

## Vulnerability Assessment Report: MS17-010 (EternalBlue) Analysis

The objective of this document shows the proficiency of utilizing Tenable Nessus for detecting the MS17-010 (EternalBlue) vulnerability in Windows 7 virtual environment, outlining threat identification abilities and CVSS metric evaluation for network risks.

### Tools Utilized:

**Tenable Nessus:** Configured and executed a Basic Network Scan to detect unpatched services and legacy vulnerabilities.

**Kali Linux:** Utilized as the primary scanning machine to interface with the Nessus web application and manage the assessment.

**Windows 7:** Served as the vulnerable target endpoint to demonstrate the MS17-010 (EternalBlue) exploit exposure.

**Proxmox VE:** Hosted the virtualized lab environment and internal network routing.

Kali Linux virtual machine, hosted in Proxmox hypervisor, shows completed Tenable Nessus vulnerability assessment results for the legacy Windows 7.

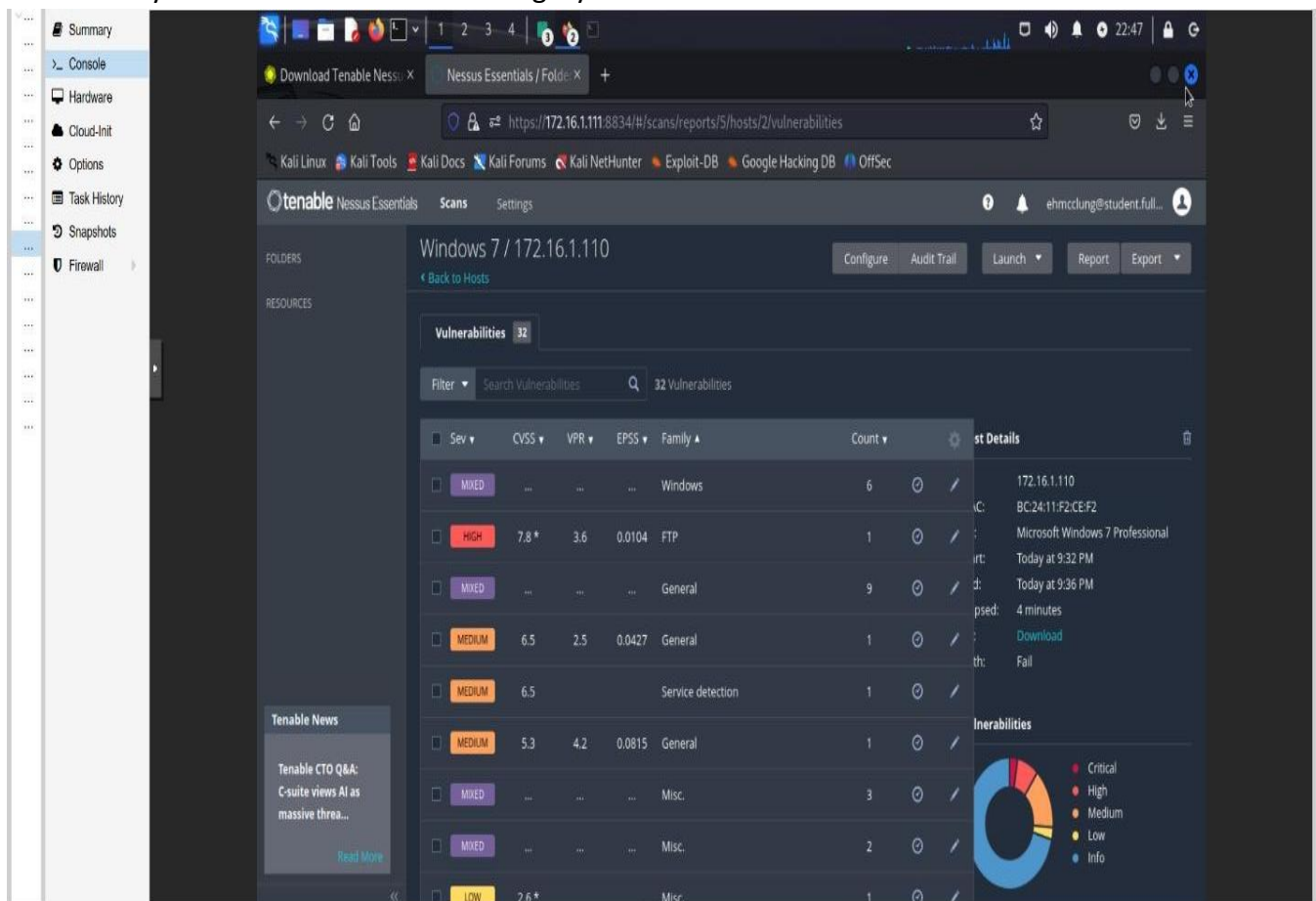
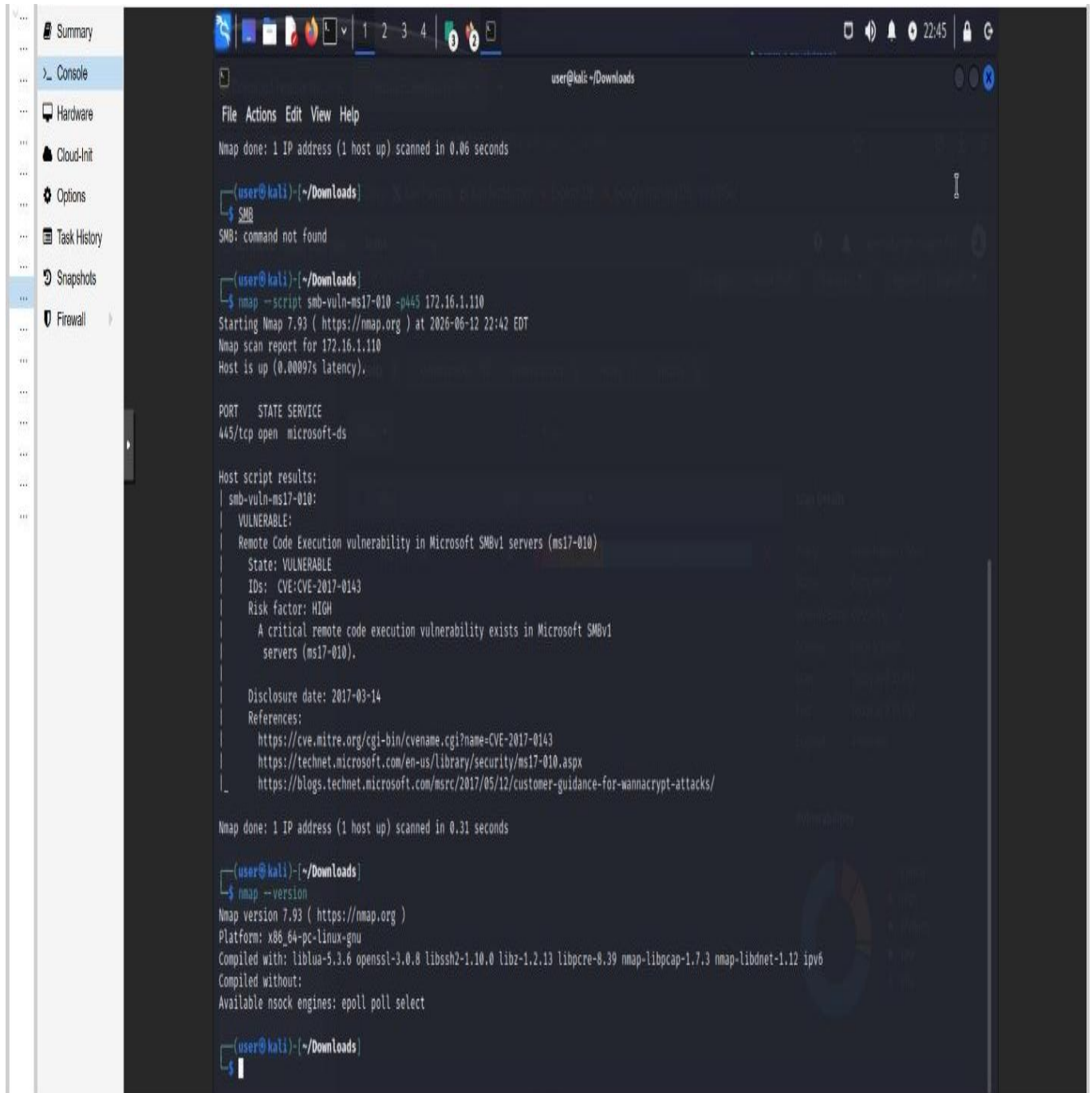


Figure 1 Full scan of Windows 7

## Vulnerability Assessment Report: MS17-010 (EternalBlue) Analysis

The initial scan shows critical exposure in the legacy Windows 7. The system is running an unpatched version of Microsoft Server Message Block 1.0 (SMBv1) service. Leaving the host vulnerable to MS17-010 remote code execution exploits.



The screenshot shows a terminal window with the following content:

```
user@kali:~/Downloads
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds

(user@kali)~/Downloads
$ smb
SMB: command not found

(user@kali)~/Downloads
$ nmap --script smb-vuln-ms17-010 -p445 172.16.1.110
Starting Nmap 7.93 ( https://nmap.org ) at 2026-06-12 22:42 EDT
Nmap scan report for 172.16.1.110
Host is up (0.00097s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
| VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE
| IDs: CVE:CVE-2017-0143
| Risk factor: HIGH
| A critical remote code execution vulnerability exists in Microsoft SMBv1
| servers (ms17-010).
|
| Disclosure date: 2017-03-14
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
| https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
| https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds

(user@kali)~/Downloads
$ nmap --version
Nmap version 7.93 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-3.0.8 libssh2-1.10.0 libz-1.2.13 libpcrc-8.39 nmap-libcap-1.7.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

Figure 2 Identifying and examining MS17-010

## Vulnerability Assessment Report: MS17-010 (EternalBlue) Analysis

A Basic Network Scan starts the assessment; the policy was configured inside the Tenable Nessus console. Parameters and scope of the scans were strictly defined to target the legacy endpoint. Configurations are ensuring the scanner will list open ports, map running services, and evaluate the host of missing patches.

### New Scan / Basic Network Scan

[← Back to Scan Templates](#)

Settings

Credentials

Plugins

BASIC

● General

Schedule

Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name  REQUIRED

Description

Folder

Targets 

Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com

The details of MS17-010 can be analyzed for the best evaluation to grasp the severity of the exposure. The scan output showed multiple Common Vulnerabilities and Exposures (CVEs), such as CVE-2017-0143 through CVE-2017-0148, that is associated with Shadow Broker exploit leaks. Confirming the setup is susceptible to unauthenticated, remote code execution via specially crafted packets.



Tenable Nessus vulnerability profile detailing the MS17-010 (EternalBlue) remote code execution flaw and associated CVEs.

#### CVSS v3.1 Base Metrics (CVE-2017-0144 / EternalBlue):

- **Attack Vector (AV):** Network
- **Attack Complexity (AC):** High
- **Privileges Required (PR):** None
- **User Interaction (UI):** None
- **Scope (S):** Unchanged
- **Confidentiality (C):** High
- **Integrity (I):** High
- **Availability (A):** High

As the MS17-010 vulnerability was spotted, critical risks to the network environments are seen due to potential for unauthenticated remote code execution. To mitigate the EternalBlue threat and secure the legacy infrastructure, these are recommended steps:

- Apply security Patches: have Microsoft official security updates for the MS17-010 to the needed Windows 7 host.
- Disable SMBv1: Disable the legacy Server Message Block version 1 (SMBv1) protocol across the network, as it is deprecated and inherently insecure.
- Network Segmentation & Firewall Rules: Ensure that network firewalls are set to block inbound traffic on TCP port 445 from external or untrusted networks.