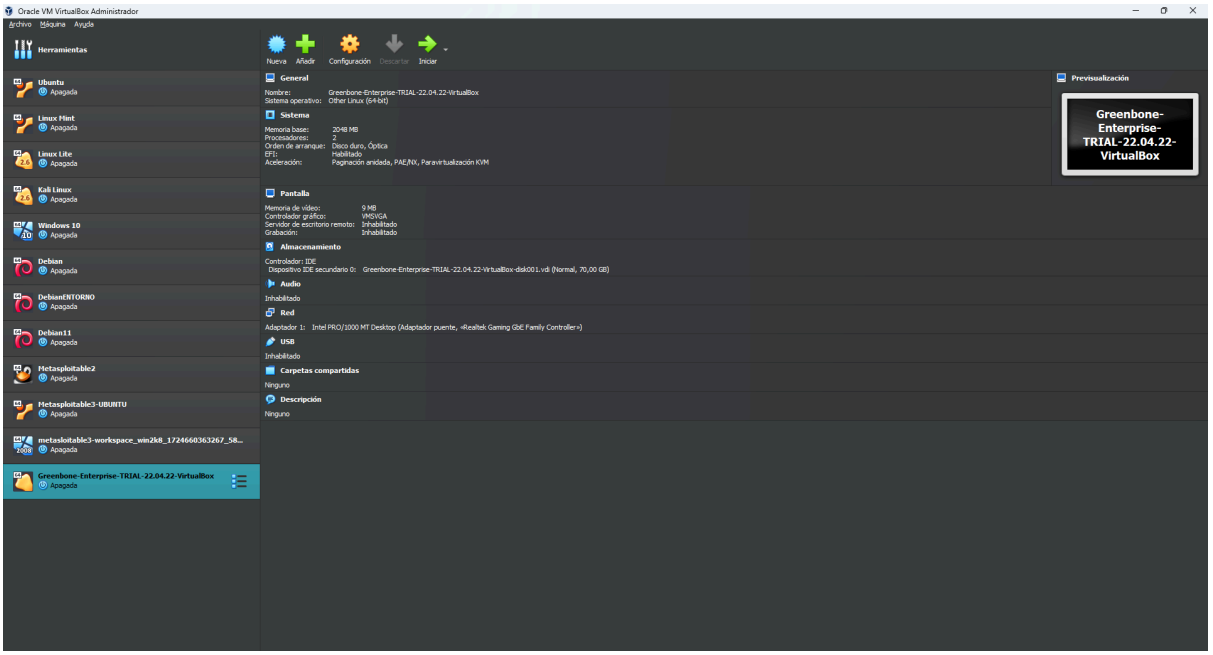
Actividad 10. Uso de la herramienta OpenVAS

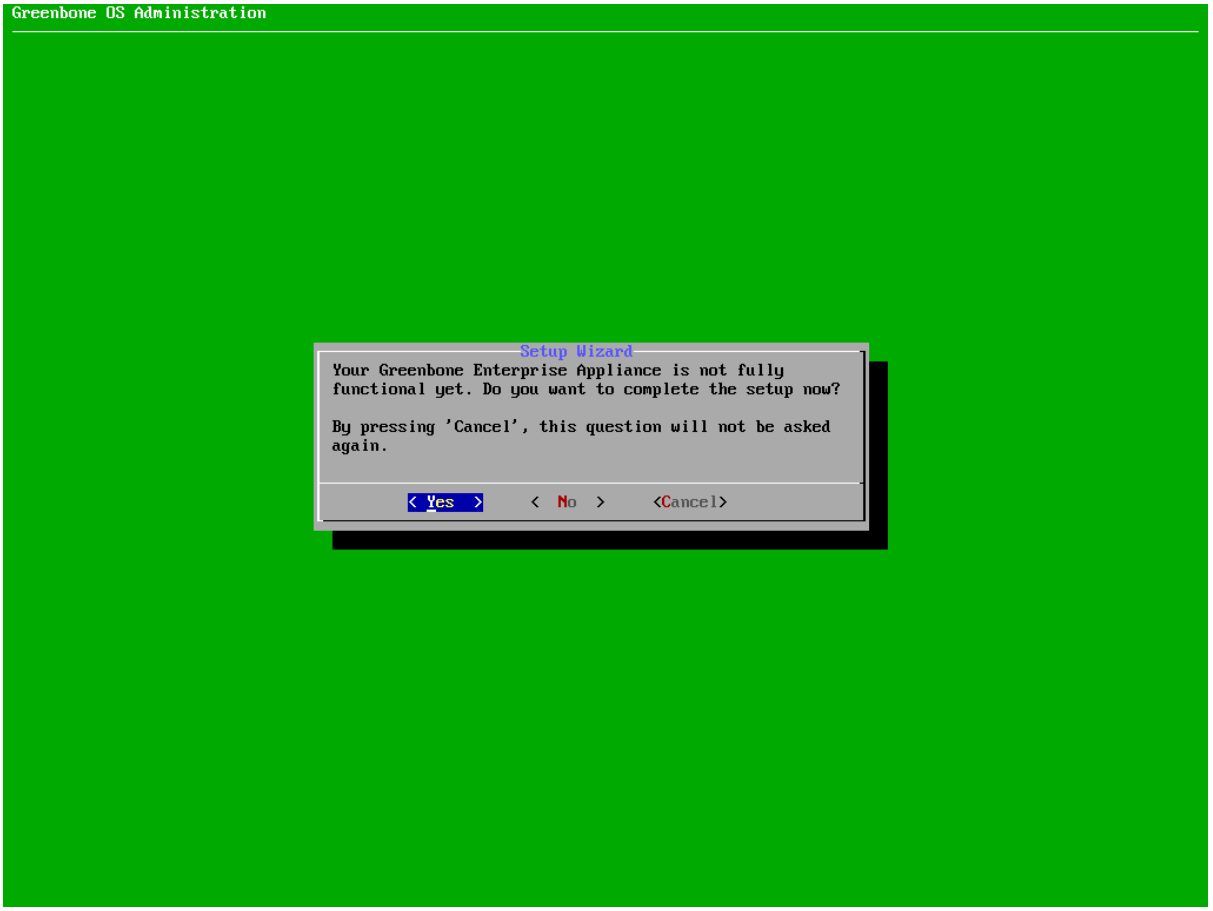
1. Instalar OpenVAS

Importamos la máquina virtual Greenbone:

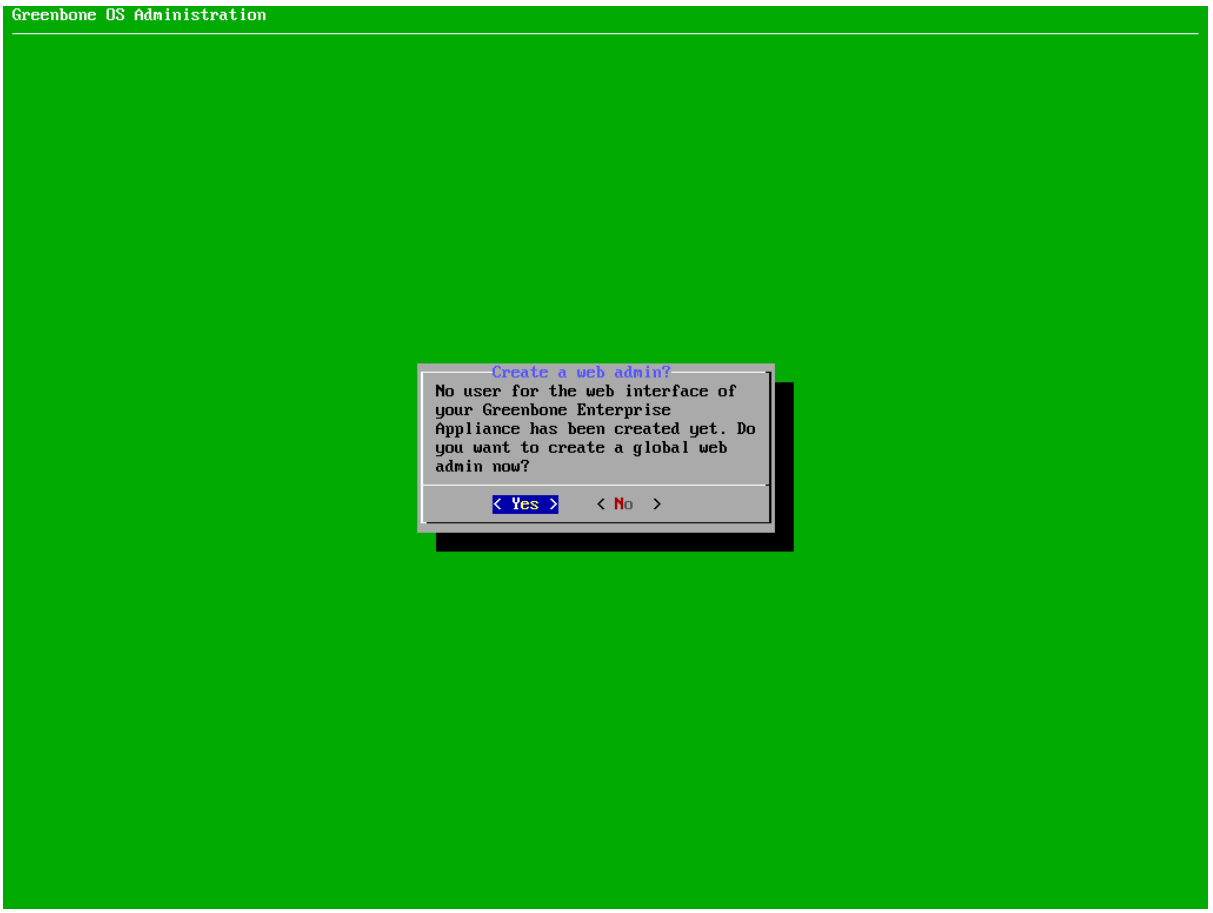


Una vez importado, iniciamos la máquina. Nos mostrará la IP de la máquina en la red y nos solicita hacer Login con usuario **admin** y contraseña: **admin**:

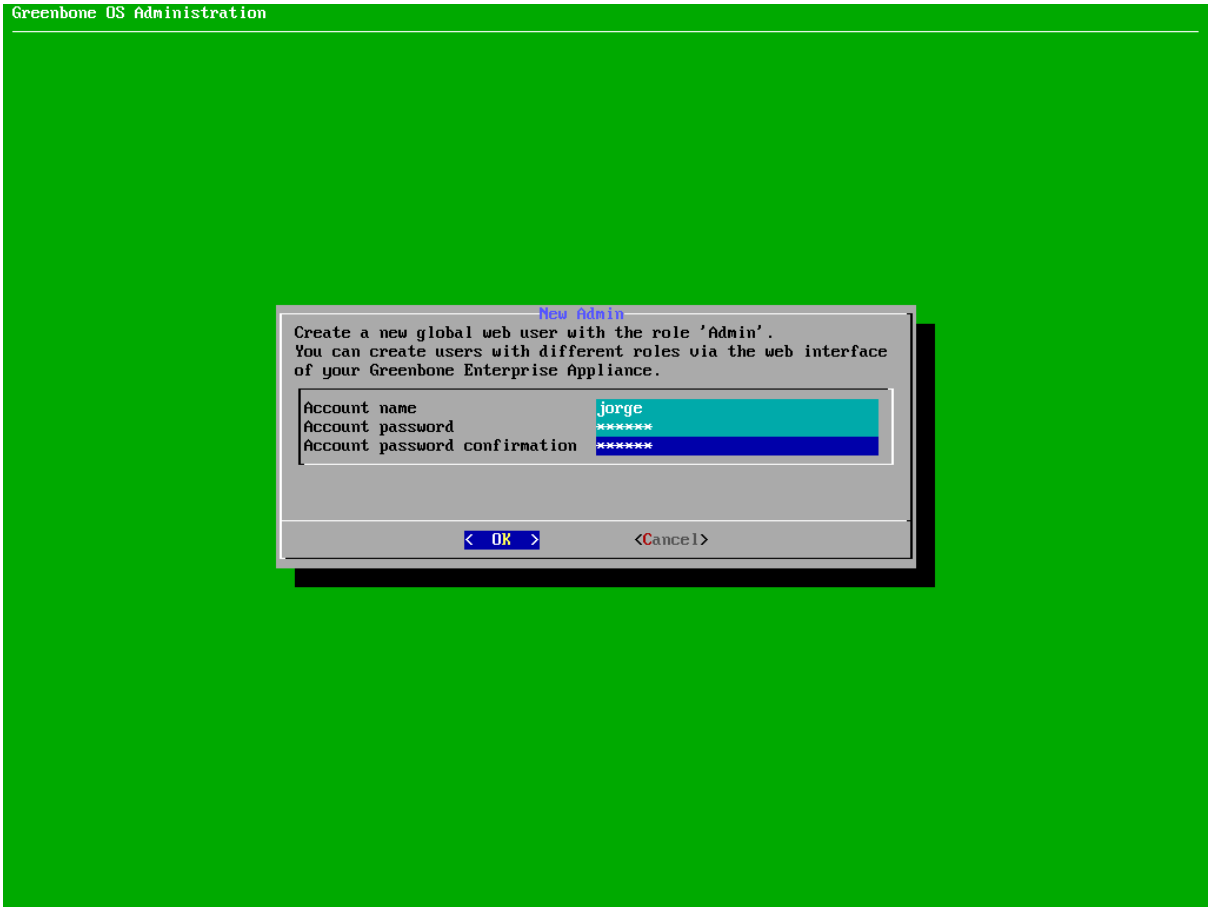
Nos pregunta si completamos la configuración. Pulsamos Yes:



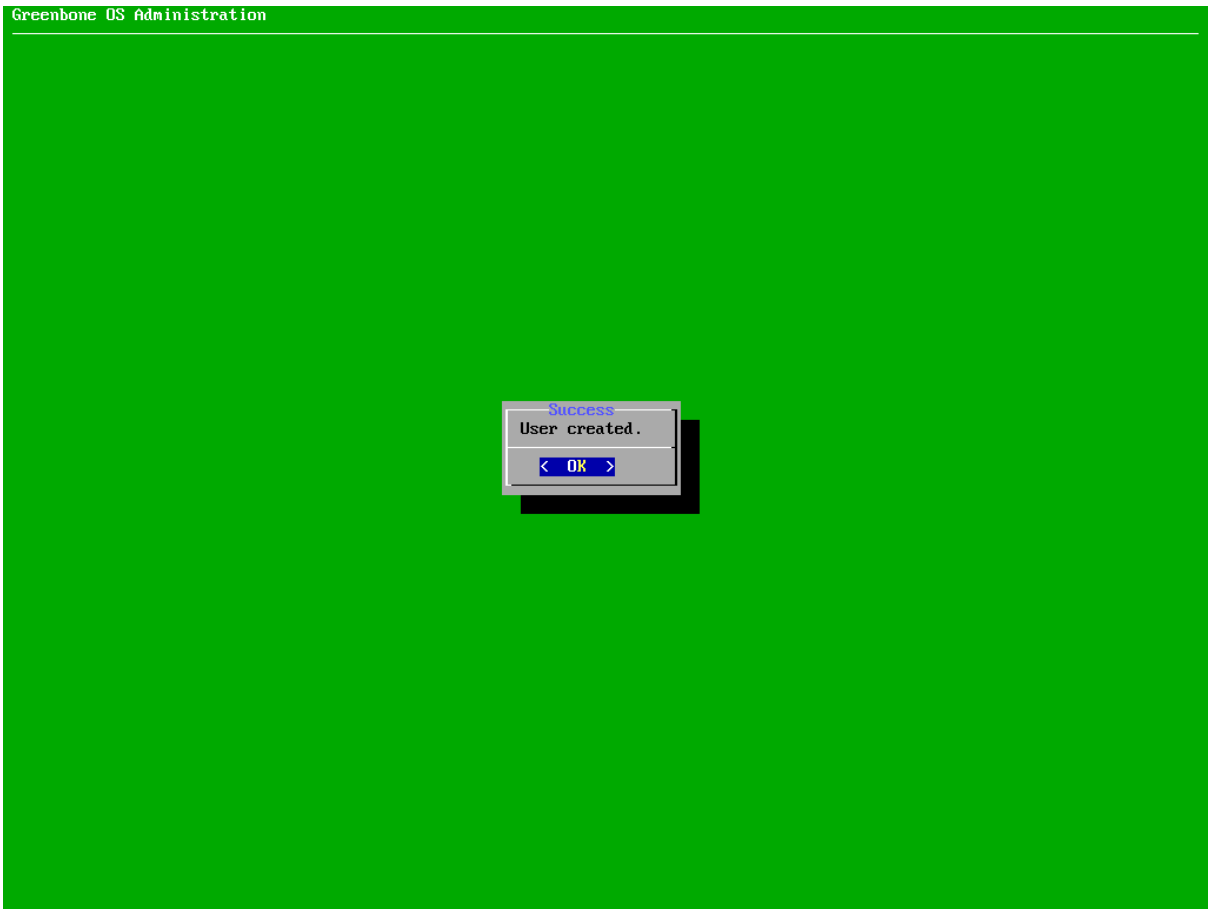
Nos pregunta si queremos crear una interfaz web de administración.
Pulsamos Yes:



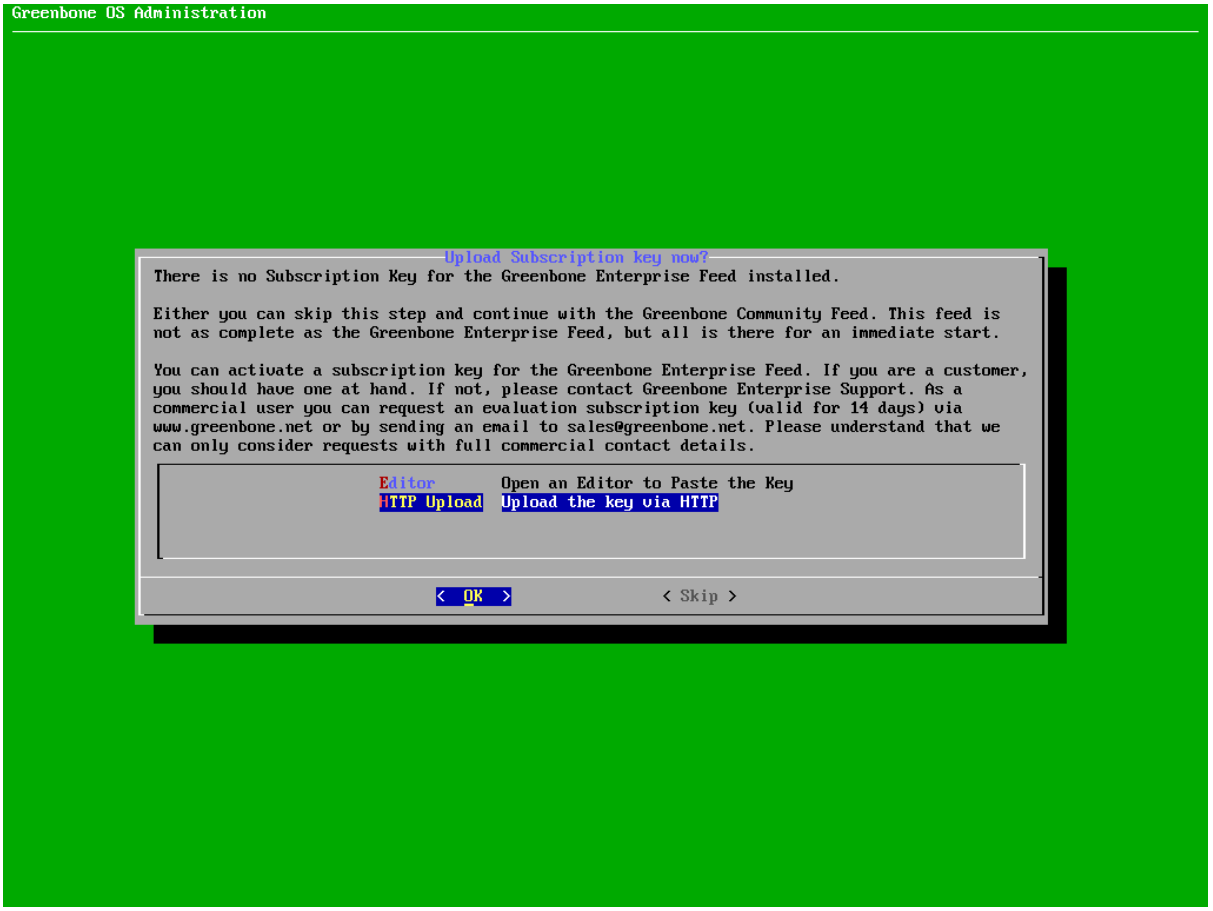
Ahora, nos solicita un usuario y contraseña de administración. Lo introducimos y pulsamos OK:



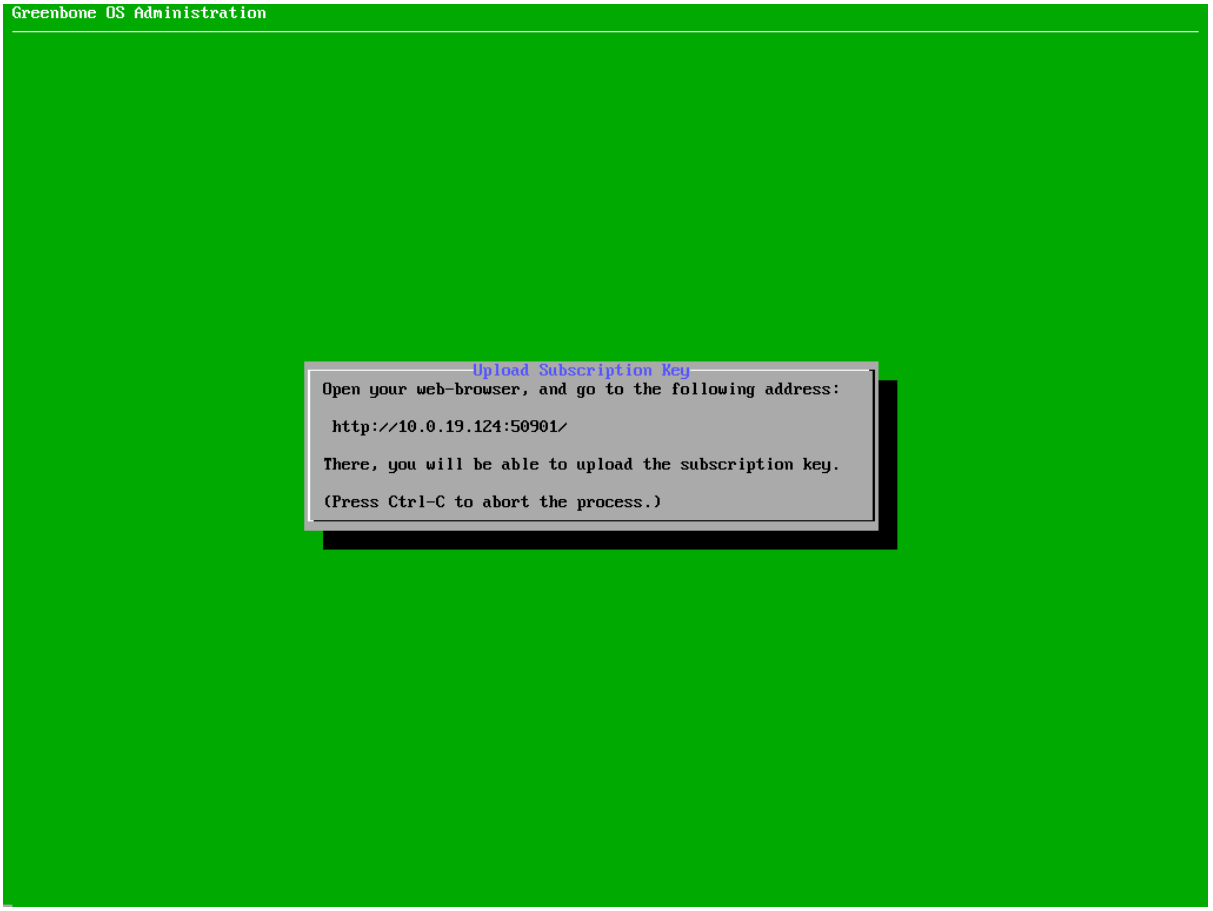
Nos indica que ha creado el usuario. Pulsamos OK:



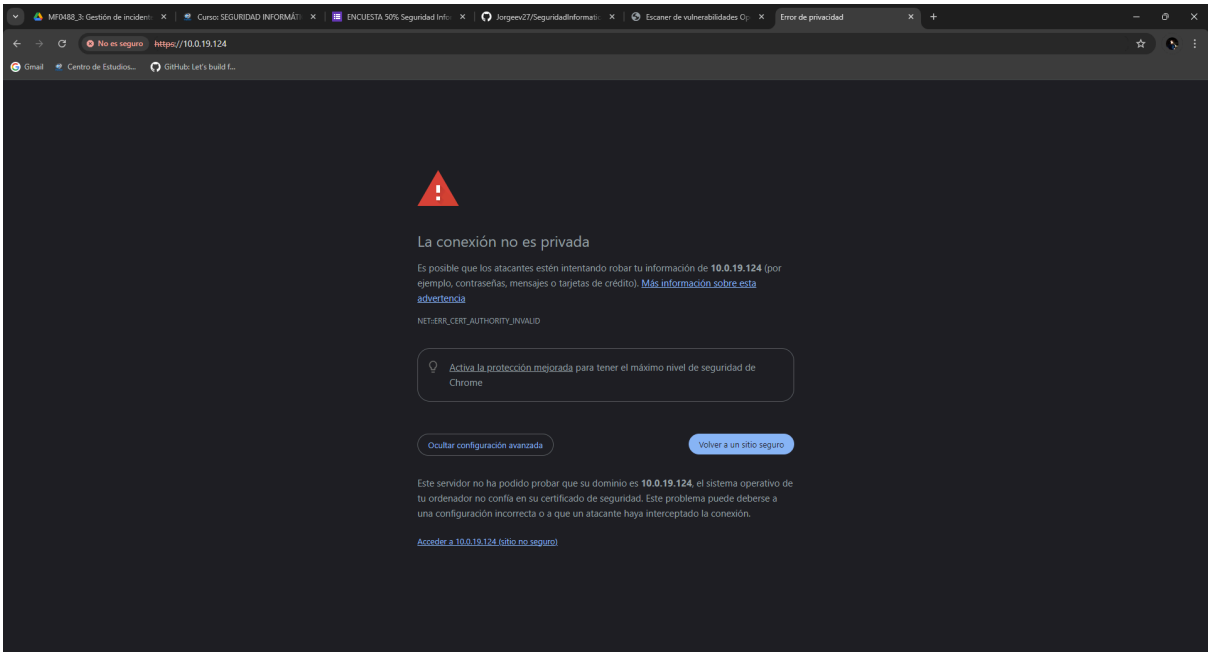
Finalmente, Seleccionamos HTTP Upload y pulsamos OK:



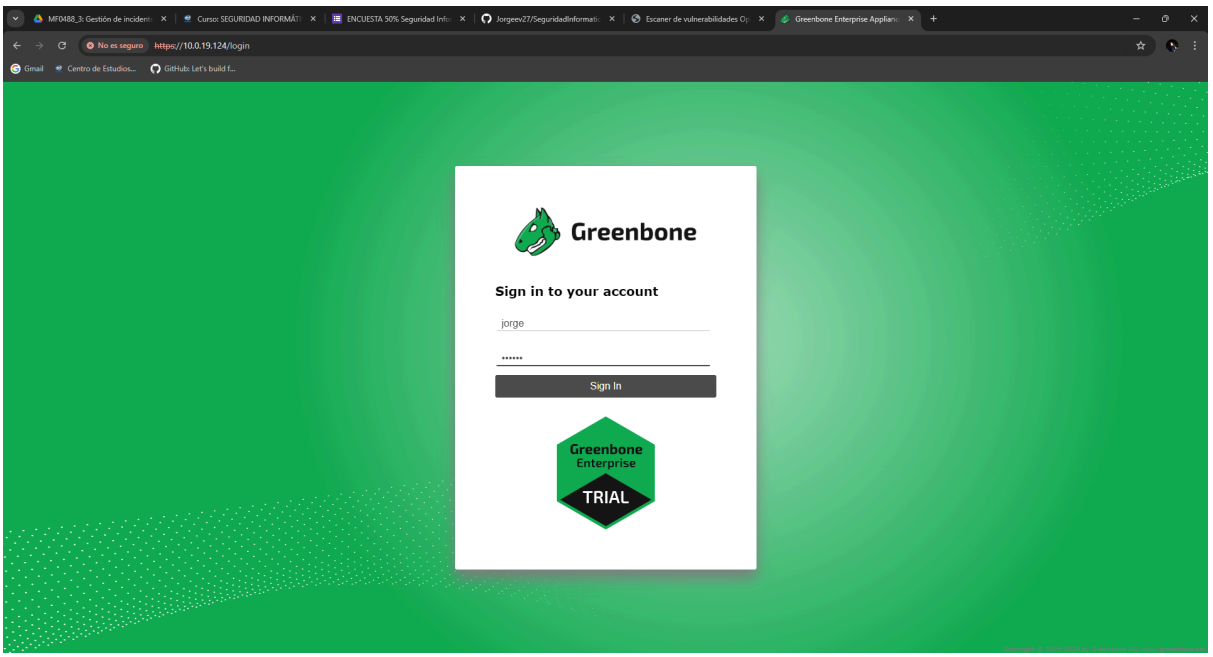
Nos aparece una ventana con la URL y el puerto:



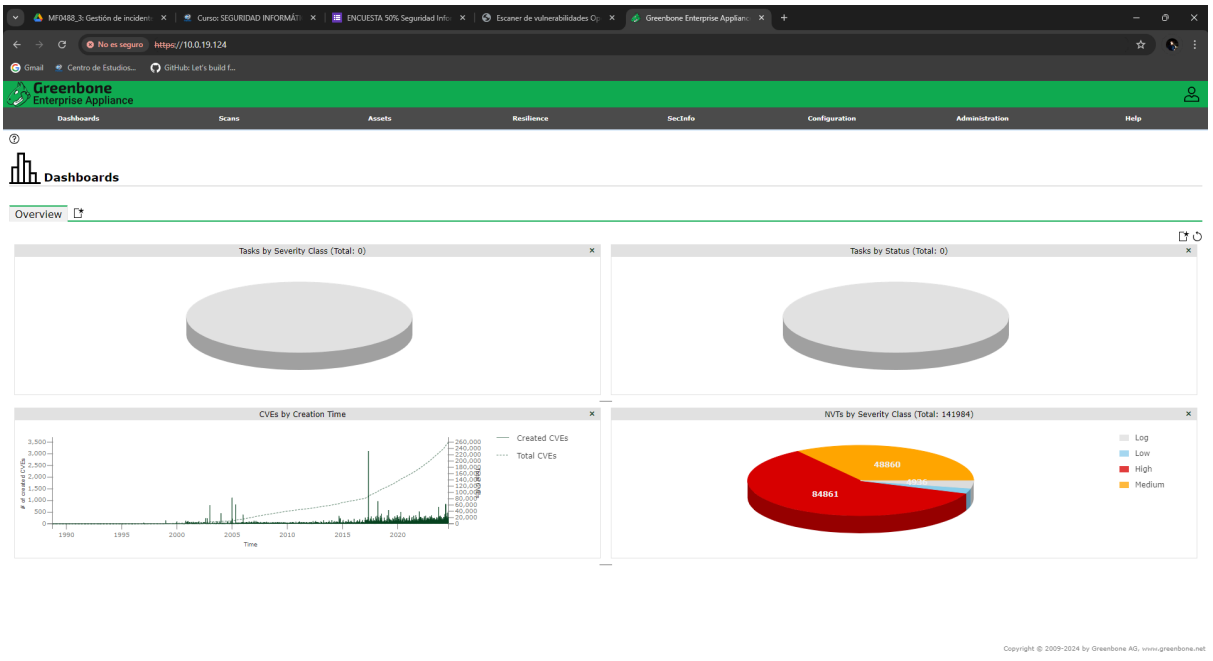
Ahora, arrancamos otra máquina en la red para entrar en el panel de administración. Abrimos un navegador y escribimos la ip de la máquina Greenbone. Pulsamos Avanzado:



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



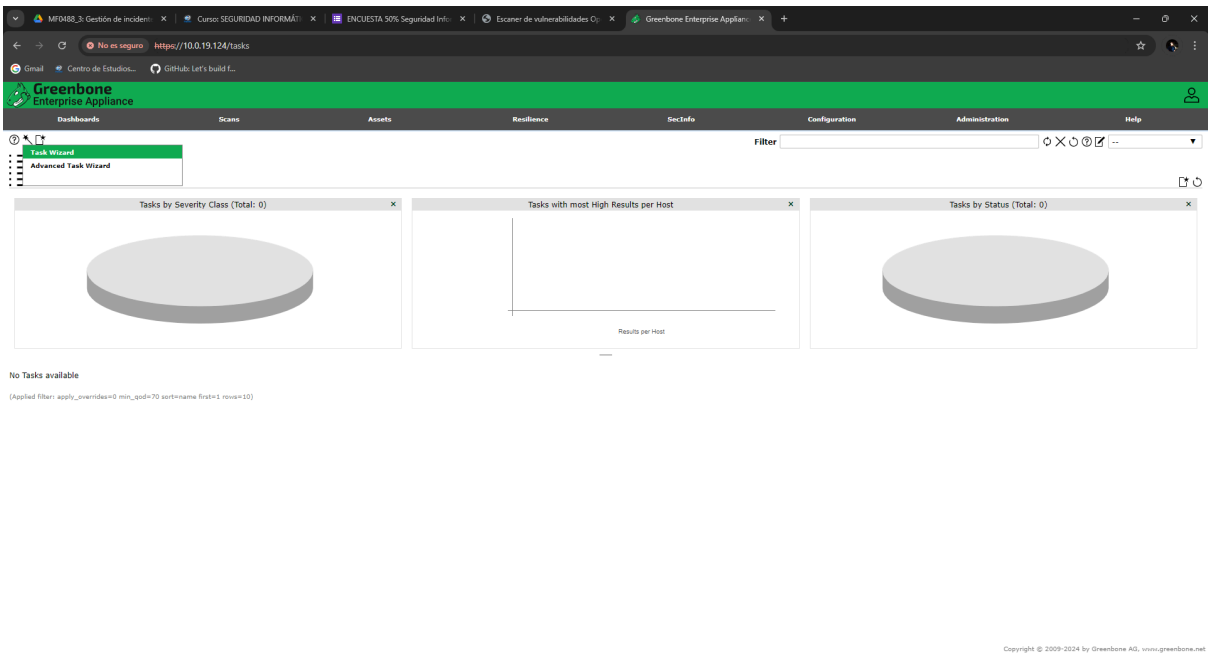
Aparece el panel de administración:



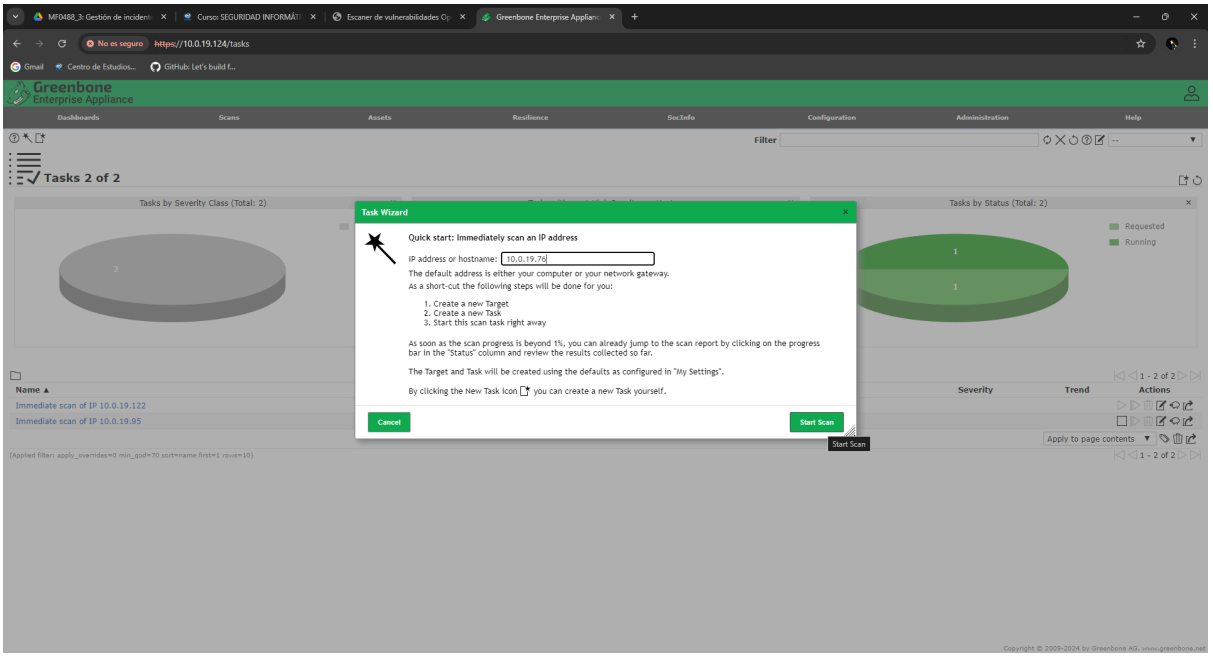
2. Ejecutar escaneo de vulnerabilidades sobre la máquina Metasploitable2 y Metasploitable3

METASPLOITABLE2:

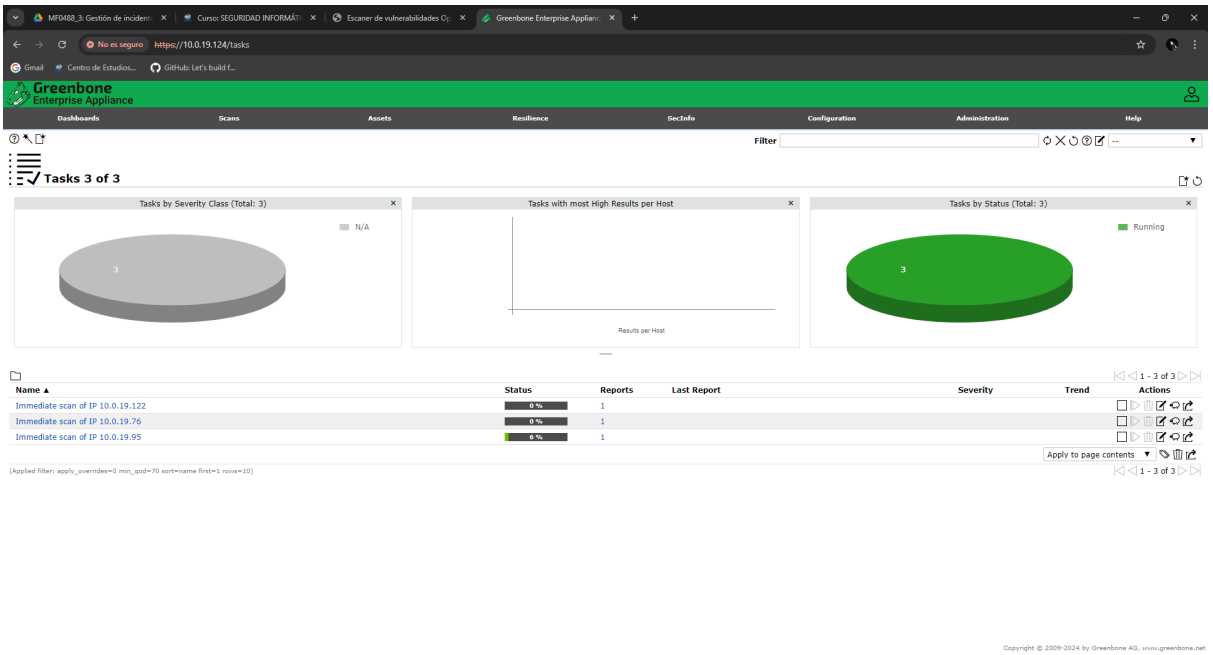
Vamos a arrancar la máquina Metasploitable2. Obtenemos su ip. Vamos a realizar el escaneo de vulnerabilidades. Para ello, pulsamos en la pestaña Scans. Pulsamos sobre el icono Task Wizard:



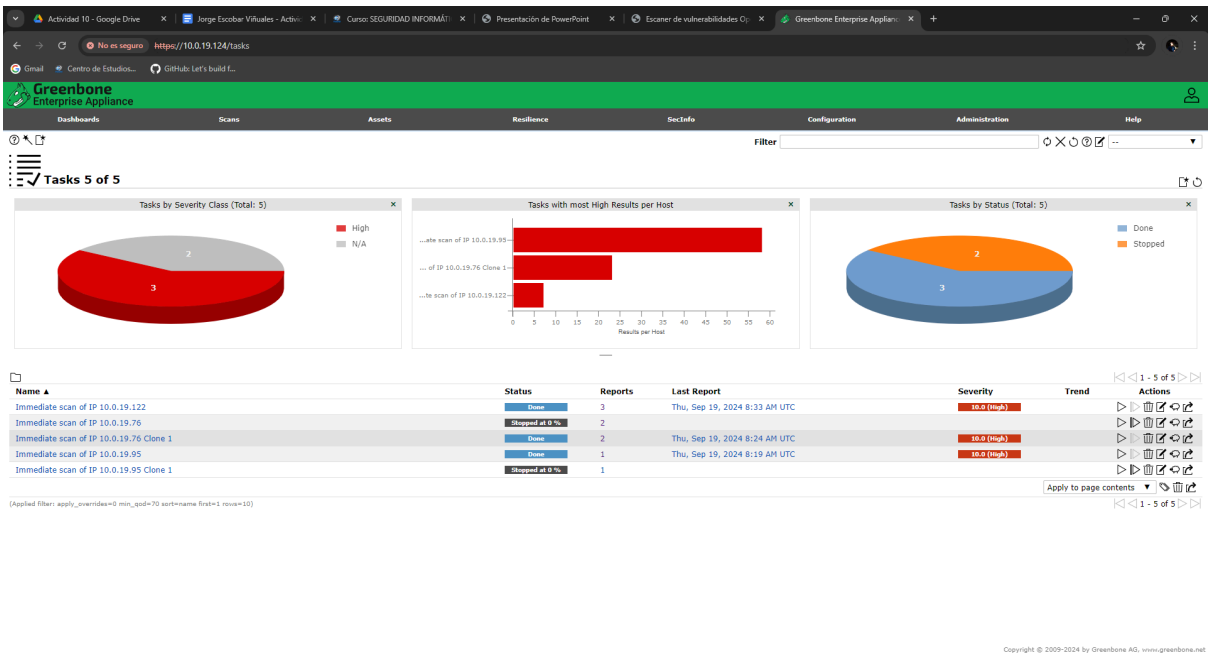
Escribimos la Ip de la máquina Metasploitable2 y pulsamos Start Scan:



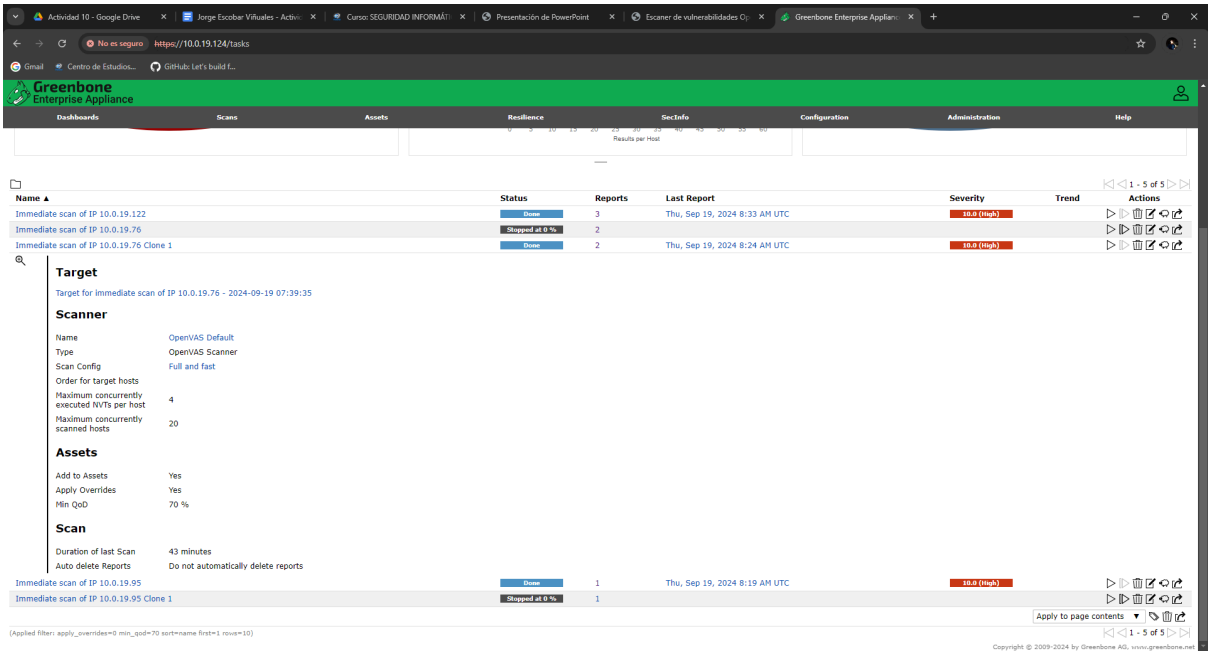
Comienza el escaneo de vulnerabilidades del sitio Web:



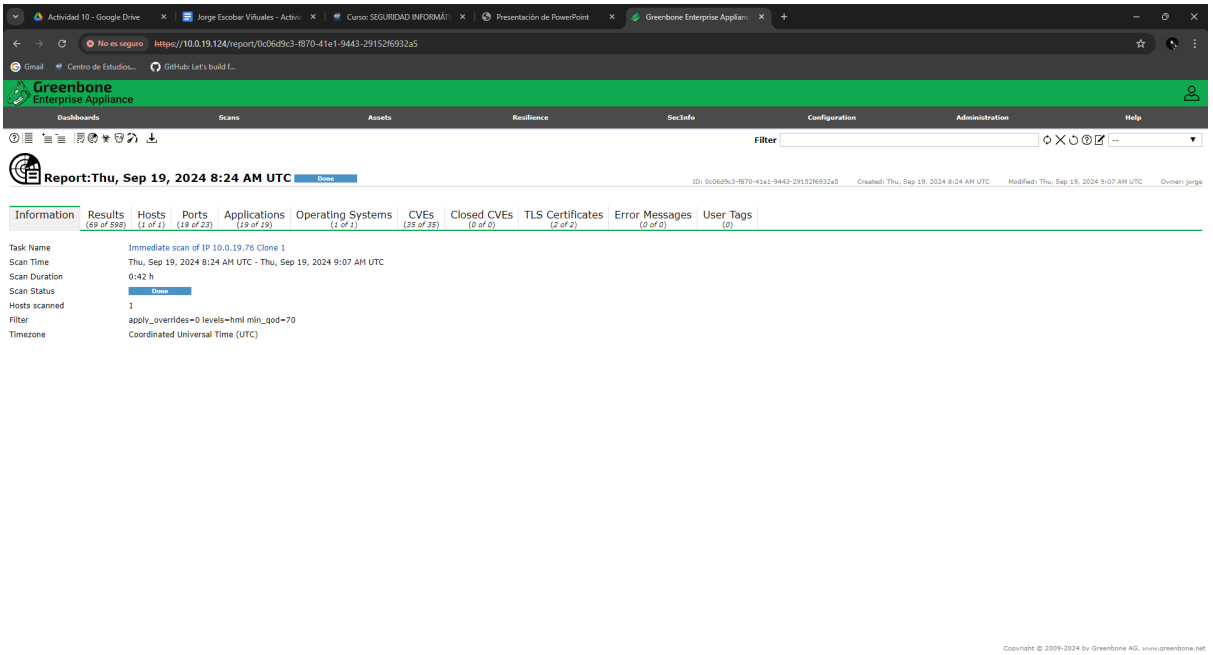
Una vez finalizado, nos muestra gráficamente el resultado:



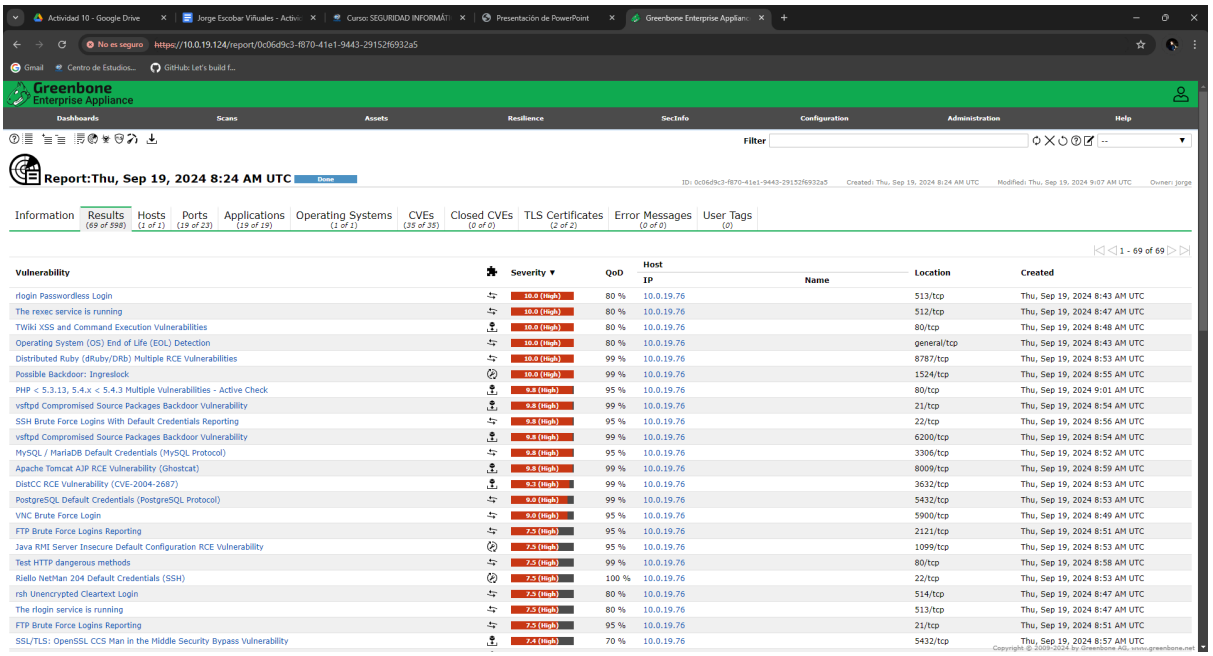
Si pulsamos en el apartado Name, nos muestra los datos generales del escaneo:

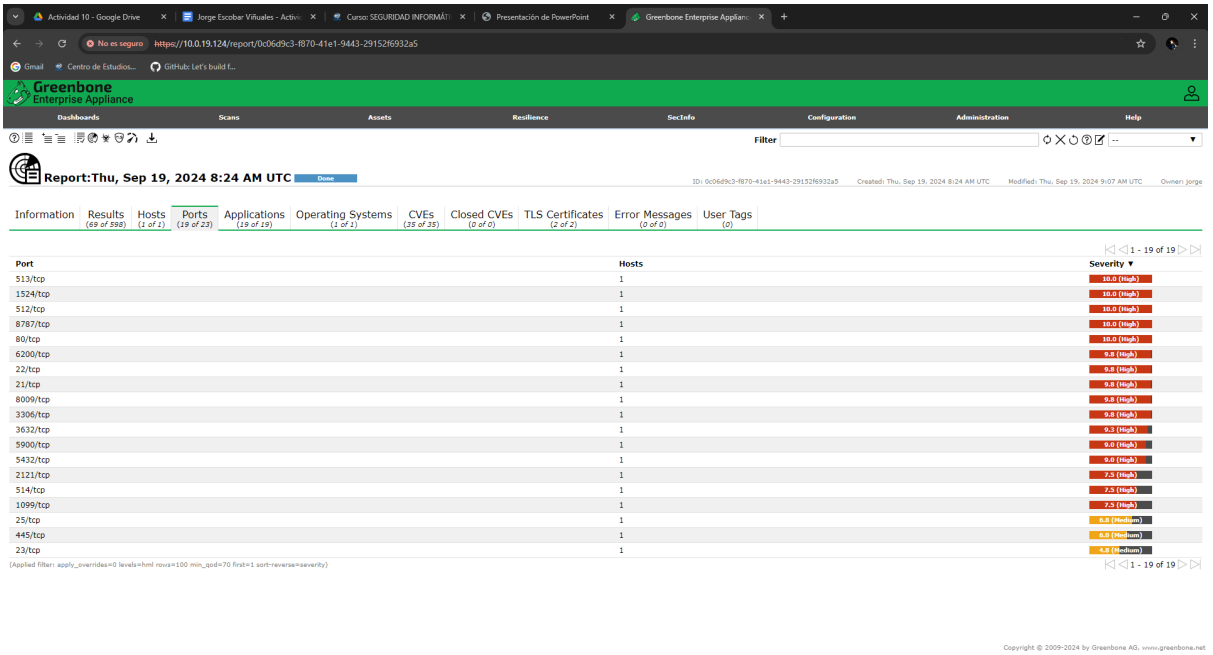


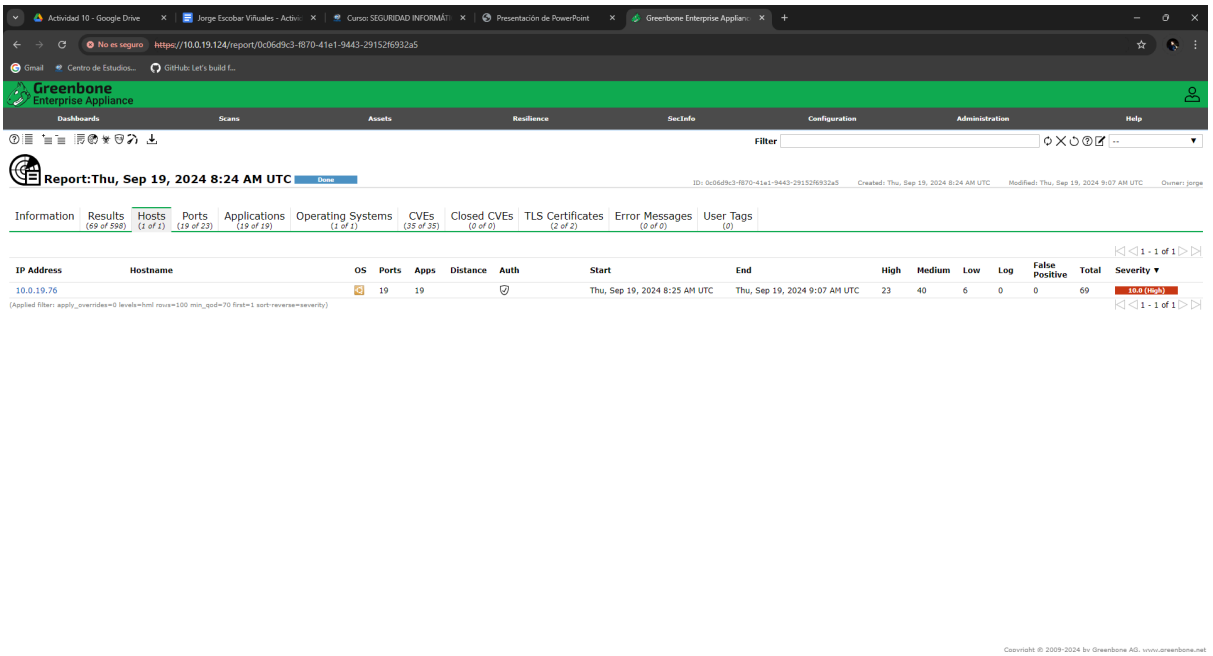
Si pulsamos en el apartado Last Report nos muestra el resultado del análisis:

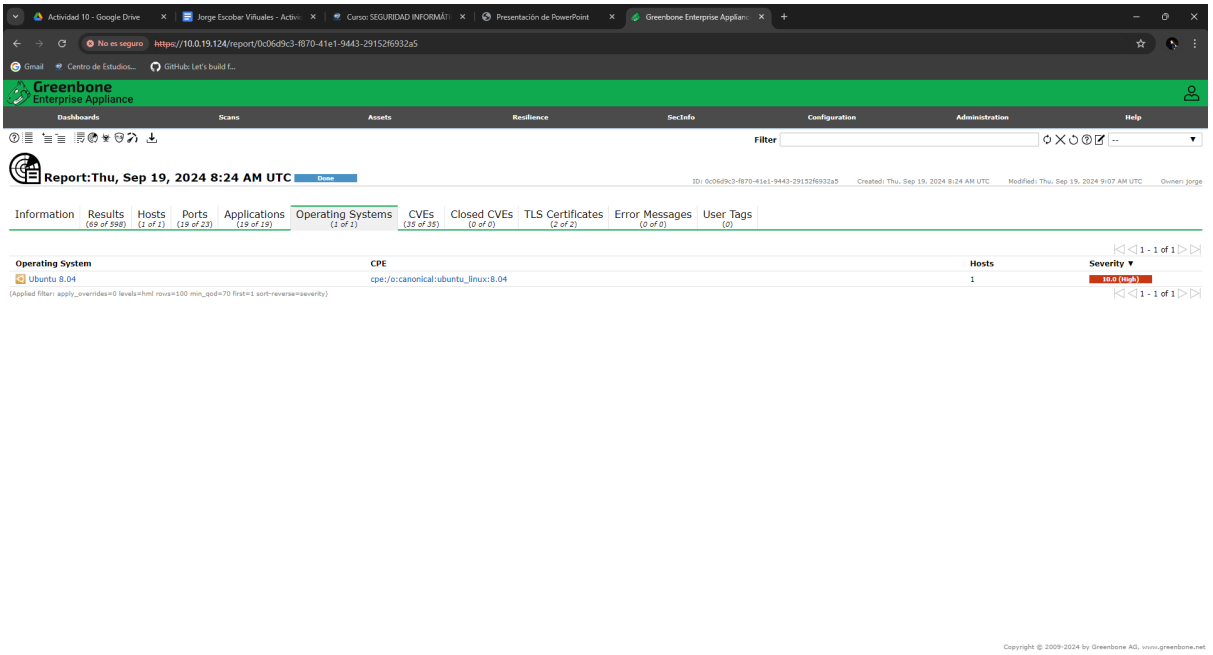


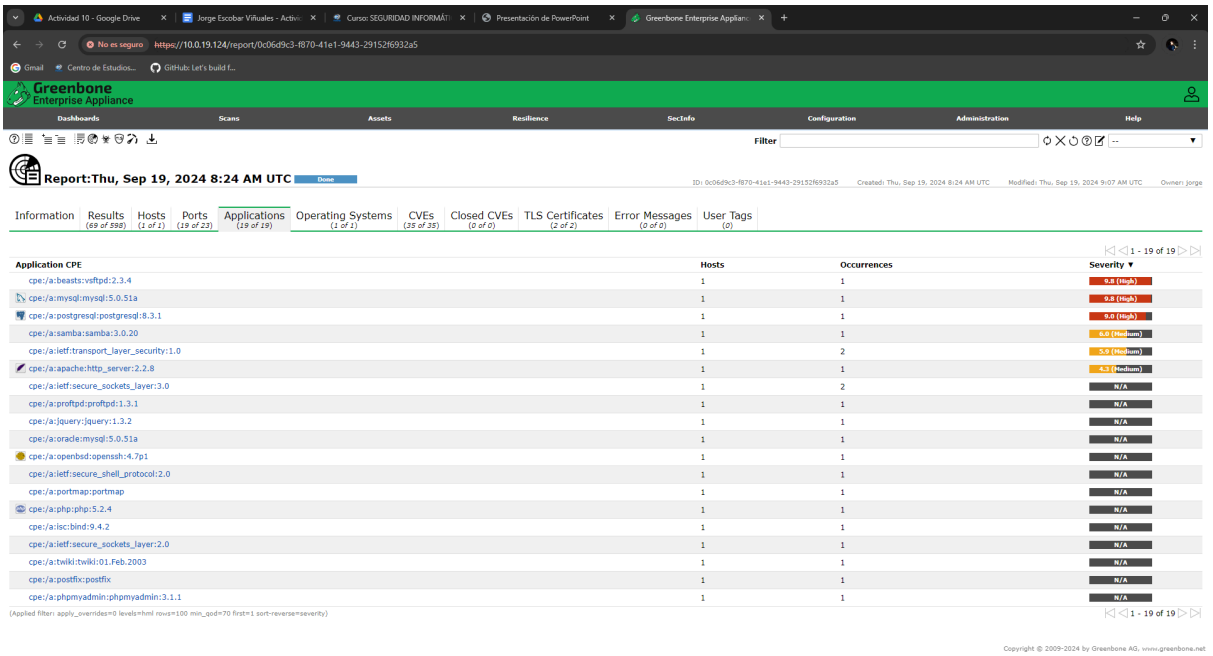
En cada una de las pestañas, nos muestra información detallada:

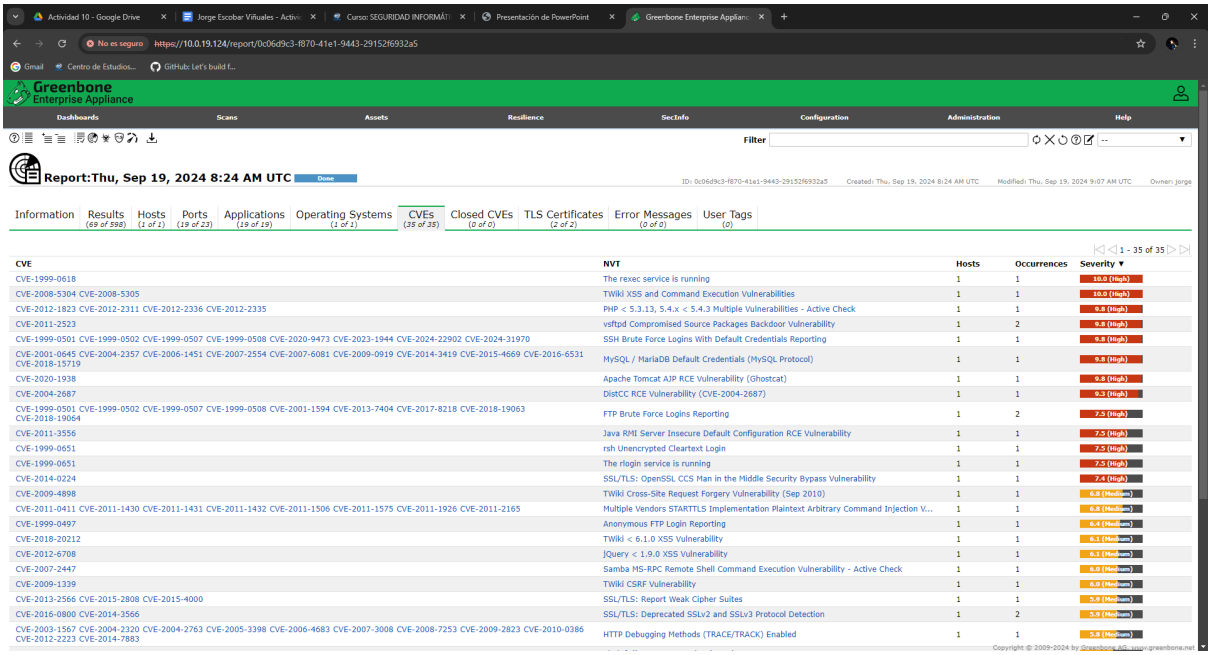



Greenbone Enterprise Appliance
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Report:Thu, Sep 19, 2024 8:24 AM UTC
Information Results Hosts Ports Applications Operating Systems CVEs Closed CVEs TLS Certificates Error Messages User Tags
Port Hosts Severity
513/tcp 1 10.0 (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)
6200/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 6.8 (Medium)
445/tcp 1 6.0 (Medium)
23/tcp 1 4.8 (Medium)


Greenbone Enterprise Appliance
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Report:Thu, Sep 19, 2024 8:24 AM UTC
Information Results Hosts Ports Applications Operating Systems CVEs Closed CVEs TLS Certificates Error Messages User Tags
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)

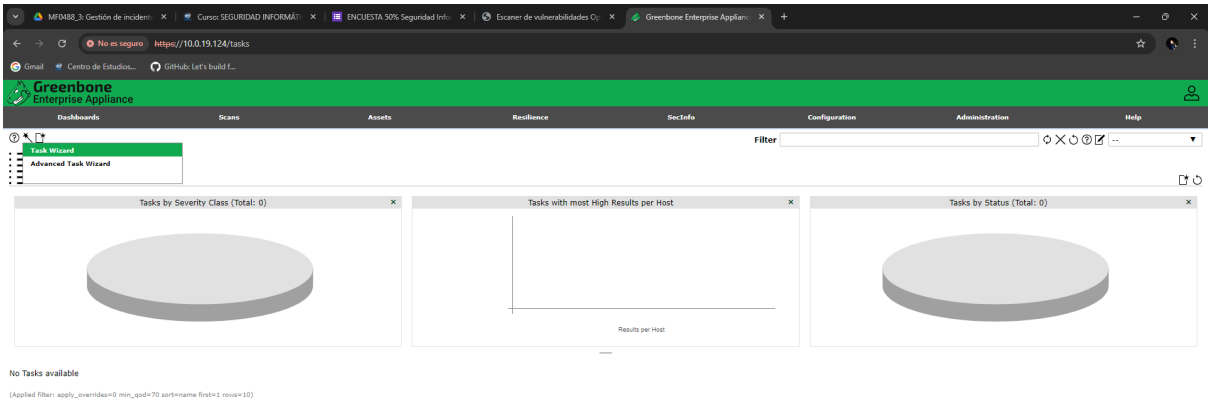

Greenbone
Enterprise Appliance
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Report:Thu, Sep 19, 2024 8:24 AM UTC
Done
Information Results (69 of 598) Hosts (1 of 1) Ports (19 of 23) Applications (19 of 19) Operating Systems (1 of 1) CVEs (35 of 35) Closed CVEs (0 of 0) TLS Certificates (2 of 2) Error Messages (0 of 0) User Tags (0)
Operating System CPE Hosts Severity
Ubuntu 8.04 cpe:/o:canonical:ubuntu_linux:8.04 1 10.0 (High)
1 - 1 of 1
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net


Greenbone
Enterprise Appliance
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Report:Thu, Sep 19, 2024 8:24 AM UTC
Done
Information Results (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)
Application CPE Hosts Occurrences Severity
cpe:/a:beasts: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 9.0 (High)
cpe:/a:samba:samba:3.0.20 1 1 6.0 (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
1 - 19 of 19
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

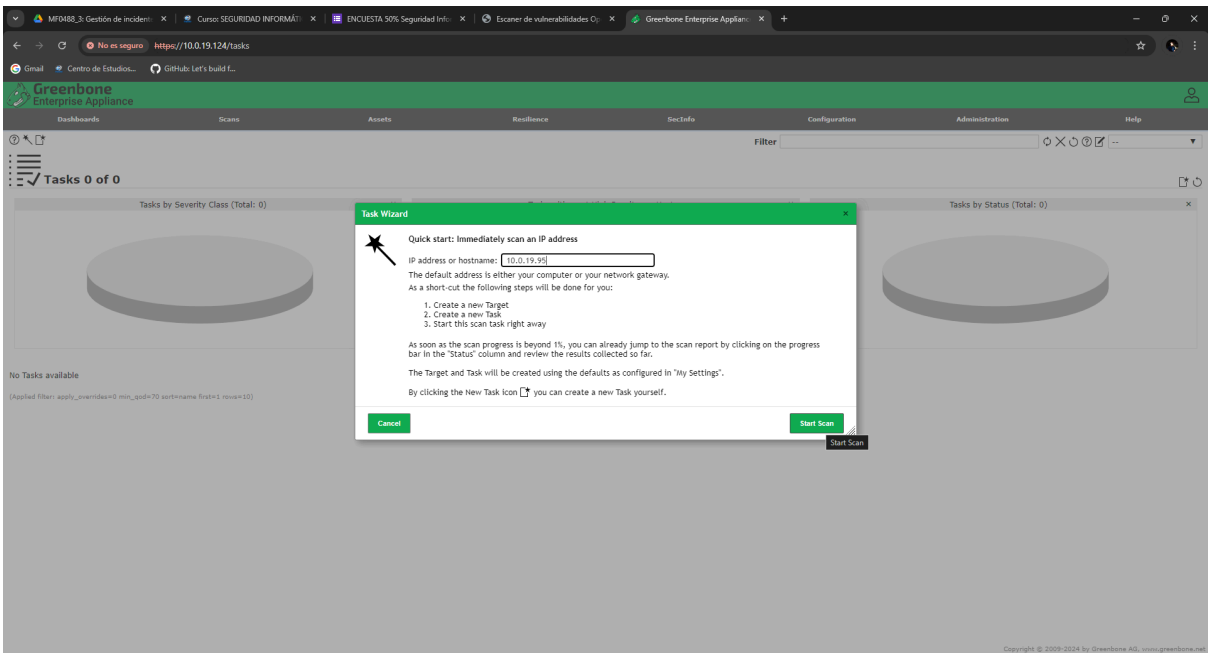


METASPLOITABLE3 WINDOWS:

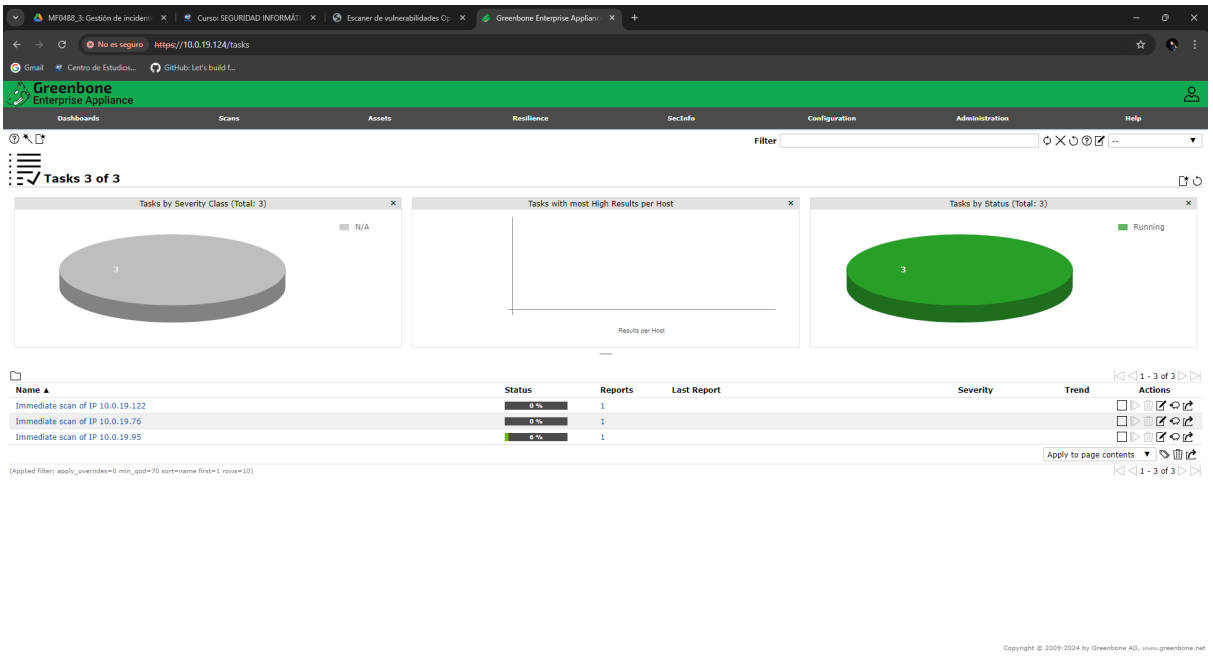
Vamos a arrancar la máquina Metasploitable3 Windows. Obtenemos su ip. Vamos a realizar el escaneo de vulnerabilidades. Para ello, pulsamos en la pestaña Scans. Pulsamos sobre el icono Task Wizard:



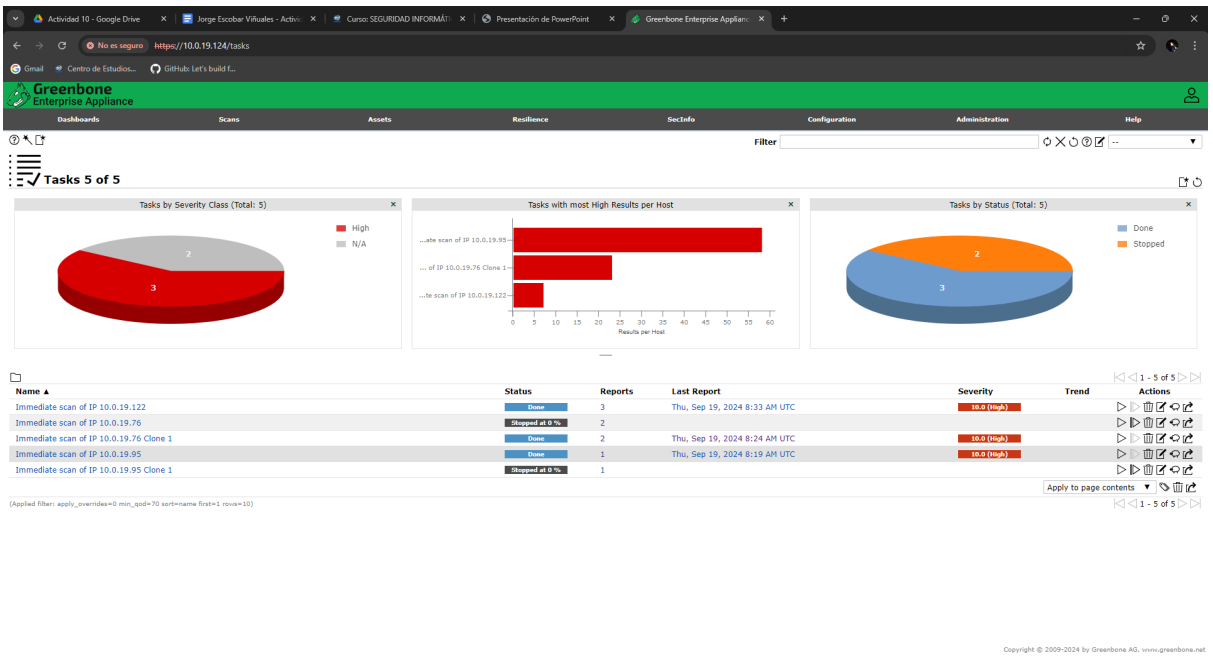
Escribimos la Ip de la máquina Metasploitable3 Ubuntu y pulsamos Start Scan:



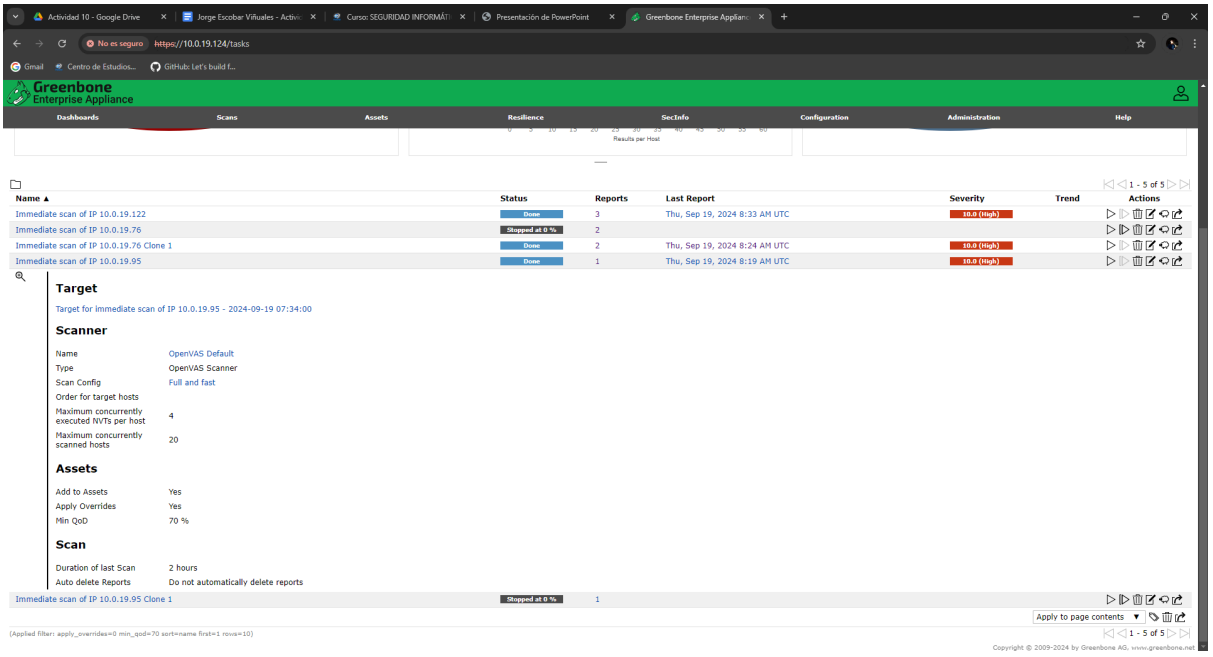
Comienza el escaneo de vulnerabilidades del sitio Web:



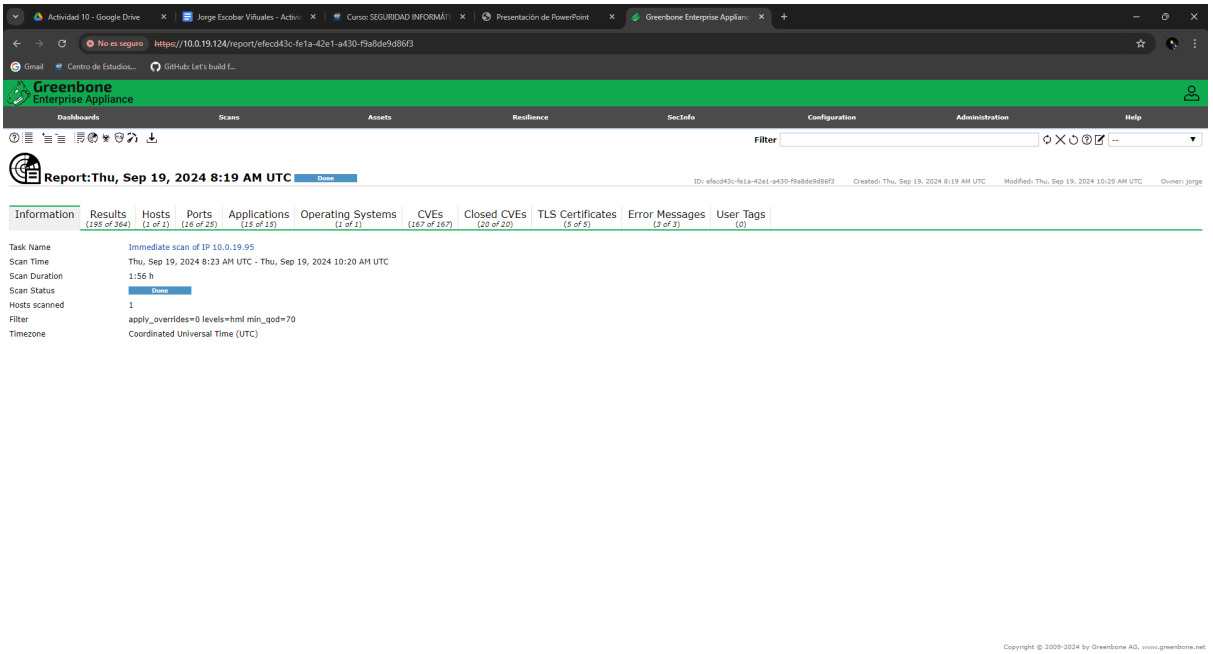
Una vez finalizado, nos muestra gráficamente el resultado:



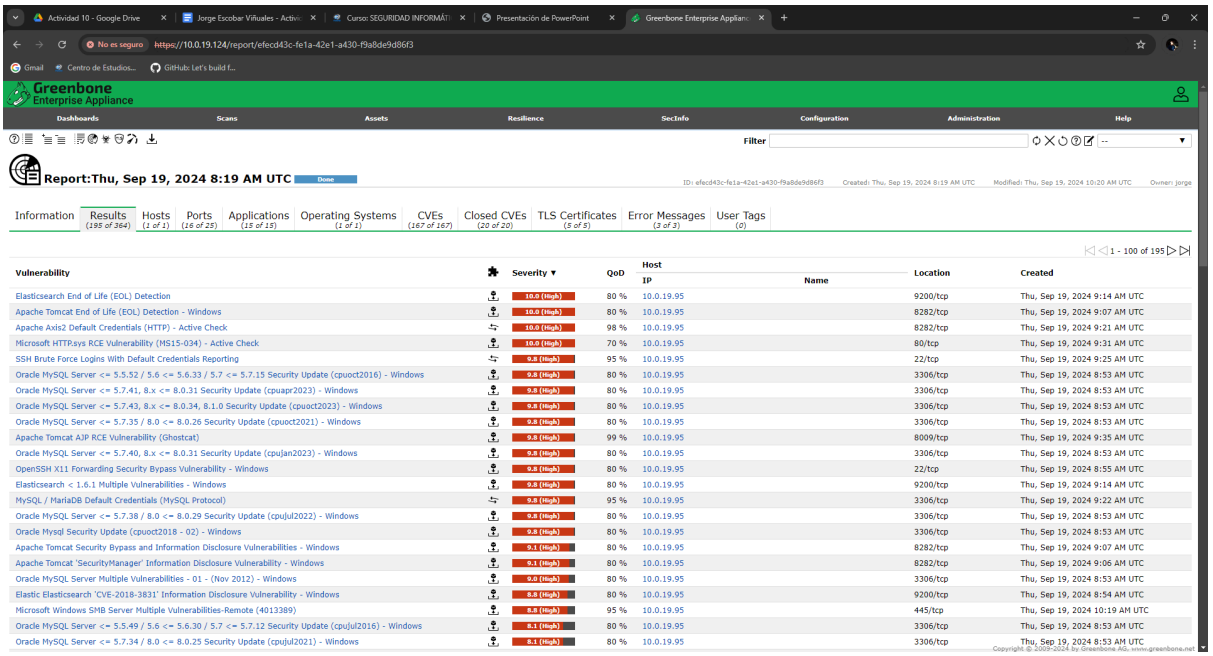
Si pulsamos en el apartado Name, nos muestra los datos generales del escaneo:

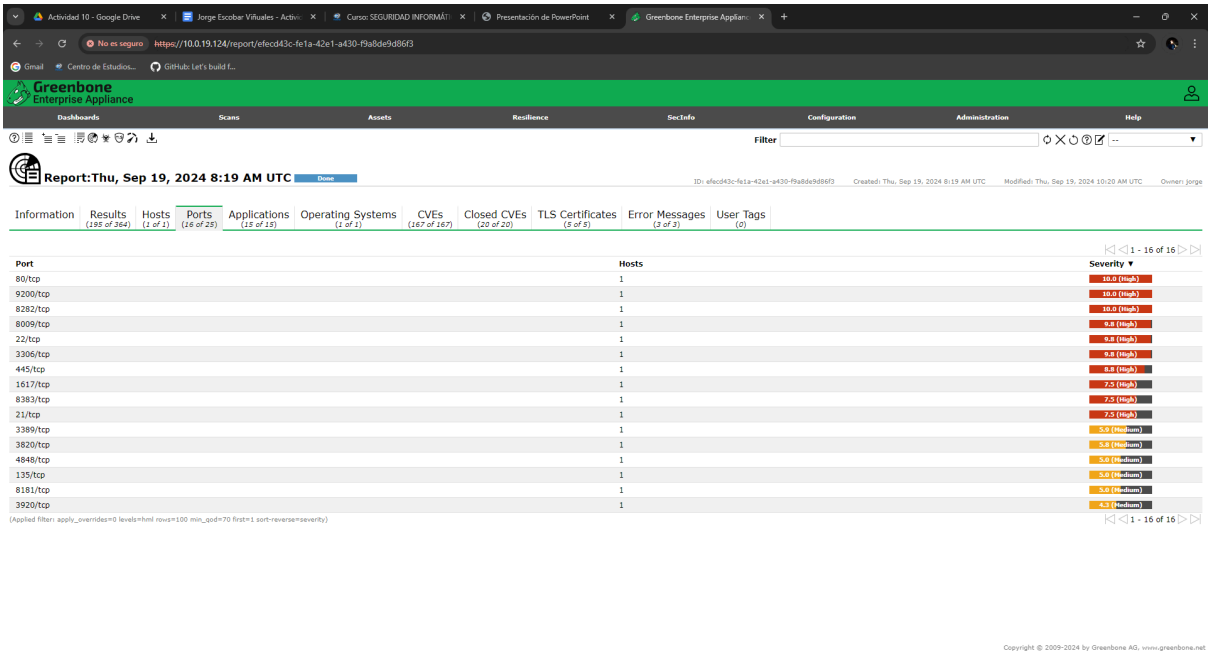


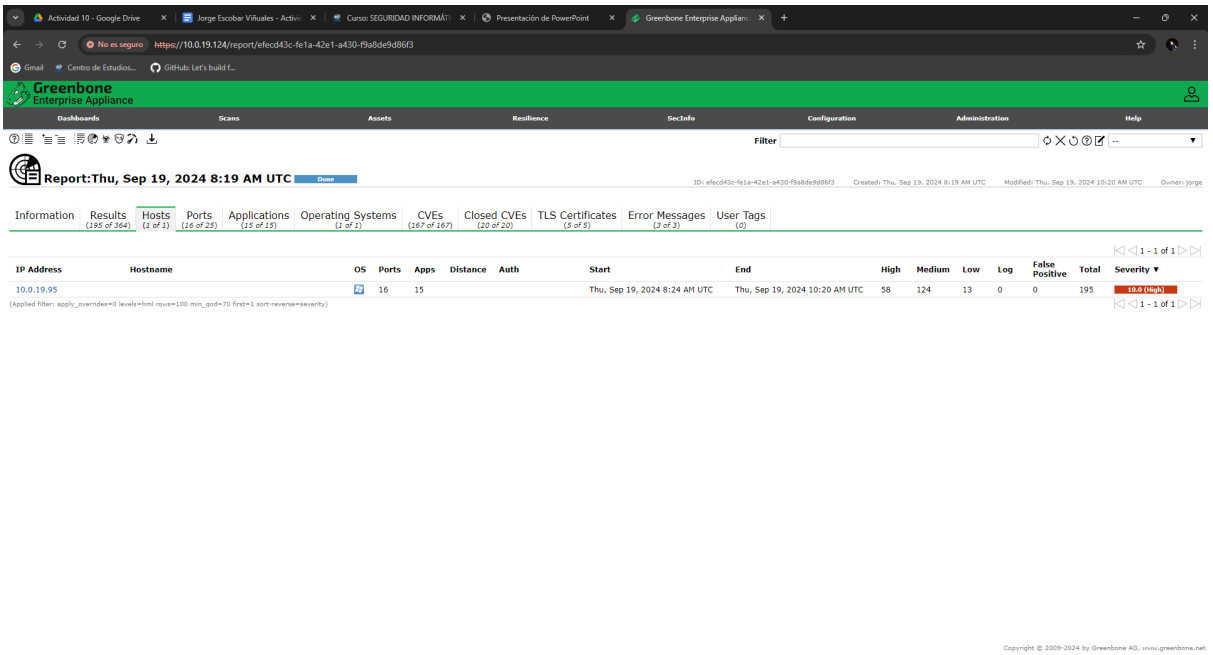
Si pulsamos en el apartado Last Report nos muestra el resultado del análisis:

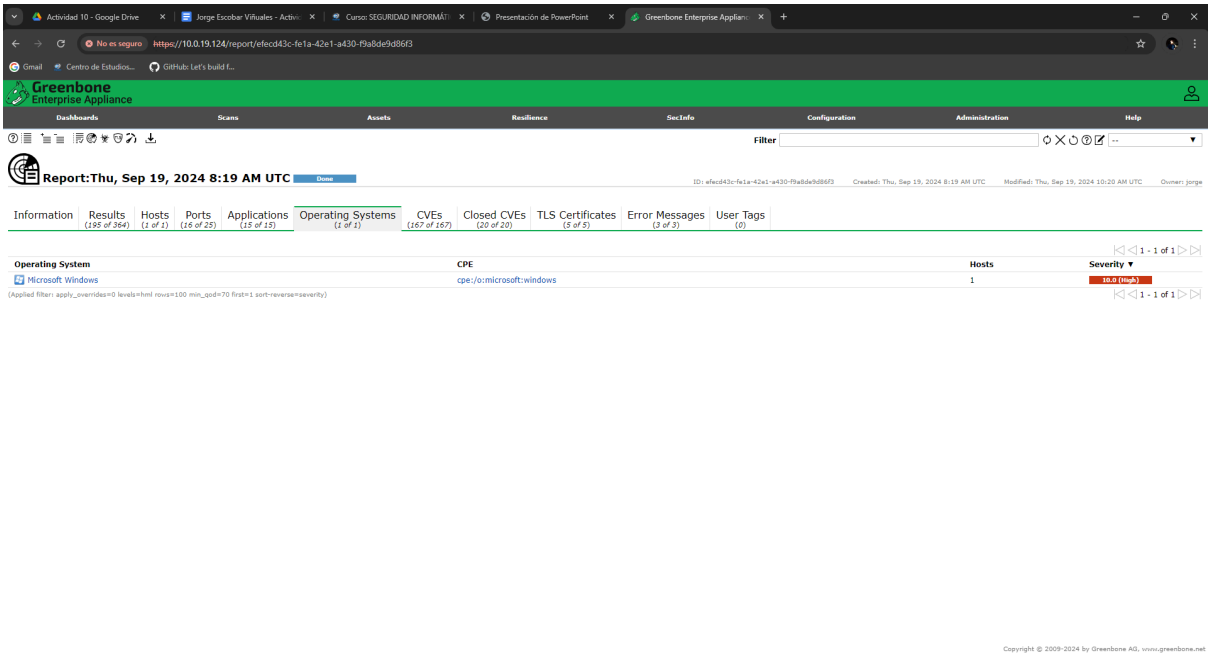


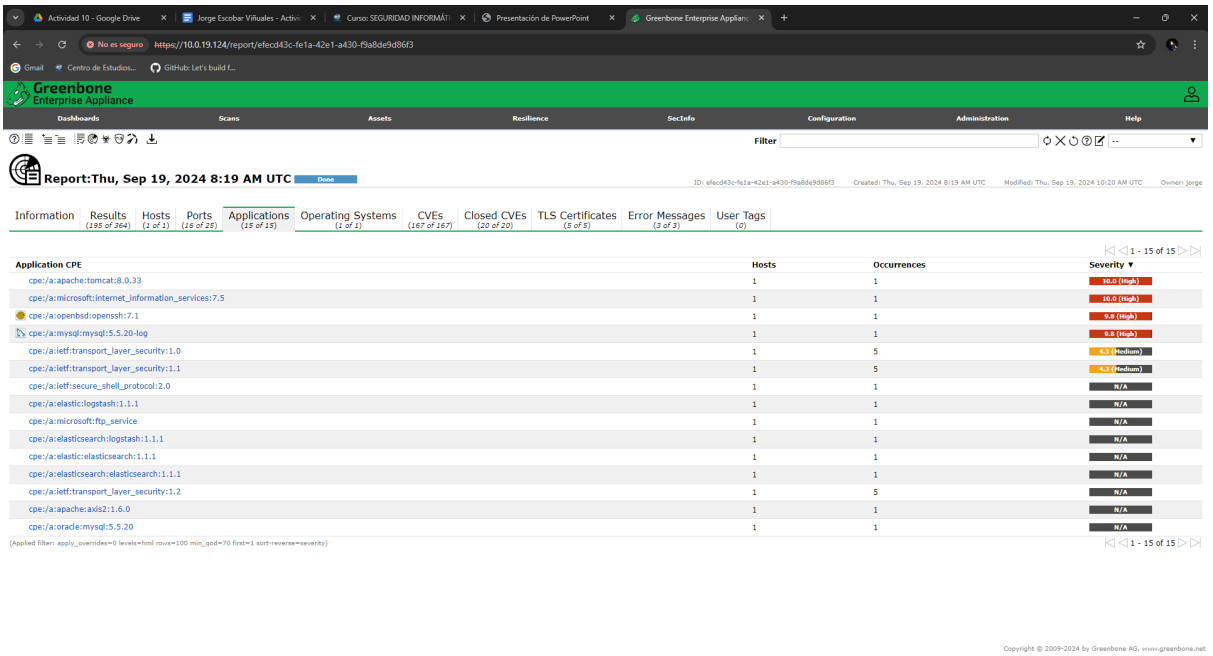
En cada una de las pestañas, nos muestra información detallada:

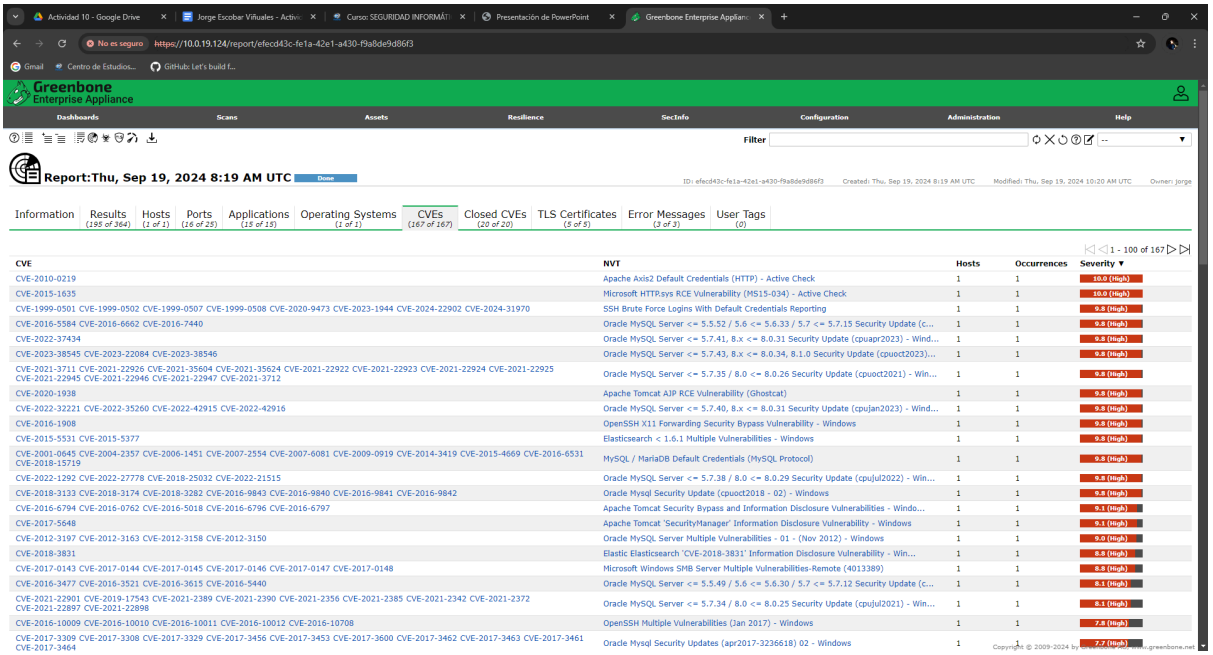


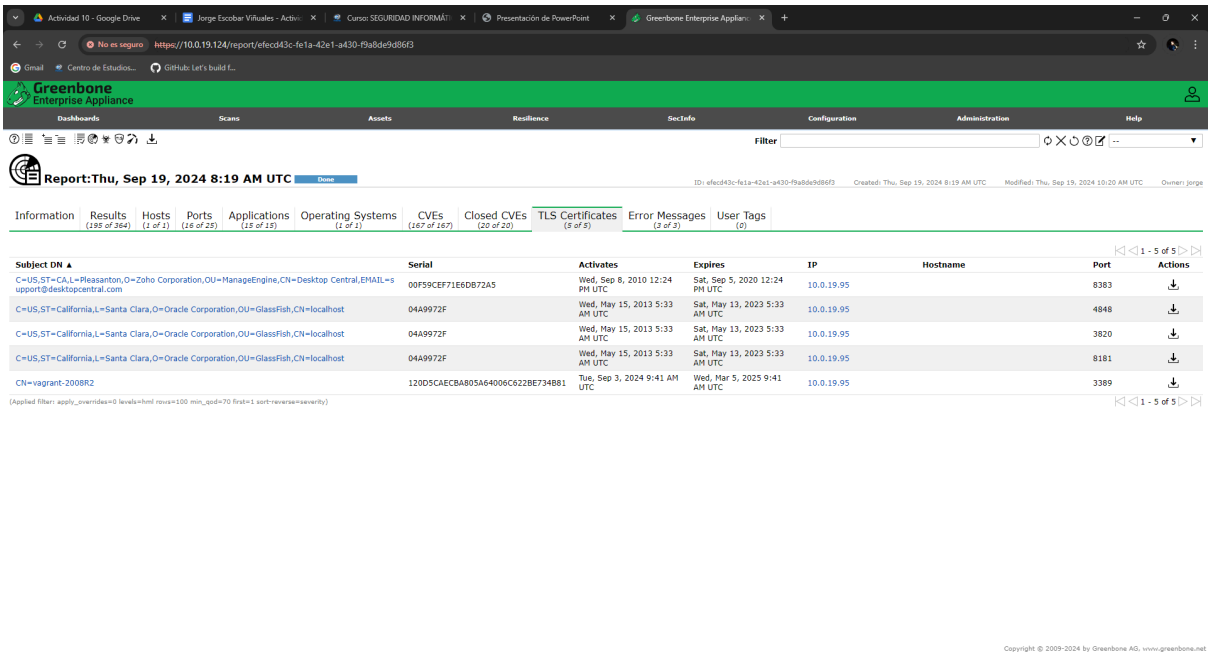

Greenbone
Enterprise Appliance
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Report:Thu, Sep 19, 2024 8:19 AM UTC
Done
Information Results (195 of 364) Hosts (1 of 1) Ports (16 of 25) Applications (15 of 15) Operating Systems (1 of 1) CVEs (167 of 167) Closed CVEs (20 of 20) TLS Certificates (5 of 5) Error Messages (3 of 3) User Tags (0)
1 - 16 of 16
Port Hosts Severity
80/tcp 1 10.0 (High)
9200/tcp 1 10.0 (High)
8282/tcp 1 10.0 (High)
8009/tcp 1 9.8 (High)
22/tcp 1 9.8 (High)
3306/tcp 1 9.8 (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 5.0 (Medium)
135/tcp 1 5.0 (Medium)
8181/tcp 1 5.0 (Medium)
3920/tcp 1 4.3 (Medium)
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)
1 - 16 of 16
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

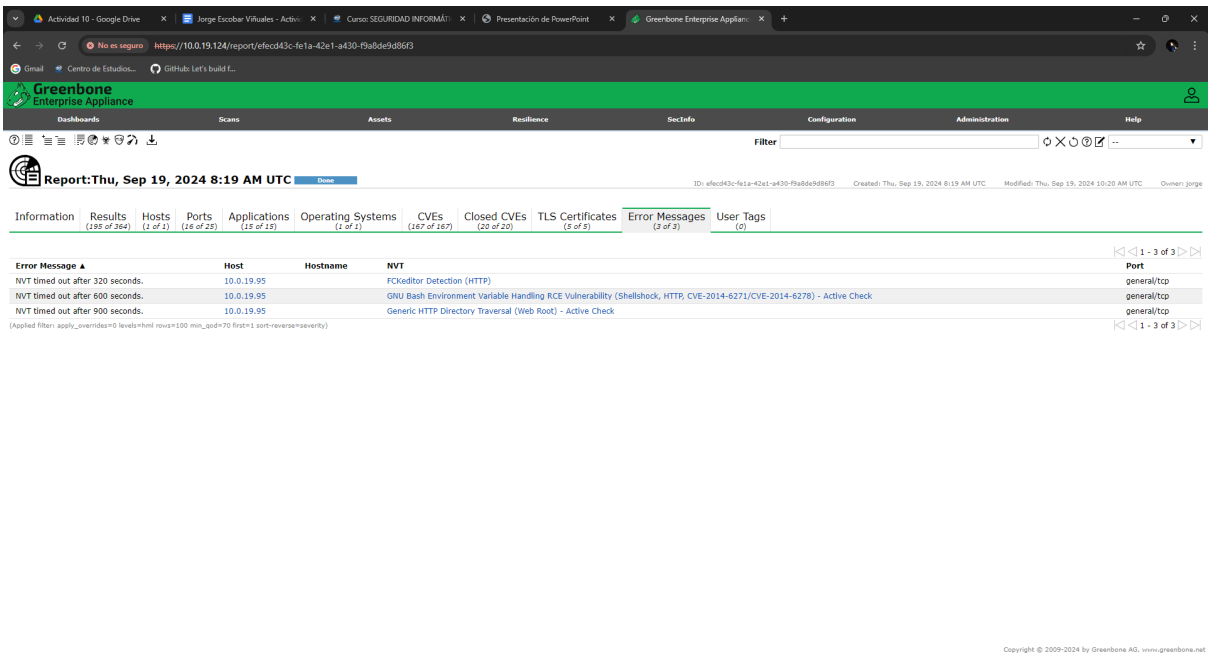

Greenbone
Enterprise Appliance
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Report:Thu, Sep 19, 2024 8:19 AM UTC
Done
Information Results (195 of 364) Hosts (1 of 1) Ports (16 of 25) Applications (15 of 15) Operating Systems (1 of 1) CVEs (167 of 167) Closed CVEs (20 of 20) TLS Certificates (5 of 5) Error Messages (3 of 3) User Tags (0)
1 - 1 of 1
IP Address Hostname OS Ports Apps Distance Auth Start End High Medium Low Log False Positive Total Severity
10.0.19.95 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)
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)
1 - 1 of 1
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net


Actividad 10 - Google Drive
Jorge Escobar Viñuales - Activi
Curso: SEGURIDAD INFORMÁTI
Presentación de PowerPoint
Greenbone Enterprise Appliance
No es seguro
https://10.0.19.124/report/efecd43c-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
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)
1 - 1 of 1
Operating System
CPE
Hosts
Severity
Microsoft Windows
cpe:/o:microsoft:windows
1
10.0 (High)
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=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 INFORMÁTI
Presentación de PowerPoint
Greenbone Enterprise Appliance
No es seguro
https://10.0.19.124/report/efecd43c-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
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)
1 - 15 of 15
Application CPE
Hosts
Occurrences
Severity
cpe:/a:apache:tomcat:8.0.33
cpe:/a:microsoft:internet_information_services:7.5
cpe:/a:openbsd:openssh:7.1
cpe:/a:mysql:mysql:5.5.20-log
cpe:/a:ietf:transport_layer_security:1.0
cpe:/a:ietf:transport_layer_security:1.1
cpe:/a:ietf:secure_shell_protocol:2.0
cpe:/a:elastic:logstash:1.1.1
cpe:/a:microsoft:ftp_service
cpe:/a:elasticsearch:logstash:1.1.1
cpe:/a:elastic:elasticsearch:1.1.1
cpe:/a:elasticsearch:elasticsearch:1.1.1
cpe:/a:ietf:transport_layer_security:1.2
cpe:/a:apache:axis2:1.6.0
cpe:/a:oracle:mysql:5.5.20
10.0 (High)
9.8 (High)
4.3 (Medium)
N/A
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net

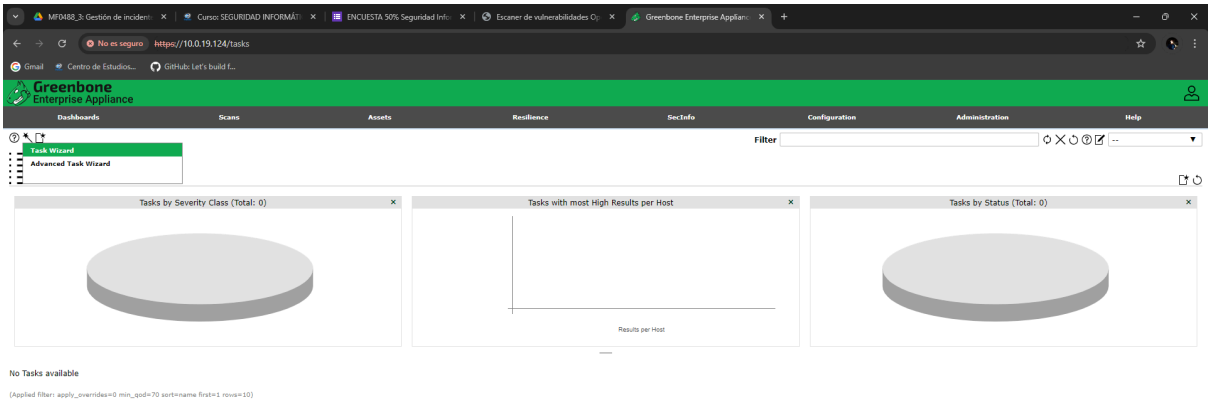

Greenbone Enterprise Appliance
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Report:Thu, Sep 19, 2024 8:19 AM UTC
Information Results Hosts Ports Applications Operating Systems CVEs Closed CVEs TLS Certificates Error Messages User Tags
CVE NVT Hosts Occurrences Severity
CVE-2010-0219 Apache Axis2 Default Credentials (HTTP) - Active Check 10.0 (High)
CVE-2015-1635 Microsoft HTTP.sys RCE Vulnerability (MS15-034) - Active Check 10.0 (High)
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 9.8 (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 (c... 9.8 (High)
CVE-2022-37434 Oracle MySQL Server <= 5.7.41, 8.x <= 8.0.31 Security Update (cpuapr2023) - Wind... 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)... 9.8 (High)
CVE-2021-3711 CVE-2021-22926 CVE-2021-35604 CVE-2021-35624 CVE-2021-22922 CVE-2021-22923 CVE-2021-22924 CVE-2021-22925 CVE-2021-22945 CVE-2021-22946 CVE-2021-22947 CVE-2021-3712 Oracle MySQL Server <= 5.7.35 / 8.0 <= 8.0.26 Security Update (cpuoct2021) - Win... 9.8 (High)
CVE-2020-1938 Apache Tomcat AJP RCE Vulnerability (Ghostcat) 9.8 (High)
CVE-2022-32221 CVE-2022-35260 CVE-2022-42915 CVE-2022-42916 Oracle MySQL Server <= 5.7.40, 8.x <= 8.0.31 Security Update (cpujan2023) - Wind... 9.8 (High)
CVE-2016-1908 OpenSSH X11 Forwarding Security Bypass Vulnerability - Windows 9.8 (High)
CVE-2015-5531 CVE-2015-5377 Elasticsearch < 1.6.1 Multiple Vulnerabilities - Windows 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 CVE-2018-15719 MySQL / MariaDB Default Credentials (MySQL Protocol) 9.8 (High)
CVE-2022-1292 CVE-2022-27778 CVE-2018-25032 CVE-2022-21515 Oracle MySQL Server <= 5.7.38 / 8.0 <= 8.0.29 Security Update (cpujul2022) - Win... 9.8 (High)
CVE-2018-3133 CVE-2018-3174 CVE-2018-3282 CVE-2016-9843 CVE-2016-9840 CVE-2016-9841 CVE-2016-9842 Oracle Mysql Security Update (cpuoct2018 - 02) - Windows 9.8 (High)
CVE-2016-6794 CVE-2016-0762 CVE-2016-5018 CVE-2016-6796 CVE-2016-6797 Apache Tomcat Security Bypass and Information Disclosure Vulnerabilities - Windo... 9.1 (High)
CVE-2017-5648 Apache Tomcat 'SecurityManager' Information Disclosure Vulnerability - Windows 9.1 (High)
CVE-2012-3197 CVE-2012-3163 CVE-2012-3158 CVE-2012-3150 Oracle MySQL Server Multiple Vulnerabilities - 01 - (Nov 2012) - Windows 9.0 (High)
CVE-2018-3831 Elastic Elasticsearch 'CVE-2018-3831' Information Disclosure Vulnerability - Win... 8.8 (High)
CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148 Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) 8.8 (High)
CVE-2016-3477 CVE-2016-3521 CVE-2016-3615 CVE-2016-5440 Oracle MySQL Server <= 5.5.49 / 5.6 <= 5.6.30 / 5.7 <= 5.7.12 Security Update (c... 8.1 (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 CVE-2021-22897 CVE-2021-22898 Oracle MySQL Server <= 5.7.34 / 8.0 <= 8.0.25 Security Update (cpujul2021) - Win... 8.1 (High)
CVE-2016-10009 CVE-2016-10010 CVE-2016-10011 CVE-2016-10012 CVE-2016-10708 OpenSSH Multiple Vulnerabilities (Jan 2017) - Windows 7.8 (High)
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-2017-3464 Oracle Mysql Security Updates (apr2017-3236618) 02 - Windows 7.7 (High)


Greenbone Enterprise Appliance
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Report:Thu, Sep 19, 2024 8:19 AM UTC
Information Results Hosts Ports Applications Operating Systems CVEs Closed CVEs TLS Certificates Error Messages User Tags
Subject DN Serial Activates Expires IP Hostname Port Actions
C=US,ST=CA,L=Pleasanton,O=Zoho Corporation,OU=ManageEngine,CN=Desktop Central,EMAIL=support@desktopcentral.com 00F59CEF71E6DB72A5 Wed, Sep 8, 2010 12:24 PM UTC Sat, Sep 5, 2020 12:24 PM UTC 10.0.19.95 8383
C=US,ST=California,L=Santa Clara,O=Oracle Corporation,OU=GlassFish,CN=localhost 04A9972F Wed, May 15, 2013 5:33 AM UTC Sat, May 13, 2023 5:33 AM UTC 10.0.19.95 4848
C=US,ST=California,L=Santa Clara,O=Oracle Corporation,OU=GlassFish,CN=localhost 04A9972F Wed, May 15, 2013 5:33 AM UTC Sat, May 13, 2023 5:33 AM UTC 10.0.19.95 3820
C=US,ST=California,L=Santa Clara,O=Oracle Corporation,OU=GlassFish,CN=localhost 04A9972F Wed, May 15, 2013 5:33 AM UTC Sat, May 13, 2023 5:33 AM UTC 10.0.19.95 8181
CN=vagrant-2008R2 120D5CAECBA805A64006C622BE734B81 Tue, Sep 3, 2024 9:41 AM UTC Wed, Mar 5, 2025 9:41 AM UTC 10.0.19.95 3389

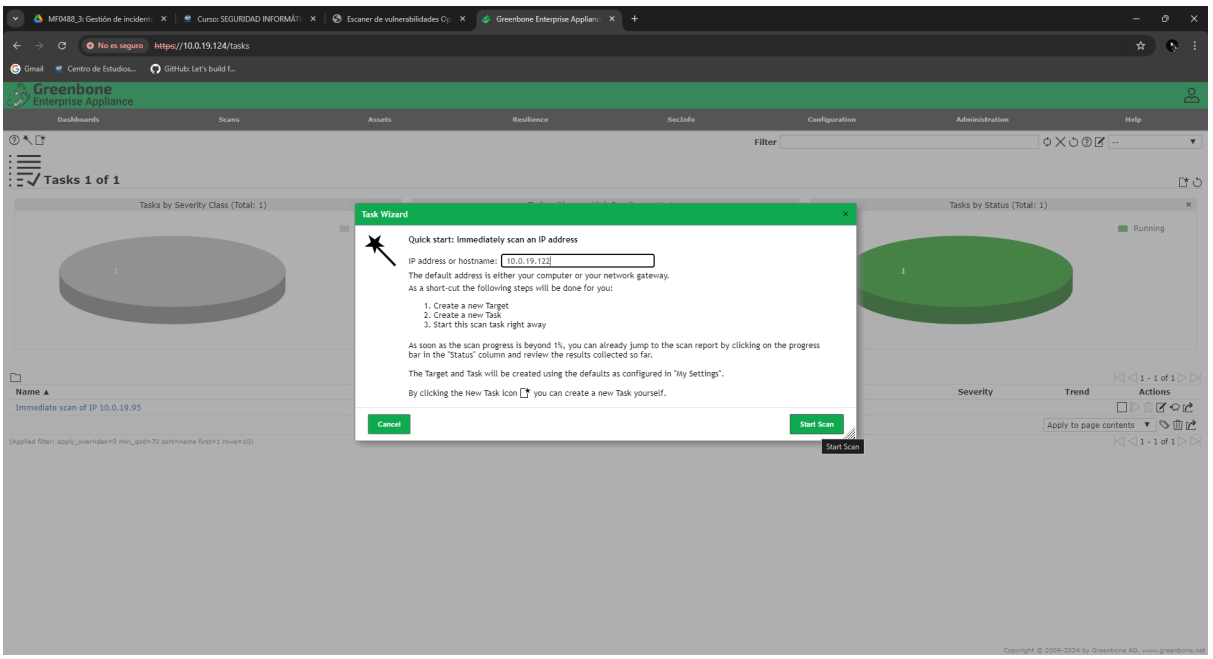


METASPLOITABLE3 UBUNTU:

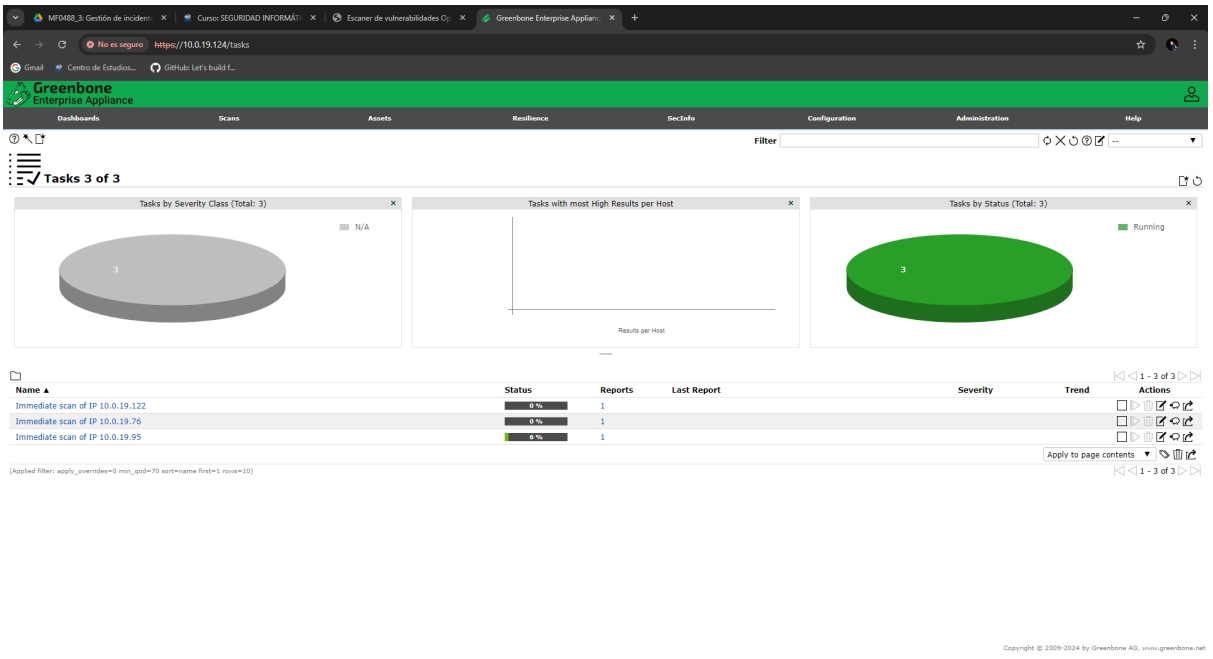
Vamos a arrancar la máquina Metasploitable3 Ubuntu. Obtenemos su ip. Vamos a realizar el escaneo de vulnerabilidades. Para ello, pulsamos en la pestaña Scans. Pulsamos sobre el icono Task Wizard:



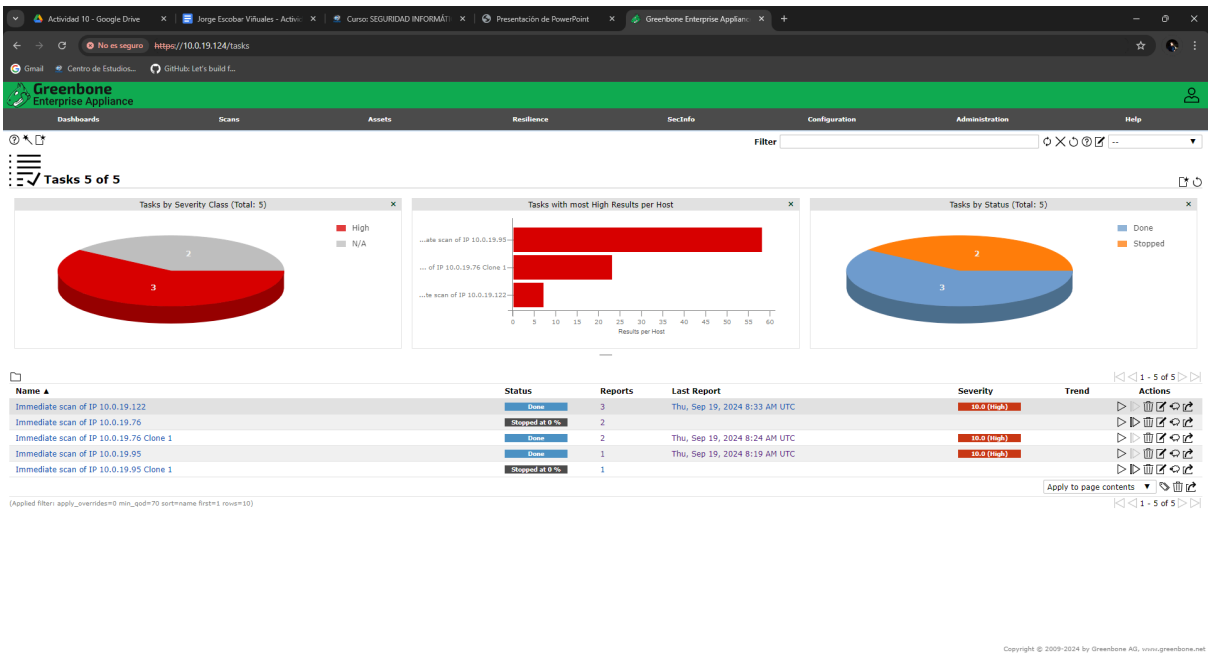
Escribimos la Ip de la máquina Metasploitable3 Ubuntu y pulsamos Start Scan:



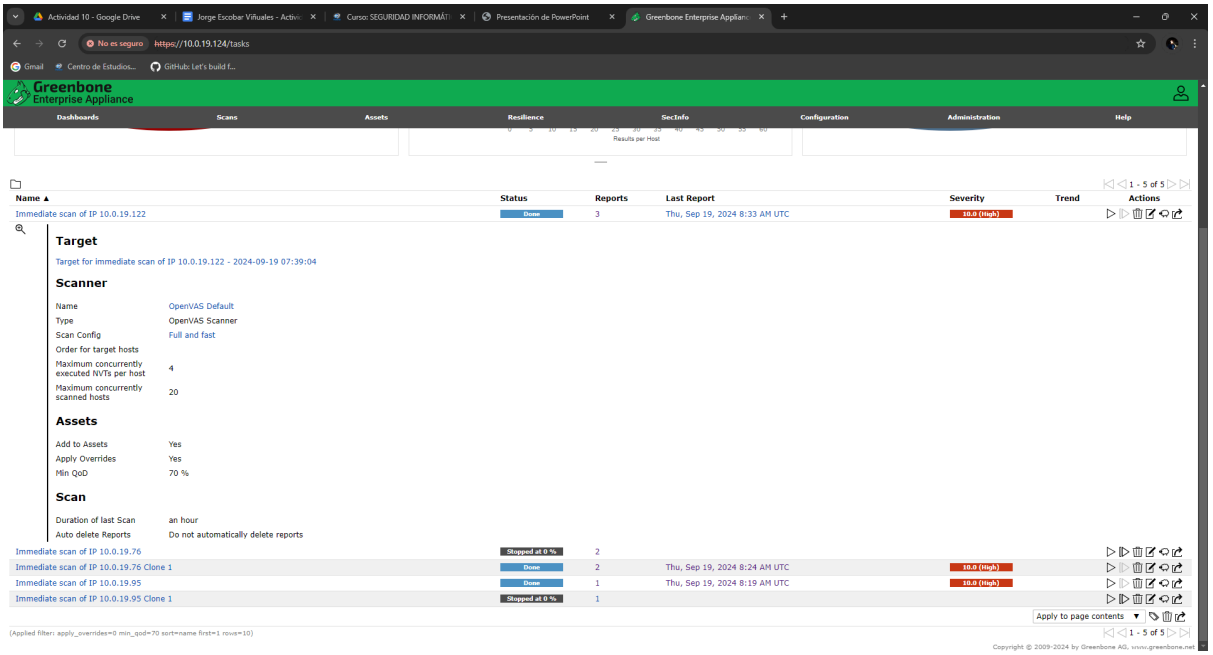
Comienza el escaneo de vulnerabilidades del sitio Web:



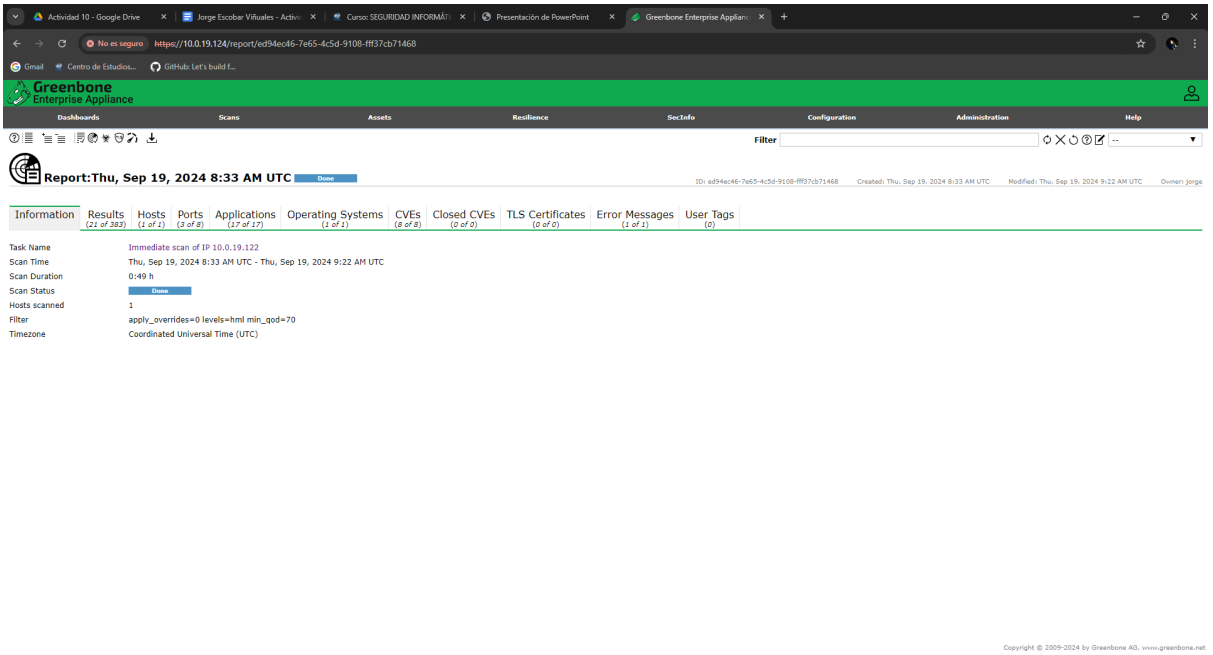
Una vez finalizado, nos muestra gráficamente el resultado:



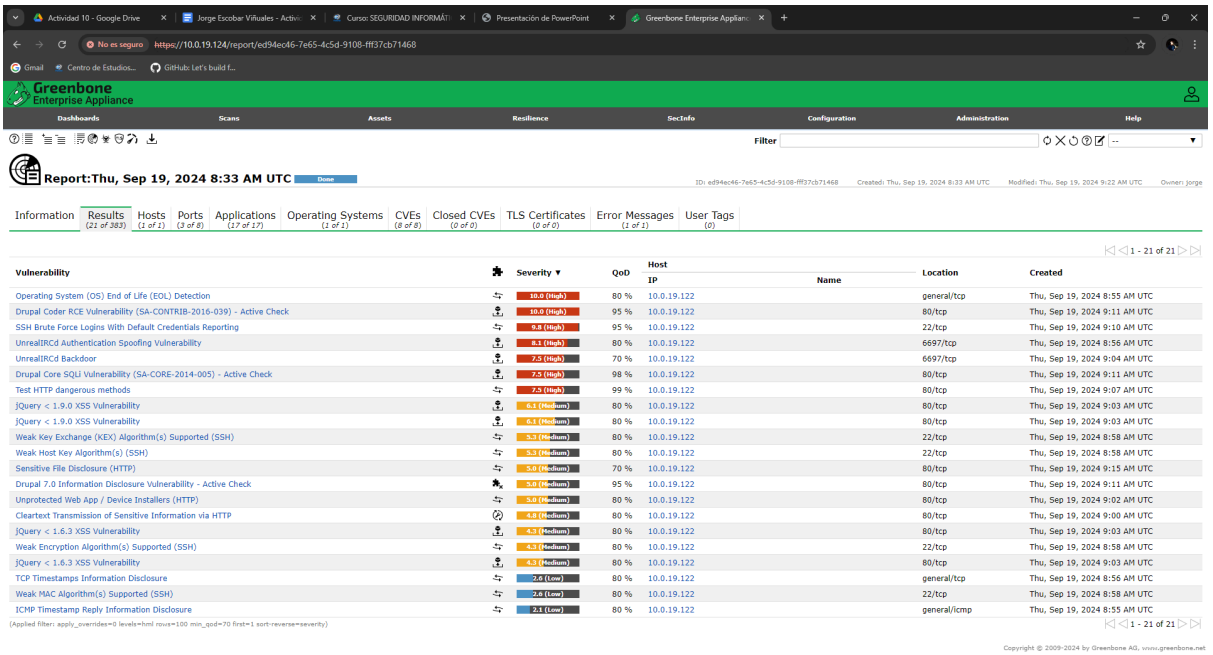
Si pulsamos en el apartado Name, nos muestra los datos generales del escaneo:

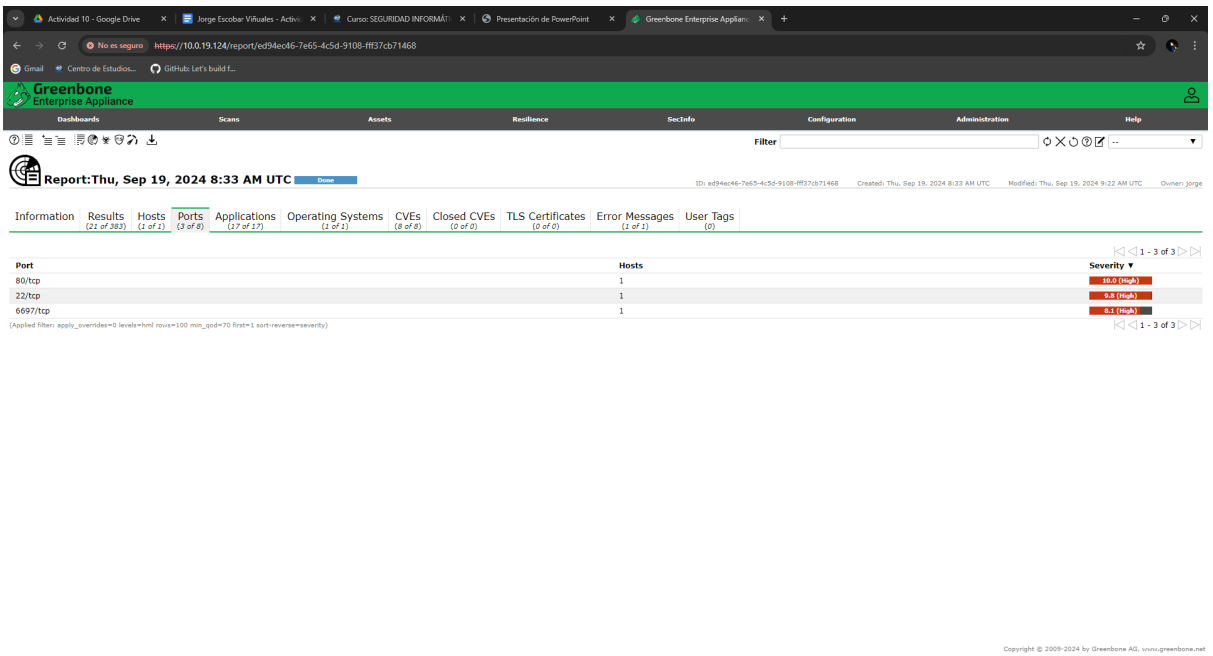


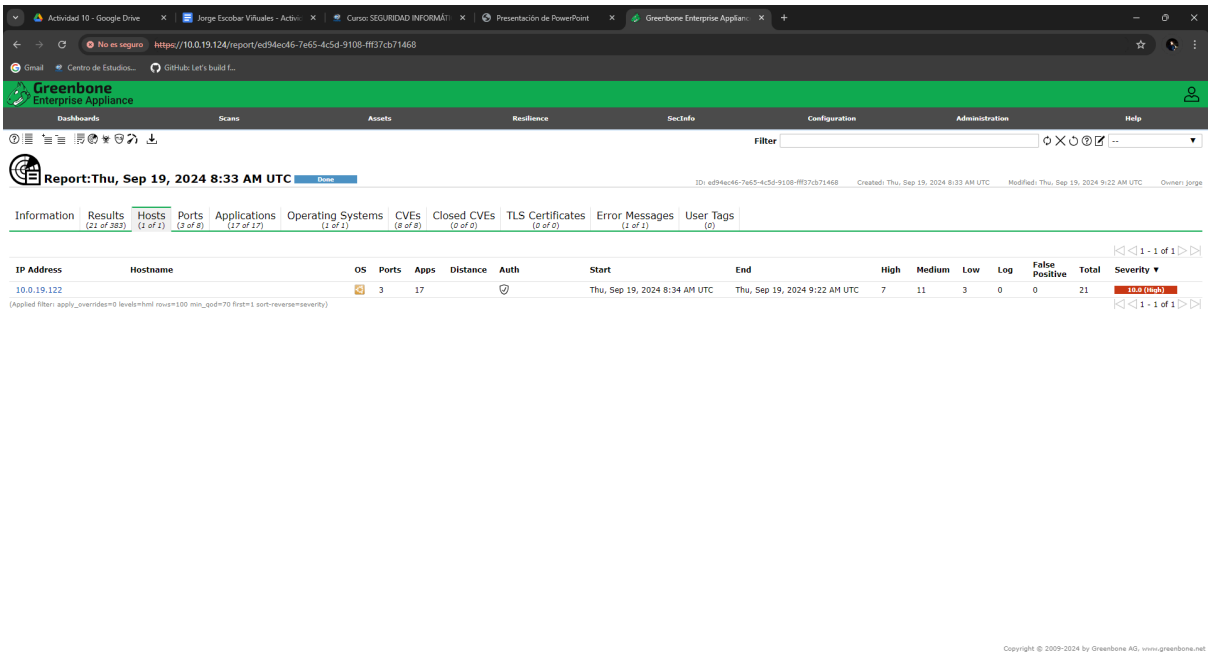
Si pulsamos en el apartado Last Report nos muestra el resultado del análisis:

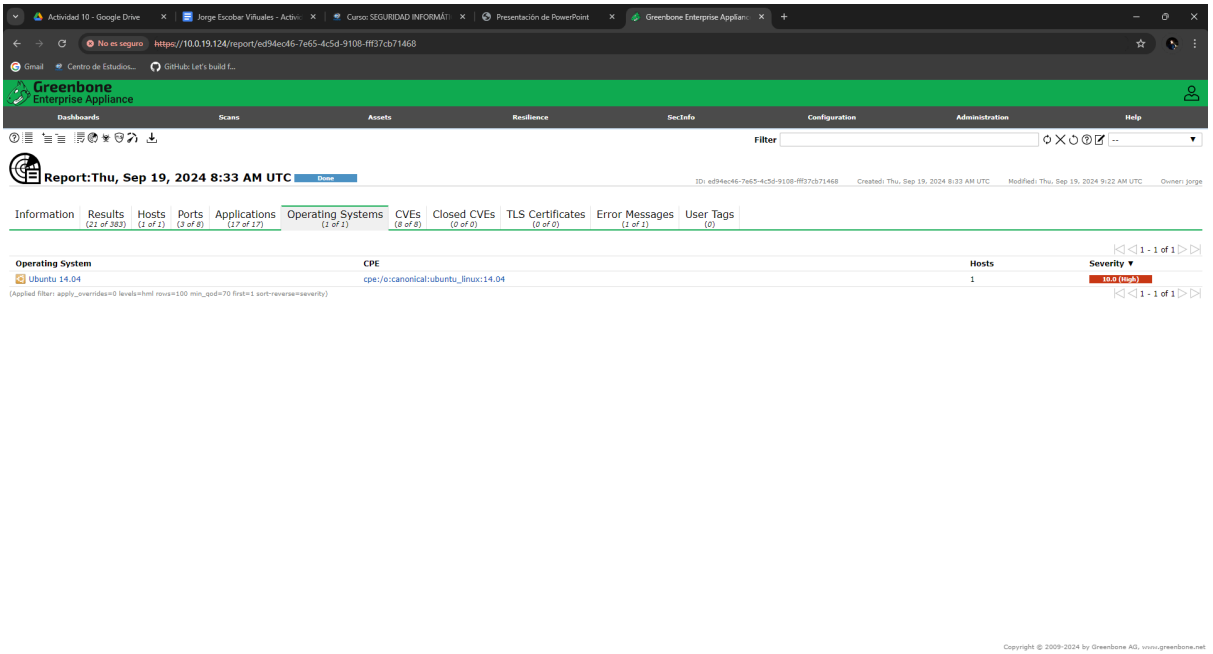


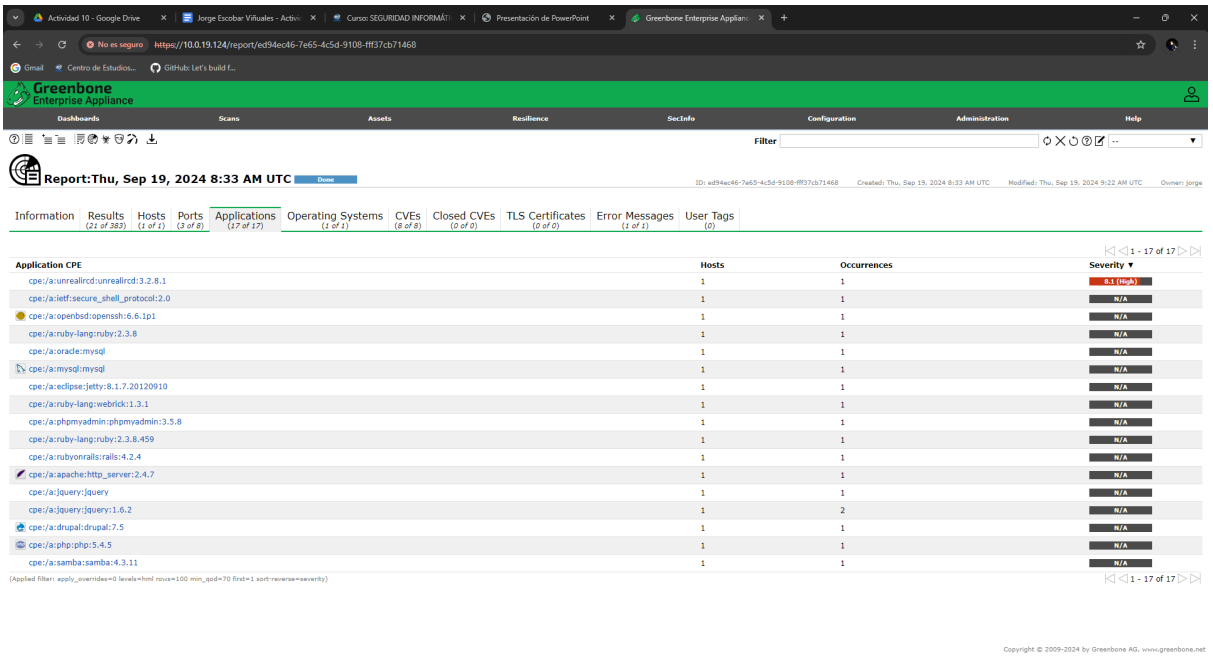
En cada una de las pestañas, nos muestra información detallada:

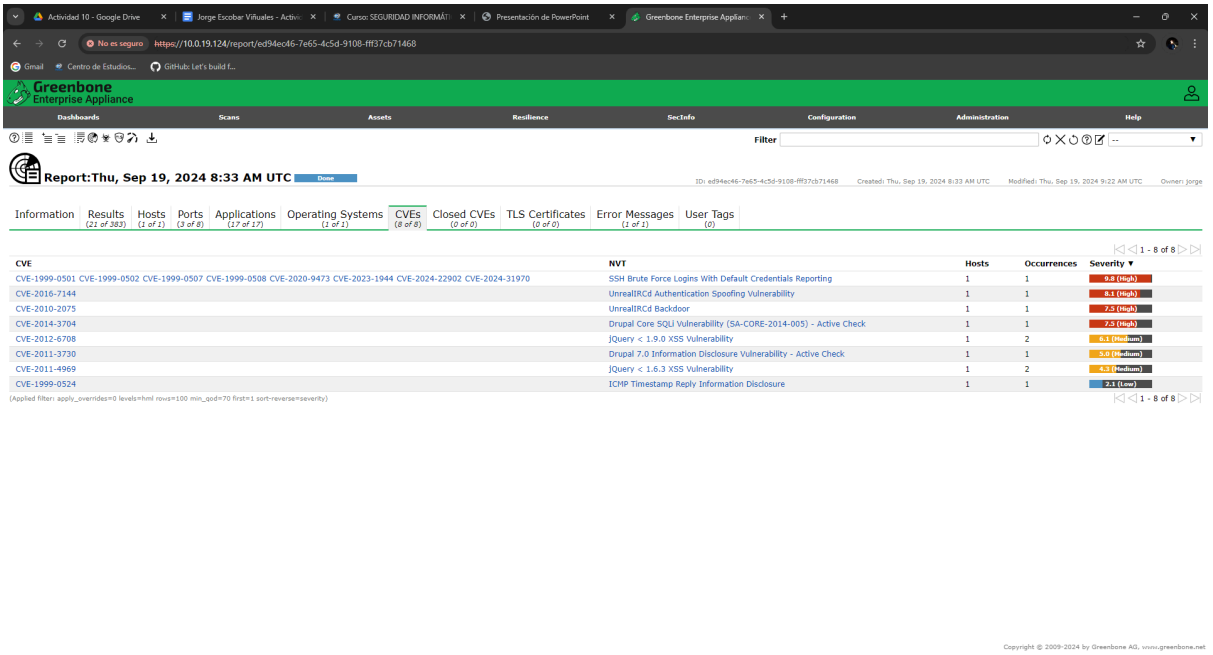


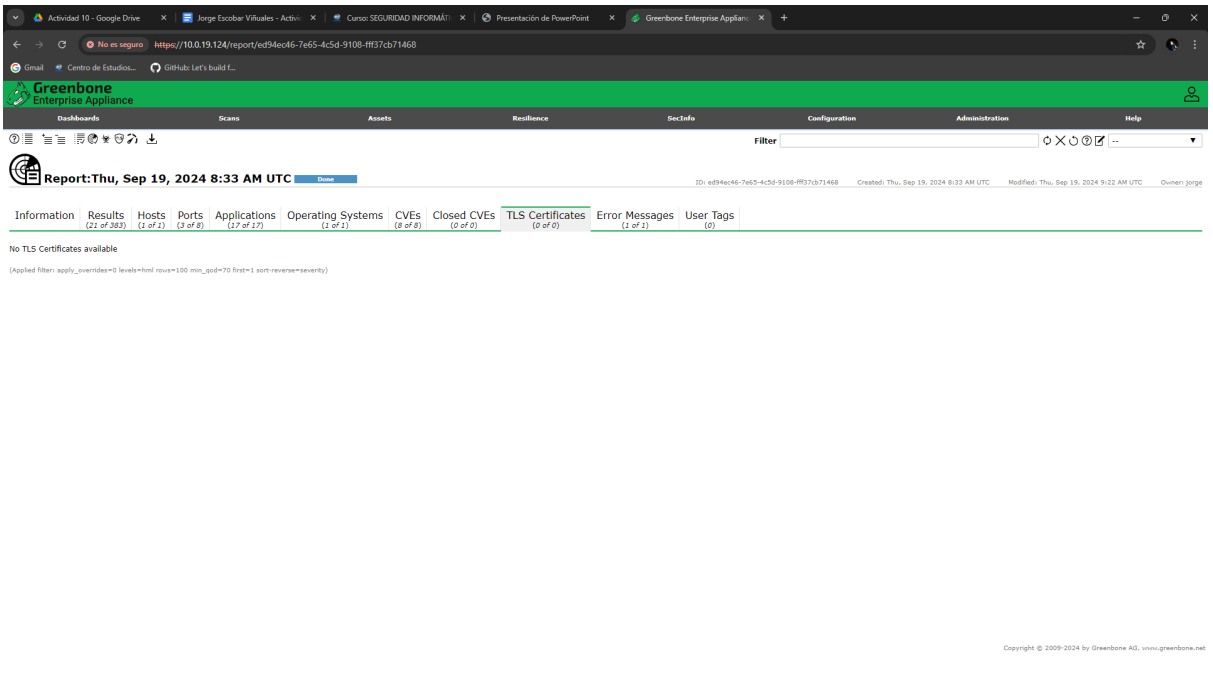

Actividad 10 - Google Drive
Jorge Escobar Viñuales - Activ
Curso: SEGURIDAD INFORMÁTI
Presentación de PowerPoint
Greenbone Enterprise Appliance
No es seguro
https://10.0.19.124/report/ed94ec46-7e65-4c5d-9108-fff37cb71468
Gmail
Centro de Estudios...
GitHub: Let's build f...
Greenbone
Enterprise Appliance
Dashboards
Scans
Assets
Resilience
SecInfo
Configuration
Administration
Help
Filter
Report:Thu, Sep 19, 2024 8:33 AM UTC
Done
ID: ed94ec46-7e65-4c5d-9108-fff37cb71468
Created: Thu, Sep 19, 2024 8:33 AM UTC
Modified: Thu, Sep 19, 2024 9:22 AM UTC
Owner: 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)
1 - 3 of 3
Port
Hosts
Severity
80/tcp
1
10.0 (High)
22/tcp
1
9.8 (High)
6697/tcp
1
8.1 (High)
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=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 - Activ
Curso: SEGURIDAD INFORMÁTI
Presentación de PowerPoint
Greenbone Enterprise Appliance
No es seguro
https://10.0.19.124/report/ed94ec46-7e65-4c5d-9108-fff37cb71468
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-fff37cb71468
Created: Thu, Sep 19, 2024 8:33 AM UTC
Modified: Thu, Sep 19, 2024 9:22 AM UTC
Owner: 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)
1 - 1 of 1
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=hml rows=100 min_qod=70 first=1 sort-reverse=severity)
1 - 1 of 1
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 8:33 AM UTC
Information Results Hosts Ports Applications Operating Systems CVEs Closed CVEs TLS Certificates Error Messages User Tags
Operating System CPE Hosts Severity
Ubuntu 14.04 cpe:/o:canonical:ubuntu_linux:14.04 1 10.0 (High)


Greenbone Enterprise Appliance
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Report:Thu, Sep 19, 2024 8:33 AM UTC
Information Results Hosts Ports Applications Operating Systems CVEs Closed CVEs TLS Certificates Error Messages User Tags
Application CPE Hosts Occurrences Severity
cpe:/a:unrealircd:unrealircd:3.2.8.1 1 1 8.1 (High)
cpe:/a:ietf:secure_shell_protocol:2.0 1 1 N/A
cpe:/a:openbsd:openssh:6.6.1p1 1 1 N/A
cpe:/a:ruby-lang:ruby:2.3.8 1 1 N/A
cpe:/a:oracle:mysql 1 1 N/A
cpe:/a:mysql:mysql 1 1 N/A
cpe:/a:eclipse:jetty:8.1.7.20120910 1 1 N/A
cpe:/a:ruby-lang:webrick:1.3.1 1 1 N/A
cpe:/a:phpmyadmin:phpmyadmin:3.5.8 1 1 N/A
cpe:/a:ruby-lang:ruby:2.3.8.459 1 1 N/A
cpe:/a:rubyonrails:rails:4.2.4 1 1 N/A
cpe:/a:apache:http_server:2.4.7 1 1 N/A
cpe:/a:jquery:jquery 1 1 N/A
cpe:/a:jquery:jquery:1.6.2 1 2 N/A
cpe:/a:drupal:drupal:7.5 1 1 N/A
cpe:/a:php:php:5.4.5 1 1 N/A
cpe:/a:samba:samba:4.3.11 1 1 N/A


Greenbone
Enterprise Appliance
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Report:Thu, Sep 19, 2024 8:33 AM UTC
Done
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)
1 - 8 of 8
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-2012-6708 JQuery < 1.9.0 XSS Vulnerability 1 2 6.1 (Medium)
CVE-2011-3730 Drupal 7.0 Information Disclosure Vulnerability - Active Check 1 1 5.0 (Medium)
CVE-2011-4969 JQuery < 1.6.3 XSS Vulnerability 1 2 4.3 (Medium)
CVE-1999-0524 ICMP Timestamp Reply Information Disclosure 1 1 2.1 (Low)
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)
1 - 8 of 8
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net


Greenbone
Enterprise Appliance
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Report:Thu, Sep 19, 2024 8:33 AM UTC
Done
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)
No TLS Certificates available
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)
Copyright © 2009-2024 by Greenbone AG, www.greenbone.net