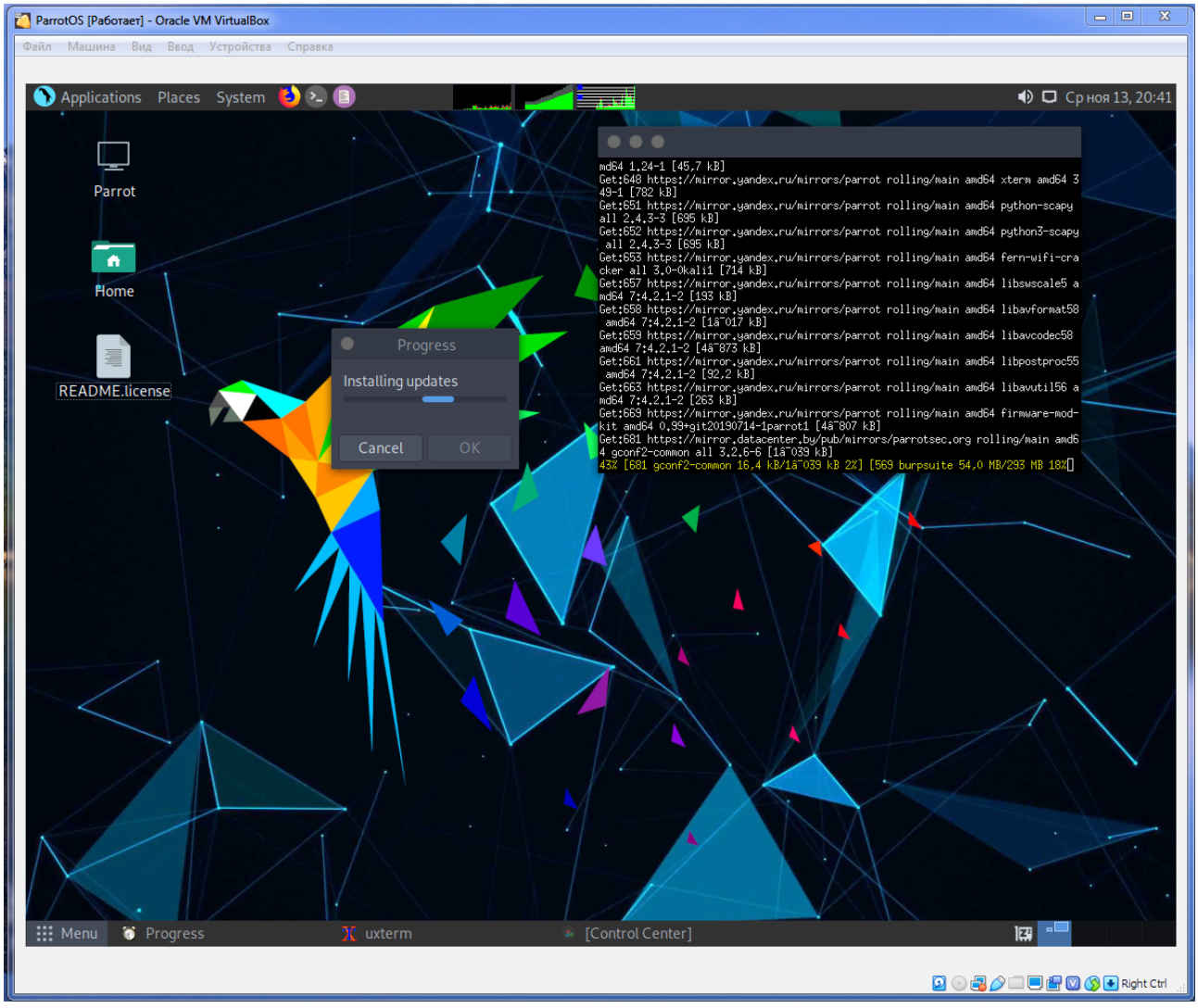
ДЗ 18
Цель: *Научиться приемам работы с сетевыми сканером OpenVAS, анализаторами и IDS/IPS системами*

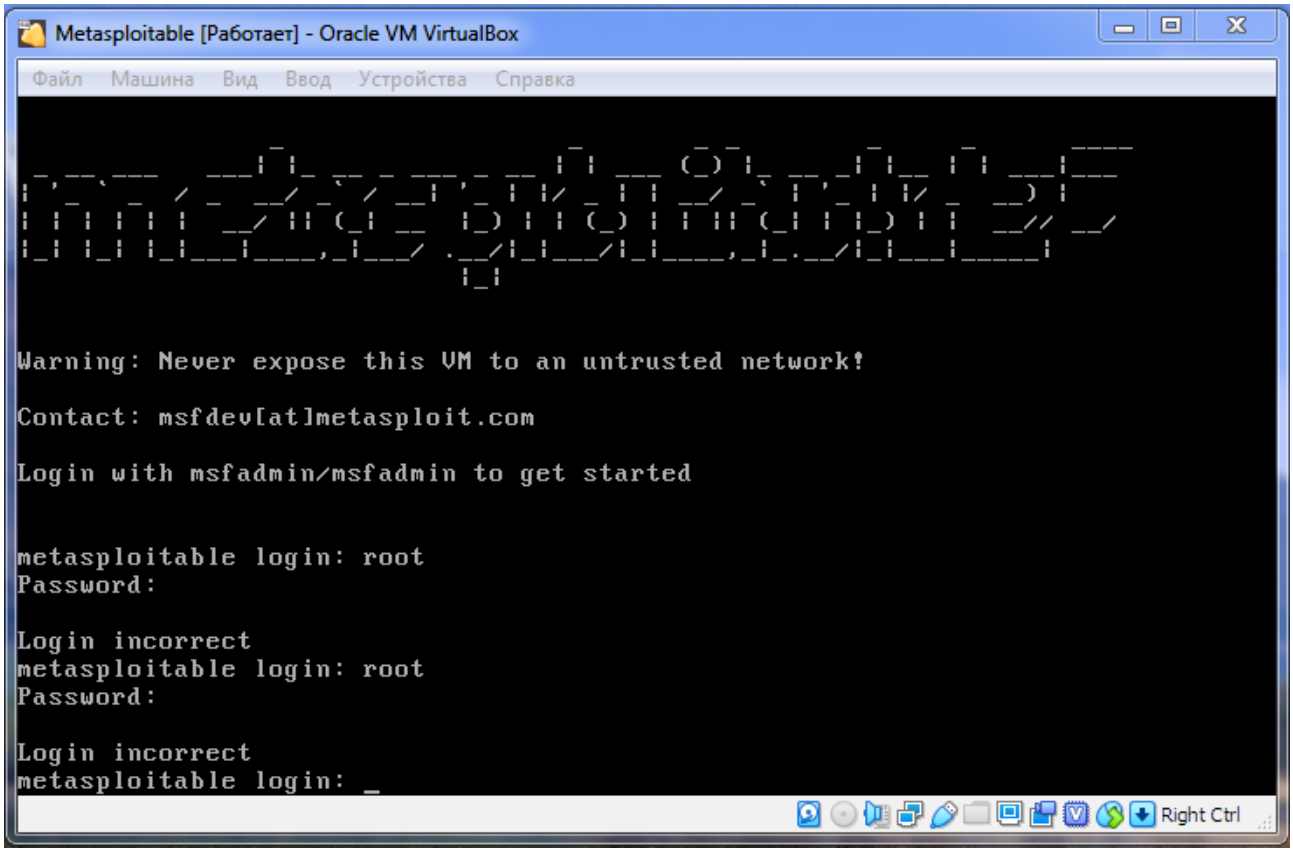
1. С помощью установленного сканера безопасности OpenVAS проверить наличие уязвимостей ПО и ядра Linux на примере Metasploitable2 и прислать отчет

1. Этап подготовительный:
На данном этапе мной было принято решение о использовании ОС ParrotOS.

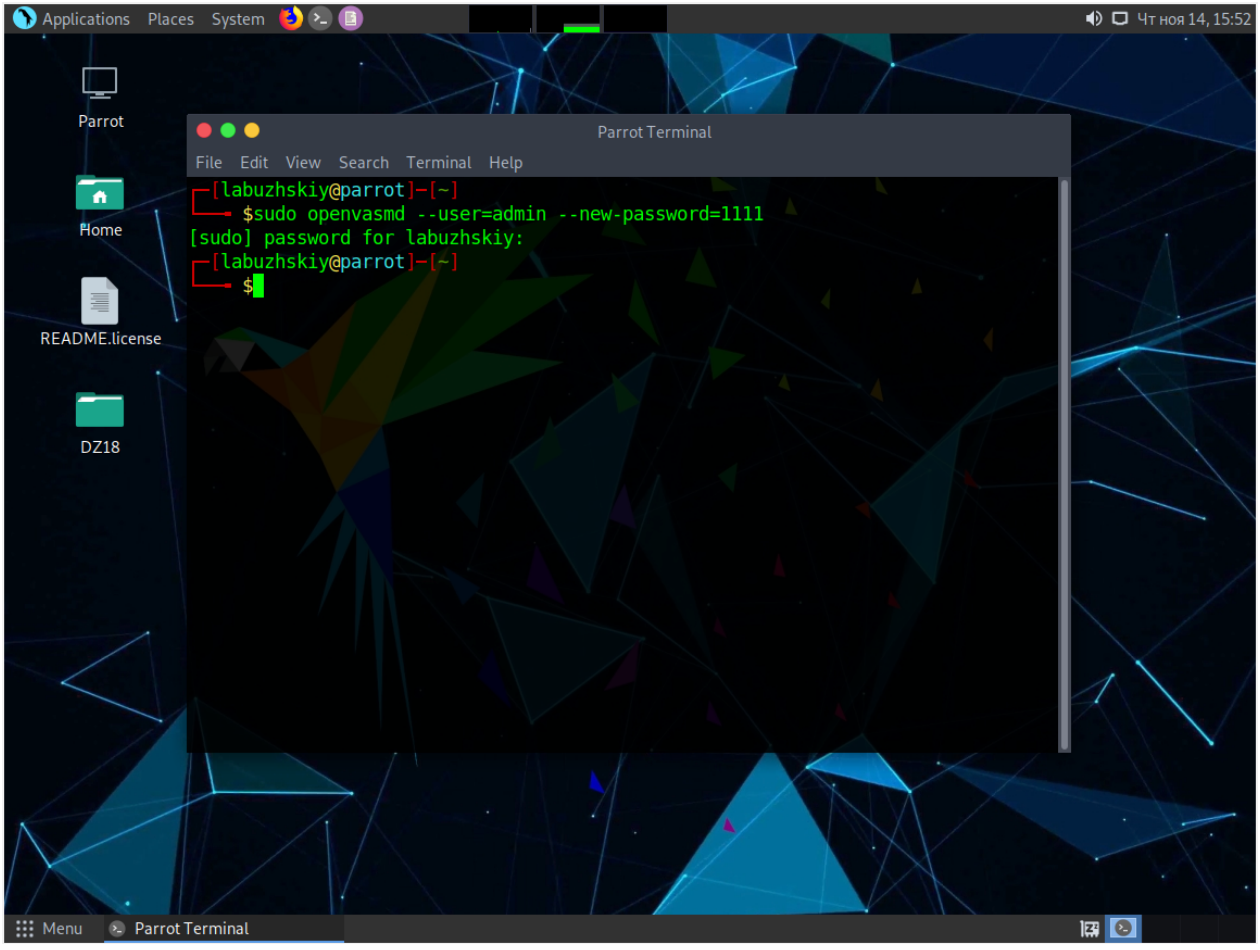
а) Скачиваем образ Parrot-security-4.7_x64.iso и разворачиваем виртуальную среду, необходимую для корректной работы OpenVAS.
NB! Важно: для корректной установки ParrotOS необходимо выделить виртуальный HDD достаточного объёма для установки. В моём случае ОС развернулась не с первой попытки, и успешный исход был при выделение динамического HDD около 50 ГБ.



б) скачиваем и разворачиваем стенд для изучения уязвимостей metasploitable-linux-2.0.0.zip
https://xakep.ru/2012/06/15/58852/
https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

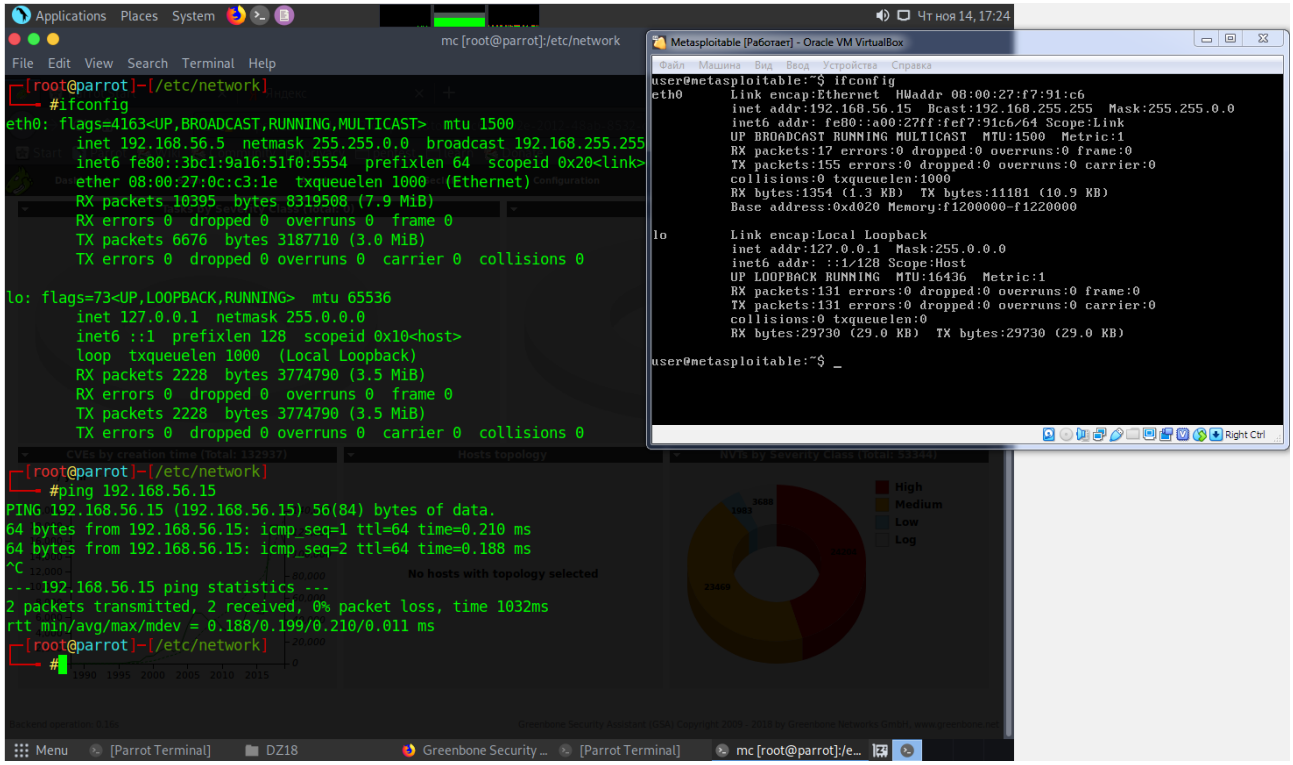


в) обновляем OpenVAS (при первом запуске все необходимые обновления будут скачены и установлены в материалах это лог-файл с именем: 1-62105-2a226f.txt)
*г) изменяем пароль встроенной учётной записи **admin,** на любой известный нам для осуществления процедуры аутентификации через веб-браузер.*

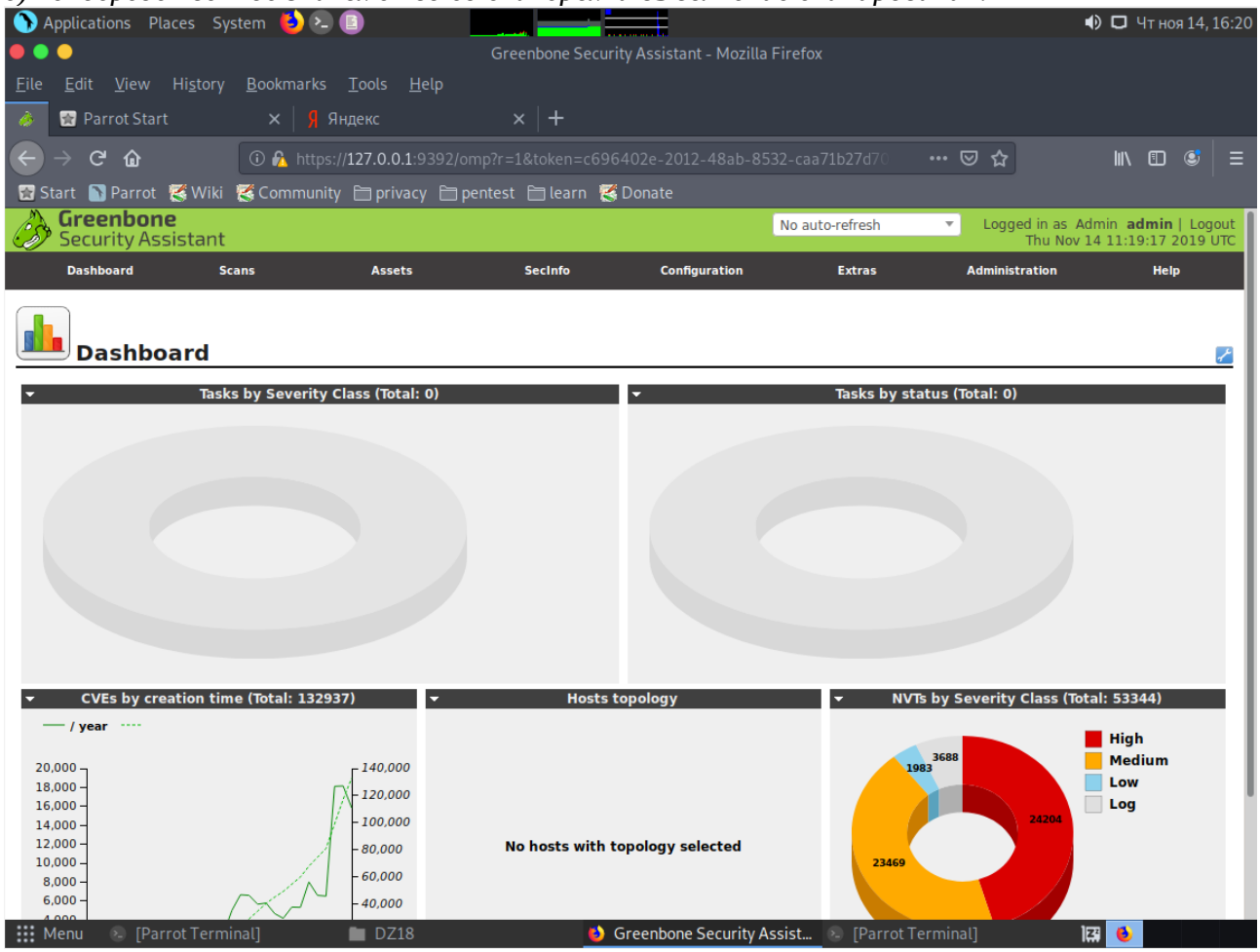


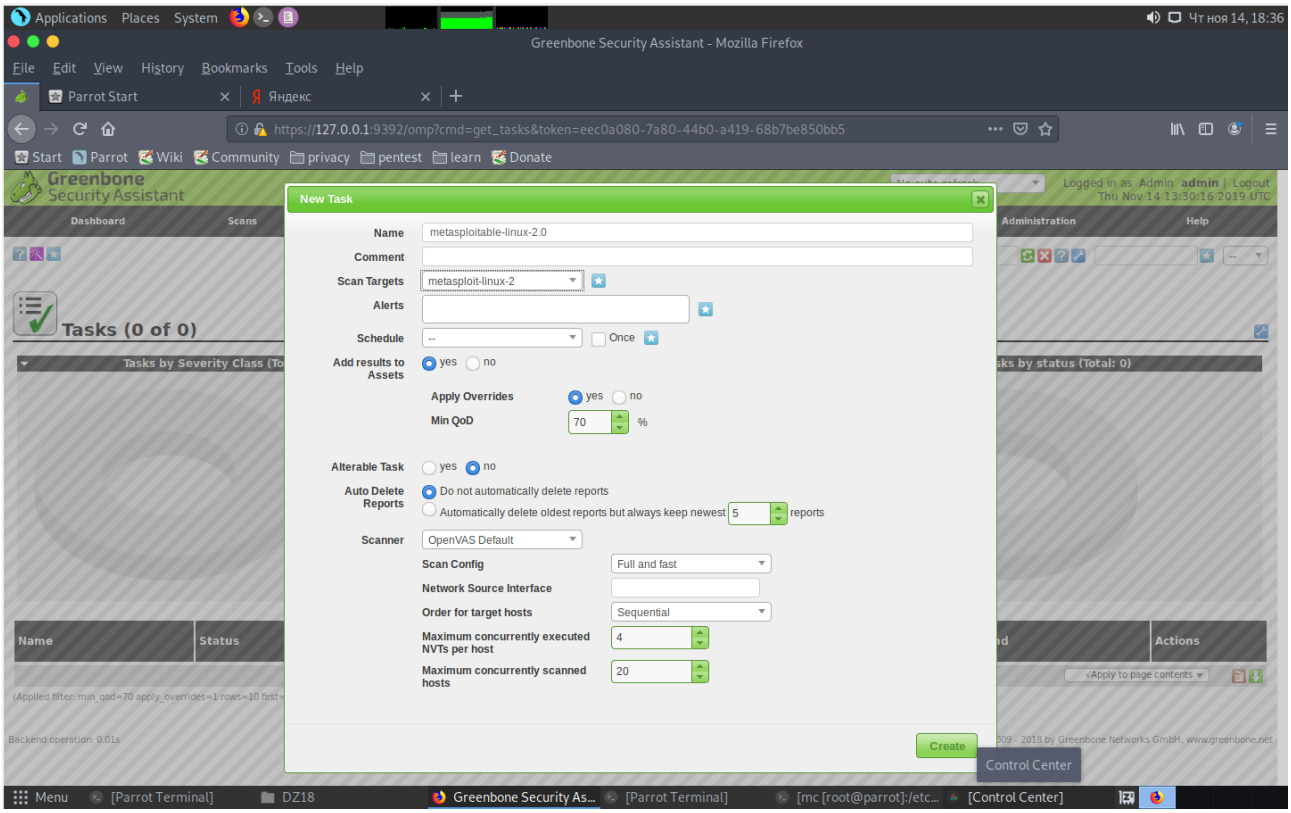
https://itsecforu.ru/2018/07/16/как-сбросить-пароль-admin-в-openvas/

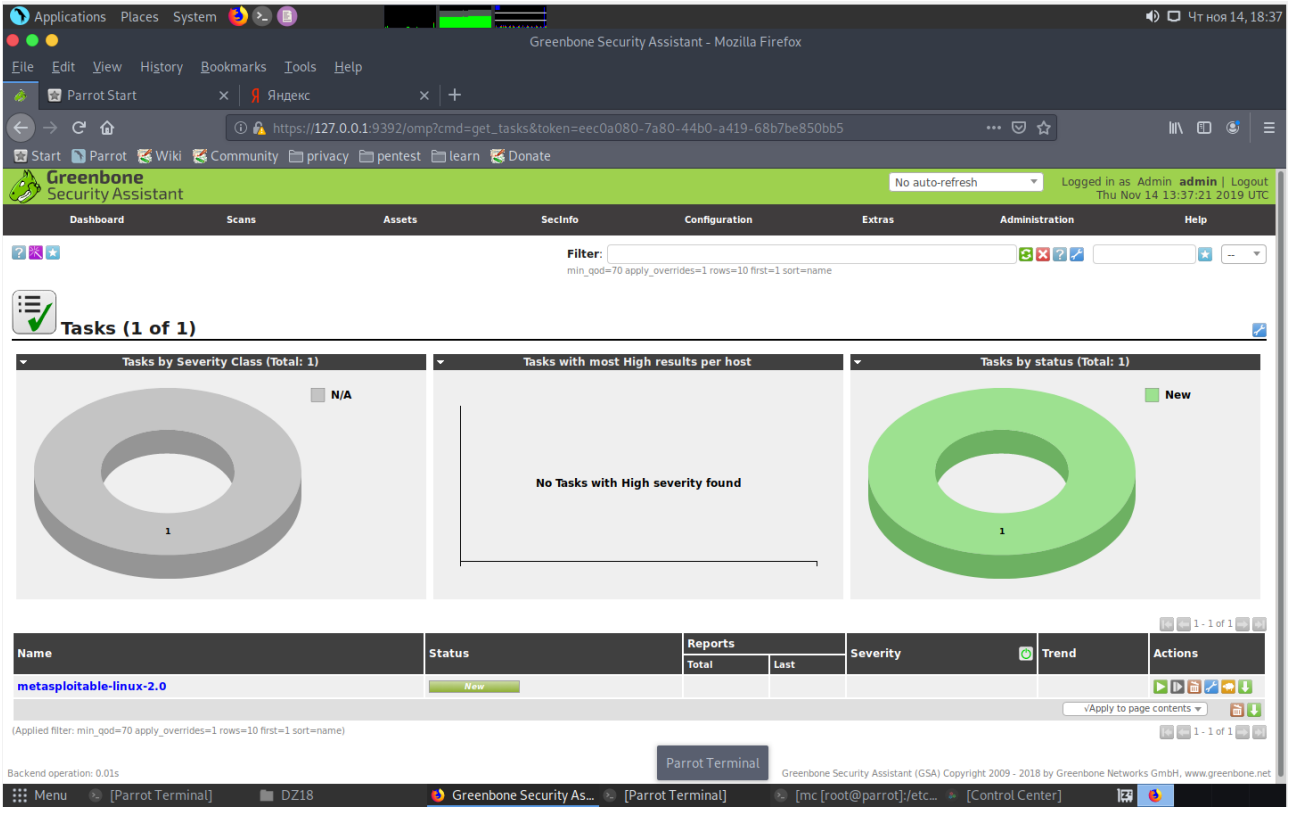
д) настраиваем ЛВС на тестовом стенде:

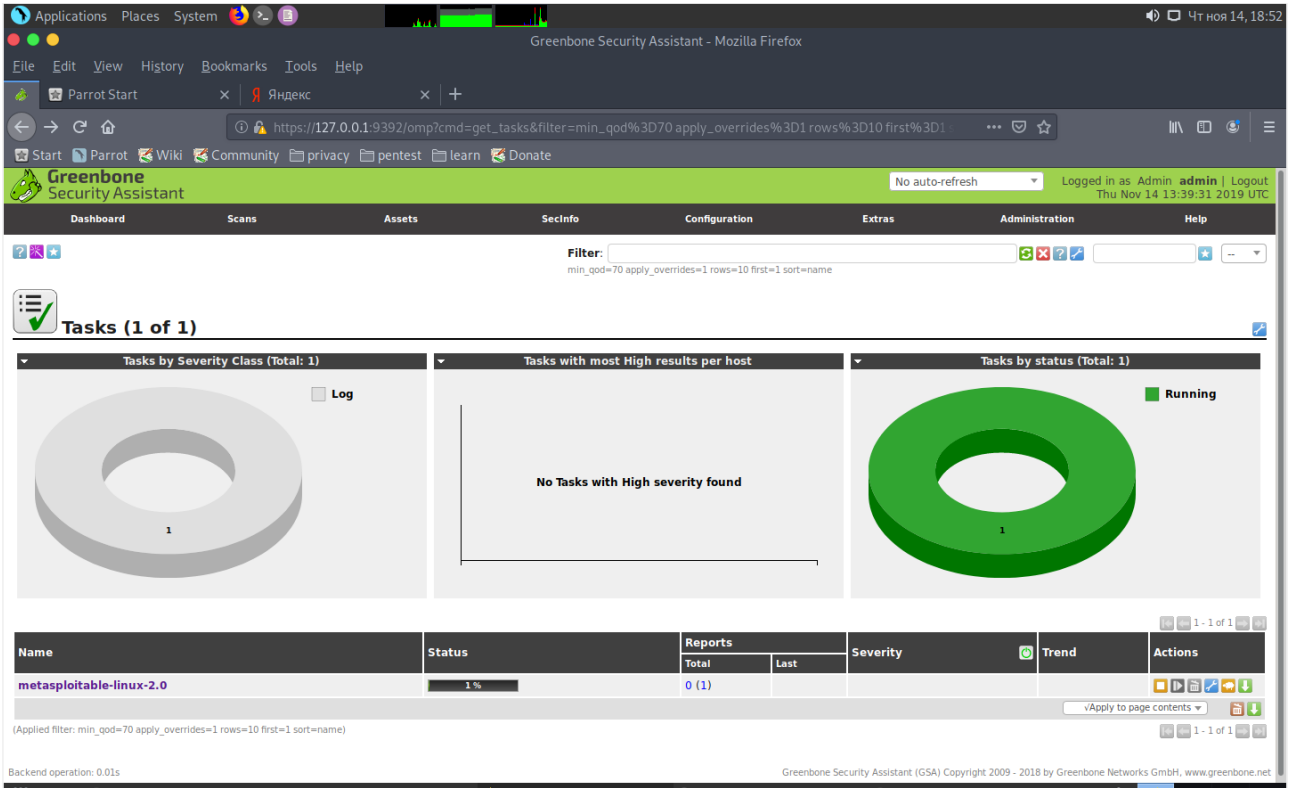


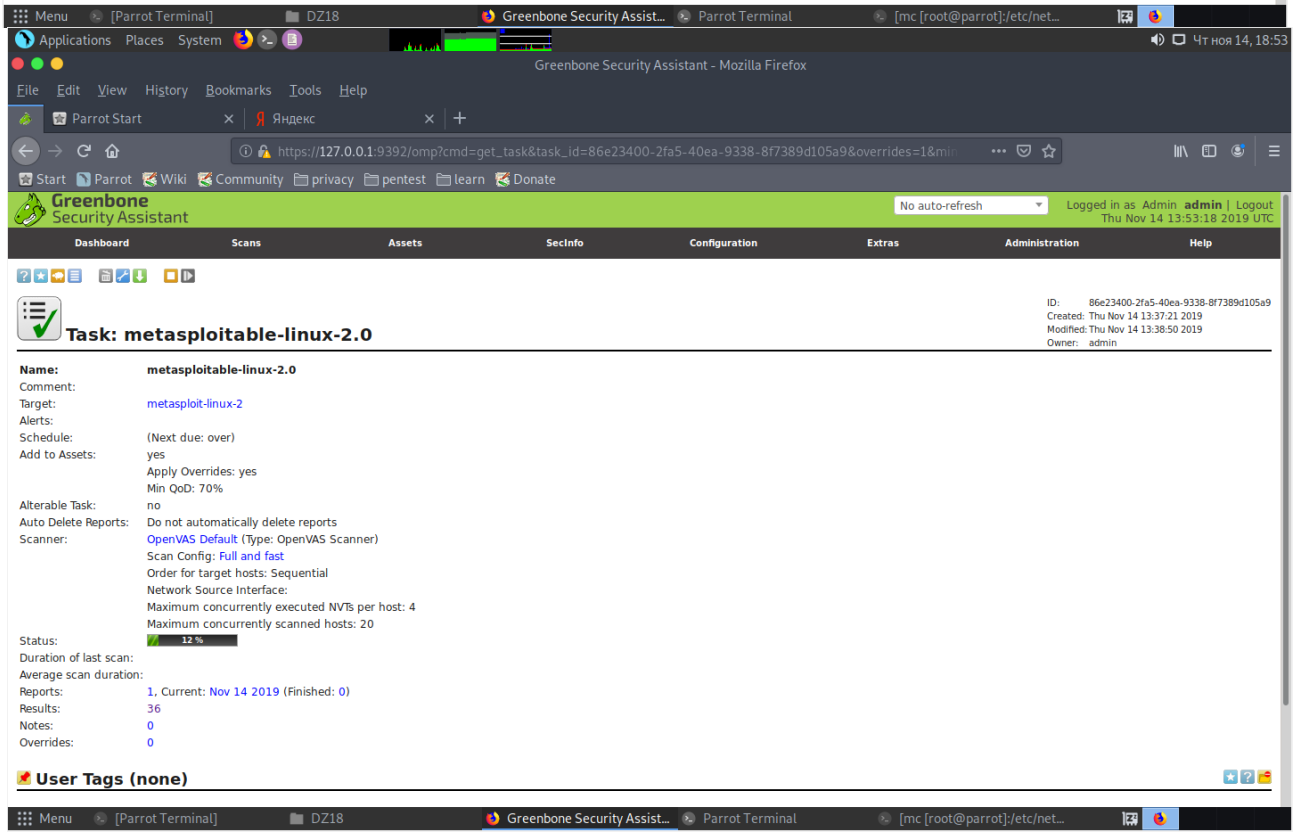
е) непосредственное знакомство со сканером и выполнение сканирования:

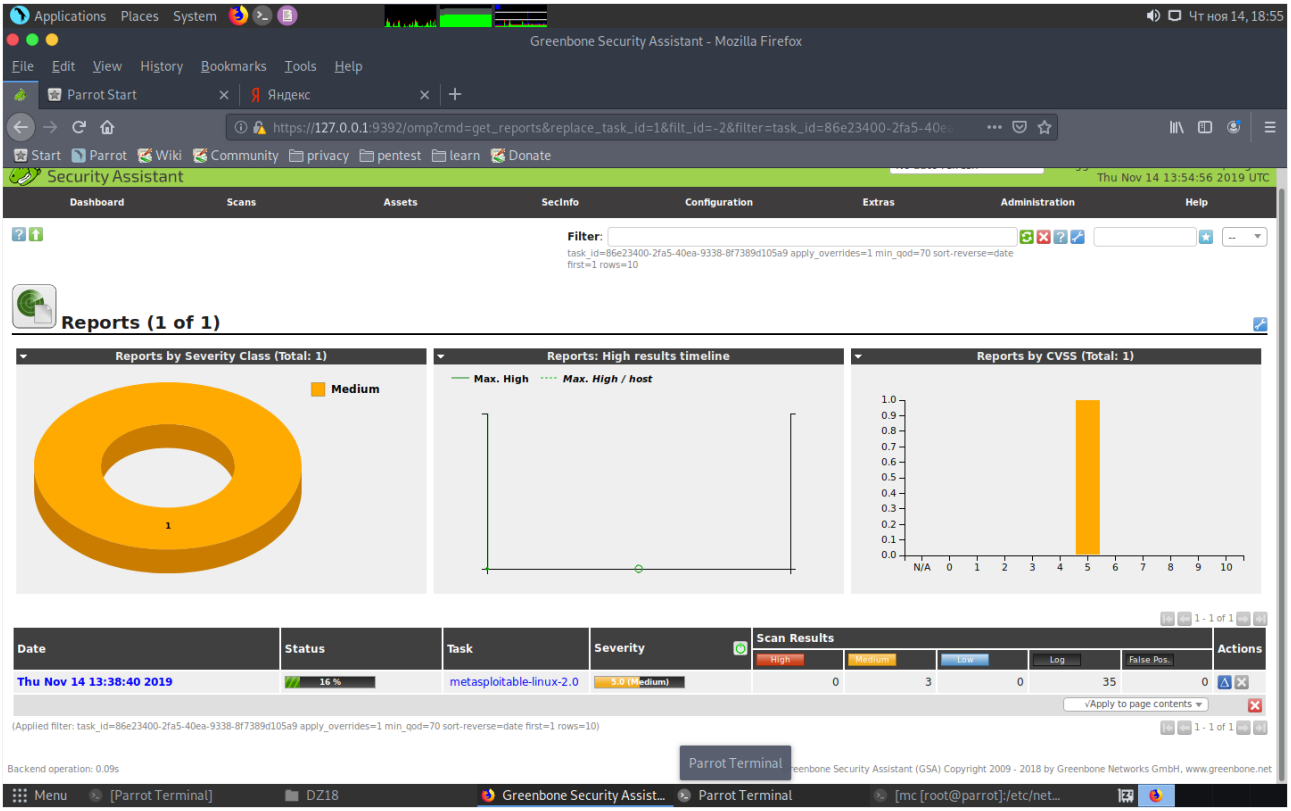


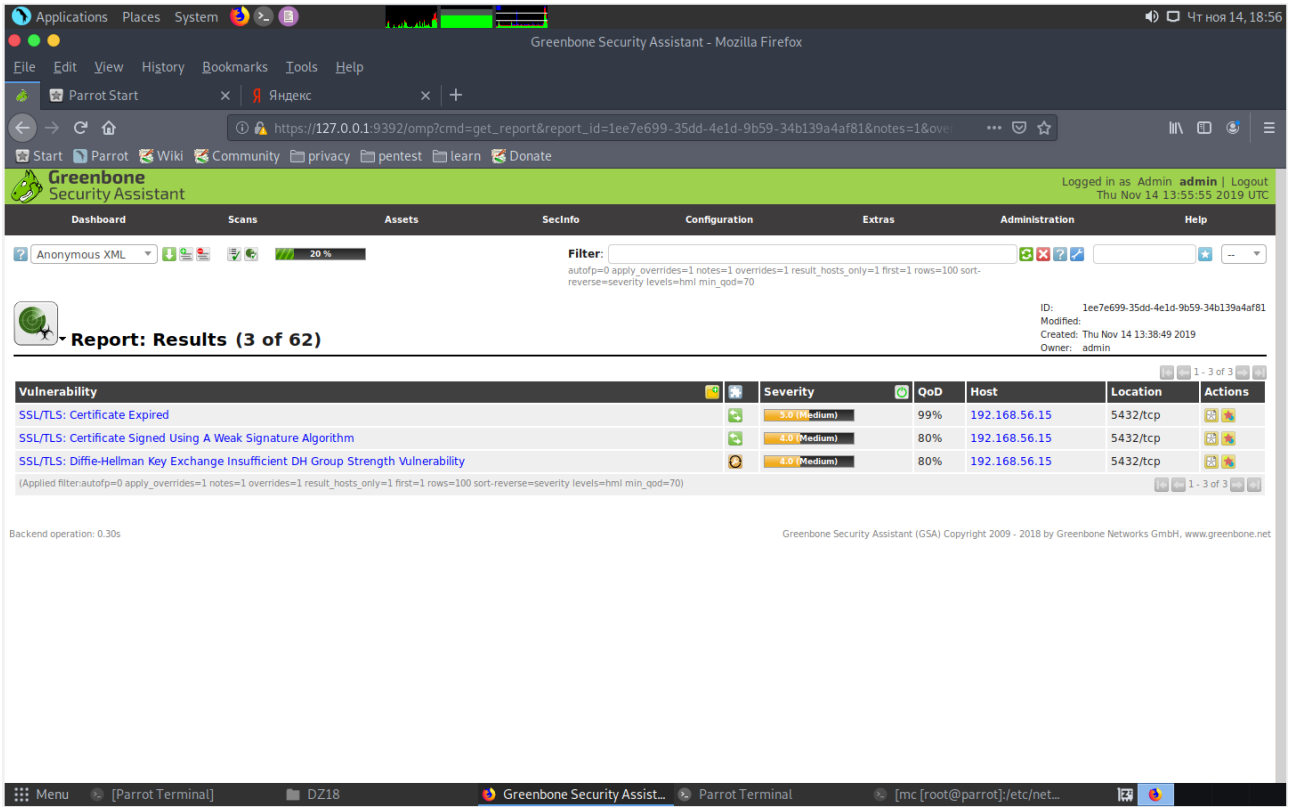

Applications Places System
Чт ноя 14, 18:36
Greenbone Security Assistant - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Parrot Start
Яндекс
https://127.0.0.1:9392/omp?cmd=get_tasks&token=eec0a080-7a80-44b0-a419-68b7be850bb5
Start Parrot Wiki Community privacy pentest learn Donate
Greenbone Security Assistant
Logged in as Admin admin | Logout
Thu Nov 14 13:30:16 2019 UTC
Dashboard Scans Administration Help
Tasks (0 of 0)
Tasks by Severity Class (To
sks by status (Total: 0)
New Task
Name metasploitable-linux-2.0
Comment
Scan Targets metasploit-linux-2
Alerts
Schedule -- Once
Add results to Assets yes no
Apply Overrides yes no
Min QoD 70 %
Alterable Task yes no
Auto Delete Reports Do not automatically delete reports
Automatically delete oldest reports but always keep newest 5 reports
Scanner OpenVAS Default
Scan Config Full and fast
Network Source Interface
Order for target hosts Sequential
Maximum concurrently executed NVTs per host 4
Maximum concurrently scanned hosts 20
Create
Name Status Actions
Control Center
Backend operation: 0.01s
Menu [Parrot Terminal] DZ18 Greenbone Security As... [Parrot Terminal] [mc [root@parrot]:/etc... [Control Center]

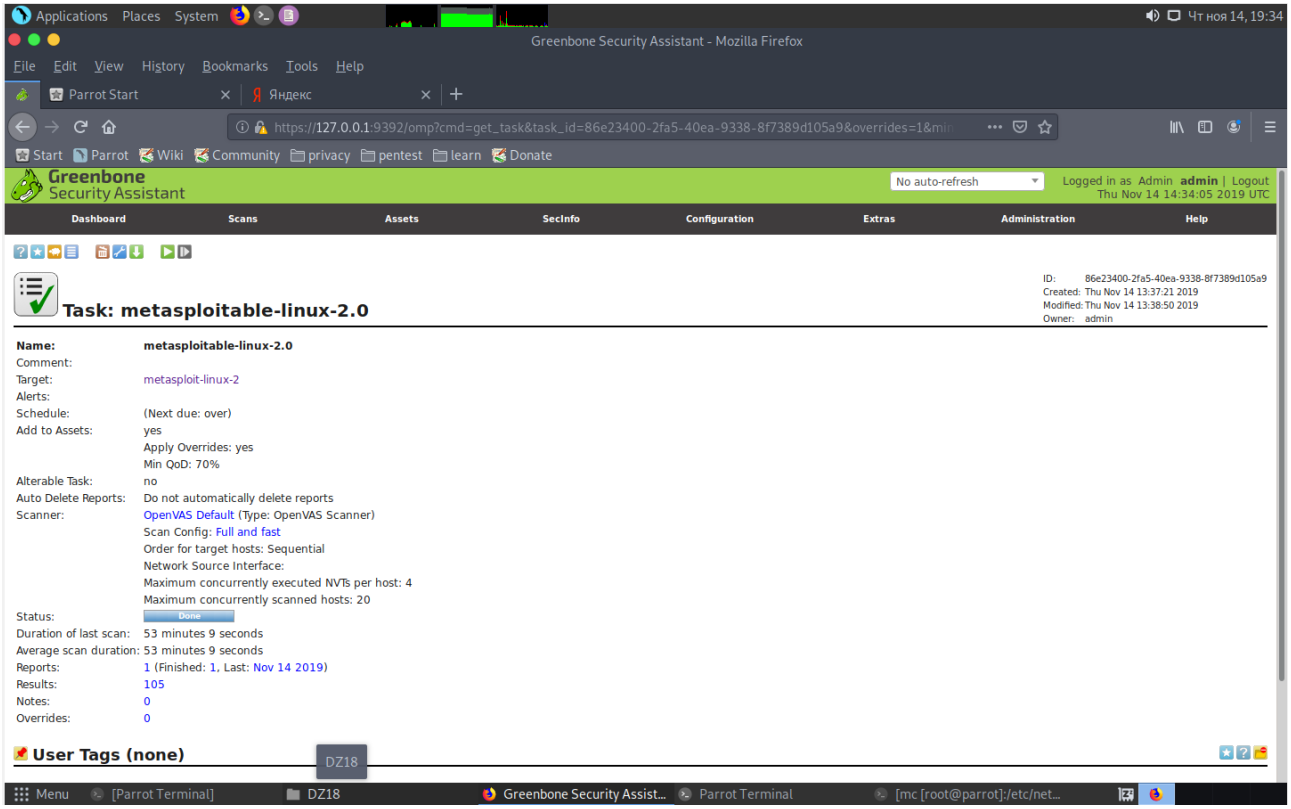

Applications Places System
Чт ноя 14, 18:37
Greenbone Security Assistant - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Parrot Start
Яндекс
https://127.0.0.1:9392/omp?cmd=get_tasks&token=eec0a080-7a80-44b0-a419-68b7be850bb5
Start Parrot Wiki Community privacy pentest learn Donate
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Thu Nov 14 13:37:21 2019 UTC
Dashboard Scans Assets SecInfo Configuration Extras Administration Help
Filter:
min_qod=70 apply_overrides=1 rows=10 first=1 sort=name
Tasks (1 of 1)
Tasks by Severity Class (Total: 1)
N/A
1
Tasks with most High results per host
No Tasks with High severity found
Tasks by status (Total: 1)
New
1
1 - 1 of 1
Name Status Reports Total Reports Last Severity Trend Actions
metasploitable-linux-2.0
New
Apply to page contents
(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)
1 - 1 of 1
Backend operation: 0.01s
Parrot Terminal
Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net
Menu [Parrot Terminal] DZ18 Greenbone Security As... [Parrot Terminal] [mc [root@parrot]:/etc... [Control Center]

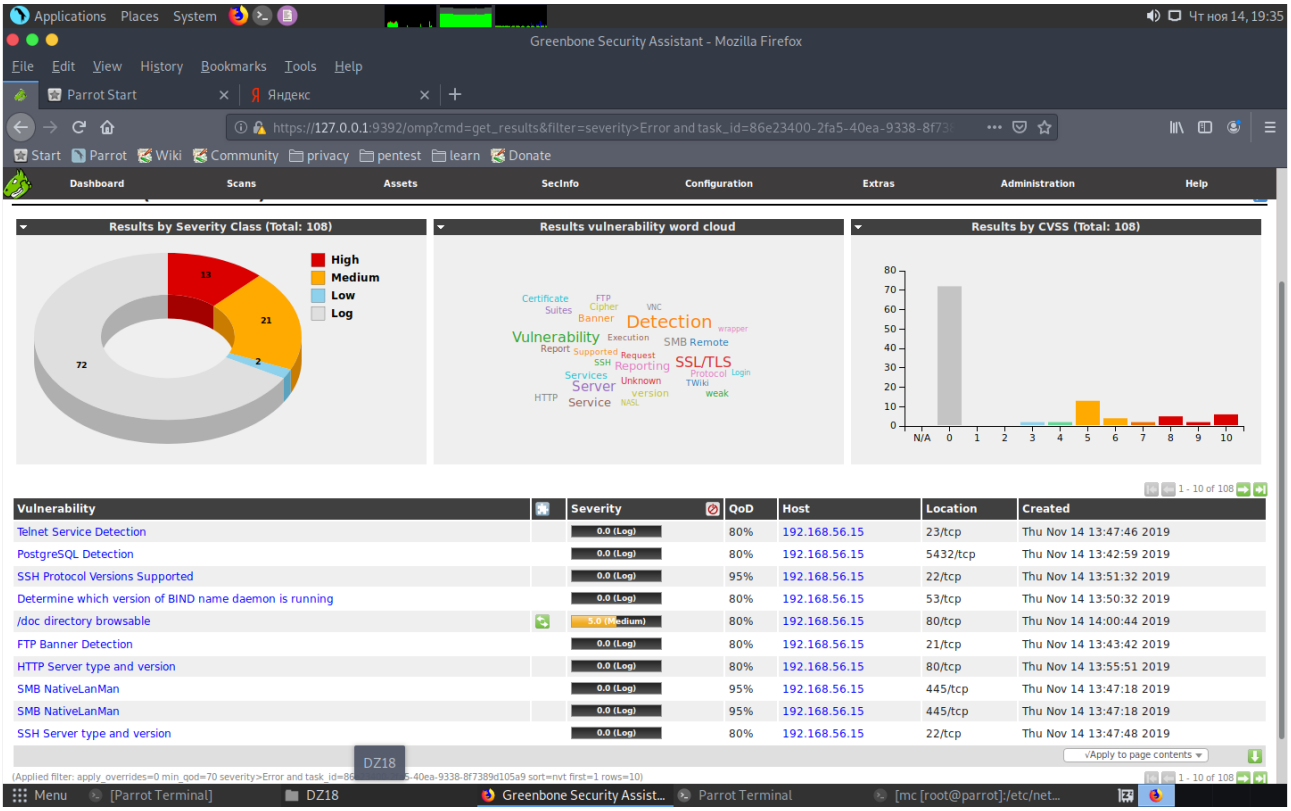

Applications Places System
Чт ноя 14, 18:52
Greenbone Security Assistant - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Parrot Start
Яндекс
https://127.0.0.1:9392/omp?cmd=get_tasks&filter=min_qod%3D70 apply_overrides%3D1 rows%3D10 first%3D1
Start Parrot Wiki Community privacy pentest learn Donate
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Thu Nov 14 13:39:31 2019 UTC
Dashboard Scans Assets SecInfo Configuration Extras Administration Help
Filter:
min_qod=70 apply_overrides=1 rows=10 first=1 sort=name
Tasks (1 of 1)
Tasks by Severity Class (Total: 1)
Log
1
Tasks with most High results per host
No Tasks with High severity found
Tasks by status (Total: 1)
Running
1
1 - 1 of 1
Name
Status
Reports
Total
Last
Severity
Trend
Actions
metasploitable-linux-2.0
1 %
0 (1)
Apply to page contents
(Applied filter: min_qod=70 apply_overrides=1 rows=10 first=1 sort=name)
1 - 1 of 1
Backend operation: 0.01s
Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net
Menu
[Parrot Terminal]
DZ18
Greenbone Security Assist...
Parrot Terminal
[mc [root@parrot]:/etc/net...

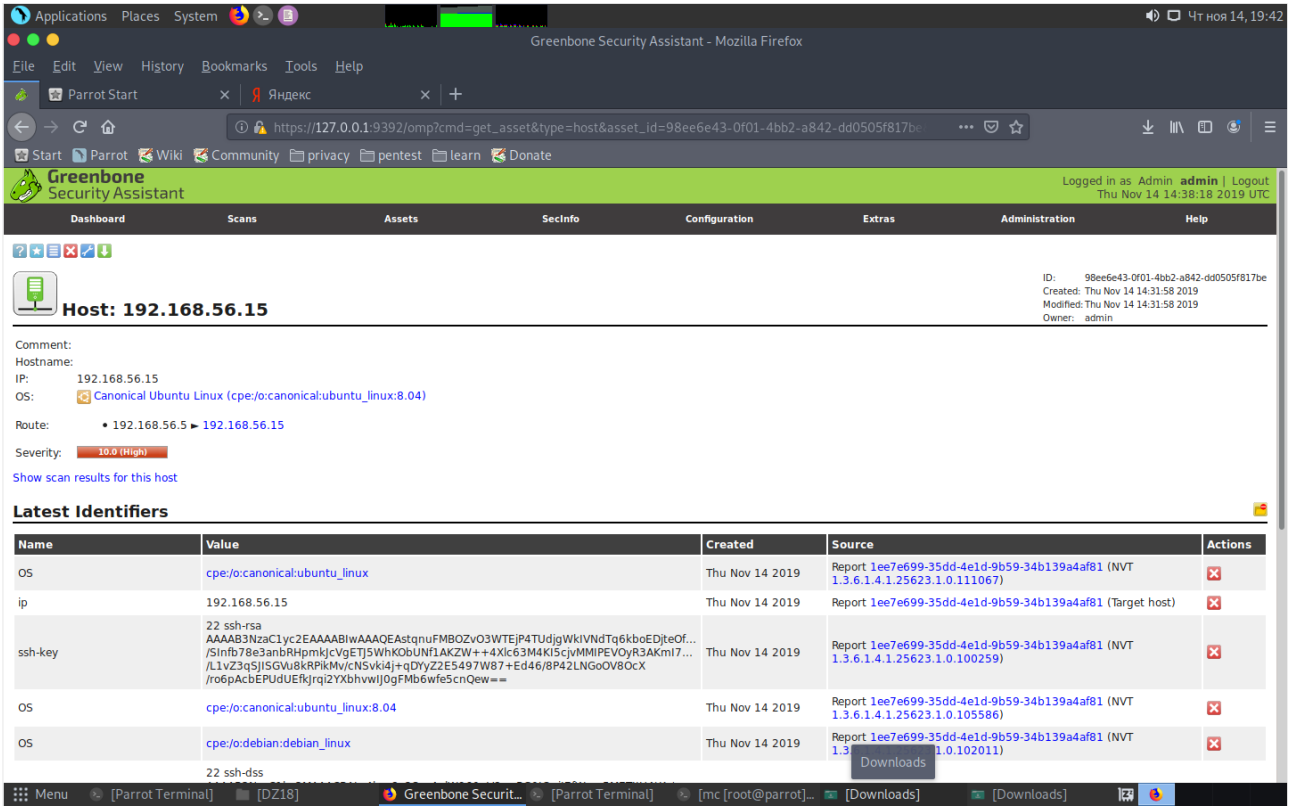

Applications Places System
Чт ноя 14, 18:53
Greenbone Security Assistant - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Parrot Start
Яндекс
https://127.0.0.1:9392/omp?cmd=get_task&task_id=86e23400-2fa5-40ea-9338-8f7389d105a9&overrides=1&min
Start Parrot Wiki Community privacy pentest learn Donate
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Thu Nov 14 13:53:18 2019 UTC
Dashboard Scans Assets SecInfo Configuration Extras Administration Help
Task: metasploitable-linux-2.0
ID: 86e23400-2fa5-40ea-9338-8f7389d105a9
Created: Thu Nov 14 13:37:21 2019
Modified: Thu Nov 14 13:38:50 2019
Owner: admin
Name: metasploitable-linux-2.0
Comment:
Target: metasploit-linux-2
Alerts:
Schedule: (Next due: over)
Add to Assets: yes
Apply Overrides: yes
Min QoD: 70%
Alterable Task: no
Auto Delete Reports: Do not automatically delete reports
Scanner: OpenVAS Default (Type: OpenVAS Scanner)
Scan Config: Full and fast
Order for target hosts: Sequential
Network Source Interface:
Maximum concurrently executed NVTs per host: 4
Maximum concurrently scanned hosts: 20
Status: 12 %
Duration of last scan:
Average scan duration:
Reports: 1, Current: Nov 14 2019 (Finished: 0)
Results: 36
Notes: 0
Overrides: 0
User Tags (none)
Menu
[Parrot Terminal]
DZ18
Greenbone Security Assist...
Parrot Terminal
[mc [root@parrot]:/etc/net...

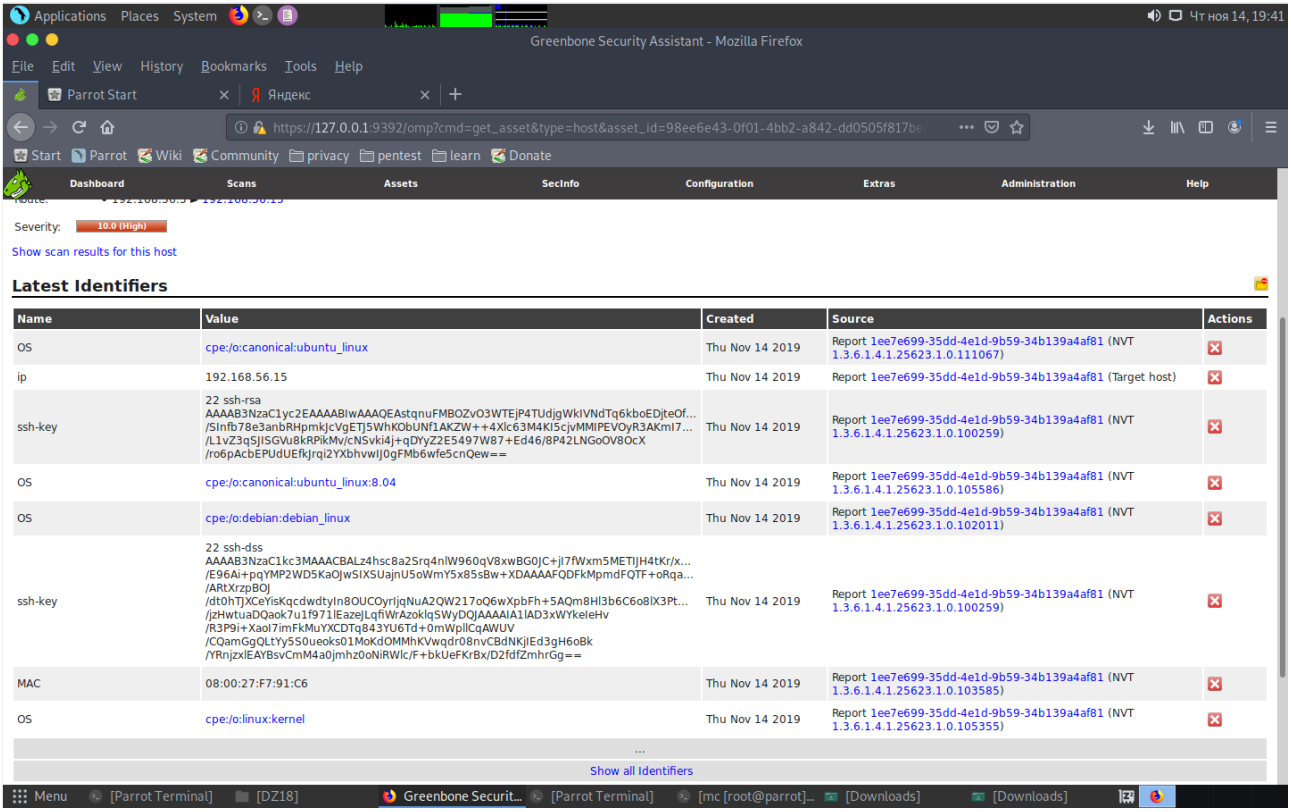

Applications Places System
Чт ноя 14, 18:55
Greenbone Security Assistant - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Parrot Start
Яндекс
https://127.0.0.1:9392/omp?cmd=get_reports&replace_task_id=1&filt_id=-2&filter=task_id=86e23400-2fa5-40e
Start Parrot Wiki Community privacy pentest learn Donate
Security Assistant
Thu Nov 14 13:54:56 2019 UTC
Dashboard Scans Assets SecInfo Configuration Extras Administration Help
Filter:
task_id=86e23400-2fa5-40ea-9338-8f7389d105a9 apply_overrides=1 min_qod=70 sort-reverse=date first=1 rows=10
Reports (1 of 1)
Reports by Severity Class (Total: 1)
Medium
1
Reports: High results timeline
Max. High
Max. High / host
Reports by CVSS (Total: 1)
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
N/A 0 1 2 3 4 5 6 7 8 9 10
1 - 1 of 1
Date Status Task Severity Scan Results Actions
High Medium Low Log False Pos.
Thu Nov 14 13:38:40 2019 16 % metasploitable-linux-2.0 5.0 (Medium) 0 3 0 35 0
Apply to page contents
(Applied filter: task_id=86e23400-2fa5-40ea-9338-8f7389d105a9 apply_overrides=1 min_qod=70 sort-reverse=date first=1 rows=10)
1 - 1 of 1
Backend operation: 0.09s
Parrot Terminal
Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net
Menu [Parrot Terminal] DZ18 Greenbone Security Assist... Parrot Terminal [mc [root@parrot]:/etc/net...

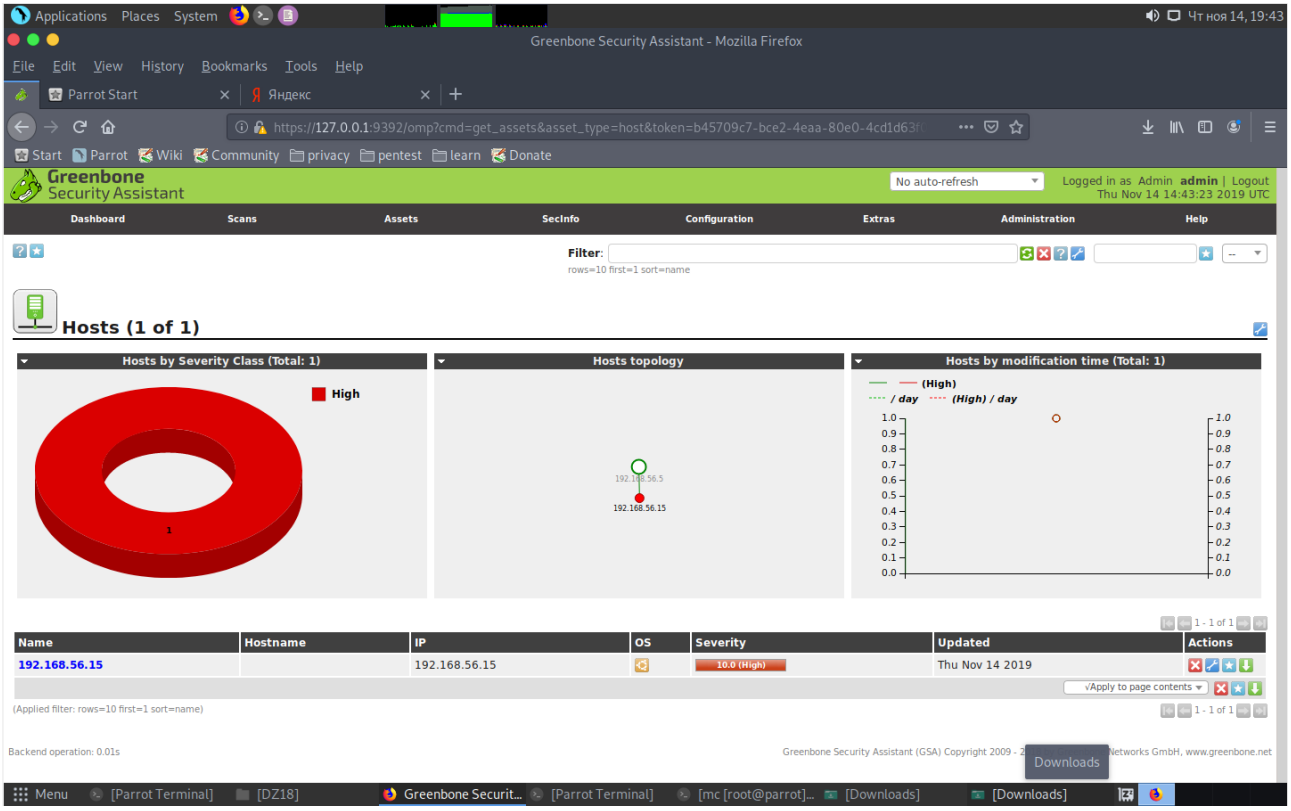

Applications Places System
Чт ноя 14, 18:56
Greenbone Security Assistant - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Parrot Start
Яндекс
https://127.0.0.1:9392/omp?cmd=get_report&report_id=1ee7e699-35dd-4e1d-9b59-34b139a4af81&notes=1&ove
Start Parrot Wiki Community privacy pentest learn Donate
Greenbone
Security Assistant
Logged in as Admin admin | Logout
Thu Nov 14 13:55:55 2019 UTC
Dashboard Scans Assets SecInfo Configuration Extras Administration Help
Anonymous XML
20 %
Filter:
autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70
Report: Results (3 of 62)
ID: 1ee7e699-35dd-4e1d-9b59-34b139a4af81
Modified:
Created: Thu Nov 14 13:38:49 2019
Owner: admin
1 - 3 of 3
Vulnerability Severity QoD Host Location Actions
SSL/TLS: Certificate Expired 5.0 (Medium) 99% 192.168.56.15 5432/tcp
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm 4.0 (Medium) 80% 192.168.56.15 5432/tcp
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability 4.0 (Medium) 80% 192.168.56.15 5432/tcp
(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70)
1 - 3 of 3
Backend operation: 0.30s
Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net
Menu [Parrot Terminal] DZ18 Greenbone Security Assist... Parrot Terminal [mc [root@parrot]:/etc/net...

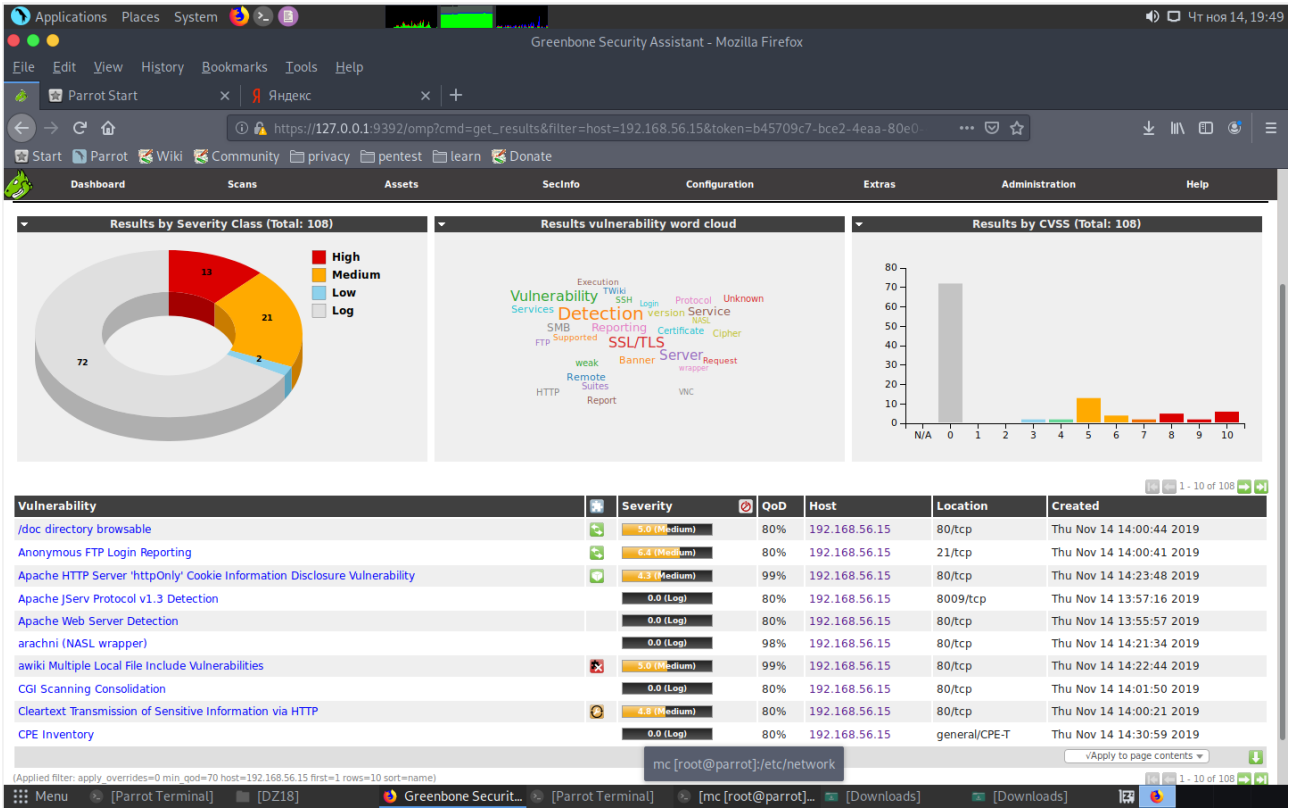

Applications Places System
Чт ноя 14, 19:34
Greenbone Security Assistant - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Parrot Start
Яндекс
https://127.0.0.1:9392/omp?cmd=get_task&task_id=86e23400-2fa5-40ea-9338-8f7389d105a9&overrides=1&mi
Start Parrot Wiki Community privacy pentest learn Donate
Greenbone Security Assistant
No auto-refresh
Logged in as Admin admin | Logout
Thu Nov 14 14:34:05 2019 UTC
Dashboard Scans Assets SecInfo Configuration Extras Administration Help
Task: metasploitable-linux-2.0
ID: 86e23400-2fa5-40ea-9338-8f7389d105a9
Created: Thu Nov 14 13:37:21 2019
Modified: Thu Nov 14 13:38:50 2019
Owner: admin
Name: metasploitable-linux-2.0
Comment:
Target: metasploit-linux-2
Alerts:
Schedule: (Next due: over)
Add to Assets: yes
Apply Overrides: yes
Min QoD: 70%
Alterable Task: no
Auto Delete Reports: Do not automatically delete reports
Scanner: OpenVAS Default (Type: OpenVAS Scanner)
Scan Config: Full and fast
Order for target hosts: Sequential
Network Source Interface:
Maximum concurrently executed NVTs per host: 4
Maximum concurrently scanned hosts: 20
Status: Done
Duration of last scan: 53 minutes 9 seconds
Average scan duration: 53 minutes 9 seconds
Reports: 1 (Finished: 1, Last: Nov 14 2019)
Results: 105
Notes: 0
Overrides: 0
User Tags (none)
DZ18
Menu [Parrot Terminal] DZ18 Greenbone Security Assist... Parrot Terminal [mc [root@parrot]:/etc/net...


Applications Places System
Чт ноя 14, 19:35
Greenbone Security Assistant - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Parrot Start
Яндекс
https://127.0.0.1:9392/omp?cmd=get_results&filter=severity>Error and task_id=86e23400-2fa5-40ea-9338-8f73
Start Parrot Wiki Community privacy pentest learn Donate
Dashboard Scans Assets SecInfo Configuration Extras Administration Help
Results by Severity Class (Total: 108)
High
Medium
Low
Log
13
21
2
72
Results vulnerability word cloud
Certificate
Suites
FTP
Cipher
Banner
VNC
Detection
wrapper
Vulnerability
Execution
SMB Remote
Report
Supported
SSH
Request
Reporting
SSL/TLS
Services
Server
Unknown
Protocol
Login
TWiki
HTTP
Service
version
NASL
weak
Results by CVSS (Total: 108)
80
70
60
50
40
30
20
10
0
N/A 0 1 2 3 4 5 6 7 8 9 10
1 - 10 of 108
Vulnerability Severity QoD Host Location Created
Telnet Service Detection 0.0 (Log) 80% 192.168.56.15 23/tcp Thu Nov 14 13:47:46 2019
PostgreSQL Detection 0.0 (Log) 80% 192.168.56.15 5432/tcp Thu Nov 14 13:42:59 2019
SSH Protocol Versions Supported 0.0 (Log) 95% 192.168.56.15 22/tcp Thu Nov 14 13:51:32 2019
Determine which version of BIND name daemon is running 0.0 (Log) 80% 192.168.56.15 53/tcp Thu Nov 14 13:50:32 2019
/doc directory browsable 5.0 (Medium) 80% 192.168.56.15 80/tcp Thu Nov 14 14:00:44 2019
FTP Banner Detection 0.0 (Log) 80% 192.168.56.15 21/tcp Thu Nov 14 13:43:42 2019
HTTP Server type and version 0.0 (Log) 80% 192.168.56.15 80/tcp Thu Nov 14 13:55:51 2019
SMB NativeLanMan 0.0 (Log) 95% 192.168.56.15 445/tcp Thu Nov 14 13:47:18 2019
SMB NativeLanMan 0.0 (Log) 95% 192.168.56.15 445/tcp Thu Nov 14 13:47:18 2019
SSH Server type and version 0.0 (Log) 80% 192.168.56.15 22/tcp Thu Nov 14 13:47:48 2019
√Apply to page contents
DZ18
(Applied filter: apply_overrides=0 min_qod=70 severity>Error and task_id=86 5-40ea-9338-8f7389d105a9 sort=nvt first=1 rows=10)
1 - 10 of 108
Menu [Parrot Terminal] DZ18 Greenbone Security Assist... Parrot Terminal [mc [root@parrot]:/etc/net...


Applications Places System
Чт ноя 14, 19:42
Greenbone Security Assistant - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Parrot Start
Яндекс
https://127.0.0.1:9392/omp?cmd=get_asset&type=host&asset_id=98ee6e43-0f01-4bb2-a842-dd0505f817be
Start Parrot Wiki Community privacy pentest learn Donate
Greenbone Security Assistant
Logged in as Admin admin | Logout
Thu Nov 14 14:38:18 2019 UTC
Dashboard Scans Assets SecInfo Configuration Extras Administration Help
Host: 192.168.56.15
ID: 98ee6e43-0f01-4bb2-a842-dd0505f817be
Created: Thu Nov 14 14:31:58 2019
Modified: Thu Nov 14 14:31:58 2019
Owner: admin
Comment:
Hostname:
IP: 192.168.56.15
OS: Canonical Ubuntu Linux (cpe:/o:canonical:ubuntu_linux:8.04)
Route: • 192.168.56.5 ► 192.168.56.15
Severity: 10.0 (High)
Show scan results for this host
Latest Identifiers
Name Value Created Source Actions
OS cpe:/o:canonical:ubuntu_linux Thu Nov 14 2019 Report 1ee7e699-35dd-4e1d-9b59-34b139a4af81 (NVT 1.3.6.1.4.1.25623.1.0.111067)
ip 192.168.56.15 Thu Nov 14 2019 Report 1ee7e699-35dd-4e1d-9b59-34b139a4af81 (Target host)
ssh-key 22 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOf... /SInfb78e3anbRHpmkJcVgETJ5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKmI7... /L1vZ3qSJISGVu8kRPikMv/cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV8OcX /ro6pAcbEPUdUEfkJrqi2YXbhvwIJ0gFMb6wfe5cnQew== Thu Nov 14 2019 Report 1ee7e699-35dd-4e1d-9b59-34b139a4af81 (NVT 1.3.6.1.4.1.25623.1.0.100259)
OS cpe:/o:canonical:ubuntu_linux:8.04 Thu Nov 14 2019 Report 1ee7e699-35dd-4e1d-9b59-34b139a4af81 (NVT 1.3.6.1.4.1.25623.1.0.105586)
OS cpe:/o:debian:debian_linux Thu Nov 14 2019 Report 1ee7e699-35dd-4e1d-9b59-34b139a4af81 (NVT 1.3 1.0.102011)
Downloads
22 ssh-dss
Menu [Parrot Terminal] [DZ18] Greenbone Securit... [Parrot Terminal] [mc [root@parrot]... [Downloads] [Downloads]


Applications Places System
Чт ноя 14, 19:41
Greenbone Security Assistant - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Parrot Start
Яндекс
https://127.0.0.1:9392/omp?cmd=get_asset&type=host&asset_id=98ee6e43-0f01-4bb2-a842-dd0505f817be
Start Parrot Wiki Community privacy pentest learn Donate
Dashboard Scans Assets SecInfo Configuration Extras Administration Help
Severity: 10.0 (High)
Show scan results for this host
Latest Identifiers
Name Value Created Source Actions
OS cpe:/o:canonical:ubuntu_linux Thu Nov 14 2019 Report 1ee7e699-35dd-4e1d-9b59-34b139a4af81 (NVT 1.3.6.1.4.1.25623.1.0.111067)
ip 192.168.56.15 Thu Nov 14 2019 Report 1ee7e699-35dd-4e1d-9b59-34b139a4af81 (Target host)
ssh-key 22 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOf... /SInfb78e3anbRHpmkJcVgETJ5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKmI7... /L1vZ3qSJISGVu8kRPikMv/cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV8OcX /ro6pAcbEPUdUEfkJrqi2YXbhvwIJ0gFMb6wfe5cnQew== Thu Nov 14 2019 Report 1ee7e699-35dd-4e1d-9b59-34b139a4af81 (NVT 1.3.6.1.4.1.25623.1.0.100259)
OS cpe:/o:canonical:ubuntu_linux:8.04 Thu Nov 14 2019 Report 1ee7e699-35dd-4e1d-9b59-34b139a4af81 (NVT 1.3.6.1.4.1.25623.1.0.105586)
OS cpe:/o:debian:debian_linux Thu Nov 14 2019 Report 1ee7e699-35dd-4e1d-9b59-34b139a4af81 (NVT 1.3.6.1.4.1.25623.1.0.102011)
ssh-key 22 ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBG0JC+jI7fWxm5METlJH4tKr/x... /E96Ai+pqYMP2WD5KaOJwSIXSUajnU5oWmY5x85sBw+XDAAAAFQDFkMpmdFQTF+oRqa... /ARtXrzpBOJ /dt0hTJXCeYisKqcdwdtyIn8OUCOyrIjqNuA2QW217oQ6wXpbFh+5AQm8Hl3b6C6o8lX3Pt... /jzHwtuaDQaok7u1f971lEazeJLqfiWrAzokIqSWyDOJAAAAIA1lAD3xWYkeleHv /R3P9i+Xaol7imFkMuYXCDTq843YU6Td+0mWpllCqAWUV /CQamGgQLtYy5S0ueoks01MoKdOMMhKVwqdr08nvCBdNKjIEd3gH6oBk /YRnjzxlEAYBsvCmM4a0jmhz0oNiRWlc/F+bkUeFKrBx/D2fdfZmhrGg== Thu Nov 14 2019 Report 1ee7e699-35dd-4e1d-9b59-34b139a4af81 (NVT 1.3.6.1.4.1.25623.1.0.100259)
MAC 08:00:27:F7:91:C6 Thu Nov 14 2019 Report 1ee7e699-35dd-4e1d-9b59-34b139a4af81 (NVT 1.3.6.1.4.1.25623.1.0.103585)
OS cpe:/o:linux:kernel Thu Nov 14 2019 Report 1ee7e699-35dd-4e1d-9b59-34b139a4af81 (NVT 1.3.6.1.4.1.25623.1.0.105355)
...
Show all Identifiers
Menu [Parrot Terminal] [DZ18] Greenbone Securit... [Parrot Terminal] [mc [root@parrot]... [Downloads] [Downloads]





Вроде бы всё. Результаты пралагаю в виде results.xml*