

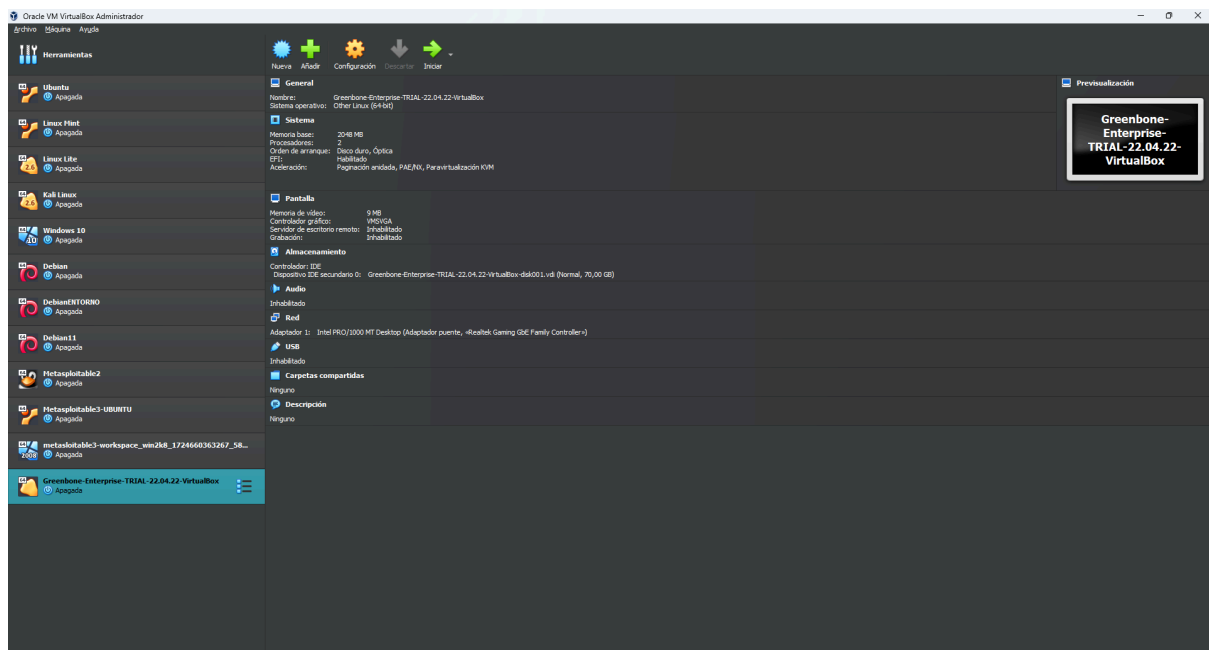
Actividad 10. Uso de la herramienta OpenVAS

1. Instalar OpenVAS

2. Ejecutar escaneo de vulnerabilidades sobre la máquina Metasploitable2 y Metasploitable3

1. Instalar OpenVAS

Importamos la máquina virtual Greenbone:



Una vez importado, iniciamos la máquina. Nos mostrará la IP de la máquina en la red y nos solicita hacer Login con usuario **admin** y contraseña: **admin**:

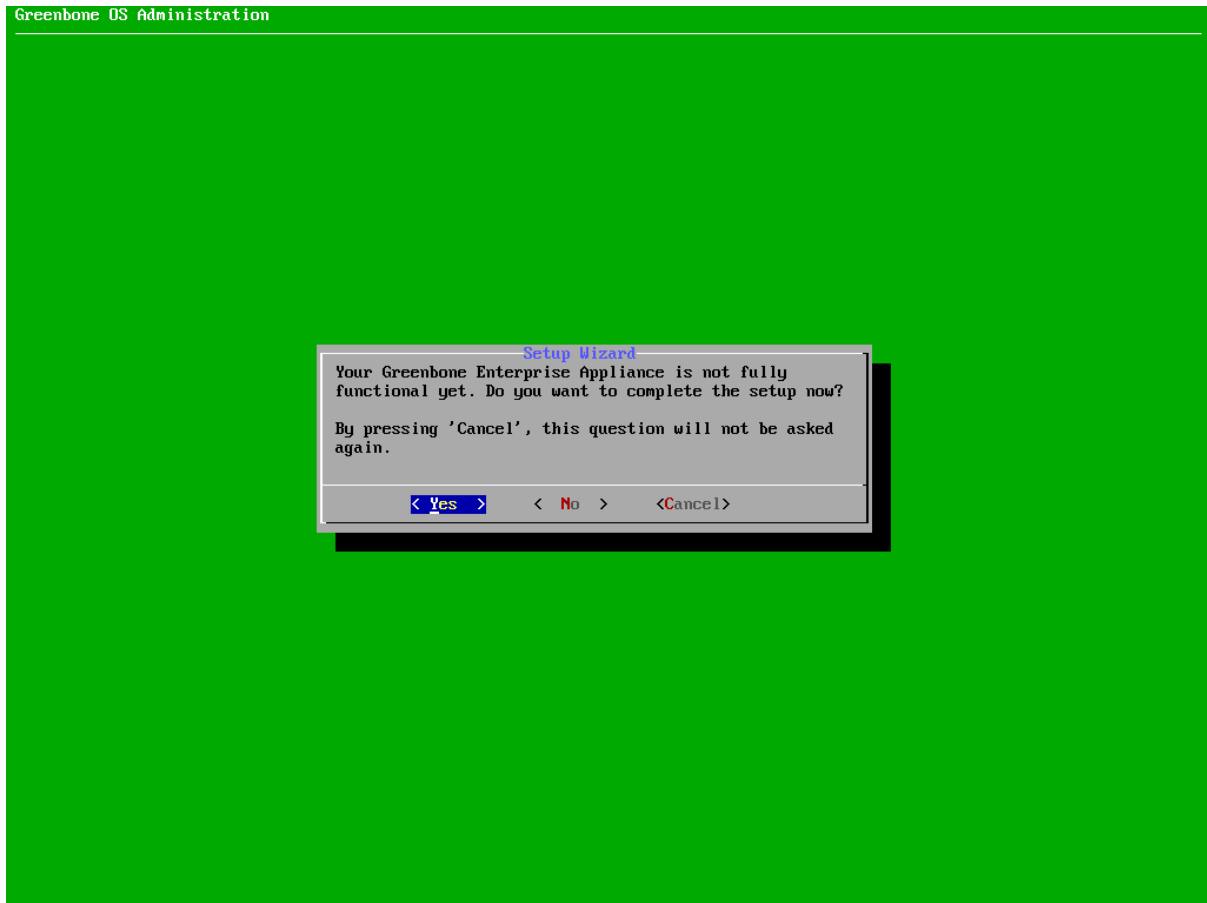
```
Welcome to Greenbone OS 22.04.22 (tty1)
```

```
The web interface is available at:
```

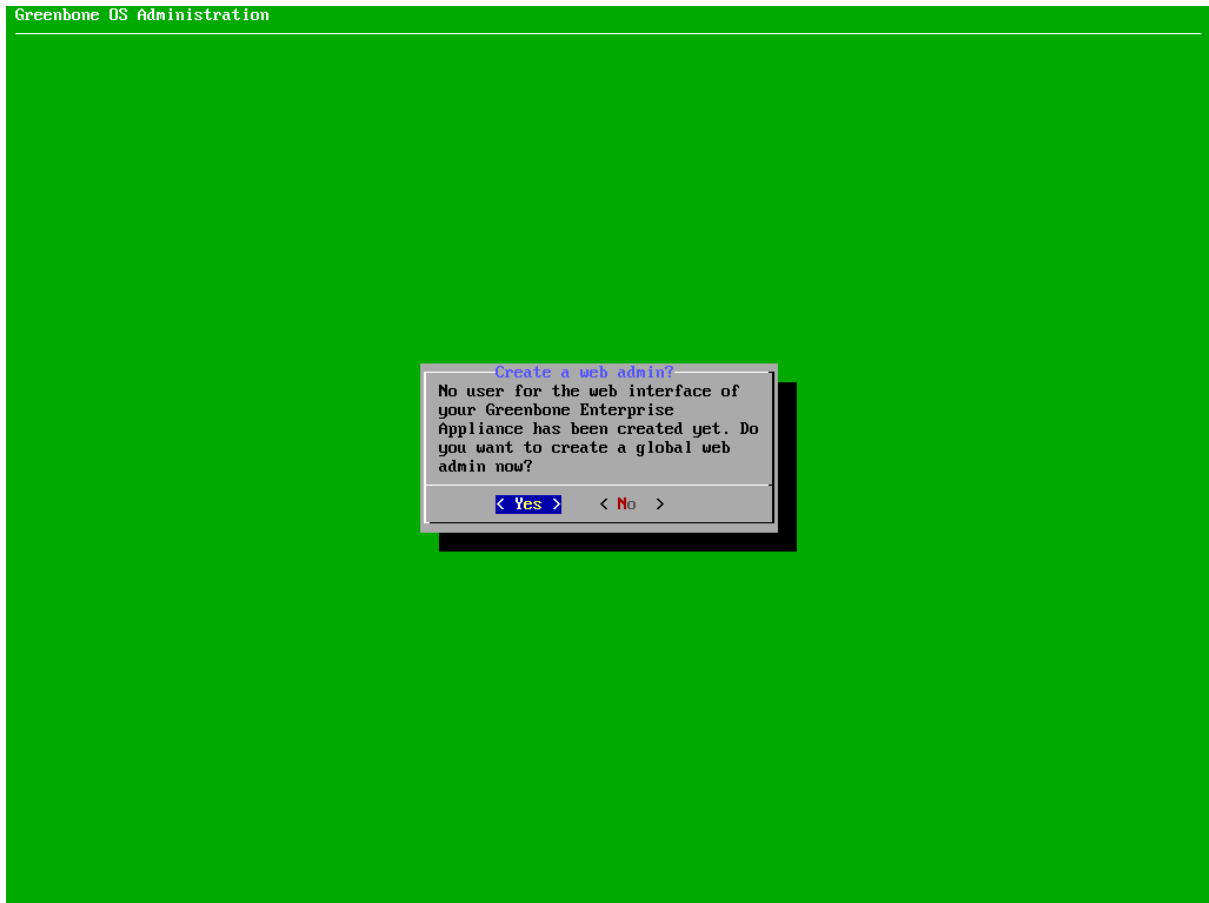
```
http://10.0.19.124
```

```
gsm login: _
```

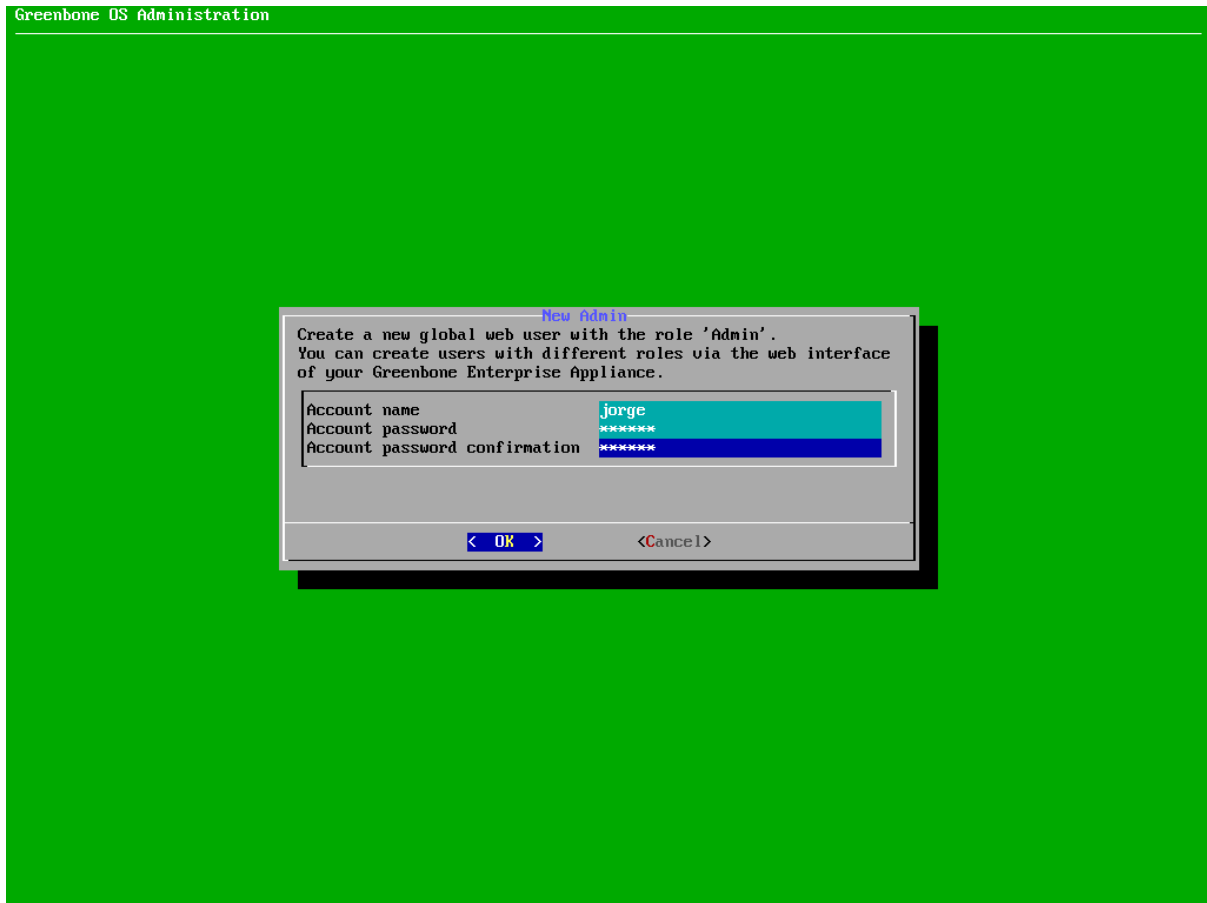
Nos pregunta si completamos la configuración. Pulsamos Yes:



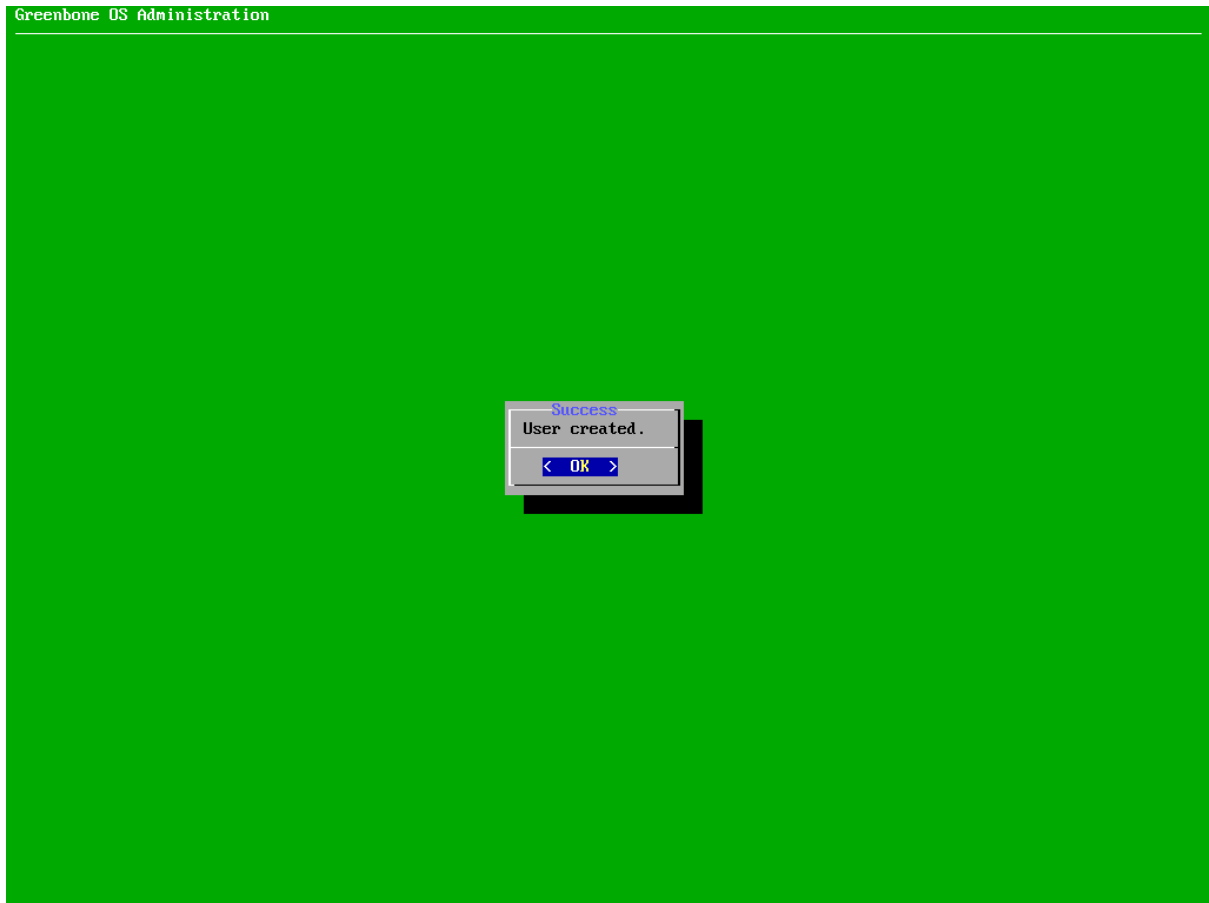
Nos pregunta si queremos crear una interfaz web de administración.
Pulsamos Yes:



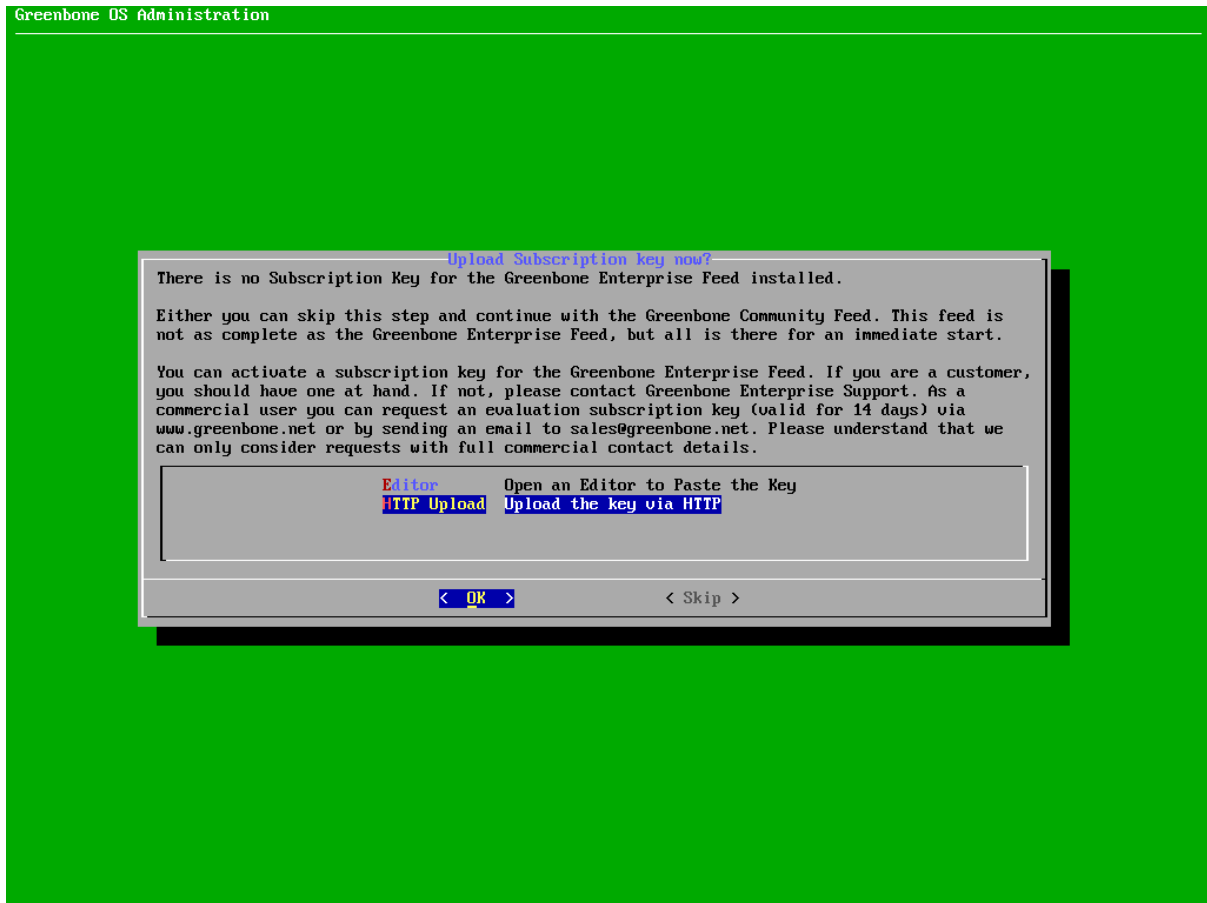
Ahora, nos solicita un usuario y contraseña de administración. Lo introducimos y pulsamos OK:



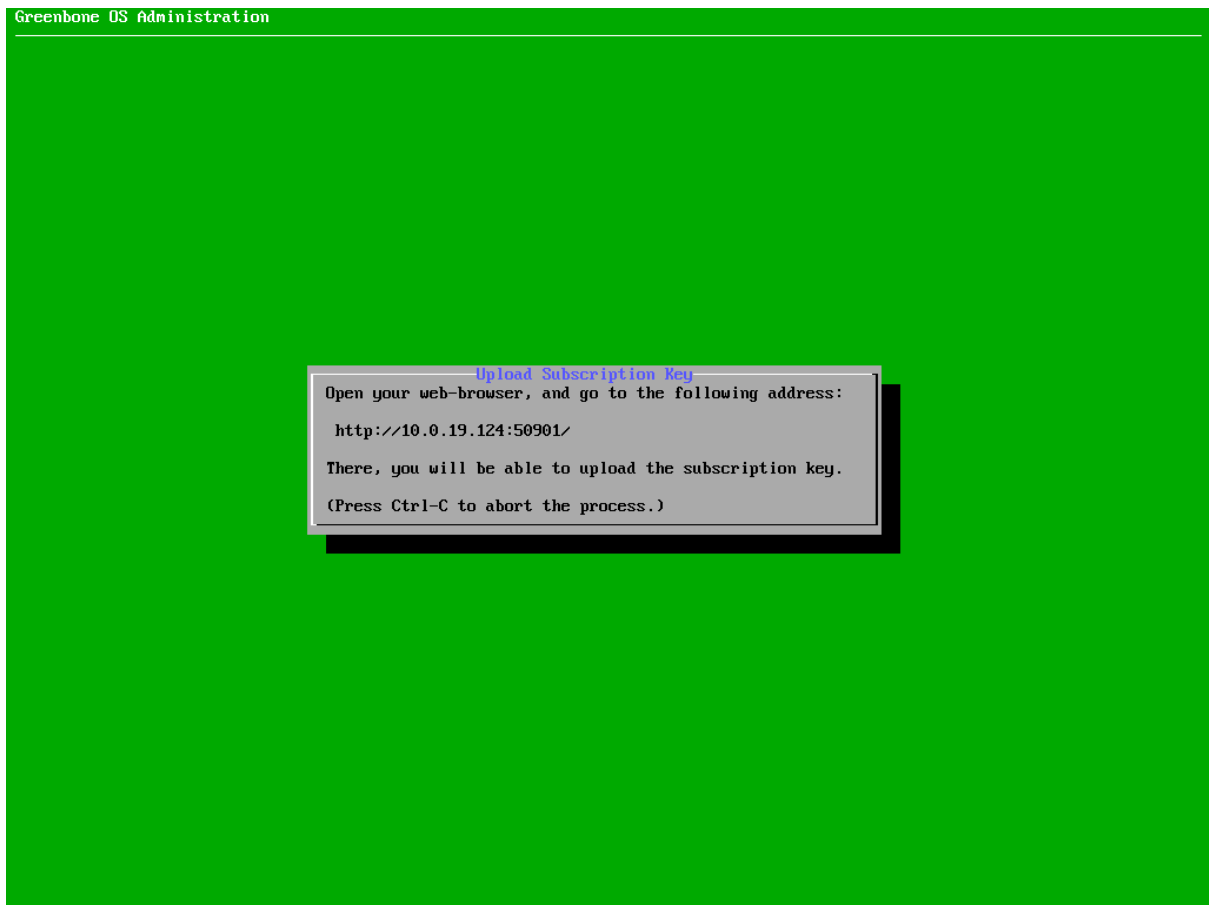
Nos indica que ha creado el usuario. Pulsamos OK:



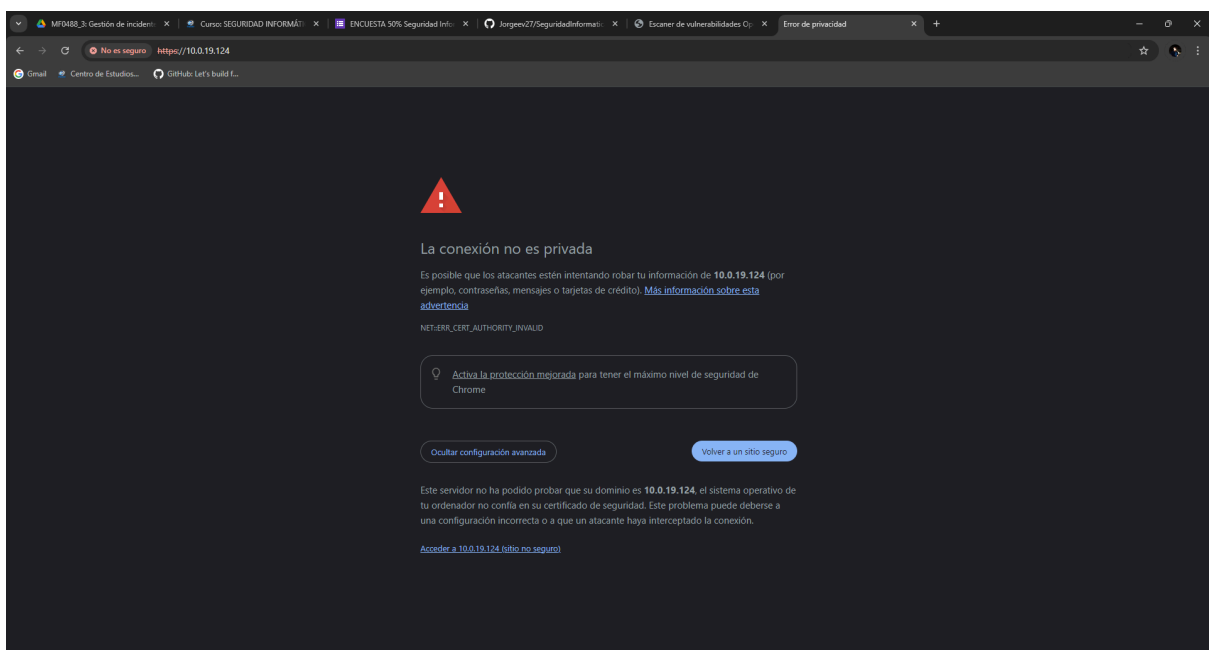
Finalmente, Seleccionamos HTTP Upload y pulsamos OK:



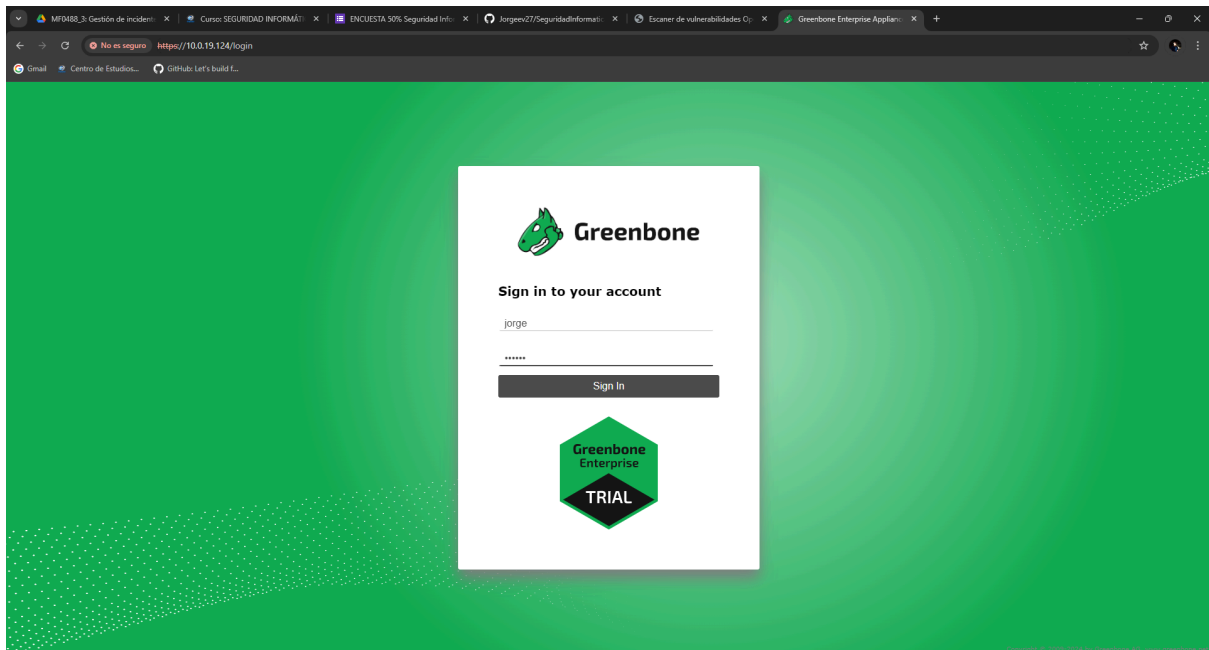
Nos aparece una ventana con la URL y el puerto:



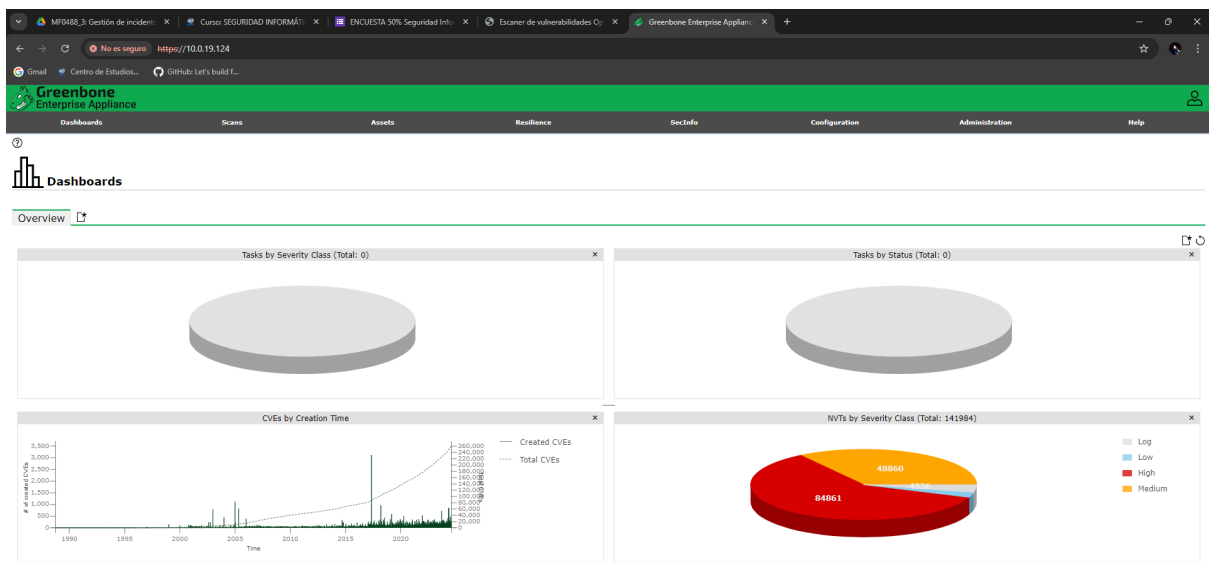
Ahora, arrancamos otra máquina en la red para entrar en el panel de administración. Abrimos un navegador y escribimos la ip de la máquina Greenbone. Pulsamos Avanzado:



Ahora, nos solicita el usuario y contraseña que le indicamos para administrar.
Lo introducimos y puldamos Sign In:



Aparece el panel de administración:

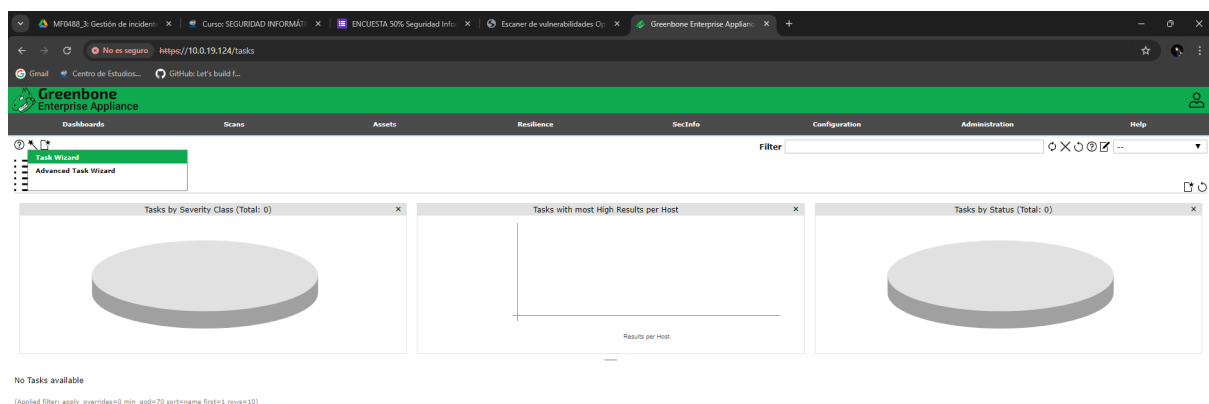


Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

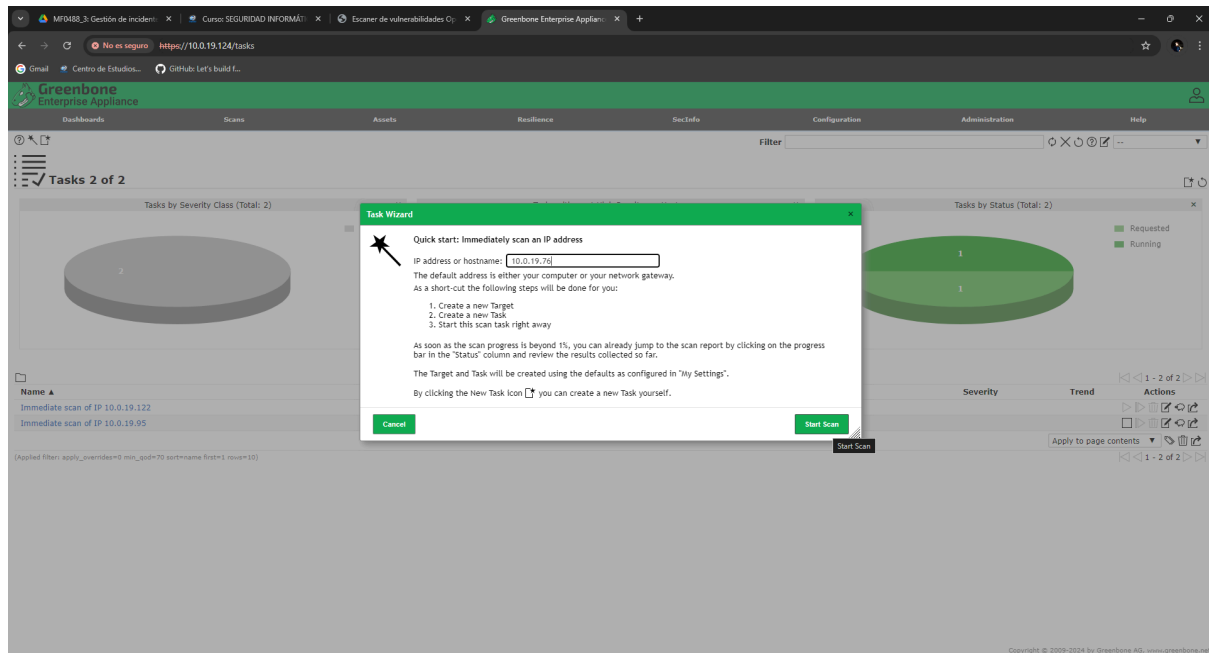
2. Ejecutar escaneo de vulnerabilidades sobre la máquina Metasploitable2 y Metasploitable3

METASPLOITABLE2:

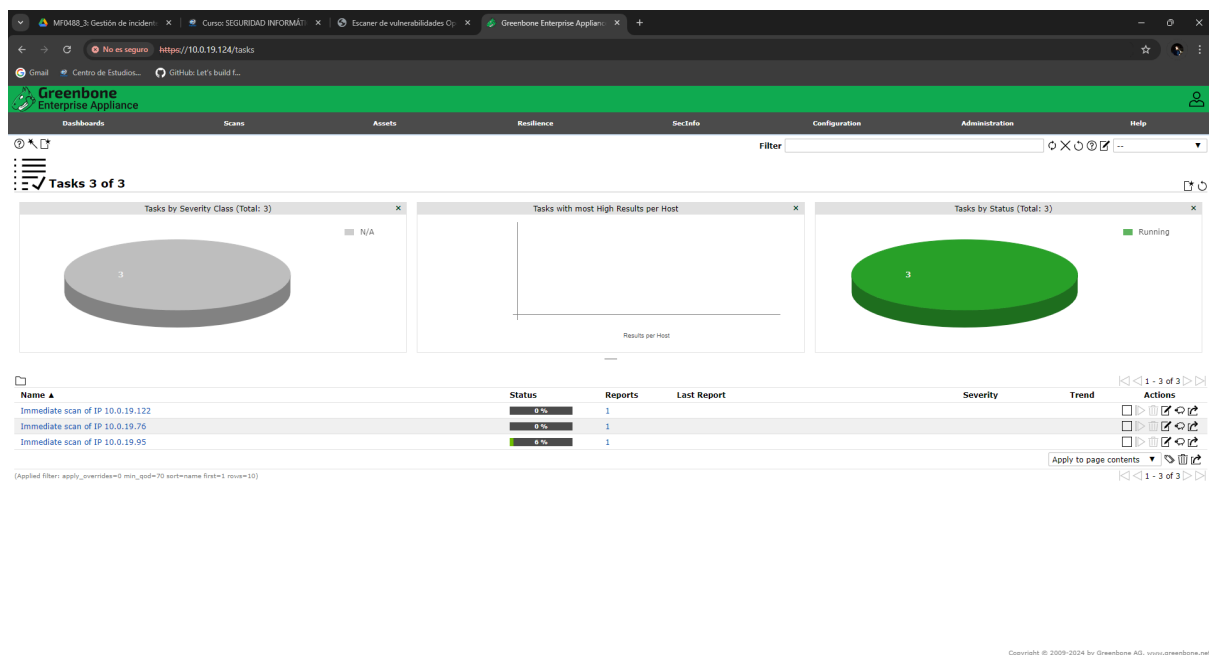
Vamos a arrancar la máquina Metasploitable2. Obtenemos su ip. Vamos a realizar el escaneo de vulnerabilidades. Para ello, pulsamos en la pestaña Scans. Pulsamos sobre el icono Task Wizard:



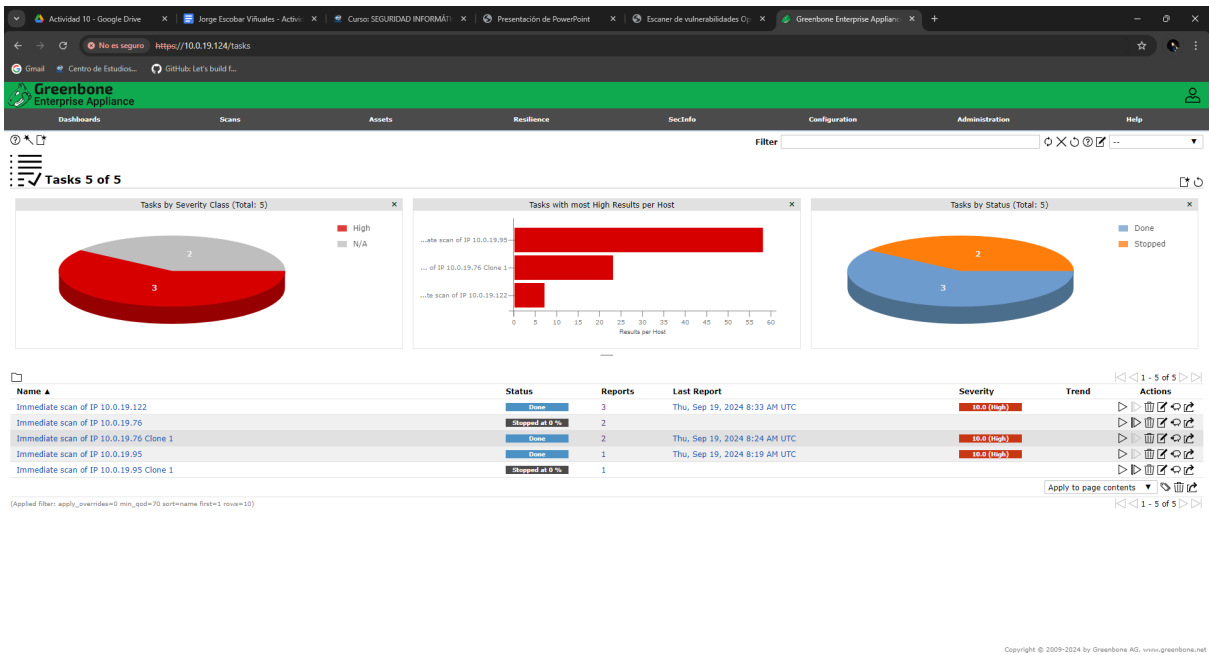
Escribimos la Ip de la máquina Metasploitable2 y pulsamos Start Scan:



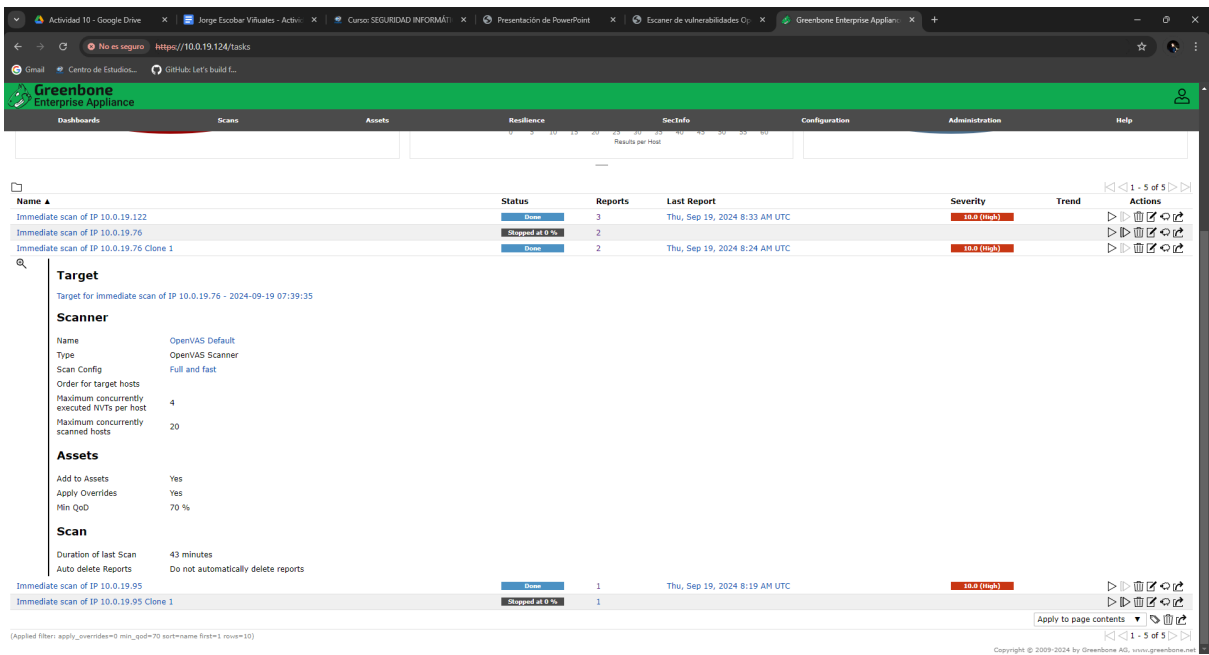
Comienza el escaneo de vulnerabilidades del sitio Web:



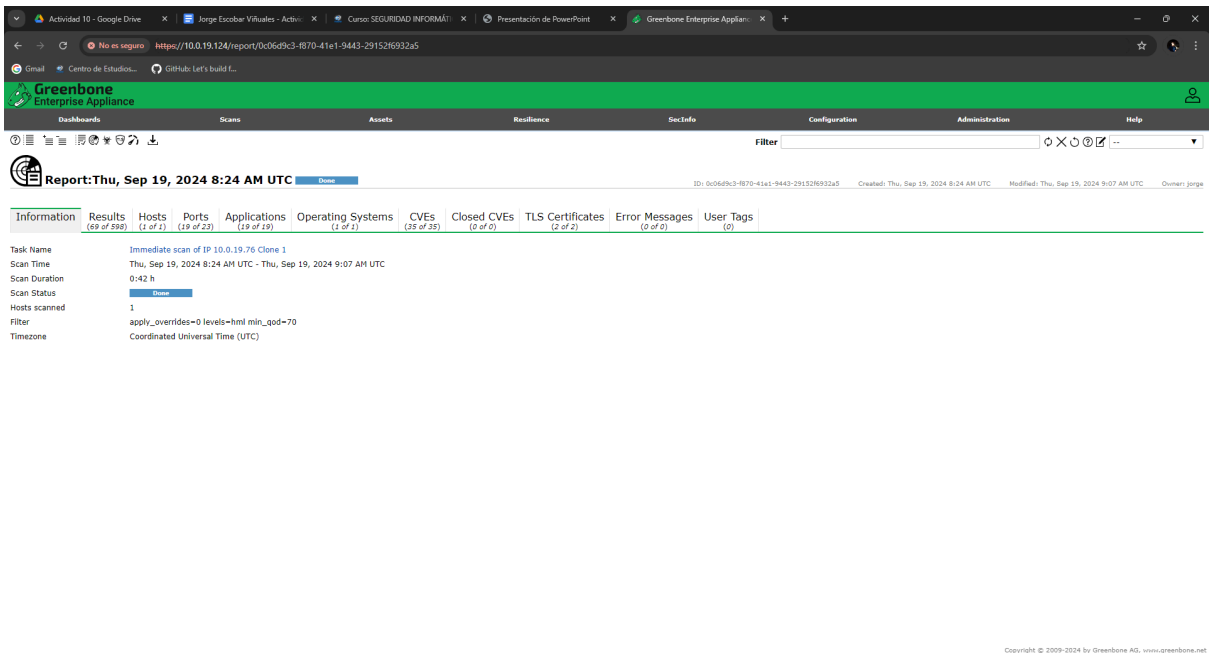
Una vez finalizado, nos muestra gráficamente el resultado:



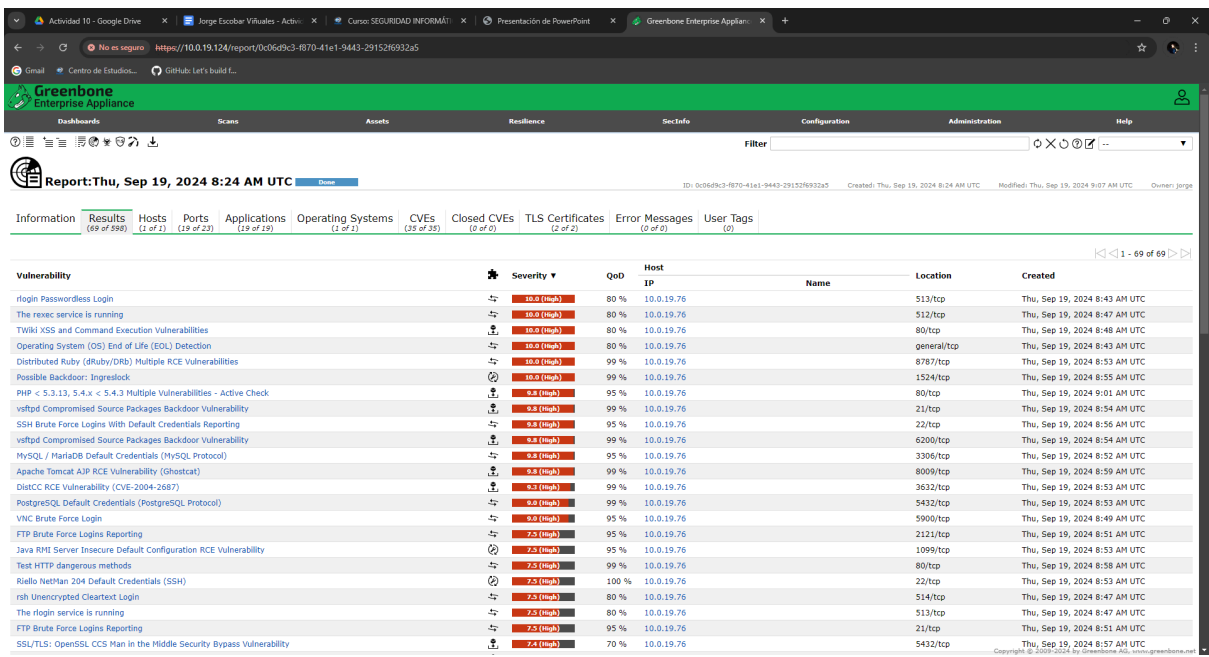
Si pulsamos en el apartado Name, nos muestra los datos generales del escaneo:



Si pulsamos en el apartado Last Report nos muestra el resultado del análisis:



En cada una de las pestañas, nos muestra información detallada:



Actividad 10 - Google Drivejorge Escobar Viñuales - Actividad 10Curso SEGURIDAD INFORMÁTICAPresentación de PowerPointGreenbone Enterprise Appliance

No es segurohttps://10.0.19.124/report/0c06d9c3-8b70-41e1-9443-29152f6932a5

Centro de Estudios...GitHub: Let's build...

GreenboneEnterprise Appliance

DashboardsScansAssetsResilienceSecInfoConfigurationAdministrationHelp

Report:Thu, Sep 19, 2024 8:24 AM UTCDone

ID: 0c06d9c3-8b70-41e1-9443-29152f6932a5Created: Thu, Sep 19, 2024 8:24 AM UTCModified: Thu, Sep 19, 2024 9:07 AM UTCOwner: jorge

InformationResults(69 of 598)Hosts(1 of 1)Ports(19 of 23)Applications(19 of 19)Operating Systems(1 of 1)CVEs(35 of 35)Closed CVEs(0 of 0)TLS Certificates(2 of 2)Error Messages(0 of 0)User Tags(0)

Port	Hosts	Severity
513/tcp	1	10.0 (high)
1524/tcp	1	10.0 (high)
512/tcp	1	10.0 (high)
8787/tcp	1	10.0 (high)
80/tcp	1	10.0 (high)
6300/tcp	1	9.8 (high)
22/tcp	1	9.8 (high)
21/tcp	1	9.8 (high)
8009/tcp	1	9.8 (high)
3306/tcp	1	9.8 (high)
3632/tcp	1	9.3 (high)
5900/tcp	1	9.0 (high)
5432/tcp	1	9.0 (high)
2121/tcp	1	7.5 (high)
514/tcp	1	7.5 (high)
1099/tcp	1	7.5 (high)
25/tcp	1	6.0 (medium)
445/tcp	1	6.0 (medium)
23/tcp	1	4.8 (medium)

[Applied filter: apply_overrides=0 levels=html rows=100 min_age=70 first=1 sort=reverse=severity]

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

Actividad 10 - Google Drivejorge Escobar Viñuales - Actividad 10Curso SEGURIDAD INFORMÁTICAPresentación de PowerPointGreenbone Enterprise Appliance

No es segurohttps://10.0.19.124/report/0c06d9c3-8b70-41e1-9443-29152f6932a5

Centro de Estudios...GitHub: Let's build...

GreenboneEnterprise Appliance

DashboardsScansAssetsResilienceSecInfoConfigurationAdministrationHelp

Report:Thu, Sep 19, 2024 8:24 AM UTCDone

ID: 0c06d9c3-8b70-41e1-9443-29152f6932a5Created: Thu, Sep 19, 2024 8:24 AM UTCModified: Thu, Sep 19, 2024 9:07 AM UTCOwner: jorge

InformationResults(69 of 598)Hosts(1 of 1)Ports(19 of 23)Applications(19 of 19)Operating Systems(1 of 1)CVEs(35 of 35)Closed CVEs(0 of 0)TLS Certificates(2 of 2)Error Messages(0 of 0)User Tags(0)

IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity
10.0.19.76		🟡	19	19		🟢	Thu, Sep 19, 2024 8:25 AM UTC	Thu, Sep 19, 2024 9:07 AM UTC	23	40	6	0	0	69	10.0 (high)

[Applied filter: apply_overrides=0 levels=html rows=100 min_age=70 first=1 sort=reverse=severity]

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

Actividad 10 - Google Drivejorge Escobar Viñuales - Actividad 10Curso SEGURIDAD INFORMÁTICAPresentación de PowerPointGreenbone Enterprise Appliance

https://10.0.19.124/report/0c06d9c3-8b70-41e1-9443-291526932a5

Centro de Estudios...GitHub: Let's build f...

Greenbone Enterprise Appliance

DashboardScansAssetsResilienceSecInfoConfigurationAdministrationHelp

Filter

Report:Thu, Sep 19, 2024 8:24 AM UTCDone

ID: 0c06d9c3-8b70-41e1-9443-291526932a5Created: Thu, Sep 19, 2024 8:24 AM UTCModified: Thu, Sep 19, 2024 9:07 AM UTCOwner: jorge

InformationResults (69 of 598)Hosts (1 of 1)Ports (19 of 23)Applications (19 of 19)Operating Systems (1 of 1)CVEs (25 of 35)Closed CVEs (0 of 0)TLS Certificates (2 of 2)Error Messages (0 of 0)User Tags (0)

Operating System	CPE	Hosts	Severity
Ubuntu 8.04	cpe:/o:canonical:ubuntu_linux:8.04	1	10.0 (high)

(Applied filter: apply_overrides=0 levels=html rows=100 min_age=70 first=1 sort=reverse=severity)

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

Actividad 10 - Google Drivejorge Escobar Viñuales - Actividad 10Curso SEGURIDAD INFORMÁTICAPresentación de PowerPointGreenbone Enterprise Appliance

https://10.0.19.124/report/0c06d9c3-8b70-41e1-9443-291526932a5

Centro de Estudios...GitHub: Let's build f...

Greenbone Enterprise Appliance

DashboardScansAssetsResilienceSecInfoConfigurationAdministrationHelp

Filter

Report:Thu, Sep 19, 2024 8:24 AM UTCDone

ID: 0c06d9c3-8b70-41e1-9443-291526932a5Created: Thu, Sep 19, 2024 8:24 AM UTCModified: Thu, Sep 19, 2024 9:07 AM UTCOwner: jorge

InformationResults (69 of 598)Hosts (1 of 1)Ports (19 of 23)Applications (19 of 19)Operating Systems (1 of 1)CVEs (25 of 35)Closed CVEs (0 of 0)TLS Certificates (2 of 2)Error Messages (0 of 0)User Tags (0)

Application CPE	Hosts	Occurrences	Severity
cpe:/a:beats:vsftpd:2.3.4	1	1	9.8 (high)
cpe:/a:mysql:mysql:5.0.51a	1	1	9.8 (high)
cpe:/a:postgresql:postgresql:8.3.1	1	1	9.8 (high)
cpe:/a:samba:samba:3.0.20	1	1	9.0 (Medium)
cpe:/a:ietf:transport_layer_security:1.0	1	2	5.9 (Medium)
cpe:/a:apache:http_server:2.2.8	1	1	4.3 (Medium)
cpe:/a:ietf:secure_sockets_layer:3.0	1	2	N/A
cpe:/a:proftpd:proftpd:1.3.1	1	1	N/A
cpe:/a:jquery:jquery:1.3.2	1	1	N/A
cpe:/a:oracle:mysql:5.0.51a	1	1	N/A
cpe:/a:openbsd:openssh:4.7p1	1	1	N/A
cpe:/a:ietf:secure_shell_protocol:2.0	1	1	N/A
cpe:/a:portmap:portmap	1	1	N/A
cpe:/a:php:php:5.2.4	1	1	N/A
cpe:/a:isc:bind:9.4.2	1	1	N/A
cpe:/a:ietf:secure_sockets_layer:2.0	1	1	N/A
cpe:/a:twiki:twiki:01_Feb.2003	1	1	N/A
cpe:/a:postfix:postfix	1	1	N/A
cpe:/a:phpmyadmin:phpmyadmin:3.1.1	1	1	N/A

(Applied filter: apply_overrides=0 levels=html rows=100 min_age=70 first=1 sort=reverse=severity)

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

Actividad 10 - Google Drivejorge Escobar Viñuales - Actividad 10Curso SEGURIDAD INFORMÁTICAPresentación de PowerPointGreenbone Enterprise Appliance

Report: Thu, Sep 19, 2024 8:24 AM UTC

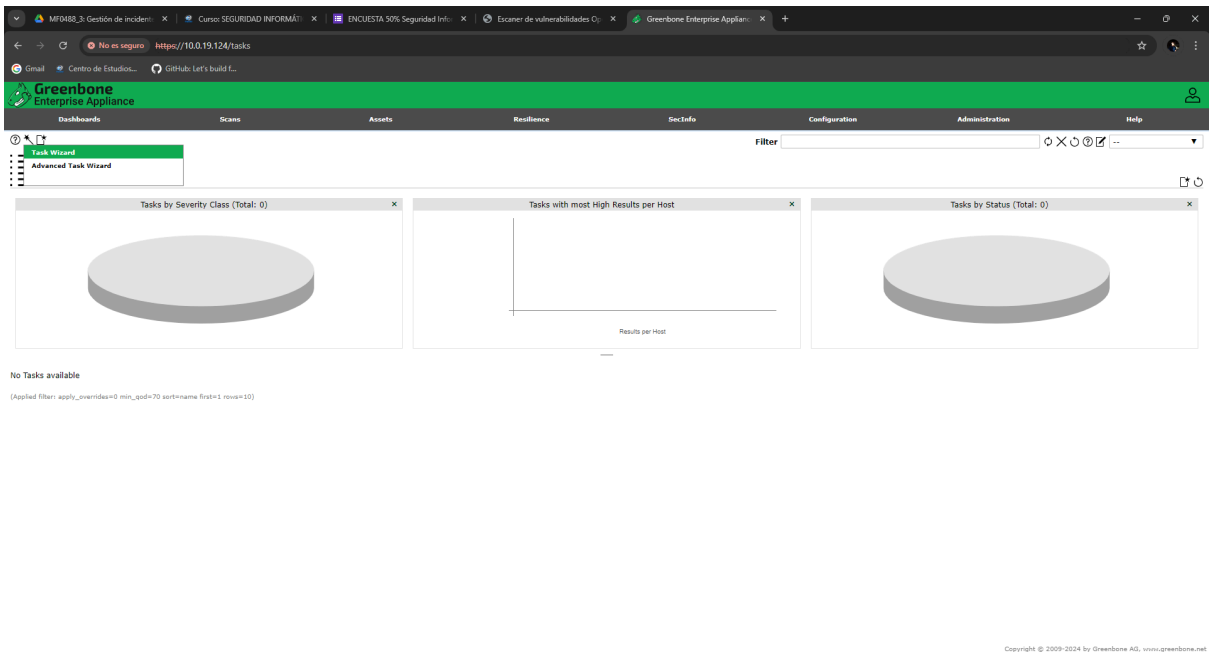
InformationResults (69 of 598)Hosts (1 of 1)Ports (19 of 23)Applications (19 of 19)Operating Systems (1 of 1)CVES (39 of 39)Closed CVEs (0 of 0)TLS Certificates (2 of 2)Error Messages (0 of 0)User Tags (0)

CVE	NVT	Hosts	Occurrences	Severity
CVE-1999-0618	The rexec service is running	1	1	10.0 (high)
CVE-2008-5304 CVE-2008-5305	TIWiki XSS and Command Execution Vulnerabilities	1	1	10.0 (high)
CVE-2012-1823 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335	PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check	1	1	9.8 (high)
CVE-2011-2523	vsftpd Compromised Source Packages Backdoor Vulnerability	1	2	9.8 (high)
CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508 CVE-2020-9473 CVE-2023-1844 CVE-2024-22903 CVE-2024-31970	SSH Brute Force Logins With Default Credentials Reporting	1	1	9.8 (high)
CVE-2001-0645 CVE-2004-2357 CVE-2006-1451 CVE-2007-2554 CVE-2007-6081 CVE-2009-0919 CVE-2014-3419 CVE-2015-4669 CVE-2016-6531	MySQL / MariaDB Default Credentials (MySQL Protocol)	1	1	9.8 (high)
CVE-2020-1938	Apache Tomcat AJP RCE Vulnerability (Ghostcat)	1	1	9.8 (high)
CVE-2004-2687	DistCC RCE Vulnerability (CVE-2004-2687)	1	1	9.3 (high)
CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508 CVE-2001-1594 CVE-2013-7404 CVE-2017-8218 CVE-2018-19063	FTP Brute Force Logins Reporting	1	2	7.5 (high)
CVE-2018-19064	Java RMI Server Insecure Default Configuration RCE Vulnerability	1	1	7.5 (high)
CVE-2011-3556	rsh Unencrypted Cleartext Login	1	1	7.5 (high)
CVE-1999-0651	The rlogin service is running	1	1	7.5 (high)
CVE-2014-0224	SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	1	1	7.4 (high)
CVE-2009-4898	TIWiki Cross-Site Request Forgery Vulnerability (Sep 2010)	1	1	6.8 (medium)
CVE-2011-0411 CVE-2011-1430 CVE-2011-1431 CVE-2011-1432 CVE-2011-1506 CVE-2011-1575 CVE-2011-1926 CVE-2011-2165	Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection V...	1	1	6.8 (medium)
CVE-1999-0497	Anonymous FTP Login Reporting	1	1	6.4 (medium)
CVE-2018-20212	TIWiki < 6.1.0 XSS Vulnerability	1	1	6.1 (medium)
CVE-2012-6708	JQuery < 1.9.0 XSS Vulnerability	1	1	6.1 (medium)
CVE-2007-2447	Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check	1	1	6.0 (medium)
CVE-2009-1339	TIWiki CSRF Vulnerability	1	1	6.0 (medium)
CVE-2013-2566 CVE-2015-2808 CVE-2015-4000	SSL/TLS: Report Weak Cipher Suites	1	1	5.8 (medium)
CVE-2016-0800 CVE-2014-3566	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	1	2	5.8 (medium)
CVE-2003-1567 CVE-2004-2320 CVE-2004-2763 CVE-2005-3398 CVE-2006-4683 CVE-2007-3008 CVE-2008-7253 CVE-2009-2823 CVE-2010-0386	HTTP Debugging Methods (TRACE/TRACK) Enabled	1	1	5.8 (medium)
CVE-2012-2223 CVE-2014-7883				

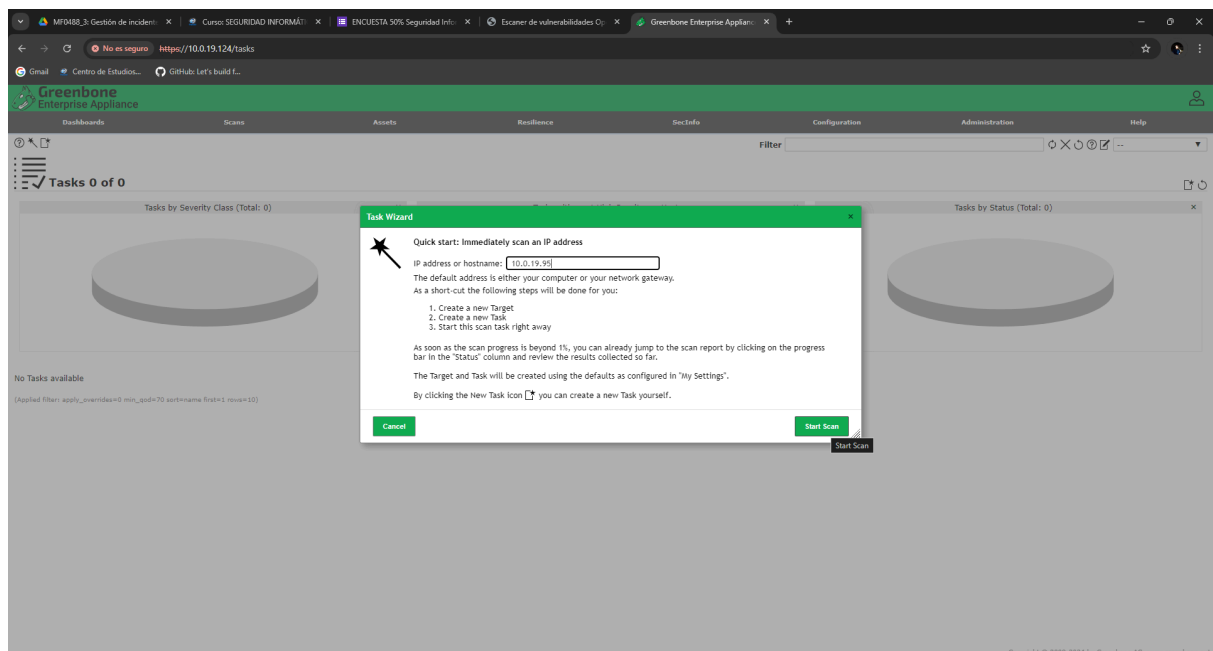
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

METASPLOITABLE3 WINDOWS:

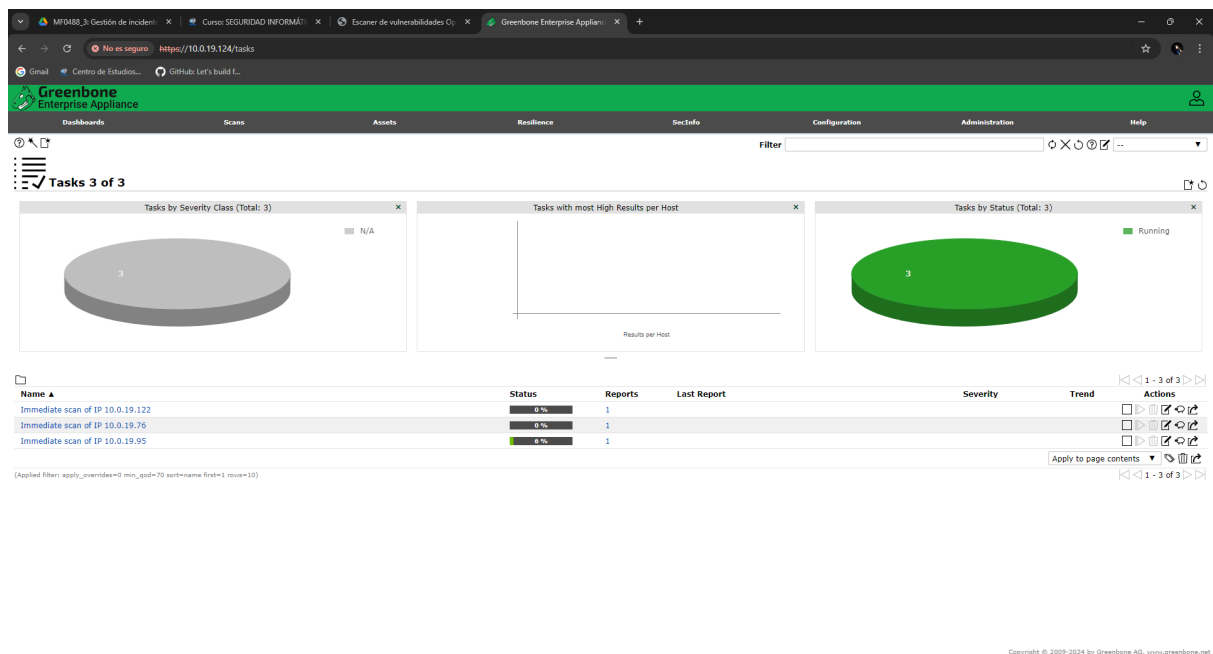
Vamos a arrancar la máquina Metasploitable3 Windows. Obtenemos su ip. Vamos a realizar el escaneo de vulnerabilidades. Para ello, pulsamos en la pestaña Scans. Pulsamos sobre el icono Task Wizard:



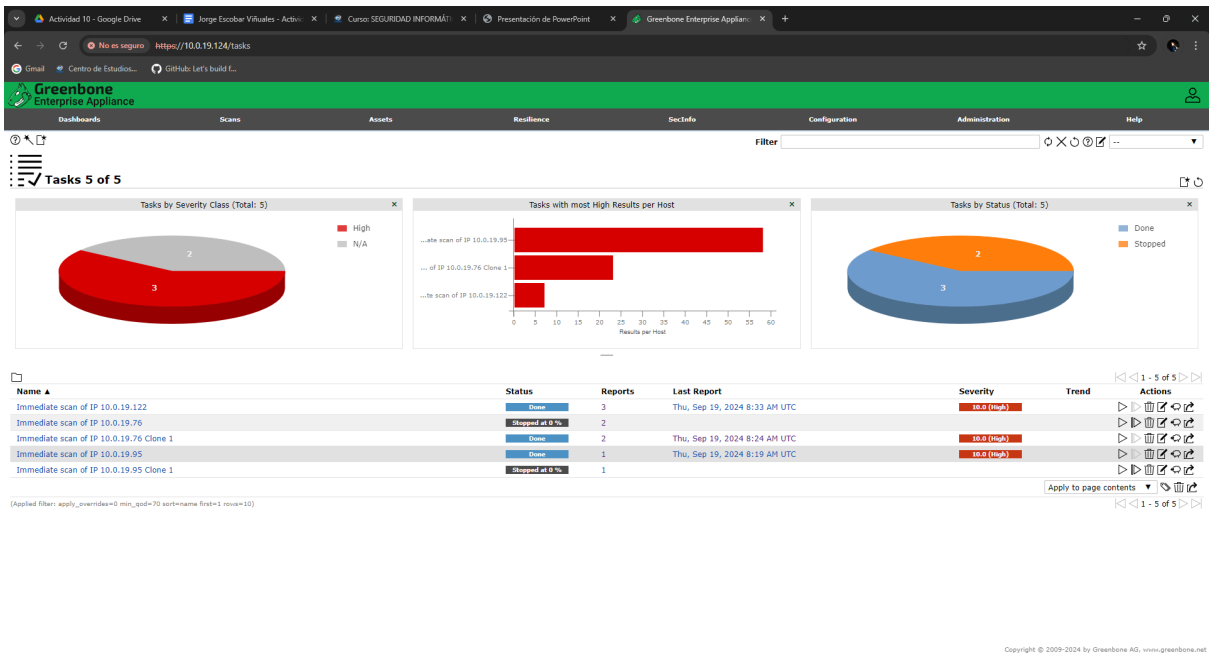
Escribimos la Ip de la máquina Metasploitable3 Ubuntu y pulsamos Start Scan:



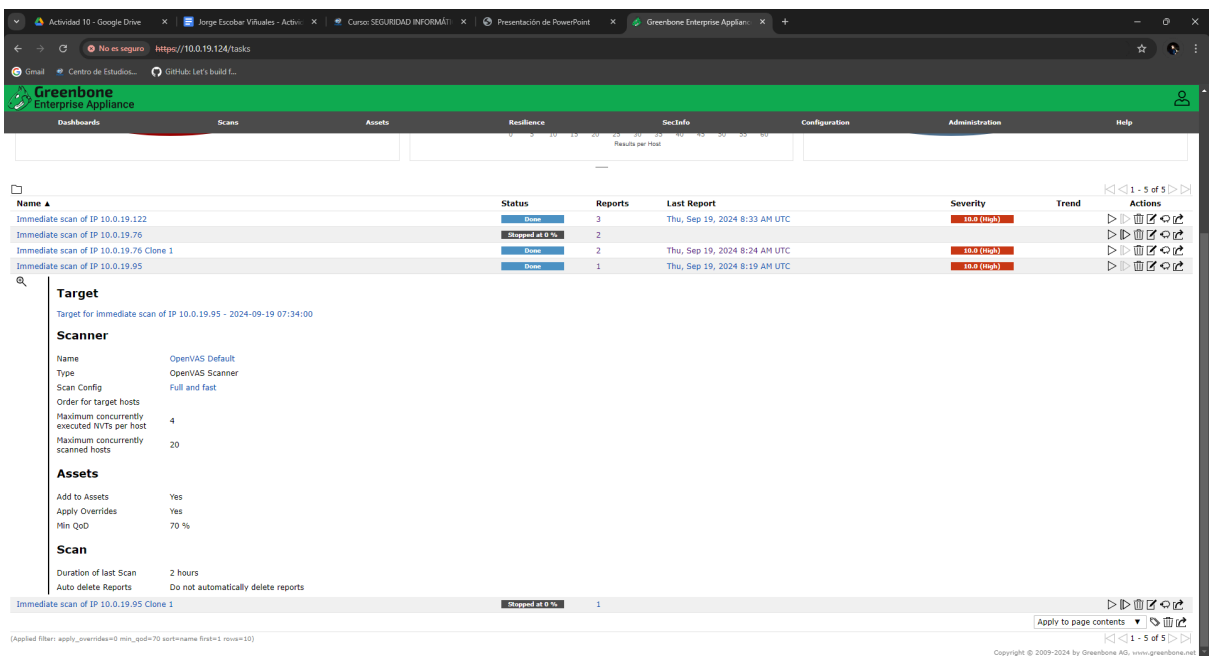
Comienza el escaneo de vulnerabilidades del sitio Web:



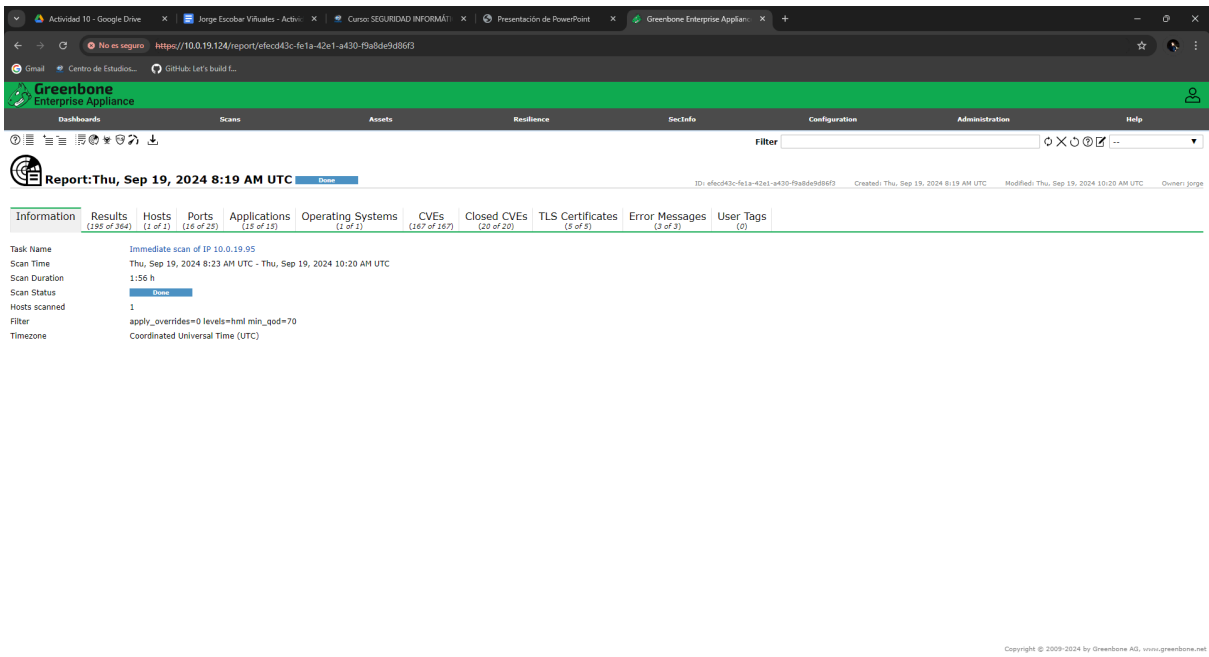
Una vez finalizado, nos muestra gráficamente el resultado:



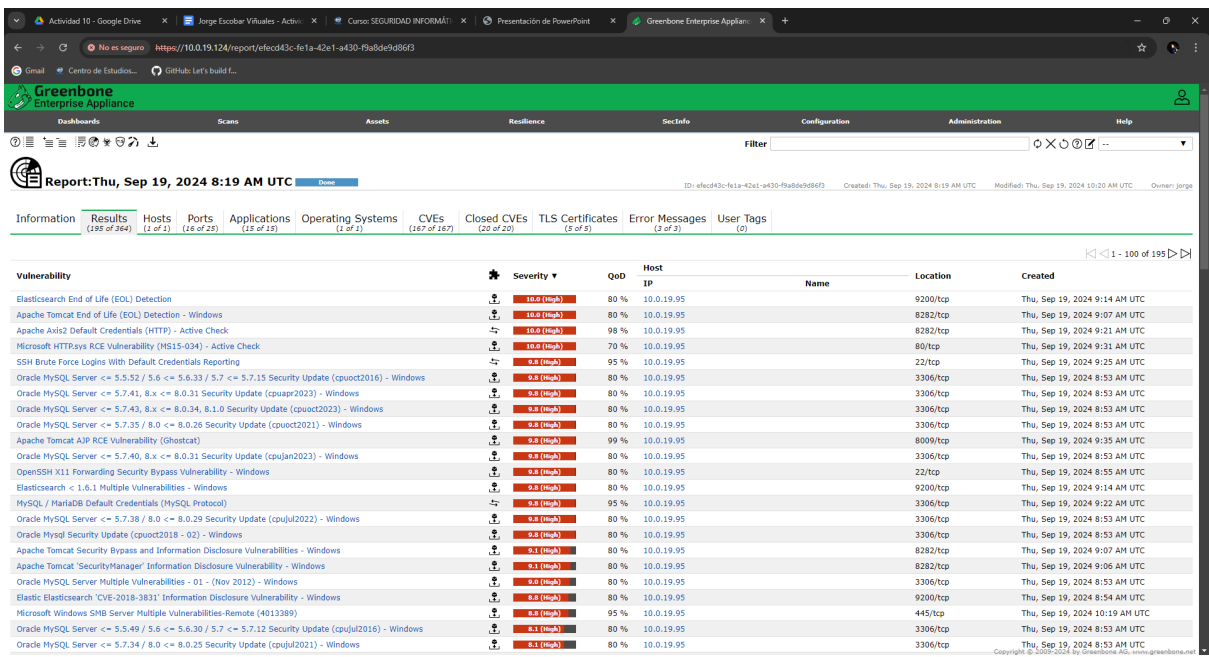
Si pulsamos en el apartado Name, nos muestra los datos generales del escaneo:



Si pulsamos en el apartado Last Report nos muestra el resultado del análisis:



En cada una de las pestañas, nos muestra información detallada:



Actividad 10 - Google Drivejorge Escobar Viñuales - Actividad 10Curso SEGURIDAD INFORMÁTICAPresentación de PowerPointGreenbone Enterprise Appliance

Report:Thu, Sep 19, 2024 8:19 AM UTC

InformationResults (188 of 364)Hosts (1 of 1)Ports (16 of 16)Applications (15 of 15)Operating Systems (1 of 1)CVEs (167 of 267)Closed CVEs (20 of 20)TLS Certificates (3 of 3)Error Messages (3 of 3)User Tags (0)

Port	Hosts	Severity
80/tcp	1	10.0 (High)
9200/tcp	1	10.0 (High)
8282/tcp	1	10.0 (High)
8009/tcp	1	8.8 (High)
22/tcp	1	8.8 (High)
3306/tcp	1	8.8 (High)
445/tcp	1	8.8 (High)
1617/tcp	1	7.5 (High)
8383/tcp	1	7.5 (High)
21/tcp	1	7.5 (High)
3389/tcp	1	5.9 (Medium)
3820/tcp	1	5.8 (Medium)
4848/tcp	1	5.8 (Medium)
135/tcp	1	5.8 (Medium)
8181/tcp	1	5.8 (Medium)
3920/tcp	1	4.3 (Medium)

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

Actividad 10 - Google Drivejorge Escobar Viñuales - Actividad 10Curso SEGURIDAD INFORMÁTICAPresentación de PowerPointGreenbone Enterprise Appliance

Report:Thu, Sep 19, 2024 8:19 AM UTC

InformationResults (188 of 364)Hosts (1 of 1)Ports (16 of 16)Applications (15 of 15)Operating Systems (1 of 1)CVEs (167 of 267)Closed CVEs (20 of 20)TLS Certificates (3 of 3)Error Messages (3 of 3)User Tags (0)

IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity
10.0.19.95		Linux	16	15			Thu, Sep 19, 2024 8:24 AM UTC	Thu, Sep 19, 2024 10:20 AM UTC	58	124	13	0	0	195	10.0 (High)

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

Actividad 10 - Google Drive

Jorge Escobar Viñuales - Activi...

Curso SEGURIDAD INFORMÁTICA

Presentación de PowerPoint

Greenbone Enterprise Appli...

No es seguro

https://10.0.19.124/report/efec43c-fe1a-42e1-a430-f9a8de9d86f3

Gmail

Centro de Estudios...

GitHub: Let's build f...

Greenbone

Enterprise Appliance

Dashboards

Scans

Assets

Resilience

SecInfo

Configuration

Administration

Help

Filter

Report:Thu, Sep 19, 2024 8:19 AM UTC

Done

ID: efec43c-fe1a-42e1-a430-f9a8de9d86f3

Created: Thu, Sep 19, 2024 8:19 AM UTC

Modified: Thu, Sep 19, 2024 10:20 AM UTC

Owner: jorge

Information

Results

(195 of 364)

Hosts

(1 of 1)

Ports

(16 of 25)

Applications

(15 of 19)

Operating Systems

(1 of 1)

CVEs

(167 of 167)

Closed CVEs

(20 of 20)

TLS Certificates

(5 of 5)

Error Messages

(3 of 3)

User Tags

(0)

Operating System

CPE

Hosts

Severity

Microsoft Windows

cpe:/o:microsoft:windows

1

10.0 (High)

(Applied filter: apply_overrides=0 levels=html rows=100 min_col=70 first=1 sort=reverse=severity)

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

Actividad 10 - Google Drive

Jorge Escobar Viñuales - Activi...

Curso SEGURIDAD INFORMÁTICA

Presentación de PowerPoint

Greenbone Enterprise Appli...

No es seguro

https://10.0.19.124/report/efec43c-fe1a-42e1-a430-f9a8de9d86f3

Gmail

Centro de Estudios...

GitHub: Let's build f...

Greenbone

Enterprise Appliance

Dashboards

Scans

Assets

Resilience

SecInfo

Configuration

Administration

Help

Filter

Report:Thu, Sep 19, 2024 8:19 AM UTC

Done

ID: efec43c-fe1a-42e1-a430-f9a8de9d86f3

Created: Thu, Sep 19, 2024 8:19 AM UTC

Modified: Thu, Sep 19, 2024 10:20 AM UTC

Owner: jorge

Information

Results

(195 of 364)

Hosts

(1 of 1)

Ports

(16 of 25)

Applications

(15 of 19)

Operating Systems

(1 of 1)

CVEs

(167 of 167)

Closed CVEs

(20 of 20)

TLS Certificates

(5 of 5)

Error Messages

(3 of 3)

User Tags

(0)

Application CPE

Hosts

Occurrences

Severity

cpe:/a:apache:tomcat:8.0.33

1

1

10.0 (High)

cpe:/a:microsoft:internet_information_services:7.5

1

1

10.0 (High)

cpe:/a:openssh:openssh:7.1

1

1

9.8 (High)

cpe:/a:mysql:mysql:5.5.20-log

1

1

9.8 (High)

cpe:/a:ietf:transport_layer_security:1.0

1

5

4.3 (Medium)

cpe:/a:ietf:transport_layer_security:1.1

1

5

4.3 (Medium)

cpe:/a:ietf:secure_shell_protocol:2.0

1

1

N/A

cpe:/a:elastic:logstash:1.1.1

1

1

N/A

cpe:/a:microsoft:ftp_service

1

1

N/A

cpe:/a:elasticsearch:logstash:1.1.1

1

1

N/A

cpe:/a:elastic:elasticsearch:1.1.1

1

1

N/A

cpe:/a:elasticsearch:elasticsearch:1.1.1

1

1

N/A

cpe:/a:ietf:transport_layer_security:1.2

1

5

N/A

cpe:/a:apache:axis2:1.6.0

1

1

N/A

cpe:/a:oracle:mysql:5.5.20

1

1

N/A

(Applied filter: apply_overrides=0 levels=html rows=100 min_col=70 first=1 sort=reverse=severity)

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

Greenbone Enterprise Appliance

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

Report: Thu, Sep 19, 2024 8:19 AM UTC

ID: efcd43c-fe1a-42e1-a430-PbaDedR8fQ Created: Thu, Sep 19, 2024 8:19 AM UTC Modified: Thu, Sep 19, 2024 10:20 AM UTC Owner: jorge

CVE	NVT	Hosts 1 of 1	Occurrences 1	Severity ▼ <div style="width: 100%;"></div>
CVE-2010-0219	Apache Axis2 Default Credentials (HTTP) - Active Check	1	1	10.0 (High)
CVE-2015-1835	Microsoft HTTP.sys RCE Vulnerability (MS15-034) - Active Check	1	1	10.0 (High)
CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508 CVE-2020-0473 CVE-2023-1944 CVE-2024-22902 CVE-2024-31970	SSM Brute Force Logins With Default Credentials Reporting	1	1	10.0 (High)
CVE-2016-5584 CVE-2016-6662 CVE-2016-7440	Oracle MySQL Server <= 5.5.52 / 5.6 <> 5.6.33 / 5.7 <> 5.7.15 Security Update (...)	1	1	9.8 (High)
CVE-2022-37434	Oracle MySQL Server <= 5.7.41, 8.x <> 8.0.31 Security Update (cpuot2023) - Win...	1	1	9.8 (High)
CVE-2023-38545 CVE-2023-22084 CVE-2023-38546	Oracle MySQL Server <= 5.7.43, 8.x <> 8.0.34, 8.1.0 Security Update (cpuoct2023) - ...	1	1	9.8 (High)
CVE-2021-3711 CVE-2021-22925 CVE-2021-35604 CVE-2021-35624 CVE-2021-22922 CVE-2021-22923 CVE-2021-22924 CVE-2021-22925	Oracle MySQL Server <= 5.7.35 / 8.0 <> 8.0.26 Security Update (cpuoct2021) - Win...	1	1	9.8 (High)
CVE-2021-22945 CVE-2021-22946 CVE-2021-22947 CVE-2021-3712	Apache Tomcat AJP RCE Vulnerability (GHOSTcat)	1	1	9.8 (High)
CVE-2020-1938	Oracle MySQL Server <= 5.7.40, 8.x <> 8.0.31 Security Update (cpujan2023) - Win...	1	1	9.8 (High)
CVE-2022-32221 CVE-2022-35260 CVE-2022-42915 CVE-2022-42916	OpenSSH X11 Forwarding Security Bypass Vulnerability - Windows	1	1	9.8 (High)
CVE-2016-1908	Elasticsearch < 1.6.1 Multiple Vulnerabilities - Windows	1	1	9.8 (High)
CVE-2015-5531 CVE-2015-5377	MySQL / MariaDB Default Credentials (MySQL Protocol)	1	1	9.8 (High)
CVE-2001-0645 CVE-2004-2357 CVE-2006-1451 CVE-2007-2554 CVE-2007-6081 CVE-2009-0919 CVE-2014-3419 CVE-2015-4669 CVE-2016-6531	Oracle MySQL Server <= 5.7.38 / 8.0 <> 8.0.29 Security Update (cpujul2022) - Win...	1	1	9.8 (High)
CVE-2018-15719	Oracle Mysal Security Update (cpuo2018 - 02) - Windows	1	1	9.8 (High)
CVE-2022-1292 CVE-2022-27778 CVE-2018-25032 CVE-2022-21515	Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities - Windo...	1	1	9.1 (High)
CVE-2018-3123 CVE-2018-3174 CVE-2018-3282 CVE-2016-9843 CVE-2016-9840 CVE-2016-9841 CVE-2016-9842	Apache Tomcat "SecurityManager" Information Disclosure Vulnerability - Windows	1	1	9.1 (High)
CVE-2016-6794 CVE-2016-0762 CVE-2016-5018 CVE-2016-6796 CVE-2016-6797	Oracle MySQL Server Multiple Vulnerabilities - 01 (Nov 2012) - Windows	1	1	9.1 (High)
CVE-2017-5648	Elastic Elasticsearch CVE-2018-3831 Information Disclosure Vulnerability - Win...	1	1	9.1 (High)
CVE-2012-3107 CVE-2012-3163 CVE-2012-3158 CVE-2012-3150	Microsoft Windows SMB Server Multiple Vulnerabilities.Remote (4013298)	1	1	9.1 (High)
CVE-2018-3831	Oracle MySQL Server <= 5.5.49 / 5.6 <> 5.6.30 / 5.7 <> 5.7.12 Security Update (...)	1	1	9.1 (High)
CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148	Oracle MySQL Server <= 5.7.34 / 8.0 <> 8.0.25 Security Update (cpujul2021) - Win...	1	1	9.1 (High)
CVE-2016-3477 CVE-2016-3521 CVE-2016-3615 CVE-2016-5440	OpenSSH Multiple Vulnerabilities [Jan 2017] - Windows	1	1	7.7 (High)
CVE-2021-22901 CVE-2019-17543 CVE-2021-2389 CVE-2021-2390 CVE-2021-2356 CVE-2021-2385 CVE-2021-2342 CVE-2021-2372	Oracle Sysad Security Updates (apr2017-3236618) 02 - Windows	1	1	7.7 (High)
CVE-2021-22897 CVE-2021-22898				
CVE-2016-10009 CVE-2016-10010 CVE-2016-10011 CVE-2016-10012 CVE-2016-10708				
CVE-2017-3309 CVE-2017-3308 CVE-2017-3329 CVE-2017-3456 CVE-2017-3453 CVE-2017-3600 CVE-2017-3462 CVE-2017-3463 CVE-2017-3461				
CVE-2017-3462				

< <- | - 100 of 167 > >

Copyright © 2009–2024 Greenbone AG. All rights reserved.

Greenbone Enterprise Appliance

Report: Thu, Sep 19, 2024 8:19 AM UTC

Information	Results (195 of 364)	Hosts (1 of 1)	Ports (16 of 25)	Applications (15 of 15)	Operating Systems (1 of 1)	CVEs (167 of 167)	Closed CVEs (20 of 20)	TLS Certificates (5 of 5)	Error Messages (3 of 3)	User Tags (0)
Subject DN *										
C=US,ST=CA,L=Pleasanton,O=Zoho Corporation,OU=ManageEngine,CN=Desktop Central,EMAIL=support@desktopcentral.com						Serial 00F59CE71E6DB72A5		Activates Wed, Sep 8, 2010 12:24 PM UTC	Expires Sat, Sep 5, 2020 12:24 PM UTC	IP 10.0.19.95
C=US,ST=California,L=Santa Clara,O=Oracle Corporation,OU=GlassFish,CN=localhost						04A9972F		AM UTC Wed, May 15, 2013 5:33 AM UTC	AM UTC Sat, May 13, 2023 5:33 AM UTC	Port 8383
C=US,ST=California,L=Santa Clara,O=Oracle Corporation,OU=GlassFish,CN=localhost						04A9972F		AM UTC Wed, May 15, 2013 5:33 AM UTC	AM UTC Sat, May 13, 2023 5:33 AM UTC	Port 4848
C=US,ST=California,L=Santa Clara,O=Oracle Corporation,OU=GlassFish,CN=localhost						04A9972F		AM UTC Wed, May 15, 2013 5:33 AM UTC	AM UTC Sat, May 13, 2023 5:33 AM UTC	Port 3820
C=US,ST=California,L=Santa Clara,O=Oracle Corporation,OU=GlassFish,CN=localhost						04A9972F		AM UTC Wed, May 15, 2013 5:33 AM UTC	AM UTC Sat, May 13, 2023 5:33 AM UTC	Port 8181
CN=vagrant-2008R2						12D05CAECB8A564006C22BE734B81		UTC Tue, Sep 3, 2024 9:41 AM UTC	UTC Wed, Mar 5, 2025 9:41 AM UTC	Port 3389

(Applied filters: apply_overrides=0 lenvls=chroot=100 min_qps=70 fixnsl=1 sort-reverse=severity)

Actividad 10 - Google Drive x Jorge Escobar Viñuales - Activi... x Curso SEGURIDAD INFORMÁTICA x Presentación de PowerPoint x Greenbone Enterprise Appli... x

No es seguro https://10.0.19.124/report/efec43c-fe1a-42e1-a430-f9a8de9d86f3

Centro de Estudios... GitHub: Let's build...

Greenbone Enterprise Appliance

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

Filter

Report: Thu, Sep 19, 2024 8:19 AM UTC Done

ID: efec43c-fe1a-42e1-a430-f9a8de9d86f3 Created: Thu, Sep 19, 2024 8:19 AM UTC Modified: Thu, Sep 19, 2024 10:20 AM UTC Owner: jorge

Information (185 of 364) Results (1 of 1) Hosts (16 of 25) Ports (15 of 15) Applications (15 of 15) Operating Systems (1 of 1) CVEs (167 of 287) Closed CVEs (20 of 20) TLS Certificates (5 of 5) Error Messages (3 of 3) User Tags (0)

Error Message	Host	Hostname	NVT	Port
NVT timed out after 320 seconds.	10.0.19.95		FCKeditor Detection (HTTP)	general/tcp
NVT timed out after 600 seconds.	10.0.19.95		GNU Bash Environment Variable Handling RCE Vulnerability (Shellshock, HTTB, CVE-2014-6271/CVE-2014-6278) - Active Check	general/tcp
NVT timed out after 900 seconds.	10.0.19.95		Generic HTTP Directory Traversal (Web Root) - Active Check	general/tcp

[Applied filter: apply_overrides=0 level=html rows=100 min_age=70 first=1 sort=reverse=severity]

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

METASPLOITABLE3 UBUNTU:

Vamos a arrancar la máquina Metasploitable3 Ubuntu. Obtenemos su ip.
Vamos a realizar el escaneo de vulnerabilidades. Para ello, pulsamos en la pestaña Scans. Pulsamos sobre el icono Task Wizard:

MRD48_3 Gestión de incident... x Curso SEGURIDAD INFORMÁTICA x ENCUESTA 30% Seguridad Info... x Escaner de vulnerabilidades O... x Greenbone Enterprise Appli... x

No es seguro https://10.0.19.124/tasks

Centro de Estudios... GitHub: Let's build...

Greenbone Enterprise Appliance

Dashboards Scans Assets Resilience SecInfo Configuration Administration Help

Filter

Task Wizard
Advanced Task Wizard

Tasks by Severity Class (Total: 0)

Tasks with most High Results per Host

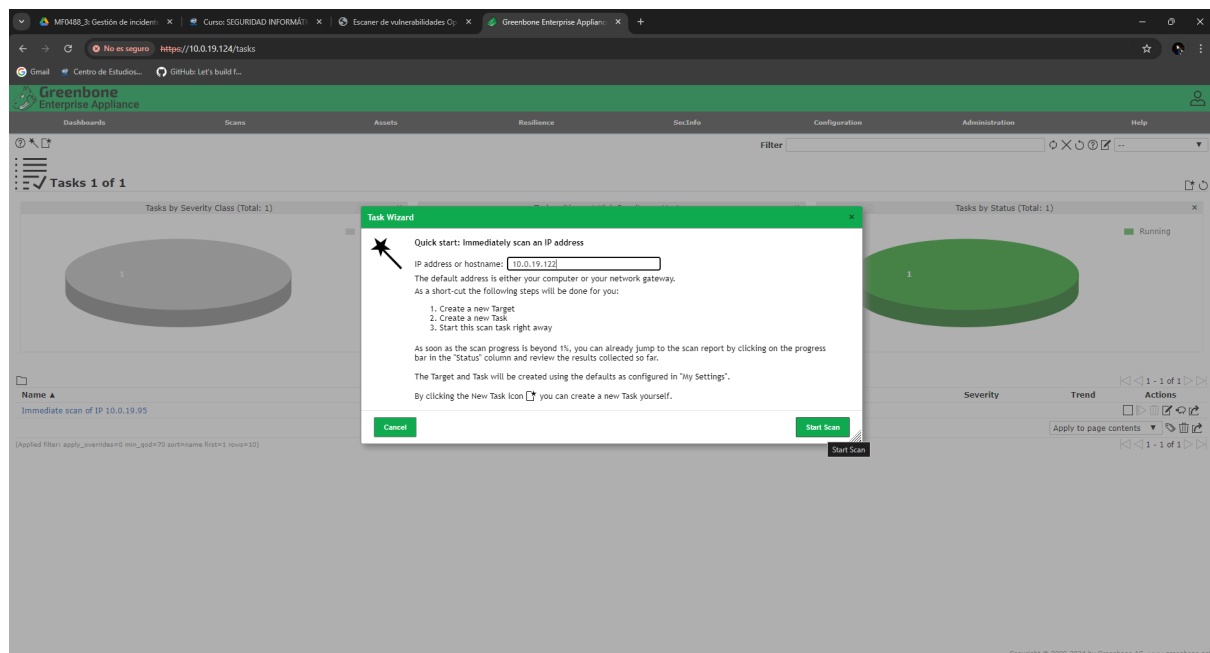
Tasks by Status (Total: 0)

No Tasks available

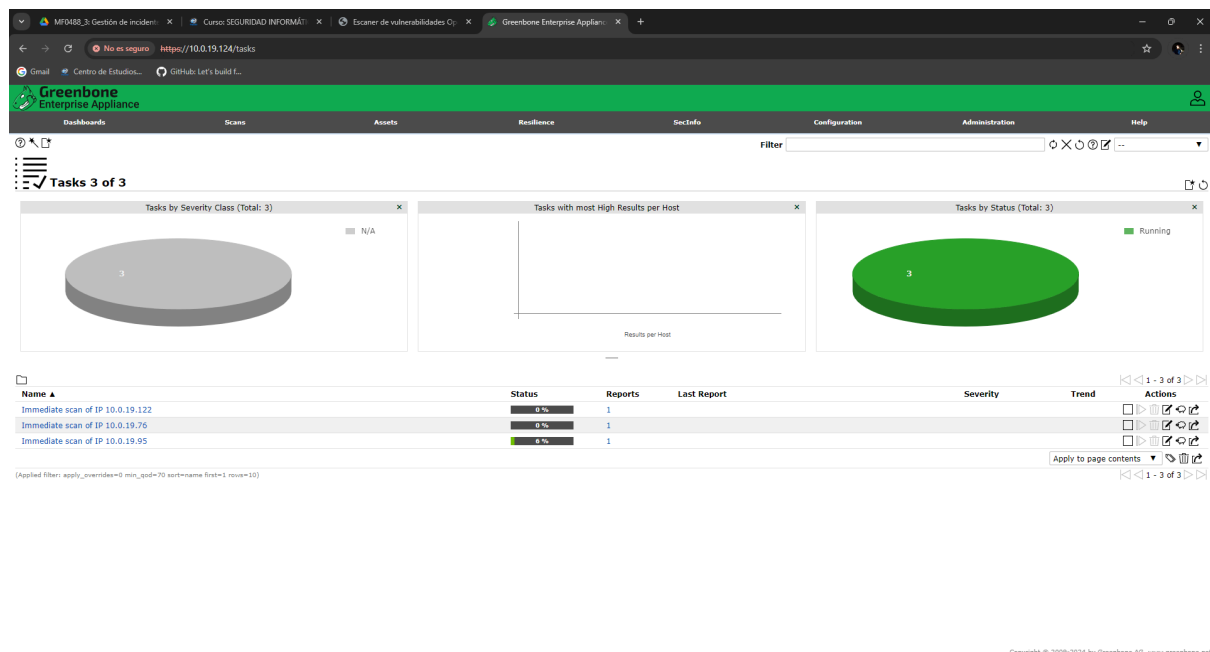
[Applied filter: apply_overrides=0 min_age=70 sort=name first=1 rows=10]

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

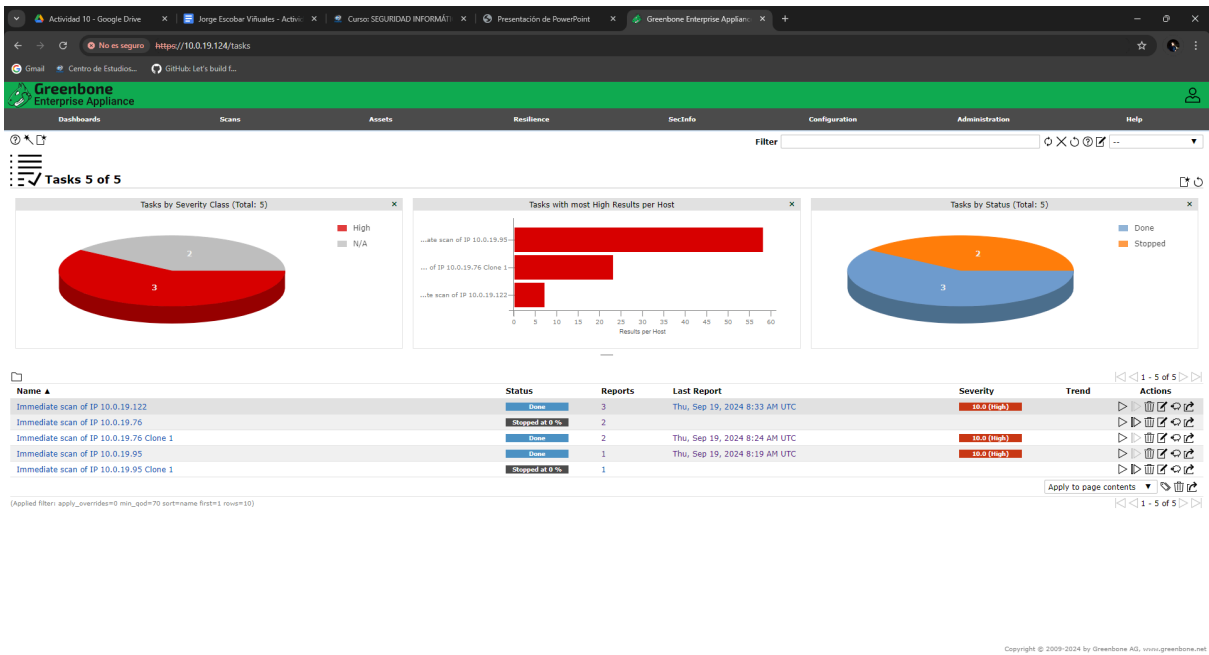
Escribimos la Ip de la máquina Metasploitable3 Ubuntu y pulsamos Start Scan:



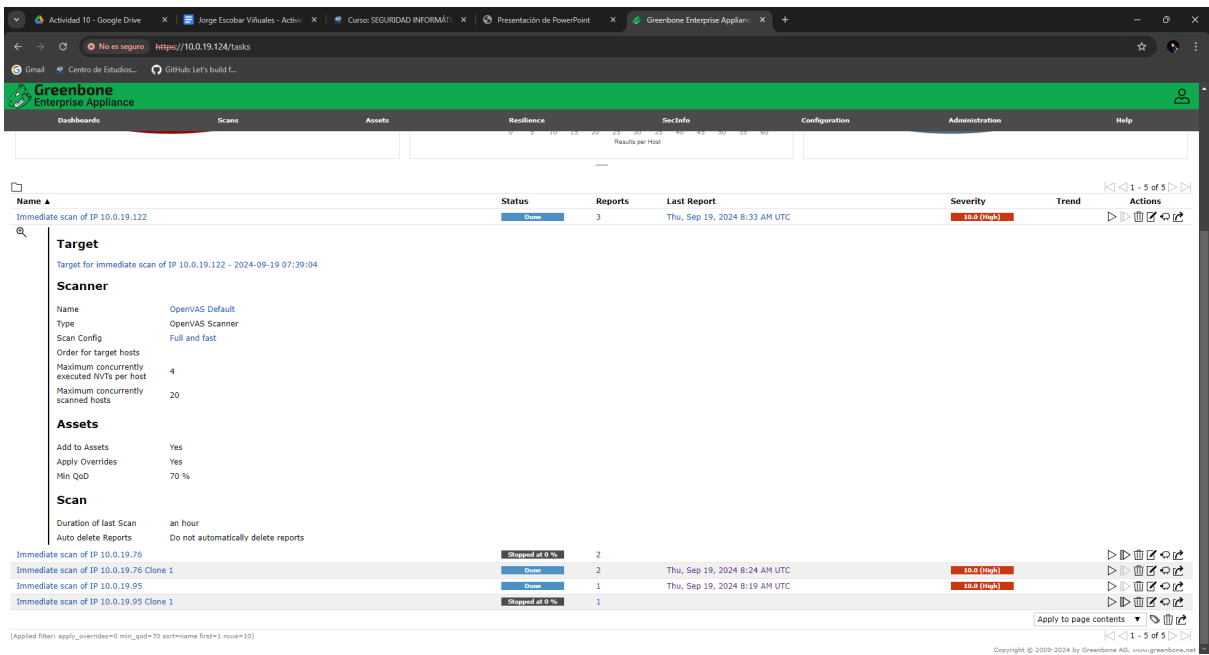
Comienza el escaneo de vulnerabilidades del sitio Web:



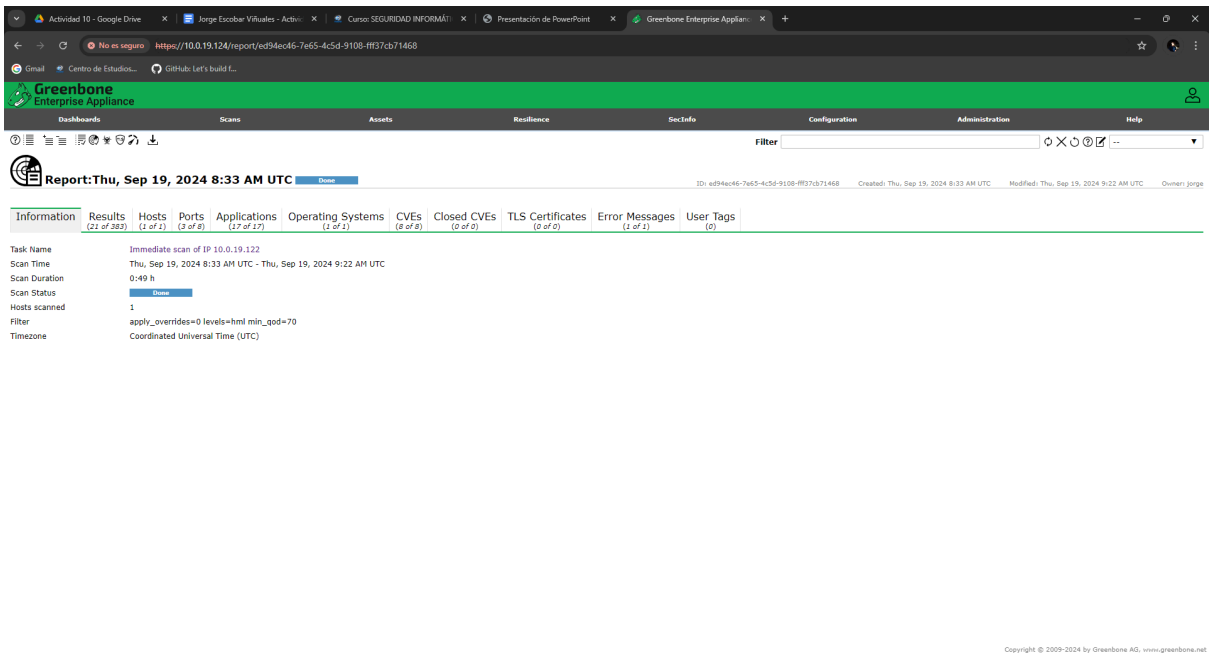
Una vez finalizado, nos muestra gráficamente el resultado:



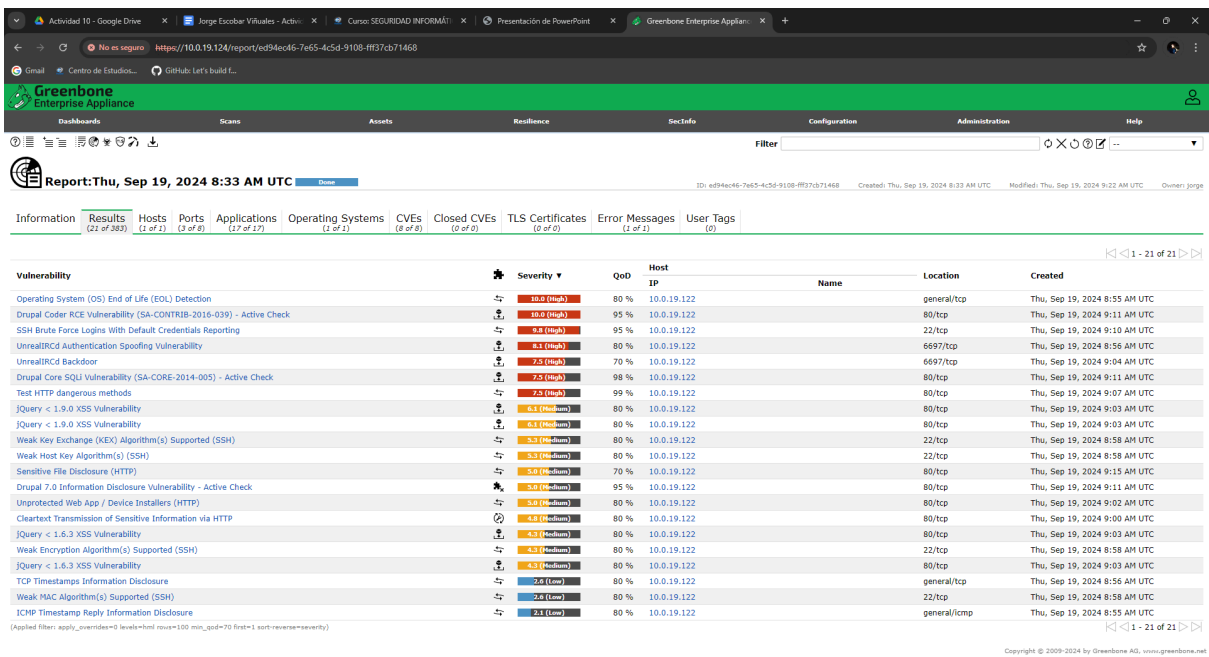
Si pulsamos en el apartado Name, nos muestra los datos generales del escaneo:



Si pulsamos en el apartado Last Report nos muestra el resultado del análisis:



En cada una de las pestañas, nos muestra información detallada:



Actividad 10 - Google Drive

jorge Escobar Viñuales - Activi...

Curso SEGURIDAD INFORMÁTICA

Presentación de PowerPoint

Greenbone Enterprise Appli...

https://10.0.19.124/report/ed94ec46-7e65-4c5d-9108-ff37cb71468

Centro de Estudios...GitHub: Let's build f...

Greenbone

Enterprise Appliance

Dashboards

Scans

Assets

Resilience

SecInfo

Configuration

Administration

Help

Filter

Report:Thu, Sep 19, 2024 8:33 AM UTC

Done

ID: ed94ec46-7e65-4c5d-9108-ff37cb71468Created: Thu, Sep 19, 2024 8:33 AM UTCModified: Thu, Sep 19, 2024 9:22 AM UTCOwner: jorge

Information

Results

(21 of 383)

Hosts

(1 of 1)

Ports

(3 of 8)

Applications

(17 of 17)

Operating Systems

(1 of 1)

CVEs

(8 of 8)

Closed CVEs

(0 of 0)

TLS Certificates

(0 of 0)

Error Messages

(1 of 1)

User Tags

(0)

Port

Hosts

Severity

80/tcp

1

10.0 (high)

22/tcp

1

0.0 (info)

6697/tcp

1

8.1 (high)

[Applied filter: apply_overrides=0 levels=html rows=100 min_age=70 first=1 sort=reverse=severity]

<<1-3 of 3>>

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

Actividad 10 - Google Drive

jorge Escobar Viñuales - Activi...

Curso SEGURIDAD INFORMÁTICA

Presentación de PowerPoint

Greenbone Enterprise Appli...

https://10.0.19.124/report/ed94ec46-7e65-4c5d-9108-ff37cb71468

Centro de Estudios...GitHub: Let's build f...

Greenbone

Enterprise Appliance

Dashboards

Scans

Assets

Resilience

SecInfo

Configuration

Administration

Help

Filter

Report:Thu, Sep 19, 2024 8:33 AM UTC

Done

ID: ed94ec46-7e65-4c5d-9108-ff37cb71468Created: Thu, Sep 19, 2024 8:33 AM UTCModified: Thu, Sep 19, 2024 9:22 AM UTCOwner: jorge

Information

Results

(21 of 383)

Hosts

(1 of 1)

Ports

(3 of 8)

Applications

(17 of 17)

Operating Systems

(1 of 1)

CVEs

(8 of 8)

Closed CVEs

(0 of 0)

TLS Certificates

(0 of 0)

Error Messages

(1 of 1)

User Tags

(0)

IP Address

Hostname

OS

Ports

Apps

Distance

Auth

Start

End

High

Medium

Low

Log

False Positive

Total

Severity

10.0.19.122

3

17

Thu, Sep 19, 2024 8:34 AM UTC

Thu, Sep 19, 2024 9:22 AM UTC

7

11

3

0

0

21

10.0 (high)

[Applied filter: apply_overrides=0 levels=html rows=100 min_age=70 first=1 sort=reverse=severity]

<<1-1 of 1>>

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

Actividad 10 - Google Drivejorge Escobar Viñuales - Actividad 10Curso SEGURIDAD INFORMÁTICAPresentación de PowerPointGreenbone Enterprise Appliance

https://10.0.19.124/report/ed94ec46-7e65-4c5d-9108-fbf37cb71468

Centro de Estudios...GitHub: Let's build...

GreenboneEnterprise Appliance

DashboardScansAssetsResilienceSecInfoConfigurationAdministrationHelp

Filter

Report:Thu, Sep 19, 2024 8:33 AM UTCDone

ID: ed94ec46-7e65-4c5d-9108-fbf37cb71468Created: Thu, Sep 19, 2024 8:33 AM UTCModified: Thu, Sep 19, 2024 9:22 AM UTCOwner: jorge

InformationResults(21 of 383)Hosts(1 of 1)Ports(3 of 8)Applications(17 of 17)Operating Systems(1 of 1)CVES(8 of 8)Closed CVES(0 of 0)TLS Certificates(0 of 0)Error Messages(2 of 1)User Tags(0)

Operating SystemCPEHostsSeverity

Ubuntu 14.04cpe:/o:canonical:ubuntu_linux:14.04110.0 (high)

(Applied filter: apply_overrides=0 levels=html rows=100 min_age=70 first=1 sort=reverse=severity)

<<<1 - 1 of 1>>>

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

Actividad 10 - Google Drivejorge Escobar Viñuales - Actividad 10Curso SEGURIDAD INFORMÁTICAPresentación de PowerPointGreenbone Enterprise Appliance

https://10.0.19.124/report/ed94ec46-7e65-4c5d-9108-fbf37cb71468

Centro de Estudios...GitHub: Let's build...

GreenboneEnterprise Appliance

DashboardScansAssetsResilienceSecInfoConfigurationAdministrationHelp

Filter

Report:Thu, Sep 19, 2024 8:33 AM UTCDone

ID: ed94ec46-7e65-4c5d-9108-fbf37cb71468Created: Thu, Sep 19, 2024 8:33 AM UTCModified: Thu, Sep 19, 2024 9:22 AM UTCOwner: jorge

InformationResults(21 of 383)Hosts(1 of 1)Ports(3 of 8)Applications(17 of 17)Operating Systems(1 of 1)CVES(8 of 8)Closed CVES(0 of 0)TLS Certificates(0 of 0)Error Messages(2 of 1)User Tags(0)

Application CPEHostsOccurrencesSeverity

cpe:/a:unrealircd:unrealircd:3.2.8.1118.1 (high)

cpe:/a:ietf:secure_shell_protocol:2.01N/A

cpe:/a:openssh:openssh:6.6.1p11N/A

cpe:/a:ruby-lang:ruby:2.3.81N/A

cpe:/a:oracle:mysql11N/A

cpe:/a:mysql:mysql11N/A

cpe:/a:eclipse:jetty:8.1.7.201209101N/A

cpe:/a:ruby-lang:webrick:1.3.11N/A

cpe:/a:phpmyadmin:phpmyadmin:3.5.81N/A

cpe:/a:ruby-lang:ruby:2.3.8.4591N/A

cpe:/a:rubyonrails:rails:4.2.41N/A

cpe:/a:apache:http_server:2.4.71N/A

cpe:/a:jquery:jquery11N/A

cpe:/a:jquery:jquery:1.6.212N/A

cpe:/a:drupal:drupal:7.51N/A

cpe:/a:php:php:5.4.51N/A

cpe:/a:samba:samba:4.3.111N/A

(Applied filter: apply_overrides=0 levels=html rows=100 min_age=70 first=1 sort=reverse=severity)

<<<1 - 17 of 17>>>

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

Página 28

Actividad 10 - Google Drive

jorge Escobar Viñuales - Activi...

Curso SEGURIDAD INFORMÁTICA

Presentación de PowerPoint

Greenbone Enterprise Appli...

No es seguro

https://10.0.19.124/report/ed94ec46-7e65-4c5d-9108-ff37cb71468

Gmail

Centro de Estudios...

GitHub: Let's build f...

Greenbone

Enterprise Appliance

Dashboards

Scans

Assets

Resilience

SecInfo

Configuration

Administration

Help

Filter

Report:Thu, Sep 19, 2024 8:33 AM UTC

Done

ID: ed94ec46-7e65-4c5d-9108-ff37cb71468

Created: Thu, Sep 19, 2024 8:33 AM UTC

Modified: Thu, Sep 19, 2024 9:22 AM UTC

Owner: jorge

Information

Results

Hosts

Ports

Applications

Operating Systems

CVEs

Closed CVEs

TLS Certificates

Error Messages

User Tags

CVE

NVT

Hosts

Occurrences

Severity

CVE-1999-0501

CVE-1999-0502

CVE-1999-0507

CVE-1999-0508

CVE-2020-9473

CVE-2023-1944

CVE-2024-22902

CVE-2024-31970

SSH Brute Force Logins With Default Credentials Reporting

1

1

9.8 (high)

CVE-2016-7144

UnrealIRCd Authentication Spoofing Vulnerability

1

1

8.1 (high)

CVE-2010-2075

UnrealIRCd Backdoor

1

1

7.5 (high)

CVE-2014-3704

Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check

1

1

7.5 (high)

CVE-2012-4708

jQuery < 1.9.0 XSS Vulnerability

1

2

6.1 (medium)

CVE-2011-3730

Drupal 7.0 Information Disclosure Vulnerability - Active Check

1

1

6.1 (medium)

CVE-2011-4969

jQuery < 1.6.3 XSS Vulnerability

1

2

6.1 (medium)

CVE-1999-0524

ICMP Timestamp Reply Information Disclosure

1

1

2.1 (low)

(Applied filter: apply_overrides=0 levels=html rows=100 min_qod=70 first=1, sort=reverse=severity)

<<

1 - 8 of 8

>>

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

Actividad 10 - Google Drive

jorge Escobar Viñuales - Activi...

Curso SEGURIDAD INFORMÁTICA

Presentación de PowerPoint

Greenbone Enterprise Appli...

No es seguro

https://10.0.19.124/report/ed94ec46-7e65-4c5d-9108-ff37cb71468

Gmail

Centro de Estudios...

GitHub: Let's build f...

Greenbone

Enterprise Appliance

Dashboards

Scans

Assets

Resilience

SecInfo

Configuration

Administration

Help

Filter

Report:Thu, Sep 19, 2024 8:33 AM UTC

Done

ID: ed94ec46-7e65-4c5d-9108-ff37cb71468

Created: Thu, Sep 19, 2024 8:33 AM UTC

Modified: Thu, Sep 19, 2024 9:22 AM UTC

Owner: jorge

Information

Results

Hosts

Ports

Applications

Operating Systems

CVEs

Closed CVEs

TLS Certificates

Error Messages

User Tags

No TLS Certificates available

(Applied filter: apply_overrides=0 levels=html rows=100 min_qod=70 first=1, sort=reverse=severity)

<<

1 - 8 of 8

>>

Copyright © 2009-2024 by Greenbone AG, www.greenbone.net