

Department of Computer Science and Engineering

University of Dhaka

Dhaka-1000
Professional Masters in Information and Cyber Security

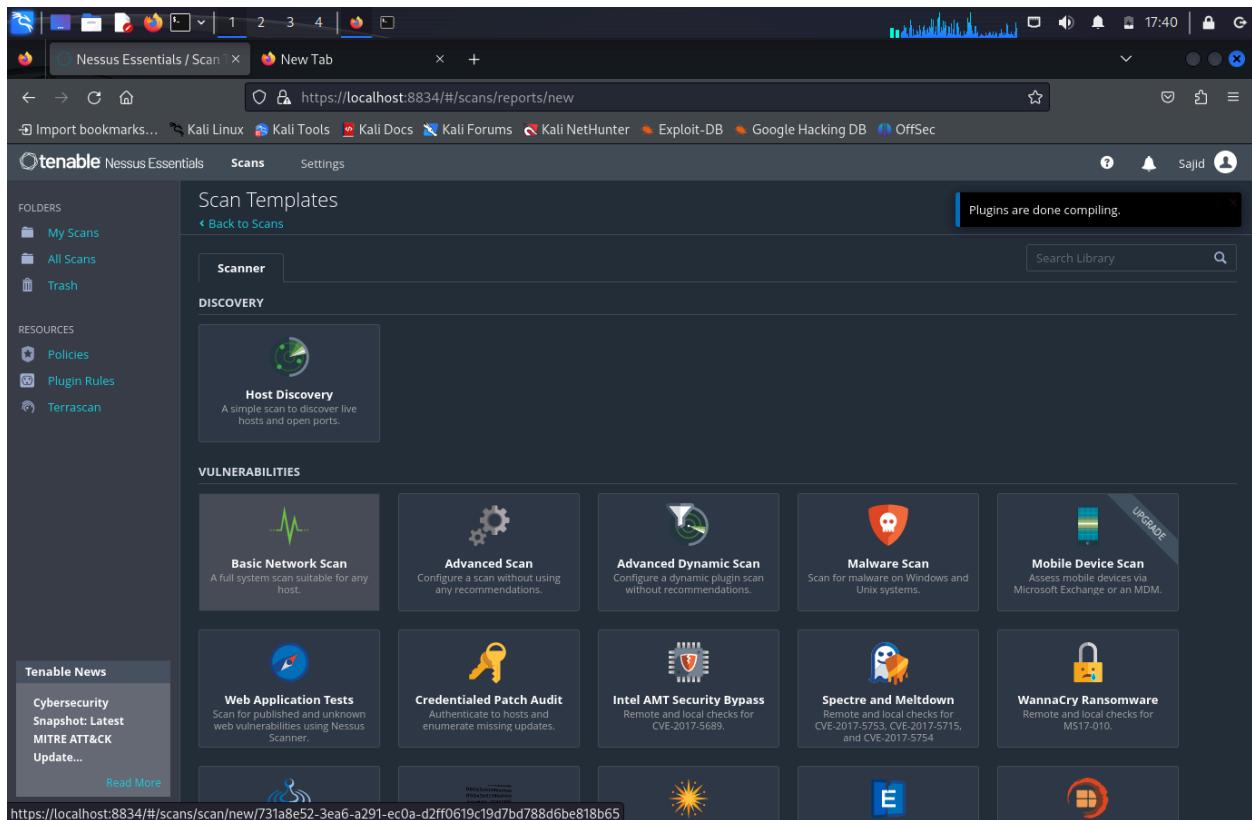
Subject: Information Infrastructure Protection

Name: Abu Syeed Sajid Ahmed

Role: 30023

Authenticated Scan:

- 1) We select 'Basic Network Scan' after selecting 'New Scan'.



2) We give Name and target ip in Settings.

The screenshot shows the Tenable Nessus Essentials interface. The top navigation bar includes tabs for 'Scans' and 'Settings'. The main content area is titled 'New Scan / Basic Network Scan' and contains a 'Back to Scan Templates' link. The 'Settings' tab is selected. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and a 'Tenable News' section. The main form has tabs for 'Settings', 'Credentials', and 'Plugins'. Under the 'Settings' tab, the 'BASIC' section is expanded, showing:

- Name:** Authenticated MSF Scan
- Description:** (empty)
- Folder:** My Scans
- Targets:** 10.0.2.6

Below the form are buttons for 'Upload Targets' and 'Add File'. At the bottom are 'Save' and 'Cancel' buttons.

3) In the credentials tab, we give the username and password of metasploitable2.

New Scan / Basic Network Scan

CATEGORIES Host

SSH

Windows

Authentication method: password

Username: msfadmin

Password (unsafe): XXXXXXXXXX

This password could be compromised if Nessus connects to a rogue SSH server. This can be mitigated by providing Nessus with a known_hosts file in the "Global Settings" section below.

Elevate privileges with: Nothing

Custom password prompt: password:

Targets to prioritize credentials:

Any hostnames or IPs or CIDR blocks (in a comma or space separated list in this field) that match a scanned system's hostname or IP will attempt to try this credential before other credentials

4) Then we launch the scan.

The screenshot shows the Tenable Nessus Essentials interface. On the left, there's a sidebar with 'Folders' containing 'My Scans' (with a warning icon), 'All Scans', and 'Trash'. Under 'Resources', there are 'Policies', 'Plugin Rules', and 'Terrascan'. A 'Tenable News' section is visible at the bottom left. The main area is titled 'Global Credential Settings' and contains the following fields:

- known_hosts file**: A 'Add File' button is shown. A note states: "Any hostnames or IPs or CRED blocks (in a comma or space separated list) in this field that match a scanned system's hostname or IP will attempt to try this credential before other credentials."
- Preferred port**: A text input field set to '22'. A note says: "This option can be set to direct Nessus to connect to SSH if it is running on a port other than 22."
- Client version**: A dropdown menu set to 'OpenSSH_5.0'. A note says: "Specifies which type of SSH client Nessus will impersonate while scanning."
- Attempt least privilege**: A checkbox is checked. A note says: "Enables or disables dynamic privilege escalation. When enabled, Nessus attempts to run the scan with an account with lesser privileges, even if the 'Elevate privileges with' option is enabled. If a command fails, Nessus will escalate privileges. Plugins 102095 and 102094 report which plugins ran with or without escalated privileges. Note: Enabling this option may increase scan run time by up to 30%."

At the bottom, there are 'Save' and 'Cancel' buttons, and a prominent 'Launch' button.

The screenshot shows the Tenable Nessus Essentials web application running in a Firefox browser. The URL is `https://localhost:8834/#/scans/Folders`. The interface has a dark theme.

Left Sidebar:

- FOLDERS: My Scans (selected), All Scans, Trash
- RESOURCES: Policies, Plugin Rules, Terrascan

Top Bar:

- Tabs: Nessus Essentials / Folders, New Tab
- Address bar: https://localhost:8834/#/scans/Folders
- Bookmarks: Import bookmarks..., Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec
- User: Sajid

Main Content Area:

My Scans

Search Scans: 2 Scans

Name	Schedule	Last Scanned
Unauthenticated MSF Scan	On Demand	Today at 5:43 PM
Authenticated MSF Scan	On Demand	Today at 5:43 PM

Bottom Left Sidebar:

Tenable News

Ivanti Avalanche
WLAvalancheService.exe Unauthenti...
[Read More](#)

Unauthenticated Scan:

- 1) We select 'Basic Network Scan' after selecting 'New Scan'.

The screenshot shows the Tenable Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and 'Tenable News' (Cybersecurity Snapshot: Latest, MITRE ATT&CK Update...). The main area is titled 'Scan Templates' with a 'Scanner' tab selected. It displays various scan types under 'DISCOVERY' and 'VULNERABILITIES'. Under 'DISCOVERY', there's a 'Host Discovery' card. Under 'VULNERABILITIES', there are ten cards: 'Basic Network Scan' (a full system scan suitable for any host), 'Advanced Scan' (a scan without recommendations), 'Advanced Dynamic Scan' (a dynamic plugin scan without recommendations), 'Malware Scan' (for malware on Windows and Unix systems), 'Mobile Device Scan' (an upgrade option for mobile devices via Microsoft Exchange or an MDM), 'Web Application Tests' (for published and unknown web vulnerabilities), 'Credentialled Patch Audit' (to authenticate hosts and enumerate missing updates), 'Intel AMT Security Bypass' (remote and local checks for CVE-2017-5689), 'Spectre and Meltdown' (remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754), and 'WannaCry Ransomware' (remote and local checks for MS17-010). A message at the top right says 'Plugins are done compiling.' The URL in the browser bar is https://localhost:8834/#/scans/reports/new.

2) We give Name and target ip in Settings.

The screenshot shows the Tenable Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and a 'Tenable News' section with a CVE-2024-4040 alert about a CrushFTP vulnerability. The main area is titled 'New Scan / Basic Network Scan' and has a 'Back to Scan Templates' link. It features three tabs: 'Settings' (selected), 'Credentials', and 'Plugins'. The 'Settings' tab is divided into sections: 'BASIC' (General, Schedule, Notifications), 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. Under 'BASIC', the 'Name' field is set to 'Unauthenticated MSF Scan', 'Folder' is set to 'My Scans', and 'Targets' is set to '10.0.2.6'. There are also 'Upload Targets' and 'Add File' buttons. At the bottom are 'Save' and 'Cancel' buttons. The top of the screen shows a browser header with tabs for 'Nessus Essentials / Scans' and 'New Tab', and a URL bar pointing to https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/. The status bar at the bottom right shows the time as 17:41.

3) Then we launch the scan.

The screenshot shows a Firefox browser window with the address bar displaying `https://localhost:8834/#/scans/folders`. The main content area is titled "My Scans" and lists one scan entry:

Name	Schedule	Last Scanned
Unauthenticated MSF Scan	On Demand	Today at 5:41 PM

The left sidebar includes sections for "FOLDERS" (My Scans, All Scans, Trash), "RESOURCES" (Policies, Plugin Rules, Terrascan), and "Tenable News". A news item titled "Operational Technology in the DoD: Ensuring a Secu..." is visible with a "Read More" link.