	443(SSL PORTS)	The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.	1
MEDIUM	SSL Self-Signed Certificate	SSL/TLS	TCP	4.3	443(SSL PORTS)	If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.	1
MEDIUM	SSL Weak Cipher Suites Supported	SSL/TLS	TCP	4.3	443(SSL PORTS)	The remote host supports the use of SSL ciphers that offer weak encryption.	1
MEDIUM	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	SSL/TLS	TCP	5.0	443(SSL PORTS)	The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time. A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g.CVE-2015-0204).	1
MEDIUM	TLS Version 1.0 Protocol Detection	SSL/TLS	TCP	5.0	443(SSL PORTS)	The server supports the outdated TLS 1.0 protocol, which contains multiple known vulnerabilities that weaken encryption and expose communications to potential interception and downgrade attacks.	1
LOW	ICMP Timestamp Request Remote Date Disclosure	ICMP	ICMP	2.1	N/A (ICMP protocol)	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date and time that are set on the targeted machine.	1
LOW	SSH Server CBC Mode Ciphers Enabled	SSH	TCP	2.1	22	The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.	1
LOW	SSH Weak Key Exchange Algorithms Enabled	SSH	TCP	2.1	22	The SSH server supports weak key exchange algorithms that are vulnerable to cryptographic attacks, potentially allowing attackers to compromise the confidentiality of the SSH session.	1

LOW	SSH Weak MAC Algorithms Enabled	SSH	TCP	2.1	22	The SSH server supports weak Message Authentication Code (MAC) algorithms, which could allow attackers to tamper with or forge data transmitted during the SSH session.	1
LOW	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported	SSL/TLS	TCP	2.1	443(SSL PORTS)	The remote host supports EXPORT DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.	1
LOW	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability	SSL/TLS	TCP	2.1	443(SSL PORTS)	The server's support for SSLv3 allows an attacker to exploit padding oracle attacks on downgraded legacy encryption, potentially decrypting sensitive data from encrypted sessions.	1
LOW	X Server Detection	X11 Server	TCP	2.1	6000 (Default x11 port)	X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client, may expose graphical display information and could allow unauthorized access if improperly secured.	1
INFO	Apache Banner Linux Distribution Disclosure	Apache HTTP Server	TCP	0	80 (Others relevant)	Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.	1
INFO	Apache HTTP Server Version	Apache HTTP Server	TCP	0	80	The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.	1
INFO	Backported Security Patch Detection (PHP)	PHP	N/A	0	N/A	Detection of backported security patches applied to PHP, indicating maintained security updates.	1
INFO	Backported Security Patch Detection (SSH)	SSH	N/A	0	N/A	Detection of backported security patches applied to SSH service, ensuring updated security fixes.	1
INFO	Backported Security Patch Detection (WWW)	Web Server	N/A	0	N/A	Detection of backported security patches applied to web services, indicating active maintenance.	1

INFO	Common Platform Enumeration (CPE)	DNS (BIND)	UDP	0	53	By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.	1
INFO	DNS Server BIND version Directive Remote Version Detection	DNS (BIND)	UDP	0	53	The remote host is running BIND or another DNS server that reports its version number when it receives a special request for the text 'version.bind' in the domain 'chaos'.	1
INFO	DNS Server Detection	DNS (BIND)	UDP	0	53	The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.	3
INFO	DNS Server hostname.bind Map Hostname Disclosure	DNS (BIND)	UDP	0	53	It is possible to learn the remote host name by querying the remote DNS server for 'hostname.bind' in the CHAOS domain.	1
INFO	Deprecated SSLv2 Connection Attempts	SSL/TLS	TCP	0	443(SSL PORTS)	This plugin enumerates and reports any SSLv2 connections which were attempted as part of a scan. This protocol has been deemed prohibited since 2011 because of security vulnerabilities.	1
INFO	Device Type	Network Device	N/A	0	N/A	Based on the remote operating system, it is possible to determine what the remote system type is (eg: aprinter, router, general-purpose computer, etc).	1
INFO	Ethernet MAC Addresses	Network Interface	N/A	0	N/A	This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig)	1
INFO	FTP Server Detection	FTP Server	TCP	0	21	It is possible to obtain the banner of the remote FTP server by connecting to a remote port.	1
INFO	HTTP Server Type and Version	HTTP Server	TCP	0	80 (Others relevant)	This plugin attempts to determine the type and the version of the remote web server.	1
INFO	HyperText Transfer Protocol (HTTP) Information	HTTP	TCP	0	80 (Others relevant)	This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...	1

INFO	IRC Daemon Version Detection	IRC Daemon	TCP	0	6667(standard IRC)	This plugin determines the version of the IRC daemon.	1
INFO	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure	Microsoft Windows SMB	TCP	0	139/445	It was possible to obtain the browse list of the remote Windows system by sending a request to the LANMAN pipe.	1
INFO	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	Microsoft Windows SMB	TCP	0	139/445	Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445.	1
INFO	Microsoft Windows SMB Service Detection	Microsoft Windows SMB	TCP	0	139/445	The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.	2
INFO	Microsoft Windows SMB Versions Supported (remote check)	Microsoft Windows SMB	TCP	0	139/445	It was possible to obtain information about the version of SMB running on the remote host.	2
INFO	NFS Share Export List	NFS	TCP / UDP	0	2049	The remote NFS server exports a list of shares.	1
INFO	Nessus Scan Information	Nessus	N/A	0	N/A	This plugin displays information about the Nessus scan	1
INFO	Nessus TCP scanner	Nessus TCP scanner	N/A	0	Variable	It is possible to determine which TCP ports are open.	25
INFO	OS Fingerprints Detected	Operating System	N/A	0	N/A	Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system.	1
INFO	OS Identification	Operating System	N/A	0	N/A	Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use.	1

INFO	OS Security Patch Assessment Not Available	Operating System	N/A	0	N/A	OS Security Patch Assessment is not available on the remote host. This does not necessarily indicate a problem with the scan.	1
INFO	OpenSSH Detection	OpenSSH	TCP	0	22	An OpenSSH-based SSH server was detected on the remote host.	2
INFO	PHP Version Detection	PHP	TCP	0	80,443	Nessus was able to determine the version of PHP available on the remote web server.	1
INFO	Patch Report	Patch Management	N/A	0	N/A	The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.	1
INFO	PostgreSQL STARTTLS Support	PostgreSQL	TCP	0	5432 def. PostgreSQL	The remote PostgreSQL server supports the use of encryption initiated during pre-login to switch from a cleartext to an encrypted communications channel.	2
INFO	RMI Registry Detection	Java RMI Registry	TCP	0	1099	The remote host is running an RMI registry, which acts as a bootstrap naming service for registering and retrieving remote objects with simple names in the Java Remote Method Invocation (RMI) system.	1
INFO	RPC Services Enumeration	RPC Services Enumeration	TCP	0	Varies (commonly dynamic)	By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port.	9
INFO	RPC portmapper (TCP)	RPC Portmapper	TCP	0	111	The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.	2
INFO	SMTP Server Detection	SMTP Server	TCP	0	25	The remote host is running a mail (SMTP) server on this port. Since SMTP servers are the targets of spammers.	1
INFO	SMTP Service STARTTLS Command Support	SMTP Service STARTTLS Support	TCP	0	25	The remote SMTP service supports the use of the 'STARTTLS' command to switch from a cleartext to an encrypted communications channel.	1
INFO	SSH Algorithms and Languages Supported	SSH	TCP	0	22	This script detects which algorithms and languages are supported by the remote service for encrypting communications.	1

INFO	SSH Password Authentication Accepted	SSH	TCP	0	22	The SSH server on the remote host accepts password authentication, which might be a security risk if weak passwords are used.	1
INFO	SSH Protocol Versions Supported	SSH	TCP	0	22	This plugin determines the versions of the SSH protocol supported by the remote SSH daemon.	1
INFO	SSH SHA-1 HMAC Algorithms Enabled	SSH	TCP	0	22	SSH server enables SHA-1 based HMAC algorithms, which are considered weak and susceptible to cryptographic attacks.	1
INFO	SSH Server Type and Version Information	SSH	TCP	0	22	It is possible to obtain information about the remote SSH server by sending an empty authentication request.	1
INFO	SSL / TLS Versions Supported	SSL/TLS	TCP	0	443(SSL PORTS)	This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.	3
INFO	SSL Certificate 'commonName' Mismatch	SSL/TLS	TCP	0	443(SSL PORTS)	Mismatch between SSL certificate commonName and the host name may cause trust issues with clients.	1
INFO	SSL Certificate Information	SSL/TLS	TCP	0	443(SSL PORTS)	SSL certificate information disclosure including issuer, validity, and fingerprint.	2
INFO	SSL Cipher Block Chaining Cipher Suites Supported	SSL/TLS	TCP	0	443(SSL PORTS)	Support of CBC (Cipher Block Chaining) cipher suites in SSL/TLS which might be vulnerable to padding oracle attacks.	1
INFO	SSL Cipher Suites Supported	SSL/TLS	TCP	0	443(SSL PORTS)	List of all cipher suites supported by the server for SSL/TLS connections to assess strength and vulnerabilities	2
INFO	SSL Compression Methods Supported	SSL/TLS	TCP	0	443(SSL PORTS)	Detection of compression methods supported by SSL/TLS which could lead to CRIME attack vulnerabilities.	1
INFO	SSL Session Resume Supported	SSL/TLS	TCP	0	443(SSL PORTS)	This script detects whether a host allows resuming SSL sessions by performing a full SSL handshake to receive a session ID, and then reconnecting with the previously used session ID.	4

INFO	SSL/TLS Recommended Cipher Suites	SSL/TLS	TCP	0	443(SSL PORTS)	The remote host has open SSL/TLS ports which advertise discouraged cipher suites.	1
INFO	Samba Server Detection	SMB	TCP	0	445 (SMB ports)	Detection of Samba server indicating file and print services are running, which may be vulnerable if not properly configured.	2
INFO	Server Message Block (SMB) Protocol Version 1 Enabled (uncredential ed check)	SMB	TCP	0	445 (SMB ports)	Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions.SMBv1 is an outdated and insecure protocol version with multiple known vulnerabilities, exposing the server to risks like WannaCry attacks.	1
INFO	Service Detection	Service Detection	TCP	0	Various	General detection of running network services to identify available attack surfaces.	9
INFO	Service Detection (HELP Request)	Service Detection (HELP request)	TCP	0	Various	It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives a 'HELP' request.	1
INFO	TCP/IP Timestamps Supported	TCP/IP Timestamp	TCP	0	N/A	TCP/IP timestamp support allows remote attackers to infer system uptime and potentially assist in OS fingerprinting.	1
INFO	TFTP Daemon Detection	TFTP Daemon Detection	UDP	0	69	The remote host is running a TFTP (Trivial File Transfer Protocol) daemon. TFTP is often used by routers and diskless hosts to retrieve their configuration. It can also be used by worms to propagate.	1
INFO	Target Credential Status by Authentication Protocol - No Credentials Provided	System	Var.	0	N/A	Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.	1
INFO	Traceroute Information	ICMP/UDP/TCP	UDP / TCP	0	N/A	It was possible to obtain traceroute information.Traceroute data revealing network path and hop information which may assist attackers in network mapping.	1
INFO	Unknown Service Detection: Banner Retrieval	Unknown Service Detection : Banner Retrieval	TCP	0	Various	There is an unknown service running on the remote host. Retrieval of service banners to identify running applications and versions for vulnerability assessment.	1

INFO	VNC Server Unencrypted Communication Detection	VNC	TCP	0	5900	Detection of VNC servers transmitting data without encryption, exposing sessions to interception.	1
INFO	VNC Server Security Type Detection	VNC	TCP	0	5900	This script checks the remote VNC server protocol version and the available 'security types'.	1
INFO	VNC Software Detection	VNC	TCP	0	5900	The remote host is running VNC (Virtual Network Computing), which uses the RFB (Remote Framebuffer) protocol to provide remote access to graphical user interfaces and thus permits a console on the remote host to be displayed on another.	1
INFO	WMI Not Available	WMI Not Available	HTTP	0	N/A	Indicates WMI service is not accessible, limiting remote management and inventory capabilities.	1
INFO	WebDAV Detection	WebDAV Detection	HTTP	0	N/A	WebDAV is an industry standard extension to the HTTP specification. It adds a capability for authorized users to remotely add and manage the content of a web server.	1
INFO	Windows NetBIOS / SMB Remote Host Information Disclosure	Netbios/ SMB	TCP	0	137/445	The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB, requests can help attackers in fingerprinting and planning attacks.	1
INFO	vsftpd Detection	vsftpd Detection	TCP	0	21	The remote host is running vsftpd, an FTP server for UNIX-like systems written in C.	1

