

- ให้นักศึกษาส่งรายงาน การตรวจสอบ metasploit2 ที่ติดตั้งในเครื่องของตัวเอง มีช่องโหว่ระดับ CRITICAL ที่ port ใดบ้าง และรัน service อะไร โดยใช้ Nessus

1.port =6667 service =iirc

**tenable** Nessus Essentials Scans Settings

**CRITICAL** UnrealIRCd Backdoor Detection

**Description**  
The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

**Solution**  
Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

**See Also**  
<https://seclists.org/fulldisclosure/2010/jun/277>  
<https://seclists.org/fulldisclosure/2010/jun/284>  
<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

**Output**  

```
The remote IRC server is running as :
uid=0 (root) gid=0 (root)
```

To see debug logs, please visit individual host

Port	Hosts
6667 / tcp / iirc	192.168.235.131

**Plugin Details**  
Severity: Critical  
ID: 46882  
Version: 1.16  
Type: remote  
Family: Backdoors  
Published: June 14, 2010  
Modified: April 11, 2022

**VPR Key Drivers**  
Threat Recency: No recorded events  
Threat Intensity: Very Low  
Exploit Code Maturity: Functional  
Age of Vuln: 730 days +  
Product Coverage: Low  
CVSSV3 Impact Score: 5.9  
Threat Sources: No recorded events

**Risk Information**  
Vulnerability Priority Rating (VPR): 7.4  
Exploit Prediction Scoring System (EPSS): 0.7216  
Risk Factor: Critical

2.port=80 service=www

**tenable** Nessus Essentials Scans Settings

**CRITICAL** Canonical Ubuntu Linux SEoL (8.04.x)

**Description**  
According to its version, Canonical Ubuntu Linux is 8.04.x. It is, therefore, no longer maintained by its vendor or provider.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.

**Solution**  
Upgrade to a version of Canonical Ubuntu Linux that is currently supported.

**See Also**  
<http://www.nessus.org/u/73bdb2d2e>

**Output**  

```
OS : Ubuntu Linux 8.04
Security End of Life : May 9, 2013
Time since Security End of Life (Est.) : >= 12 years
```

To see debug logs, please visit individual host

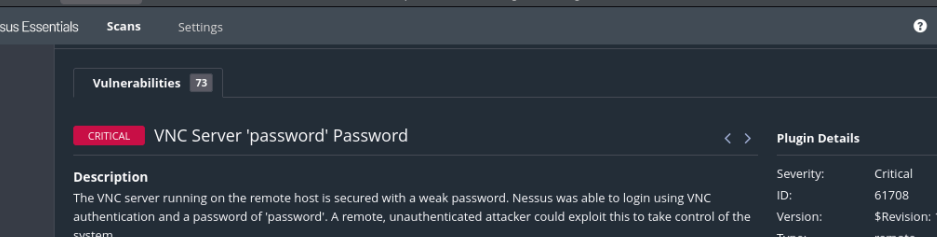
Port	Hosts
80 / tcp / www	192.168.235.131

**Plugin Details**  
Severity: Critical  
ID: 201352  
Version: 1.2  
Type: combined  
Family: General  
Published: July 3, 2024  
Modified: March 26, 2025

**Risk Information**  
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/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

**Vulnerability Information**  
CPE: cpe:/o:canonical:ubuntu\_linux  
Unsupported by vendor: true

```
3.port =5900 service=vnc
```



The screenshot displays the Nessus Essentials web interface. The top navigation bar includes the Tenable logo, 'Nessus Essentials', and tabs for 'Scans' and 'Settings'. The left sidebar contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). A 'Tenable News' section at the bottom left features an article about Forrester Names. The main content area shows a vulnerability report for 'VNC Server 'password' Password', marked as 'CRITICAL'. The report includes a description of the VNC server's weak password, a solution to use a strong password, and an output log showing a successful login. On the right, 'Plugin Details' and 'Risk Information' are provided, including severity, ID, version, type, family, published date, modified date, risk factor, CVSS scores, and vector.

**Vulnerabilities** 73

**CRITICAL** VNC Server 'password' Password

**Description**  
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.

**Solution**  
Secure the VNC service with a strong password.

**Output**

```
Nessus logged in using a password of "password".
```

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.235.131

**Plugin Details**

Severity: Critical  
ID: 61708  
Version: \$Revision: 1.2 \$  
Type: remote  
Family: Gain a shell remotely  
Published: August 29, 2012  
Modified: September 24, 2015

**Risk Information**

Risk Factor: Critical  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/AU:N/C:C/!/C/A/C

**Vulnerability Information**

Default Account: true  
Exploited by Nessus: true

**Tenable News**

Forrester Names  
Tenable a Leader in  
the Q3 2025 Un...

[Read More](#)

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

[illegible]

5.port =1524 service=wild\_shell

The screenshot shows the Nessus Essentials interface. The left sidebar contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area displays the 'Bind Shell Backdoor Detection' plugin details, which is marked as 'CRITICAL'. The description 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 suggests: 'Verify if the remote host has been compromised, and reinstall the system if necessary.' The output section shows a truncated output of the 'snip' command, indicating a successful connection to the remote host. The risk information section shows a 'Risk Factor: Critical' and a 'CVSS v3.0 Base Score: 9.8'. The bottom right corner shows the user 'nessus' and a profile icon.

**tenable** Nessus Essentials Scans Settings

**CRITICAL** Bind Shell Backdoor Detection

**Description**  
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.

**Solution**  
Verify if the remote host has been compromised, and reinstall the system if necessary.

**Output**

```
Nessus was able to execute the command "id" using the following request :

----- snip -----
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

----- snip -----
```

To see debug logs, please visit individual host

Port	Hosts
1524 / tcp / wild_shell	192.168.235.131

**Plugin Details**

Severity: Critical  
ID: 51988  
Version: 1.10  
Type: remote  
Family: Backdoors  
Published: February 15, 2011  
Modified: April 11, 2022

**Risk Information**

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

**Tenable News**

How Exposure Management Can Turn a Torrent of Data...  
[Read More](#)

6.port =5432 service= postgresql

port = 25 service=smtp

port = 22 service=ssh

The screenshot shows the Nessus Essentials interface. The left sidebar contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area displays the 'Debian OpenSSH/OpenSSL Package Random Number Generator Weakness' plugin details, which is marked as 'CRITICAL'. The description 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 suggests: 'Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.' The output section shows 'No output recorded.' The risk information section shows a 'Risk Factor: Critical' and a 'CVSS v3.0 Base Score: 9.8'. The bottom right corner shows the user 'nessus' and a profile icon.

**tenable** Nessus Essentials Scans Settings

**CRITICAL** Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

**Description**  
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 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.

**Solution**  
Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

**See Also**  
<http://www.nessus.org/u?107f9bdc>  
<http://www.nessus.org/u?f14f4224>

**Output**

No output recorded.

To see debug logs, please visit individual host

Port	Hosts
5432 / tcp / postgresql	192.168.235.131
25 / tcp / smtp	192.168.235.131

**Plugin Details**

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**

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

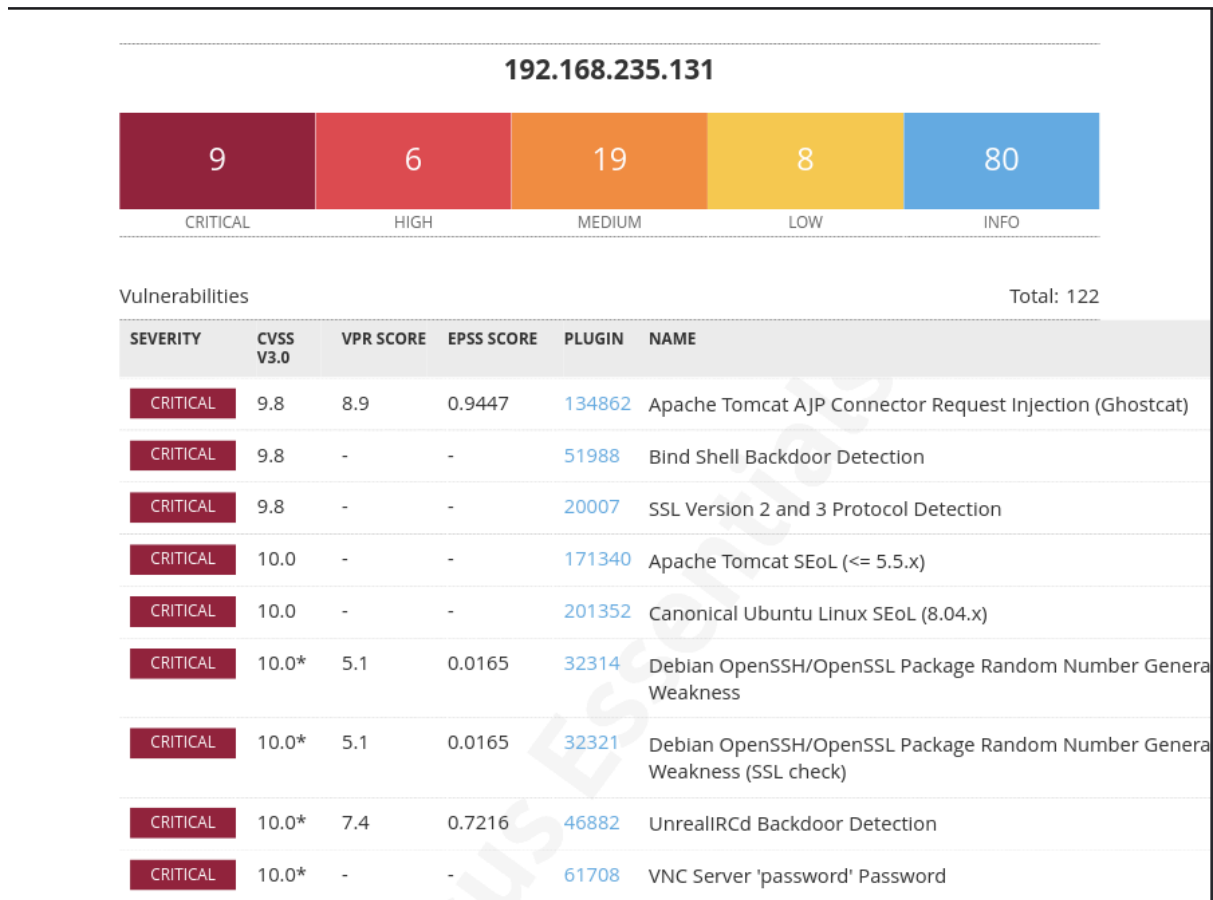
**Risk Information**

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

**Tenable News**

Oracle Cloud Remote Code Execution Vulnerability o...  
[Read More](#)

## 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="https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html">https://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="https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html">https://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://w3c.github.io/webappsec-csp/">https://w3c.github.io/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.hackplayers.de/archives/892-introducing-snaggy-a-tool-to-scan-for-secrets-on-web-servers.html">https://blog.hackplayers.de/archives/892-introducing-snaggy-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/03-Information_Gathering/08-Fingerprint_Web_Application_Framework">https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/03-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/windows-internet-explorer/ie-developer/compatibility/99522941(v=vs.85)">https://learn.microsoft.com/en-us/previous-versions/windows-internet-explorer/ie-developer/compatibility/99522941(v=vs.85)</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/windows-internet-explorer/ie-developer/compatibility/99522941(v=vs.85)">https://learn.microsoft.com/en-us/previous-versions/windows-internet-explorer/ie-developer/compatibility/99522941(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>