Name of Individual Conducting Scanning:	Zuan
Nessus Scanner IP (IP of Kali VM):	10.0.2.5
Target Host IP	10.0.2.5
Date & Time Scan Started:	12/5/2024 at 2:00 am MYT
Date & Time Scan Finished:	12/5/2024 at 2:20 am MYT
Scan Details	Policy: Basic Network Scan Severity Base: CVSS v3.0
Security Issues Identified:	72 vulnerabilities found

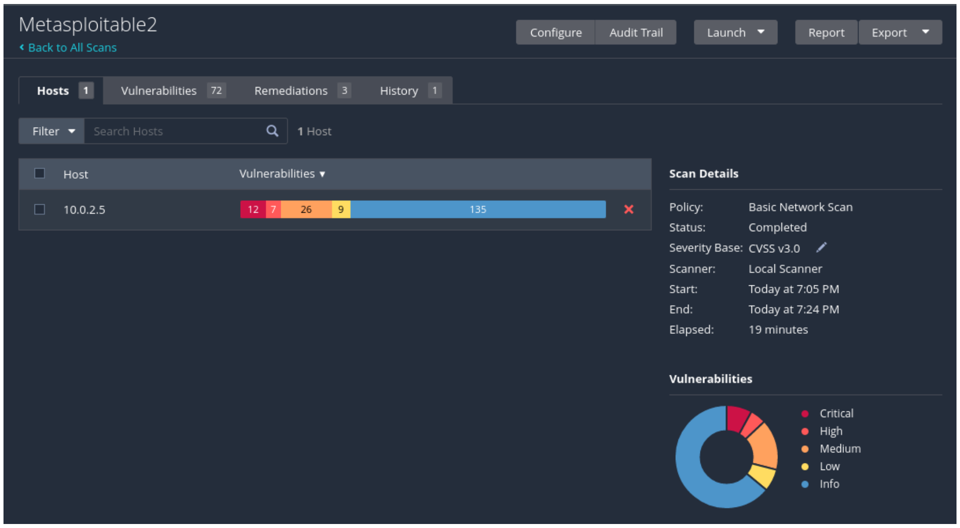
Instructions

1. Please refer to the Course Challenge Brief for instructions on what you are being asked to do.
2. Answer all questions mentioned below.

Overview

A vulnerability assessment was performed on May 12, 2024, using Nessus scanner on the 'Metasploitable 2' system with the IP address 10.0.2.5. The goal was to find vulnerabilities and gauge the system's overall security status. After a basic network scan, it uncovered 72 vulnerabilities of varying severity levels. Based on these results, the system's security level is assessed as critical, high, medium, low, and info.

Scan Results



☐	Host	Vulnerabilities ▾
☐	10.0.2.5	12 7 26 9 135 ✕

Scan Details

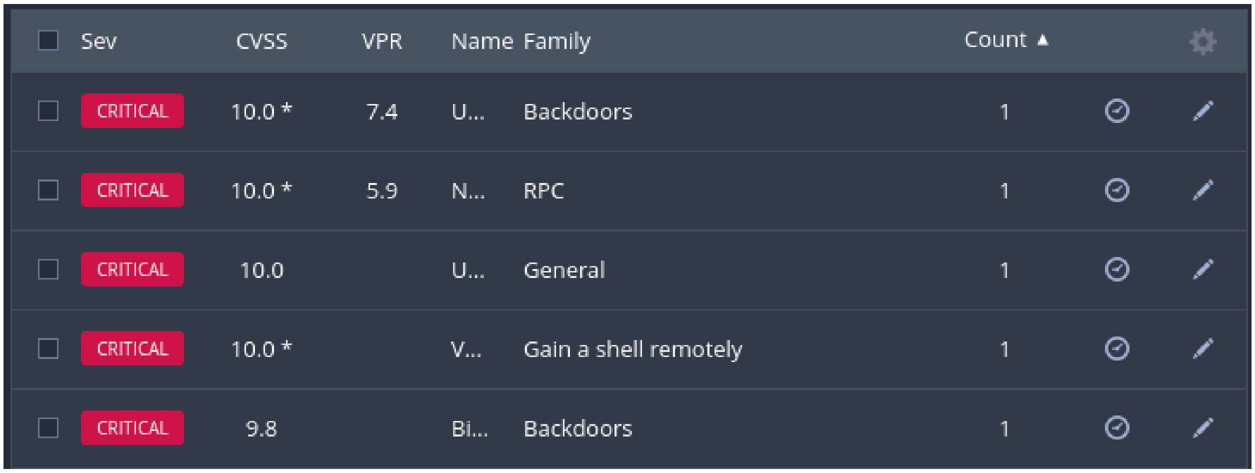
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:05 PM
End: Today at 7:24 PM
Elapsed: 19 minutes

The result of the scan is as follows:

- 12 (6.35 %) Critical Severity vulnerabilities were found
- 7 (3.70%) High Severity vulnerabilities were found
- 26 (13.76%) Medium Severity vulnerabilities were found
- 9 (4.76%) Low Severity vulnerabilities were found
- 135 (71.43%) Info findings about the system

The high number of Critical and High Severity vulnerabilities, comprising 10.05% of the total findings, indicates a significant level of vulnerability. Additionally, the presence of Medium and Low Severity vulnerabilities further contributes to the system's vulnerability. Therefore, based on the scan results, it can be concluded that the system is vulnerable.

Top 5 Most Serious Security Issues (In priority order - most important first):



□	Sev	CVSS	VPR	Name	Family	Count ▲		⚙
□	CRITICAL	10.0 *	7.4	U...	Backdoors	1	⊙	✎
□	CRITICAL	10.0 *	5.9	N...	RPC	1	⊙	✎
□	CRITICAL	10.0		U...	General	1	⊙	✎
□	CRITICAL	10.0 *		V...	Gain a shell remotely	1	⊙	✎
□	CRITICAL	9.8		Bi...	Backdoors	1	⊙	✎

The image above shows the top 5 most serious security issues which can be found at the vulnerability section. The 5 most serious security issues are as shown below:

1. **UnrealIRCd Backdoor Detection (CVS 10.0):** The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.
2. **NFS Exported Share Information Disclosure Security flaw (CVS 10.0):** At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.
3. **Unix Operating System Unsupported Version Detection Security flaw (CVS 10.0):** The Unix operating system on the remote host is reported to be using an outdated version that is no longer supported. This means the vendor no longer provides security patches or updates for it. As a result, the system is likely to have security vulnerabilities due to the absence of ongoing support and updates.
4. **VNC Server 'password' Password (CVS 10.0):** The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

5. **SSL Version 2 and 3 Protocol Detection (CVS 9.8):** The remote service on the system accepts connections that use outdated encryption protocols like SSL 2.0 and SSL 3.0. These versions have known cryptographic vulnerabilities, such as insecure padding schemes and flawed session renegotiation. Attackers can exploit these weaknesses to intercept communications via man-in-the-middle attacks or decrypt data.

Top 5 - Remediations (In priority order - most important first):

1. **UnrealIRCd Backdoor Detection (CVS 10.0):** Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.
2. **NFS Exported Share Information Disclosure Security flaw (CVS 10.0):** Configure NFS on the remote host so that only authorized hosts can mount its remote shares.
3. **Unix Operating System Unsupported Version Detection Security flaw (CVS 10.0):** Upgrade to a version of the Unix operating system that is currently supported.
4. **VNC Server 'password' Password (CVS 10.0):** Secure the VNC service with a strong password.
5. **SSL Version 2 and 3 Protocol Detection (CVS 9.8):** Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.