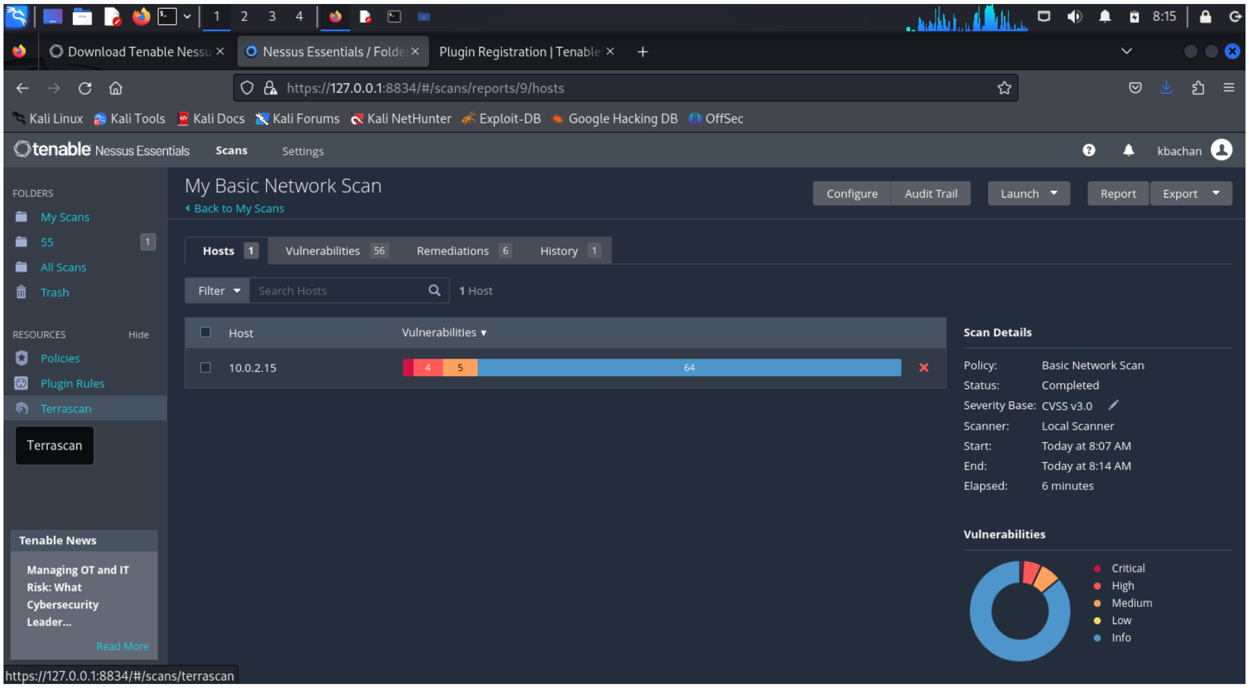
Introduction to Vulnerability Management - Course Challenge Report Template

Name of Individual Conducting Scanning:	Kbachan
Nessus Scanner IP (IP of Kali VM):	10.0.2.15
Date & Time Scan Started:	10/15/2024 8:07 am
Date & Time Scan Finished:	10/15/2024 8:14 am
Security Issues Identified:	56 Vulnerabilities Identified

The vulnerability scan concluded with 1 critical, 6 high, 7 medium vulnerabilities detected from the target host (10.0.2.15). Making the system highly vulnerable from attackers that might exploit the system. Severity score is determined using the Common Vulnerabilities Scoring System (CVSS) to measure the impact of a vulnerability on a system, and help in prioritization in remediation efforts. Urgent attention to address the critical and high severity vulnerabilities is highly recommended.



My Basic Network Scan

10.0.2.15

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 8:07 AM
End: Today at 8:14 AM
Elapsed: 6 minutes

Vulnerabilities

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

1. **UnrealIRCd Backdoor Detection** – The remote IRC server is a version of UnrealIRCd that has a backdoor that allows threat actors to execute arbitrary code on the host. A threat actor can exploit this vulnerability to compromise a system, allowing them to execute commands such as; running malware, modifying files, manipulate system configurations, and many more. The potential impact of this vulnerability can negatively affect an organization financially, bring

reputational damage, as well as legal repercussions and regulatory fines.

2. **NFS Exported Share Information Disclosure** –The scanning host can mount at least one of the NFS shares exported by the target host, making it possible for an attacker to access and modify files on the remote host. This vulnerability when exploited gives the attacker unauthorized access to files, making it possible to perform attacks such as; malware injection and data exfiltration.

3. **Unix Operating System Unsupported Version Detected** – The operating system that the target host is running is no longer supported, so it doesn't receive the latest security patches released by the vendor. As the threat landscape evolves daily, systems are required to be updated to mitigate the risks presented by these threats. This vulnerability presents an increased risk to exploitation, leading to unauthorized access to systems, data breaches, and system compromise.

4. **VNC Server 'password' Password** – The VNC server running on the target host is using a weak password, specifically the word "password". VNC or "Virtual Network Computing" is a screen sharing system created to gain remote access to another computer. By exploiting this vulnerability, a threat actor can take unauthorized control over a system.

5. **SSL Version 2 and 3 Protocol Detected** – Remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0, which are affected by cryptographic flaws. The vulnerabilities within these versions can be exploited by a threat actor to perform man-in-the-middle attacks or decrypt ongoing communications, negatively affecting the confidentiality and integrity of information.

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

1. UnrealIRCd Backdoor Detection – Reinstallation of the software is needed, the downloaded software must be verified using the published MD5 or SHA1 checksums from the official vendor.

2. NFS Exported Share Information Disclosure – Reconfiguration of NFS on the target host to only allow mounting of remote shares by authorized hosts or users.

3. Unix Operating System Unsupported Version Detected – Upgrade the target hosts operating system to version that is currently supported or up-to-date.

4. VNC Server 'password' Password - Employ a strong password that follows the organizations password policy to secure the VNC service.

5. SSL Version 2 and 3 Protocol Detected – Disable both SSL 2.0 and SSL 3.0. And use TLS 1.2 or higher instead.