

Name: Hemant Jain

Lab Progress Report Due Date: 04/05/2021

Current Week Since Start Date: Week 11 (04/07/2021– 04/13/2021)

Reporting Week: From Mar 30, 2021 to Apr 05, 2021

Summary about the Test Out Module-11 Learning:

From the Test Out LabSim, I learnt about Security Assessments. The module initially started with the discussion on Penetration Testing: Types of Penetration Tests, Security Teams, Documentation/Contracts, Penetration Testing Life Cycle. The four different types of penetration test types discussed were White Box, Black Box, Gray box, Bug bounties. The security team's brief description and detailing out the Red Team, Blue Team, Purple Team, and White team. There were various documentation and contract types are discussed which outline the goals and guidelines of the tests and the scope of work and rules.

Documentation Types like Scope of work is a very detailed document that defines exactly what is going to be included in the penetration test and the Rules of Engagement document defines exactly how the penetration test will be carried out. Penetration Testing Life Cycle starts with Performing Reconnaissance, Scan/Enumerate, Gain Access, Maintain Access, Report.

In the Monitoring and reconnaissance lessons learnt how to perform the port and ping scans on the virtual machines. Performed Reconnaissance with Nmap and Harvester tool. Discussed some tools which are important to monitor the health of a network. Defining Reconnaissance also known as foot printing, is the process of gathering as much information about a target before beginning in any penetration test or security audit. Passive and Active Reconnaissance exists; with each one including some 4-5 methods to gather information on the target with no direct interaction with that target.

Continuing further learnt how to implement intrusion monitoring and intrusion prevention and using **squid** and **squert**. Read about the difference between IDSs and IPSs. Detection methods like Signature-based and Heuristic-based and the host-based and network-based device implementation of IDS/IPS. Performed lab on Scanning for Windows, Linux, Domain Controller, Security Appliance, Web Application Protection (WAP) vulnerabilities.

Threat hunting which is the human-based, proactive and methodical searching and monitoring of the network, includes three steps: Trigger, Investigation and Resolution.

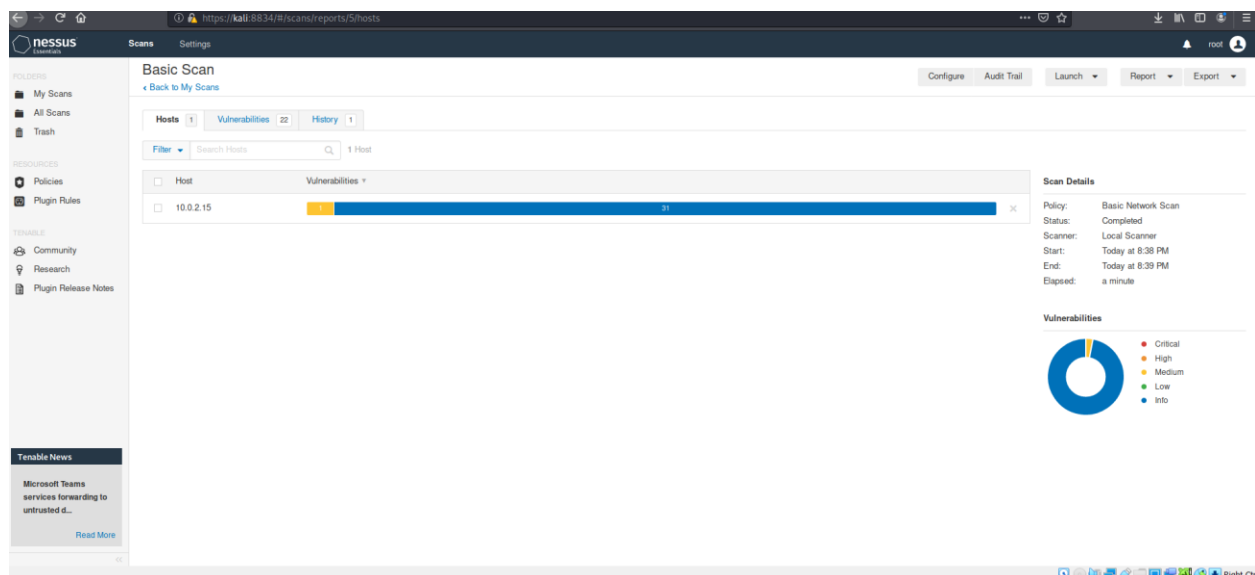
Read in detail about the Security Information and Event Management (SIEM) systems and Security Orchestration, Automation and Responses (SOAR) systems. Reading about how the protocol analyzers work and uses of protocol analyzers was one of my favorite topic to read in detail while going through the coursework. And in the end, learnt about the Poison ARP and analyses with Wireshark, Poison DNS, and Perform and analyze a SYN flood. Malicious Code Facts with Python, Command Shells, Macros.

Lab on cracking a password using rainbow tables and with John the Ripper was a repetitive task of our previous lab which already performed in our curriculum in past.

Class Labs Screenshots:

Nessus Tool Diagnosis Results:

Metasploitable Virtual Machine ---- 10.0.2.15 IP



The screenshot shows the Nessus web interface for an "Advanced Scan". The left sidebar contains navigation links for "My Scans", "All Scans", "Trash", "Policies", "Plugin Rules", "Community", "Research", and "Plugin Release Notes". The main content area displays the scan results for host 10.0.2.15. A table lists the host and its vulnerabilities, with a progress bar indicating the scan status. The "Scan Details" panel on the right shows the policy "Advanced Scan", status "Completed", scanner "Local Scanner", start time "Today at 8:40 PM", end time "Today at 8:41 PM", and elapsed time "a minute". A donut chart titled "Vulnerabilities" shows the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Host	Vulnerabilities
10.0.2.15	22

Scan Details

- Policy: Advanced Scan
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 8:40 PM
- End: Today at 8:41 PM
- Elapsed: a minute

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

The screenshot shows the Nessus web interface for "Web Application Tests". The left sidebar is the same as the previous screenshot. The main content area displays the scan results for web application tests. A table lists the tests, including the start time, last modified time, and status. The "Scan Details" panel on the right shows the policy "Web Application Tests", status "Completed", scanner "Local Scanner", start time "Today at 8:45 PM", end time "Today at 8:47 PM", and elapsed time "2 minutes". A donut chart titled "Vulnerabilities" shows the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Start Time	Last Modified	Status
Current	Today at 8:45 PM	Completed

Scan Details

- Policy: Web Application Tests
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 8:45 PM
- End: Today at 8:47 PM
- Elapsed: 2 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Kali Linux 2020 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Nessus Essentials / Folders / View Scan - Mozilla Firefox

Download Nessus | Tenable x | Nessus Essentials / Folders | root@kali: ~/Downloads | [Downloads - File Mana...]

08:56 PM 97%

https://kali:8834/#/scans/reports/14/history

Badlock Detection

Configure Audit Trail Launch Report Export

Back to My Scans

Hosts 1 Vulnerabilities 2 History 1

Search History 1 History

Start Time	Last Modified	Status
Completed Today at 8:55 PM	Today at 8:56 PM	Completed

Scan Details

Policy: Badlock Detection
Status: Completed
Scanner: Local Scanner
Start: Today at 8:55 PM
End: Today at 8:56 PM
Elapsed: a few seconds

Vulnerabilities

1 Critical
1 High
0 Medium
0 Low
0 Info

Tenable News

Secomex
GateManager Multiple
Vulnerabilities

Read More

Nessus Essentials / Folders / View Scan - Mozilla Firefox

Download Nessus | Tenable x | Nessus Essentials / Folders | root@kali: ~/Downloads | [Downloads - File Mana...]

08:58 PM 97%

https://kali:8834/#/scans/reports/17/history

Bash Shellshock Detection

Configure Audit Trail Launch Report Export

Back to My Scans

Hosts 1 Vulnerabilities 2 History 1

Search History 1 History

Start Time	Last Modified	Status
Completed Today at 8:57 PM	Today at 8:57 PM	Completed

Scan Details

Policy: Bash Shellshock Detection
Status: Completed
Scanner: Local Scanner
Start: Today at 8:57 PM
End: Today at 8:57 PM
Elapsed: a few seconds

Vulnerabilities

1 Critical
1 High
0 Medium
0 Low
0 Info

Tenable News

CVE-2021-32986: FS
Patches Several
Critical Vulner...

Read More

The screenshot displays the Nessus Essentials web interface. The left sidebar contains navigation links for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules), and TENABLE (Community, Research, Plugin Release Notes). The main content area is titled "DROWN Detection" and includes a "Back to My Scans" link. Below the title are tabs for Hosts (1), Vulnerabilities (2), and History (1). A search bar for history is present. A table lists scan results:

Start Time	Last Modified	Status
Completed Today at 8:59 PM	Today at 8:59 PM	Completed

Scan Details on the right:

- Policy: DROWN Detection
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 8:59 PM
- End: Today at 8:59 PM
- Elapsed: a few seconds

A "Vulnerabilities" section shows a donut chart with a legend: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). The chart is currently empty.

Tenable News at the bottom left mentions "Microsoft Teams services forwarding to untrusted..." with a "Read More" link.

The screenshot displays the Nessus Essentials web interface for a scan titled "Intel AMT Security Bypass". The left sidebar is identical to the previous screenshot. The main content area shows the scan title and a "Back to My Scans" link. Below are tabs for Hosts (0), Vulnerabilities (0), and History (1). A search bar for history is present. A table lists scan results:

Start Time	Last Modified	Status
Completed Today at 9:00 PM	Today at 9:00 PM	Completed

Scan Details on the right:

- Policy: Intel AMT Security Bypass
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 9:00 PM
- End: Today at 9:00 PM
- Elapsed: a few seconds

Tenable News at the bottom left mentions "JSDom Improper Loading of Local Resources" with a "Read More" link.

The screenshot displays the Nessus Essentials web interface in a browser window. The main heading is "Shadow Brokers Scan". Below it, there are tabs for "Hosts", "Vulnerabilities", and "History". The "Vulnerabilities" tab is active, showing a table with one entry: "Current" with a status of "Completed". To the right, the "Scan Details" section shows: Policy: Shadow Brokers Scan, Status: Completed, Scanner: Local Scanner, Start: Today at 9:02 PM, End: Today at 9:02 PM, and Elapsed: a few seconds. Below this, a "Vulnerabilities" donut chart shows 100% of the results are "Info" level. The left sidebar contains navigation links for Folders, Resources, and Tenable News. The bottom of the sidebar shows a "Tenable News" section with a link to "CVE-2021-22986: PS Patches Several Critical Vulnerabilities".

Start Time	Last Modified	Status
Current	Today at 9:02 PM	Completed

Scan Details

- Policy: Shadow Brokers Scan
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 9:02 PM
- End: Today at 9:02 PM
- Elapsed: a few seconds

Vulnerabilities

- 100% Info

The screenshot displays the Nessus Essentials web interface in a browser window. The main heading is "Spectre and Meltdown". Below it, there are tabs for "Hosts", "Vulnerabilities", and "History". The "Vulnerabilities" tab is active, showing a table with one entry: "Current" with a status of "Completed". To the right, the "Scan Details" section shows: Policy: Spectre and Meltdown, Status: Completed, Scanner: Local Scanner, Start: Today at 9:05 PM, End: Today at 9:05 PM, and Elapsed: a few seconds. Below this, a "Vulnerabilities" donut chart shows 100% of the results are "Info" level. The left sidebar contains navigation links for Folders, Resources, and Tenable News. The bottom of the sidebar shows a "Tenable News" section with a link to "Dell EMC OpenManage Server Administrator Authenticates".

Start Time	Last Modified	Status
Current	Today at 9:05 PM	Completed

Scan Details

- Policy: Spectre and Meltdown
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 9:05 PM
- End: Today at 9:05 PM
- Elapsed: a few seconds

Vulnerabilities

- 100% Info

The screenshot shows the Nessus Essentials web interface. The left sidebar contains navigation links for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules), and TENABLE (Community, Research, Plugin Release Notes). The main content area is titled 'WannaCry Ransomware' and includes tabs for Hosts (1), Vulnerabilities (1), and History (1). A table lists scan results with columns for Start Time, Last Modified, and Status. The status is 'Completed'. To the right, 'Scan Details' are provided, including Policy (WannaCry Ransomware), Status (Completed), Scanner (Local Scanner), Start (Today at 9:06 PM), End (Today at 9:06 PM), and Elapsed (a few seconds). A 'Vulnerabilities' donut chart shows the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Start Time	Last Modified	Status
Today at 9:06 PM	Today at 9:06 PM	Completed

Scan Details

- Policy: WannaCry Ransomware
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 9:06 PM
- End: Today at 9:06 PM
- Elapsed: a few seconds

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

The screenshot shows the Nessus Essentials web interface. The left sidebar contains navigation links for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules), and TENABLE (Community, Research, Plugin Release Notes). The main content area is titled 'Ripple20 Remote Scan' and includes tabs for Hosts (1), Vulnerabilities (3), and History (1). A table lists scan results with columns for Start Time, Last Modified, and Status. The status is 'Completed'. To the right, 'Scan Details' are provided, including Policy (Ripple20 Remote Scan), Status (Completed), Scanner (Local Scanner), Start (Today at 9:07 PM), End (Today at 9:08 PM), and Elapsed (a few seconds). A 'Vulnerabilities' donut chart shows the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Start Time	Last Modified	Status
Today at 9:07 PM	Today at 9:08 PM	Completed

Scan Details

- Policy: Ripple20 Remote Scan
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 9:07 PM
- End: Today at 9:08 PM
- Elapsed: a few seconds

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

File Machine View Input Devices Help

Nessus Essentials / Folders / View Scan - Mozilla Firefox

Download Nessus | Tenable x

https://kali8834/#/scans/reports/38/history

nessus

Scans Settings

root

Zerologon Remote Scan

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 3 History 1

Search History 1 History

Start Time	Last Modified	Status
Completed Today at 9:11 PM	Today at 9:11 PM	✓ Completed

Scan Details

Policy: Zerologon Remote Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 9:11 PM
End: Today at 9:11 PM
Elapsed: a few seconds

Vulnerabilities

Critical
High
Medium
Low
Info

Tenable News

Secomex
GataManager Multiple
Vulnerabilities

Read More

File Machine View Input Devices Help

Nessus Essentials / Folders / View Scan - Mozilla Firefox

Download Nessus | Tenable x

https://kali8834/#/scans/reports/41/history

nessus

Scans Settings

root

Solorigate

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 2 History 1

Search History 1 History

Start Time	Last Modified	Status
Completed Today at 9:12 PM	Today at 9:13 PM	✓ Completed

Scan Details

Policy: Solorigate
Status: Completed
Scanner: Local Scanner
Start: Today at 9:12 PM
End: Today at 9:13 PM
Elapsed: a few seconds

Vulnerabilities

Critical
High
Medium
Low
Info

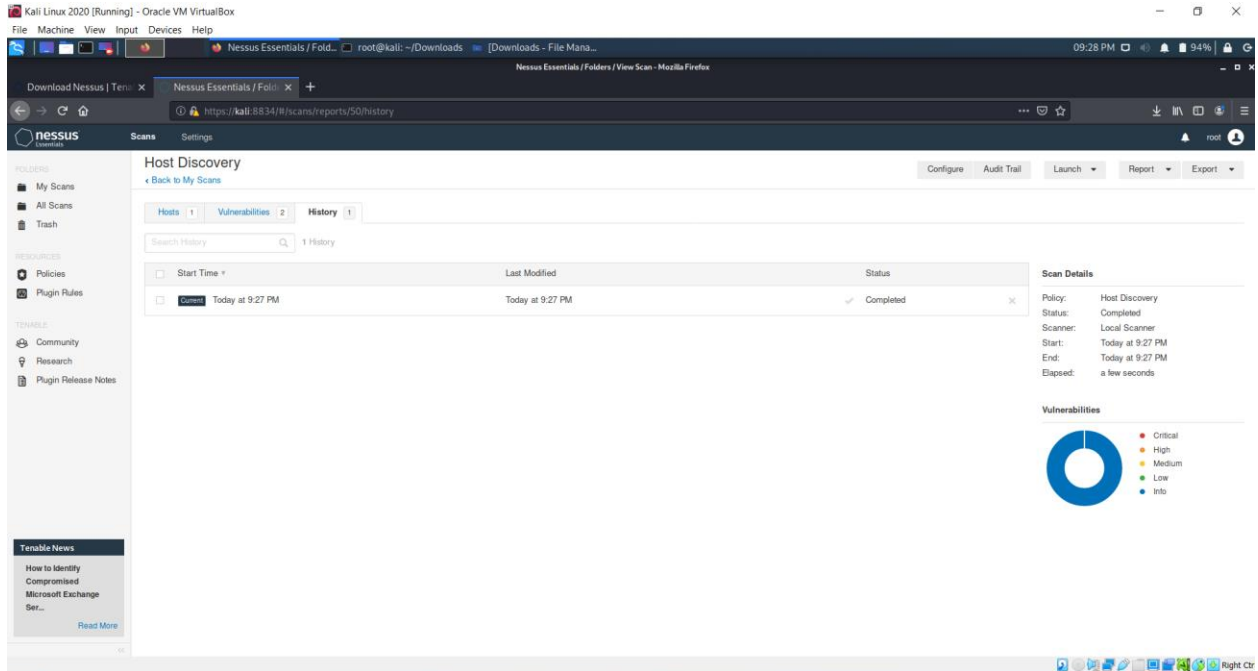
Tenable News

CVE-2021-22986: FS
Patches Several
Critical Vulner...

Read More

The screenshot shows the Nessus Essentials web interface in a browser. The main heading is "2020 Threat Landscape Retrospective (TLR)". Below it, there are tabs for "Hosts", "Vulnerabilities", and "History". The "Hosts" tab is active, showing a table with one host: "10.0.2.15". To the right, the "Scan Details" section shows: Policy: 2020 Threat Landscape Retrospective (TLR), Status: Completed, Scanner: Local Scanner, Start: Today at 9:14 PM, End: Today at 9:14 PM, Elapsed: a few seconds. Below this, a "Vulnerabilities" section features a donut chart with a legend: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). The chart is mostly blue, indicating a high number of information-level vulnerabilities. A "Tenable News" sidebar on the left contains a link to "Dell EMC OpenManage Server Administrator Authentication...".

The screenshot shows the Nessus Essentials web interface for a scan titled "ProxyLogon : MS Exchange". The "History" tab is active, displaying a table with one entry: "Current" (Start Time), "Today at 9:16 PM" (Last Modified), and "Completed" (Status). The "Scan Details" section on the right shows: Policy: ProxyLogon : MS Exchange, Status: Completed, Scanner: Local Scanner, Start: Today at 9:16 PM, End: Today at 9:16 PM, Elapsed: a few seconds. The "Tenable News" sidebar on the left contains a link to "Cyber Hygiene: 5 Advanced Tactics to Maximize Your...".



The screenshot shows the Nessus web interface in a browser window. The main content area displays the 'Host Discovery' scan results. A table lists the scan details, showing a single scan completed at 9:27 PM. To the right, a 'Scan Details' section provides further information about the scan. Below this, a 'Vulnerabilities' section features a donut chart showing the distribution of vulnerability severity levels.

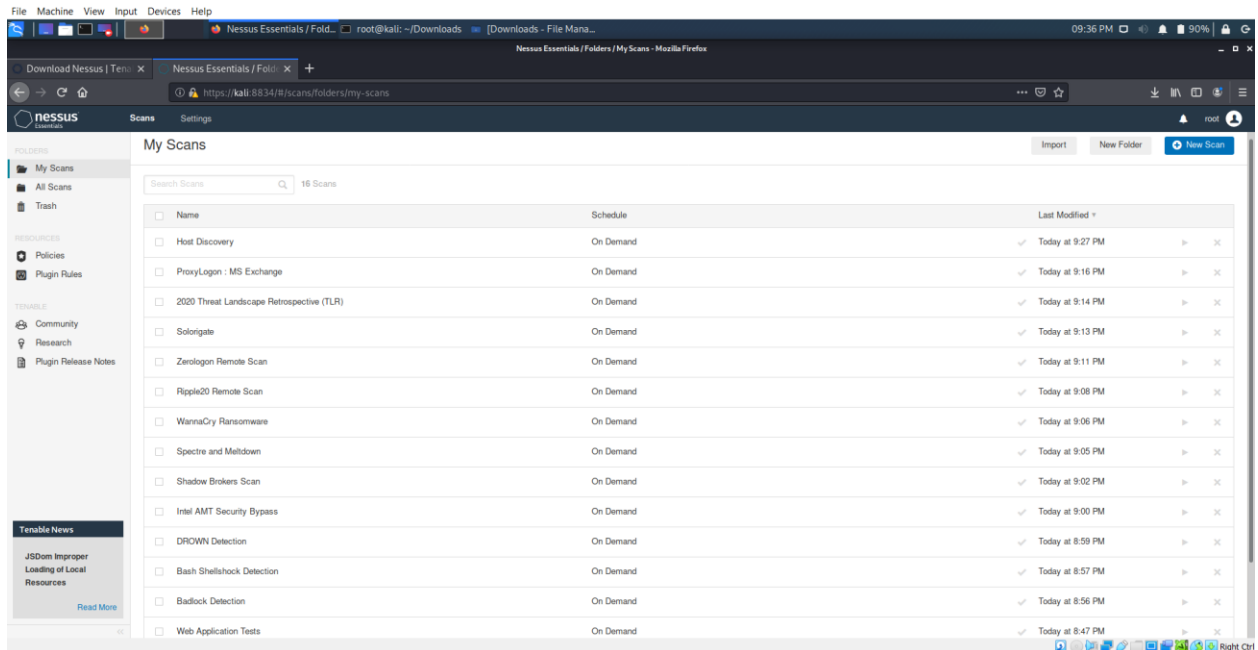
Start Time	Last Modified	Status
Current: Today at 9:27 PM	Today at 9:27 PM	Completed

Scan Details

- Policy: Host Discovery
- Status: Completed
- Scanner: Local Scanner
- Start: Today at 9:27 PM
- End: Today at 9:27 PM
- Elapsed: a few seconds

Vulnerabilities

A donut chart showing the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). The chart is predominantly blue, indicating a high number of information-level vulnerabilities.



The screenshot shows the 'My Scans' page in the Nessus web interface. A table lists various scans, including Host Discovery, ProxyLogon, 2020 Threat Landscape Retrospective, Soligate, Zerologon, Ripple20, WannaCry, Spectre and Meltdown, Shadow Brokers, Intel AMT Security Bypass, DROWN Detection, Bash Shellshock Detection, Badlock Detection, and Web Application Tests. Each scan entry includes its name, schedule, and last modified time.

Name	Schedule	Last Modified
Host Discovery	On Demand	Today at 9:27 PM
ProxyLogon : MS Exchange	On Demand	Today at 9:16 PM
2020 Threat Landscape Retrospective (TLR)	On Demand	Today at 9:14 PM
Soligate	On Demand	Today at 9:13 PM
Zerologon Remote Scan	On Demand	Today at 9:11 PM
Ripple20 Remote Scan	On Demand	Today at 9:08 PM
WannaCry Ransomware	On Demand	Today at 9:06 PM
Spectre and Meltdown	On Demand	Today at 9:05 PM
Shadow Brokers Scan	On Demand	Today at 9:02 PM
Intel AMT Security Bypass	On Demand	Today at 9:00 PM
DROWN Detection	On Demand	Today at 8:59 PM
Bash Shellshock Detection	On Demand	Today at 8:57 PM
Badlock Detection	On Demand	Today at 8:56 PM
Web Application Tests	On Demand	Today at 8:47 PM

SEED Ubuntu Virtual Machine ---- 10.0.2.15 IP

The image displays two screenshots of the Nessus Essentials web interface, showing the results of a scan performed on the host 10.0.2.15.

Top Screenshot: Basic Scan

- Hosts:** 1
- Vulnerabilities:** 22
- History:** 2
- Filter:** Search Hosts
- Hosts Table:**

Host	Vulnerabilities
10.0.2.15	31
- Scan Details:**
 - Policy: Basic Network Scan
 - Status: Completed
 - Scanner: Local Scanner
 - Start: Today at 9:37 PM
 - End: Today at 9:38 PM
 - Elapsed: a minute
- Vulnerabilities:** A donut chart showing the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Bottom Screenshot: Advanced Scan

- Hosts:** 1
- Vulnerabilities:** 22
- History:** 2
- Filter:** Search Hosts
- Hosts Table:**

Host	Vulnerabilities
10.0.2.15	31
- Scan Details:**
 - Policy: Advanced Scan
 - Status: Completed
 - Scanner: Local Scanner
 - Start: Today at 9:37 PM
 - End: Today at 9:39 PM
 - Elapsed: 2 minutes
- Vulnerabilities:** A donut chart showing the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

The image displays two screenshots of the Nessus web interface, showing scan results for two different policies: 'Web Application Tests' and 'Badlock Detection'.

Top Screenshot: Web Application Tests

- Policy:** Web Application Tests
- Status:** Completed
- Scanner:** Local Scanner
- Start:** Today at 9:37 PM
- End:** Today at 9:40 PM
- Elapsed:** 3 minutes

Vulnerabilities: A donut chart showing the distribution of vulnerability severity levels. The chart is predominantly blue, indicating a high number of 'Info' level vulnerabilities.

Bottom Screenshot: Badlock Detection

- Policy:** Badlock Detection
- Status:** Completed
- Scanner:** Local Scanner
- Start:** Today at 9:37 PM
- End:** Today at 9:40 PM
- Elapsed:** 4 minutes

Vulnerabilities: A donut chart showing the distribution of vulnerability severity levels. The chart is predominantly blue, indicating a high number of 'Info' level vulnerabilities.

The image displays two screenshots of the Nessus Essentials web interface, showing scan results for two different vulnerabilities.

Top Screenshot: Bash Shellshock Detection

- Policy:** Bash Shellshock Detection
- Status:** Completed
- Scanner:** Local Scanner
- Start:** Today at 9:37 PM
- End:** Today at 9:41 PM
- Elapsed:** 4 minutes

Vulnerabilities: A donut chart showing the distribution of vulnerability severity levels. The chart is predominantly blue, indicating a high percentage of 'Info' level vulnerabilities.

Bottom Screenshot: DROWN Detection

- Policy:** DROWN Detection
- Status:** Completed
- Scanner:** Local Scanner
- Start:** Today at 9:37 PM
- End:** Today at 9:41 PM
- Elapsed:** 4 minutes

Vulnerabilities: A donut chart showing the distribution of vulnerability severity levels. The chart is predominantly blue, indicating a high percentage of 'Info' level vulnerabilities.

The image displays two screenshots of the Nessus Essentials web interface, showing scan results for two different policies.

Top Screenshot: Intel AMT Security Bypass

The interface shows the scan results for the 'Intel AMT Security Bypass' policy. The scan is completed, and the status is 'Completed'. The scan details show the policy name, status, scanner (Local Scanner), start time (Today at 9:37 PM), end time (Today at 9:41 PM), and elapsed time (4 minutes).

Start Time	Last Modified	Status
Today at 9:37 PM	Today at 9:41 PM	Completed
Today at 9:00 PM	Today at 9:00 PM	Completed

Bottom Screenshot: Shadow Brokers Scan

The interface shows the scan results for the 'Shadow Brokers Scan' policy. The scan is completed, and the status is 'Completed'. The scan details show the policy name, status, scanner (Local Scanner), start time (Today at 9:37 PM), end time (Today at 9:47 PM), and elapsed time (10 minutes).

Host	Vulnerabilities
10.0.2.15	3

The 'Vulnerabilities' section shows a donut chart with the following data:

- Critical: 0
- High: 0
- Medium: 0
- Low: 0
- Info: 3

The image displays two screenshots of the Nessus Essentials web interface, showing scan results for two different policies: 'Spectre and Meltdown' and 'WannaCry Ransomware'.

Screenshot 1: Spectre and Meltdown

- Hosts:** 1 host (10.0.2.15) is listed.
- Vulnerabilities:** 3 vulnerabilities are listed for the host 10.0.2.15.
- Scan Details:**
 - Policy: Spectre and Meltdown
 - Status: Completed
 - Scanner: Local Scanner
 - Start: Today at 9:37 PM
 - End: Today at 9:48 PM
 - Elapsed: 11 minutes
- Vulnerabilities:** A donut chart shows the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Screenshot 2: WannaCry Ransomware

- Hosts:** 1 host (10.0.2.15) is listed.
- Vulnerabilities:** 1 vulnerability is listed for the host 10.0.2.15.
- Scan Details:**
 - Policy: WannaCry Ransomware
 - Status: Completed
 - Scanner: Local Scanner
 - Start: Today at 9:37 PM
 - End: Today at 9:48 PM
 - Elapsed: 11 minutes
- Vulnerabilities:** A donut chart shows the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

The image displays two screenshots of the Nessus Essentials web interface, showing scan results for two different targets.

Top Screenshot: Ripple20 Remote Scan

- Hosts:** 1 Host (10.0.2.15)
- Vulnerabilities:** 3 (Critical: 1, High: 1, Medium: 1, Low: 0, Info: 0)
- Scan Details:**
 - Policy: Ripple20 Remote Scan
 - Status: Completed
 - Scanner: Local Scanner
 - Start: Today at 9:37 PM
 - End: Today at 9:48 PM
 - Elapsed: 11 minutes

Bottom Screenshot: Solorigate

- Hosts:** 1 Host (10.0.2.15)
- Vulnerabilities:** 3 (Critical: 1, High: 1, Medium: 1, Low: 0, Info: 0)
- Scan Details:**
 - Policy: Solorigate
 - Status: Completed
 - Scanner: Local Scanner
 - Start: Today at 9:37 PM
 - End: Today at 9:49 PM
 - Elapsed: 12 minutes

The screenshot displays the Nessus Essentials web interface in a browser window. The main content area shows the 'Zeroologon Remote Scan' results. On the left, a sidebar contains navigation links for 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', 'Community', 'Research', and 'Plugin Release Notes'. The main panel has tabs for 'Hosts', 'Vulnerabilities', and 'History'. The 'Hosts' tab is active, showing a table with one host: 10.0.2.15. The 'Vulnerabilities' tab shows a donut chart representing the distribution of vulnerability severity levels. The 'Scan Details' panel on the right provides information about the scan: Policy: Zeroologon Remote Scan, Status: Completed, Scanner: Local Scanner, Start: Today at 9:37 PM, End: Today at 9:49 PM, Elapsed: 12 minutes. The 'Vulnerabilities' section shows a donut chart with a legend for Critical, High, Medium, Low, and Info.

Zeroologon Remote Scan

Hosts: 1 | Vulnerabilities: 3 | History: 2

Filter Search Hosts 1 Host

Host	Vulnerabilities
10.0.2.15	4

Scan Details

Policy: Zeroologon Remote Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 9:37 PM
End: Today at 9:49 PM
Elapsed: 12 minutes

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Host Discovery

Hosts: 1 | Vulnerabilities: 2 | History: 2

Filter Search Hosts 1 Host

Host	Vulnerabilities
10.0.2.15	2

Scan Details

Policy: Host Discovery
Status: Completed
Scanner: Local Scanner
Start: Today at 9:37 PM
End: Today at 9:49 PM
Elapsed: 12 minutes

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Kali Linux 2020 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Nessus Essentials / Folders / View Scan - Mozilla Firefox

10:21 PM 70%

Download Nessus | Tenable x | Nessus Essentials / Folders x +

https://kali-8834/r/scans/reports/44/hosts

nessus Tenable Scans Settings root

2020 Threat Landscape Retrospective (TLR)

Configure Audit Trail Launch Report Export

Back to My Scans

Hosts 1 Vulnerabilities 5 History 2

Filter Search Hosts 1 Host

Host	Vulnerabilities
10.0.2.15	

Scan Details

Policy: 2020 Threat Landscape Retrospective (TLR)

Status: Completed

Scanner: Local Scanner

Start: Today at 9:37 PM

End: Today at 9:49 PM

Elapsed: 12 minutes

Vulnerabilities

Legend: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue)

Tenable News

CVE-2021-32986: FS Patches Several Critical Vulner...

Read More

Progress Embedded Image of Progress Report from LabSim:

Score Sheet: TestOut Security Pro: Jain, Hemant

Product: TestOut Security Pro 7.0

Resources to Show: ☒ Exams ☐ Labs ☐ Lessons ☐ Videos

☐ Date Range

Start: End:

☐ Show scores as points

Resource	Time In Resource	Newest Score	Highest Score	Lowest Score	Average Score	Points Possible	Attempts
9.5.6 Section Quiz	11 minutes	90% (3/22/2021 4:02 ...	90% (3/22/2021 4:02 ...	90% (3/22/2021 4:02 ...	90%	10	1
9.6.7 Section Quiz	1 minute 32 seconds	100% (3/22/2021 6:03...	100% (3/22/2021 6:03...	100% (3/22/2021 6:03...	100%	10	1
9.7.7 Section Quiz	1 minute 12 seconds	100% (3/22/2021 5:03...	100% (3/22/2021 5:03...	100% (3/22/2021 5:03...	100%	10	1
9.8.7 Section Quiz	2 minutes 35 seconds	100% (3/22/2021 6:13...	100% (3/22/2021 6:13...	100% (3/22/2021 6:13...	100%	10	1
9.9.6 Section Quiz	1 minute 35 seconds	100% (3/22/2021 5:05...	100% (3/22/2021 5:05...	100% (3/22/2021 5:05...	100%	10	1
10.1.9 Section Quiz	1 minute 44 seconds	100% (3/27/2021 10:5...	100% (3/27/2021 10:5...	100% (3/27/2021 10:5...	100%	10	1
10.2.3 Section Quiz	1 minute 6 seconds	100% (3/27/2021 11:0...	100% (3/27/2021 11:0...	100% (3/27/2021 11:0...	100%	10	1
10.3.16 Section Quiz	1 minute 6 seconds	100% (3/27/2021 11:0...	100% (3/27/2021 11:0...	100% (3/27/2021 11:0...	100%	10	1
10.4.14 Section Quiz	1 minute 1 second	100% (3/27/2021 11:0...	100% (3/27/2021 11:0...	100% (3/27/2021 11:0...	100%	10	1
11.1.4 Section Quiz	12 minutes 46 seconds	80% (4/5/2021 11:31 ...	80% (4/5/2021 11:31 ...	80% (4/5/2021 11:31 ...	80%	10	1
11.2.9 Section Quiz	13 minutes 18 seconds	80% (4/5/2021 11:44 ...	80% (4/5/2021 11:44 ...	80% (4/5/2021 11:44 ...	80%	10	1
11.3.6 Section Quiz	7 minutes	100% (4/5/2021 11:52 ...	100% (4/5/2021 11:52 ...	100% (4/5/2021 11:52 ...	100%	10	1
11.4.12 Section Quiz	14 minutes 31 seconds	80% (4/5/2021 12:08 ...	80% (4/5/2021 12:08 ...	80% (4/5/2021 12:08 ...	80%	10	1
11.5.4 Section Quiz	1 minute 16 seconds	100% (4/5/2021 8:55 ...	100% (4/5/2021 8:55 ...	100% (4/5/2021 8:55 ...	100%	10	1
11.6.12 Section Quiz	54 seconds	100% (4/5/2021 8:53 ...	100% (4/5/2021 8:53 ...	100% (4/5/2021 8:53 ...	100%	10	1
11.7.8 Section Quiz	3 minutes 9 seconds	100% (4/5/2021 8:52 ...	100% (4/5/2021 8:52 ...	100% (4/5/2021 8:52 ...	100%	10	1
12.1.5 Section Quiz						10	0
12.2.5 Section Quiz						10	0
12.3.11 Section Quiz						10	0