

1. ให้ นักศึกษาส่งรายงาน การตรวจสอบ metasploit2 ที่ติดตั้งในเครื่องของตัวเอง มีช่อง ให้ว่าระดับ CRITICAL ที่ port ใดบ้าง และรัน service อะไร โดยใช้ Nessus

### 1.port =6667 service =irc

The screenshot shows the 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' (Anthropic MCP Inspector Remote Code Execution). The main panel displays a finding for 'UnrealIRCd Backdoor Detection' (CRITICAL). The 'Description' section states: 'The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.' The 'Solution' section advises: 'Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.' The 'Output' section shows command-line logs: 'The remote IRC server is running as : uid=0(root) gid=0(root)' and 'To see debug logs, please visit individual host'. A table lists 'Port' (6667 /tcp /irc) and 'Hosts' (192.168.235.131). To the right, the 'Plugin Details' section provides technical details: Severity: Critical, ID: 46882, Version: 1.16, Type: remote, Family: Backdoors, Published: June 14, 2010, Modified: April 11, 2022. The 'VPR Key Drivers' section includes Threat Recency, Threat Intensity, Exploit Code Maturity, Age of Vuln, Product Coverage, CVSSV3 Impact Score (5.9), and Threat Sources. The 'Risk Information' section shows Vulnerability Priority Rating (VPR: 7.4), Exploit Prediction Scoring System (EPSS: 0.7216), and Risk Factor (Critical).

### 2.port=80 service=www

The screenshot shows the Nessus Essentials interface. The left sidebar is identical to the previous one. The main panel displays a finding for 'Canonical Ubuntu Linux SEoL (8.04.x)' (CRITICAL). The 'Description' section states: 'According to its version, Canonical Ubuntu Linux is 8.04.x. It is, therefore, no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.' The 'Solution' section advises: 'Upgrade to a version of Canonical Ubuntu Linux that is currently supported.' The 'Output' section shows command-line logs: 'OS : Ubuntu Linux 8.04 Security End of Life : May 9, 2013 Time since Security End of Life (Est.) : >= 12 years' and 'To see debug logs, please visit individual host'. A table lists 'Port' (80 /tcp /www) and 'Hosts' (192.168.235.131). To the right, the 'Plugin Details' section provides technical details: Severity: Critical, ID: 201352, Version: 1.2, Type: combined, Family: General, Published: July 3, 2024, Modified: March 26, 2025. The 'Risk Information' section shows Risk Factor (Critical), CVSS v3.0 Base Score (10.0), CVSS v3.0 Vector (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/H/I/H/A:H), CVSS v2.0 Base Score (10.0), CVSS v2.0 Vector (CVSS2#AV:N/AC:L/Au:N/C:C/I/C/A:C), and Vulnerability Information (CPE: cpe:/o:canonical:ubuntu\_linux, Unsupported by vendor: true).

### 3.port =5900 service=vnc

The screenshot shows the Tenable Nessus Essentials interface. The left sidebar includes 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', and 'Terrascan'. A 'Tenable News' section highlights 'Forrester Names Tenable a Leader in the Q3 2025 Un...'. The main content area displays a 'Vulnerabilities' section with 73 items. One item is highlighted as 'CRITICAL' for 'VNC Server 'password' Password'. The 'Description' section states: '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.' The 'Solution' section advises: 'Secure the VNC service with a strong password.' The 'Output' section shows: 'Nessus logged in using a password of "password". To see debug logs, please visit individual host'. The 'Hosts' table lists a single host: '5900 /tcp /vnc' with IP '192.168.235.131'. The 'Plugin Details' section provides metadata: Severity: Critical, ID: 61708, Version: \$Revision: 1.2 \$, Type: remote, Family: Gain a shell remotely, Published: August 29, 2012, Modified: September 24, 2015. The 'Risk Information' section includes: Risk Factor: Critical, CVSS v2.0 Base Score: 10.0, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:/C:A/C. The 'Vulnerability Information' section notes: Default Account: true, Exploited by Nessus: true.

### 4.port= 25 service=smtp port =5432 service=postgresql

The screenshot shows the Tenable Nessus Essentials interface. The left sidebar includes 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', and 'Terrascan'. A 'Tenable News' section highlights 'Oracle Cloud Remote Code Execution Vulnerability o...'. The main content area displays two 'Output' sections. The top section is for port 25/tcp/smtp, showing: '- SSLv2 is enabled and the server supports at least one cipher. Low Strength Ciphers (<= 64-bit key)' followed by a table:

Name	Code	KEX	Auth	Encryption
MAC	.....	....	....	....
more...	....	....	....	....

To see debug logs, please visit individual host. The bottom section is for port 5432/tcp/postgresql, showing: '- SSLv3 is enabled and the server supports at least one cipher. Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3' followed by a table:

Name	Code	KEX	Auth	Encryption
MAC	.....	....	....	....
more...	....	....	....	....

To see debug logs, please visit individual host.

## 5.port =1524 service=wild\_shell

The screenshot shows the Tenable Nessus Essentials interface. The left sidebar includes 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', and 'Terrascan'. A 'Tenable News' section highlights 'How Exposure Management Can Turn a Torrent of Data...'. The main content area displays a 'Bind Shell Backdoor Detection' finding. The 'Description' section states: 'A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.' The 'Solution' section advises: 'Verify if the remote host has been compromised, and reinstall the system if necessary.' The 'Output' section shows command-line interaction: 'Nessus was able to execute the command "id" using the following request :'. Below this is truncated output: '..... snip ..... root@metasploitable:~# uid=0(root) gid=0(root) groups=0(root) root@metasploitable:~# ..... snip .....'. A table lists 'Port' (1524) and 'Hosts' (192.168.235.131). To the right, 'Plugin Details' show: Severity: Critical, ID: 51988, Version: 1.10, Type: remote, Family: Backdoors, Published: February 15, 2011, Modified: April 11, 2022. 'Risk Information' includes: Risk Factor: Critical, CVSS v3.0 Base Score: 9.8, CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/Ui:N/S:U/C:H/I:H/A:H, CVSS v2.0 Base Score: 10.0, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:/C:A/C.

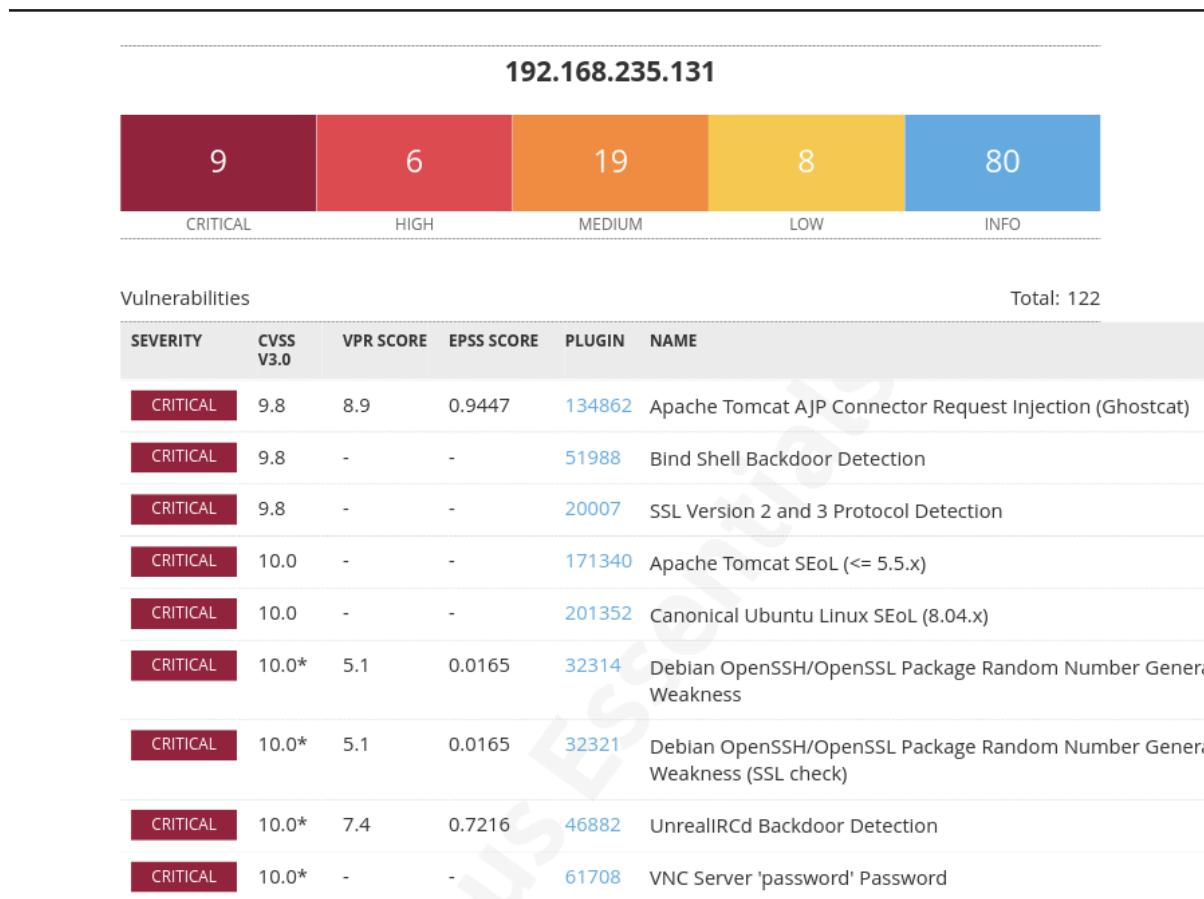
## 6.port =5432 service= postgresql

port = 25 service=smtp

port = 22 service=ssh

The screenshot shows the Tenable Nessus Essentials interface. The left sidebar includes 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', and 'Terrascan'. A 'Tenable News' section highlights 'Oracle Cloud Remote Code Execution Vulnerability o...'. The main content area displays a 'Debian OpenSSH/OpenSSL Package Random Number Generator Weakness' finding. The 'Description' section states: 'The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.' The 'Solution' section advises: 'The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL. An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.' The 'See Also' section links to: <http://www.nessus.org/u?107f9bdc> and <http://www.nessus.org/u?14f4224>. The 'Output' section shows: 'No output recorded.' A table lists 'Port' (5432) and 'Hosts' (192.168.235.131). To the right, 'Plugin Details' show: Severity: Critical, ID: 32321, Version: 1.27, Type: remote, Family: Gain a shell remotely, Published: May 15, 2008, Modified: November 16, 2020. 'VPR Key Drivers' include: Threat Recency: No recorded events, Threat Intensity: Very Low, Exploit Code Maturity: Functional, Age of Vuln: 730 days +, Product Coverage: Medium, CVSSv3 Impact Score: 3.6, Threat Sources: No recorded events. 'Risk Information' includes: Vulnerability Priority Rating (VPR): 5.1, Exploit Prediction Scoring System (EPSS): 0.0165, Risk Factor: Critical, CVSS v2.0 Base Score: 10.0, CVSS v2.0 Temporal Score: 8.3, CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:/C:A/C.

## 2. เปรียบเทียบผลลัพธ์ที่ได้จากข้อ 1 กับ ที่ได้จาก ZAP



## Appendix

### Alert types

This section contains additional information on the types of alerts in the report.

#### Remote Code Execution - CVE-2012-1823

Source	raised by an active scanner ( <a href="#">Remote Code Execution - CVE-2012-1823</a> )
CWE ID	20
WASC ID	20
Reference	<ul style="list-style-type: none"><li>▪ <a href="https://owasp.org/www-community/vulnerabilities/Improper_Data_Validation">https://owasp.org/www-community/vulnerabilities/Improper_Data_Validation</a></li><li>▪ <a href="http://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html">http://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html</a></li><li>▪ <a href="https://cwe.mitre.org/data/definitions/89.html">https://cwe.mitre.org/data/definitions/89.html</a></li></ul>

#### Content Security Policy (CSP) Header Not Set

Source	raised by a passive scanner ( <a href="#">Content Security Policy (CSP) Header Not Set</a> )
CWE ID	693
WASC ID	15
Reference	<ul style="list-style-type: none"><li>▪ <a href="https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy">https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy</a></li><li>▪ <a href="http://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html">http://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html</a></li><li>▪ <a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a></li><li>▪ <a href="https://github.com/webappsec/csp/">https://github.com/webappsec/csp/</a></li><li>▪ <a href="https://web.dev/articles/csp">https://web.dev/articles/csp</a></li><li>▪ <a href="https://icanuse.com/#feat=contentsecuritypolicy">https://icanuse.com/#feat=contentsecuritypolicy</a></li><li>▪ <a href="https://content-security-policy.com/">https://content-security-policy.com/</a></li></ul>

#### Hidden File Found

Source	raised by an active scanner ( <a href="#">Hidden File Finder</a> )
CWE ID	538
WASC ID	13
Reference	<ul style="list-style-type: none"><li>▪ <a href="https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html">https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html</a></li><li>▪ <a href="https://www.php.net/manual/en/function.phpinfo.php">https://www.php.net/manual/en/function.phpinfo.php</a></li></ul>

#### Missing Anti-clickjacking Header

Source	raised by a passive scanner ( <a href="#">Anti-clickjacking Header</a> )
CWE ID	1021
WASC ID	15
Reference	<ul style="list-style-type: none"><li>▪ <a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</a></li></ul>

#### Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Source	raised by a passive scanner ( <a href="#">Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)</a> )
CWE ID	497
WASC ID	13
Reference	<ul style="list-style-type: none"><li>▪ <a href="https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework">https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework</a></li><li>▪ <a href="https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html">https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html</a></li></ul>

#### Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner ( <a href="#">HTTP Server Response Header</a> )
CWE ID	497
WASC ID	13
Reference	<ul style="list-style-type: none"><li>▪ <a href="https://httpd.apache.org/docs/current/mod/core.html#servertokens">https://httpd.apache.org/docs/current/mod/core.html#servertokens</a></li><li>▪ <a href="https://learn.microsoft.com/en-us/previous-versions/msp-n-p/f648552(v=fp10)">https://learn.microsoft.com/en-us/previous-versions/msp-n-p/f648552(v=fp10)</a></li><li>▪ <a href="https://www.troyhunt.com/shhh-dont-let-your-response-headers/">https://www.troyhunt.com/shhh-dont-let-your-response-headers/</a></li></ul>

#### X-Content-Type-Options Header Missing

Source	raised by a passive scanner ( <a href="#">X-Content-Type-Options Header Missing</a> )
CWE ID	693
WASC ID	15
Reference	<ul style="list-style-type: none"><li>▪ <a href="https://learn.microsoft.com/en-us/previous-versions/internet-explorer/ie-developer/compatibility/99622941(v=vs.85)">https://learn.microsoft.com/en-us/previous-versions/internet-explorer/ie-developer/compatibility/99622941(v=vs.85)</a></li><li>▪ <a href="https://owasp.org/www-community/Security_Headers">https://owasp.org/www-community/Security_Headers</a></li></ul>