МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Департамент информационной безопасности

Гусев Михаил Дмитриевич
Кудрявцева Юлия Андреевна
Увакин Данил Павлович

M9120-09.04.02ИБКФС

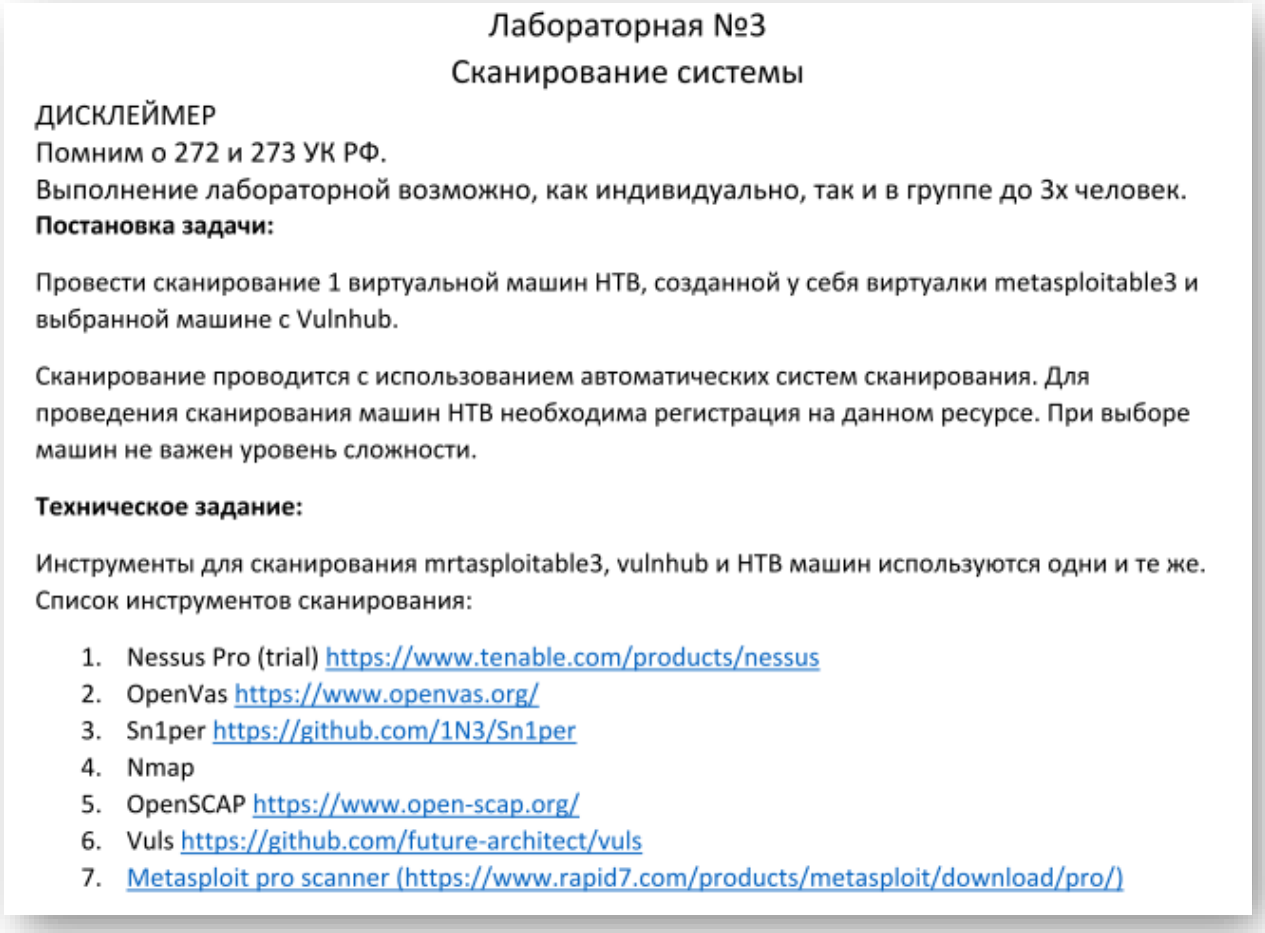
Отчет к лабораторной работе № 3
Сканирование системы

по дисциплине: «Аудит безопасности информационных систем»

г. Владивосток

2022

Постановка задачи:



Лабораторная №3

Сканирование системы

ДИСКЛЕЙМЕР

Помним о 272 и 273 УК РФ.

Выполнение лабораторной возможно, как индивидуально, так и в группе до 3х человек.

Постановка задачи:

Провести сканирование 1 виртуальной машин HTB, созданной у себя виртуалки metasploitable3 и выбранной машине с Vulnhub.

Сканирование проводится с использованием автоматических систем сканирования. Для проведения сканирования машин HTB необходима регистрация на данном ресурсе. При выборе машин не важен уровень сложности.

Техническое задание:

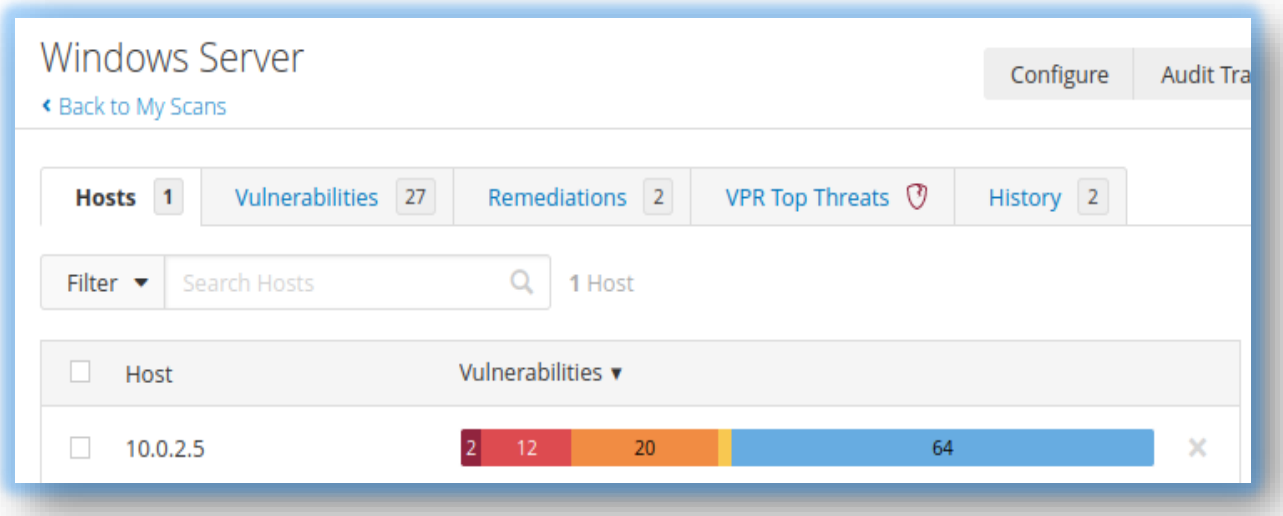
Инструменты для сканирования mrtasploitable3, vulnhub и HTB машин используются одни и те же. Список инструментов сканирования:

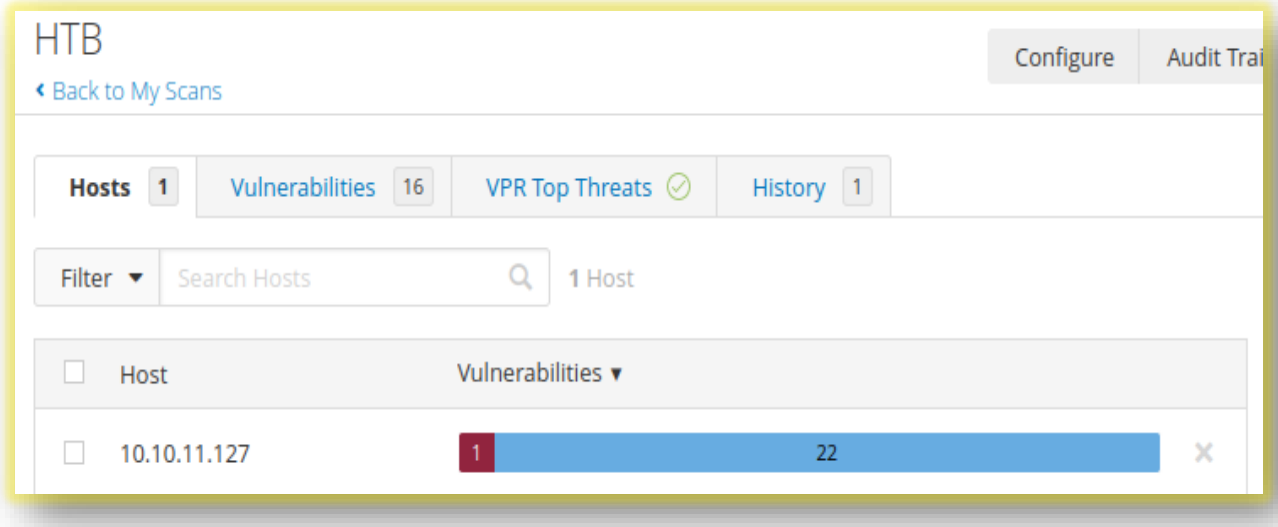
1. Nessus Pro (trial) https://www.tenable.com/products/nessus
2. OpenVas https://www.openvas.org/
3. Sn1per https://github.com/1N3/Sn1per
4. Nmap
5. OpenSCAP https://www.open-scap.org/
6. Vuls https://github.com/future-architect/vuls
7. Metasploit pro scanner (https://www.rapid7.com/products/metasploit/download/pro/)

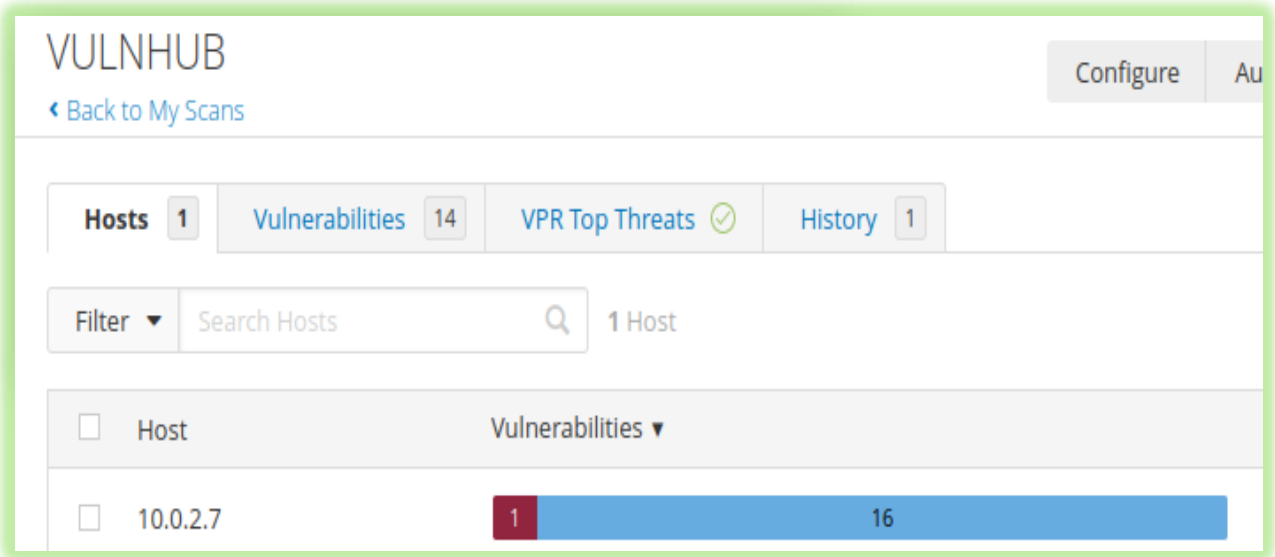
В качестве виртуальных машин были выбраны:

1) Windows Server 2008 a.k. metasploitable3
2) FINGERPRINT – HTB машина уровня Insane
3) HACKERHOUSE: BSIDES LONDON 2017 – Vulnhub машина

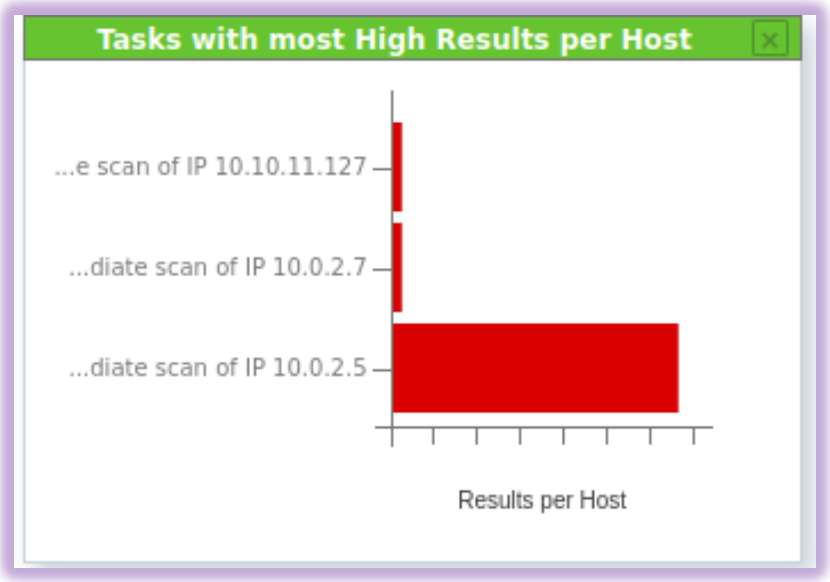
1. Nessus Pro (trial)







2. OPENVAS



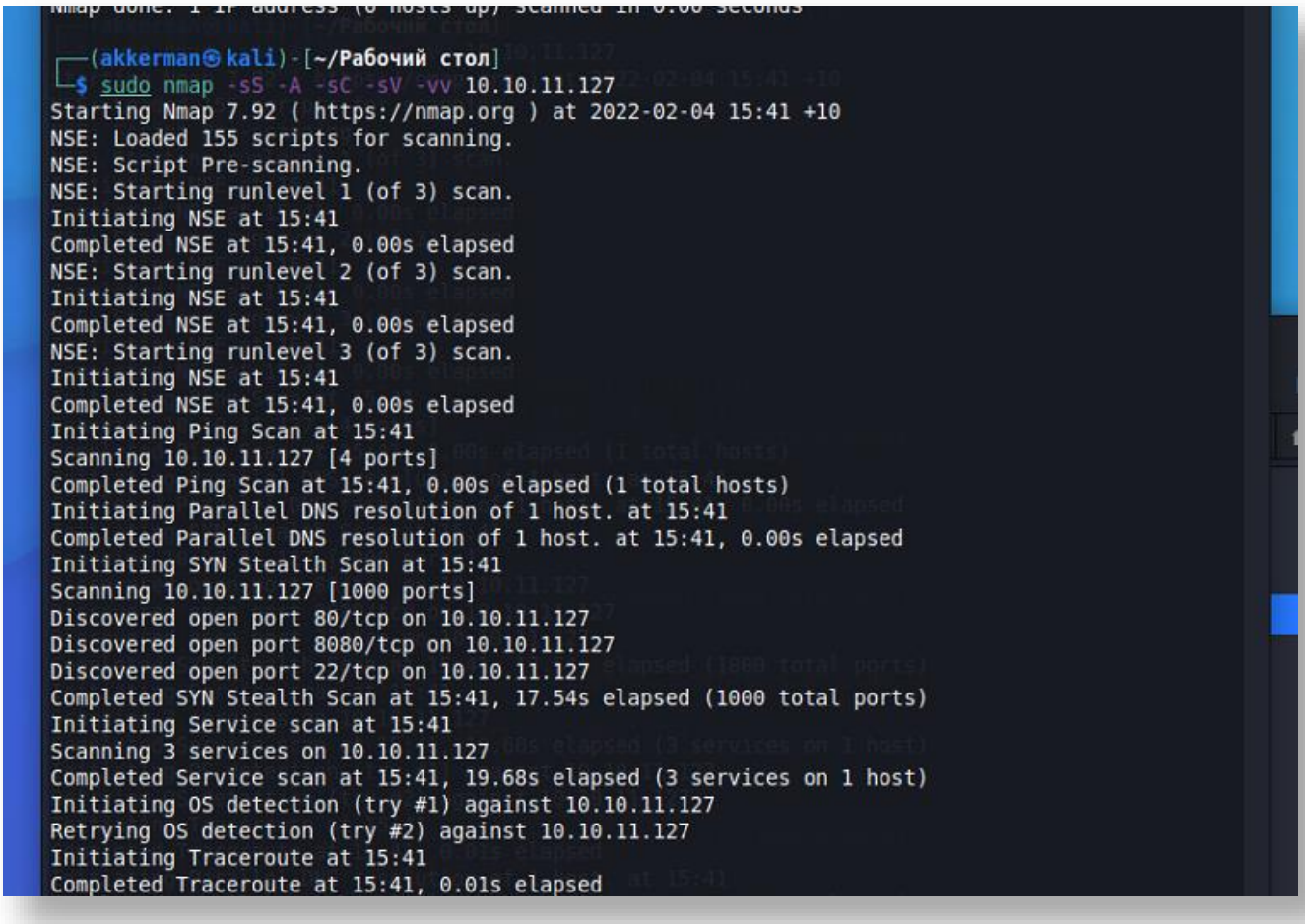
3. Sn1per

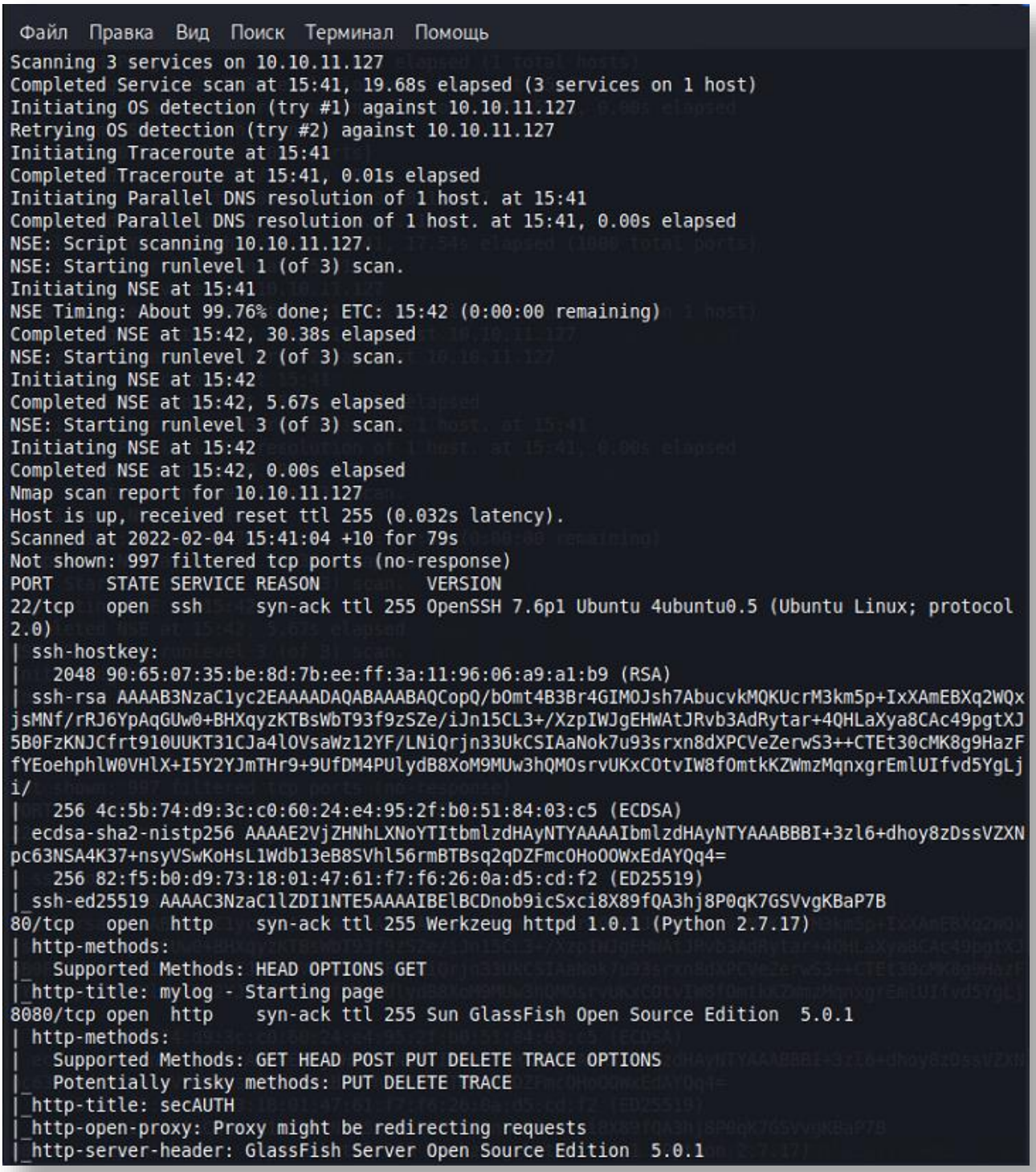
```
 RUNNING TCP PORT SCAN
 + -- --=[Port 80 opened... running tests...
 CHECKING HTTP HEADERS AND METHODS
HTTP/1.1 200 OK
Date: Sun, 30 Jan 2022 15:44:34 GMT
Server: Apache/2.4.10 (Debian)
Last-Modified: Fri, 02 Jun 2017 15:43:40 GMT
ETag: "62-550fc04704300"
Accept-Ranges: bytes
Content-Length: 98
Vary: Accept-Encoding
Content-Type: text/html

HTTP/1.1 200 OK
Date: Sun, 30 Jan 2022 15:44:34 GMT
Server: Apache/2.4.10 (Debian)
Last-Modified: Fri, 02 Jun 2017 15:43:40 GMT
ETag: "62-550fc04704300"
Accept-Ranges: bytes
Content-Length: 98
Vary: Accept-Encoding
Content-Type: text/html

Allow: GET,HEAD,POST,OPTIONS
 DISPLAYING META GENERATOR TAGS
 DISPLAYING COMMENTS
 DISPLAYING SITE LINKS
```

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.10 ((Debian))
| vulners:
|   cpe:/a:apache:http_server:2.4.10:
|       CVE-2021-44790  7.5     https://vulners.com/cve/CVE-2021-44790
|       CVE-2021-39275  7.5     https://vulners.com/cve/CVE-2021-39275
|       CVE-2021-26691  7.5     https://vulners.com/cve/CVE-2021-26691
|       CVE-2017-7679   7.5     https://vulners.com/cve/CVE-2017-7679
|       CVE-2017-7668   7.5     https://vulners.com/cve/CVE-2017-7668
|       CVE-2017-3169   7.5     https://vulners.com/cve/CVE-2017-3169
|       CVE-2017-3167   7.5     https://vulners.com/cve/CVE-2017-3167
|       MSF:ILITIES/UBUNTU-CVE-2018-1312/       6.8     https://vulners.com/
```

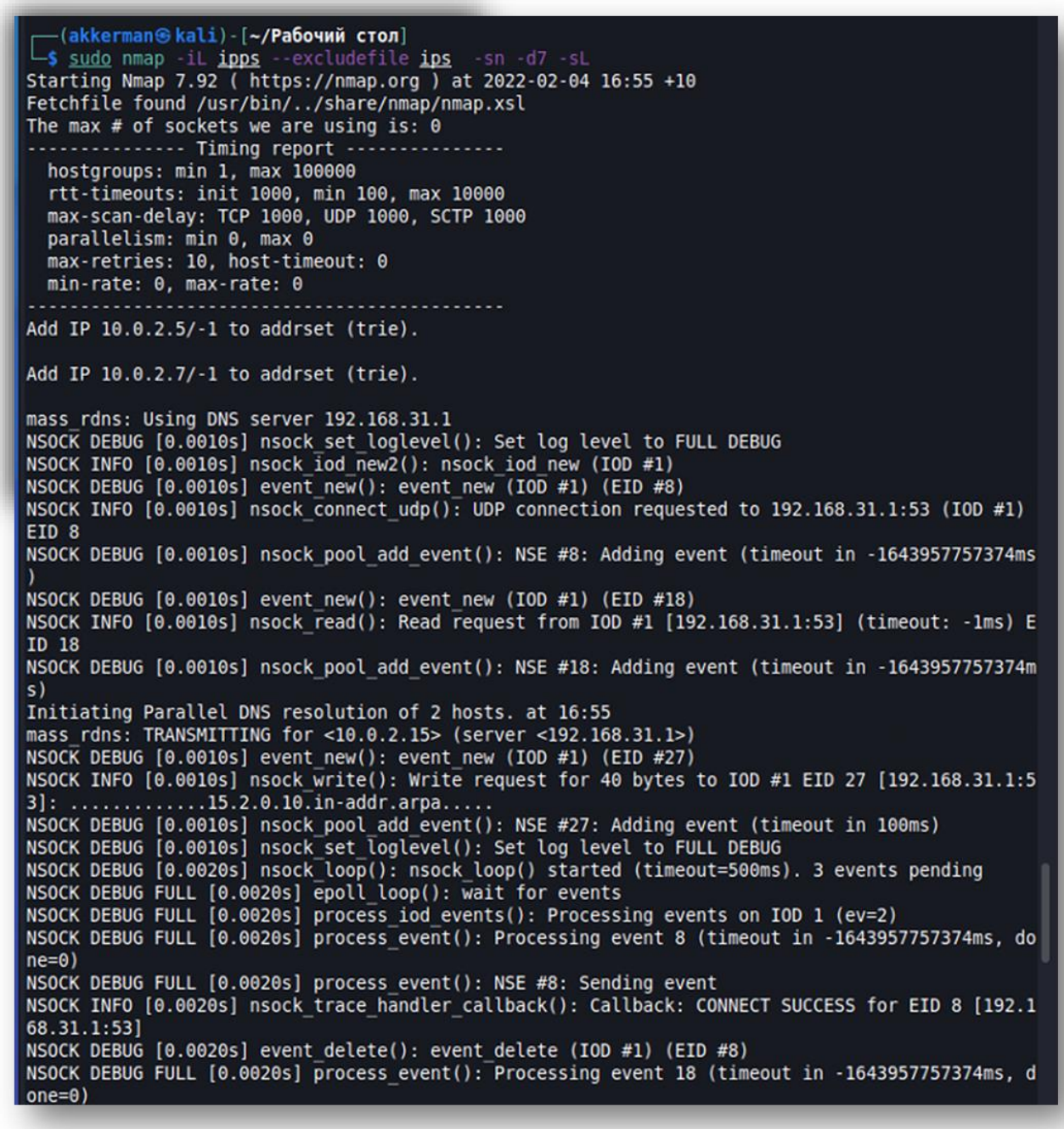
4. NMAP

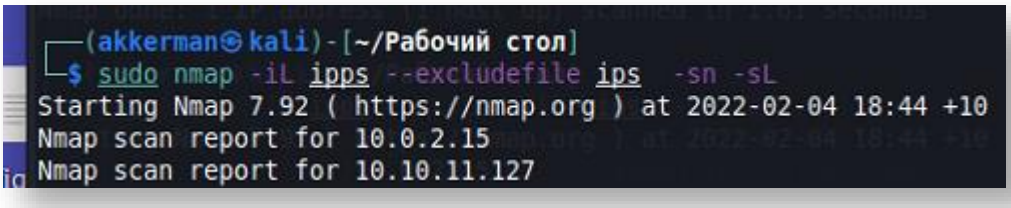
10.10.11.127	
-sS	TCP SYN/с использованием системного вызова Connect()/ACK/Window/Maimon сканирования
–A	Активировать функции определения ОС и версии, сканирование с использованием скриптов и трассировки
–sC	эквивалентно опции --script=default []
–sV	Исследовать открытые порты для определения информации о службе/версии
–vv	Увеличить уровень вербальности (задать дважды или более для увеличения эффекта)





ipps[4 ip]- ips [2 ip]	
-iL	Использовать список хостов/сетей из файла
-sn	Пинг сканирование - просто определить, работает ли хост
-d7	Увеличить или установить уровень отладки (до 9) (исп при багах)
-sL	Сканирование с целью составления списка - просто составить список целей для сканирования
excludefile	Исключить список из файла





10.0.2.7	
-Pn	Расценивать все хосты как работающие -- пропустить обнаружение хостов
-PE	Пингование с использованием ICMP эхо запросов, запросов временной метки и сетевой маски
-sS	TCP SYN/c использованием системного вызова Connect()/ACK/Window/Maimon сканирования
-O	Активировать функцию определения ОС

```
┌──(akkerman㉿kali)-[~/Рабочий стол]
└─$ sudo nmap  -Pn -PE -sS -O 10.0.2.7
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-04 17:07 +10
Nmap scan report for 10.0.2.7
Host is up (0.00020s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:E3:2C:95 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.16 - 4.6
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds

┌──(akkerman㉿kali)-[~/Рабочий стол]
└─$
```

10.0.2.7	
-top-ports 7	Сканировать < 7 > наиболее распространенных портов
--reason	Выводить причину нахождения порта в определенном состоянии
-PS	TCP SYN/ACK или UDP пингование заданных хостов
-R	DNS разрешение -Всегда производить разрешение
-sU	UDP сканирование
-sN	Null сканирование Не устанавливаются никакие биты (Флагов в TCP заголовоке 0)

```
┌──(akkerman㉿kali)-[~/Рабочий стол]
└─$ sudo nmap 10.0.2.7 -top-ports 7 --reason -PS -R -sN -sU
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-04 17:59 +10
Nmap scan report for 10.0.2.7
Host is up, received arp-response (0.00026s latency).

PORT     STATE         SERVICE       REASON
21/tcp   open|filtered ftp           no-response
22/tcp   open|filtered ssh           no-response
23/tcp   open|filtered telnet        no-response
25/tcp   open|filtered smtp          no-response
80/tcp   open|filtered http          no-response
443/tcp  open|filtered https         no-response
3389/tcp open|filtered ms-wbt-server no-response
123/udp  closed        ntp           port-unreach ttl 64
137/udp  closed        netbios-ns    port-unreach ttl 64
138/udp  closed        netbios-dgm   port-unreach ttl 64
161/udp  closed        snmp          port-unreach ttl 64
445/udp  closed        microsoft-ds  port-unreach ttl 64
631/udp  closed        ipp           port-unreach ttl 64
1434/udp closed        ms-sql-m      port-unreach ttl 64
MAC Address: 08:00:27:E3:2C:95 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.47 seconds
```

iR	
-iR	Выбрать произвольные цели
-sO	Сканирование IP протокола
-p	Сканирование IP протокола

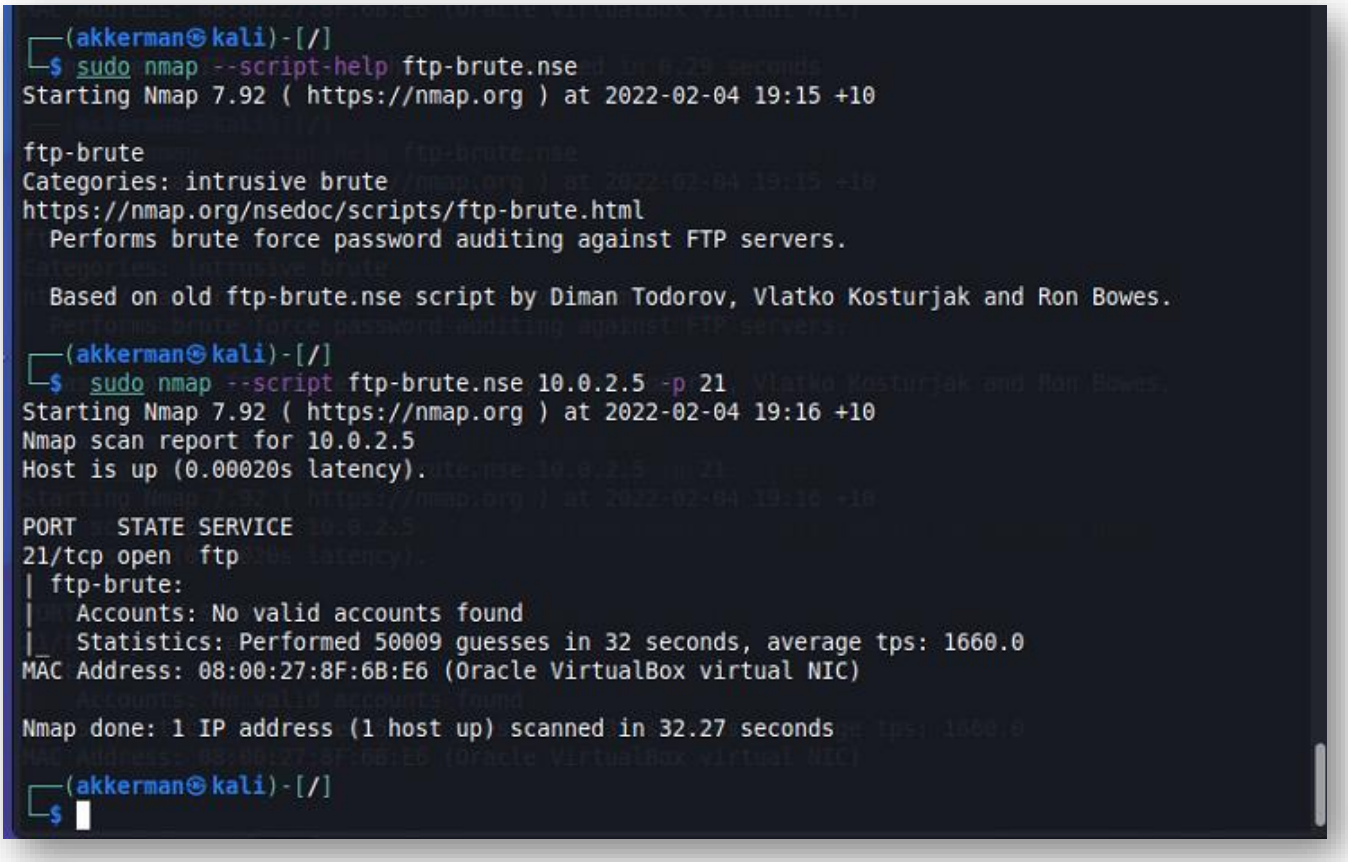
```
┌──(akkerman㉿kali)-[~/Рабочий стол]
└─$ sudo nmap -iR 3 -sO -p1-80
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-04 18:15 +10
Nmap scan report for a23-79-96-228.deploy.static.akamaitechnologies.com (23.79.96.228)
Host is up (0.045s latency).
Not shown: 78 open|filtered n/a protocols (no-response)
PROTOCOL STATE SERVICE
1        open  icmp
6        open  tcp

Nmap scan report for 134.111.255.192
Host is up (0.00064s latency).
Not shown: 79 open|filtered n/a protocols (no-response)
PROTOCOL STATE SERVICE
6        open  tcp

Nmap scan report for pool-100-34-7-215.phlapa.fios.verizon.net (100.34.7.215)
Host is up (0.049s latency).
Not shown: 78 open|filtered n/a protocols (no-response)
PROTOCOL STATE SERVICE
1        open  icmp
6        open  tcp

Nmap done: 3 IP addresses (3 hosts up) scanned in 7.57 seconds
```

10.0.2.5	
-R	Всегда производить разрешение
-r	Сканировать порты последовательно - не использовать случайный порядок портов
--host-timeout	Прекращает сканирование медленных целей
--open	Показывать только открытые (или возможно открытые) порты

```
┌──(akkerman㉿kali)-[~/Рабочий стол]
└─$ sudo nmap -R -r --host-timeout 10 --open 10.0.2.5
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-04 18:33 +10
Nmap scan report for 10.0.2.5
Host is up (0.00013s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49175/tcp open  unknown
49176/tcp open  unknown
MAC Address: 08:00:27:8F:6B:E6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.39 seconds
```

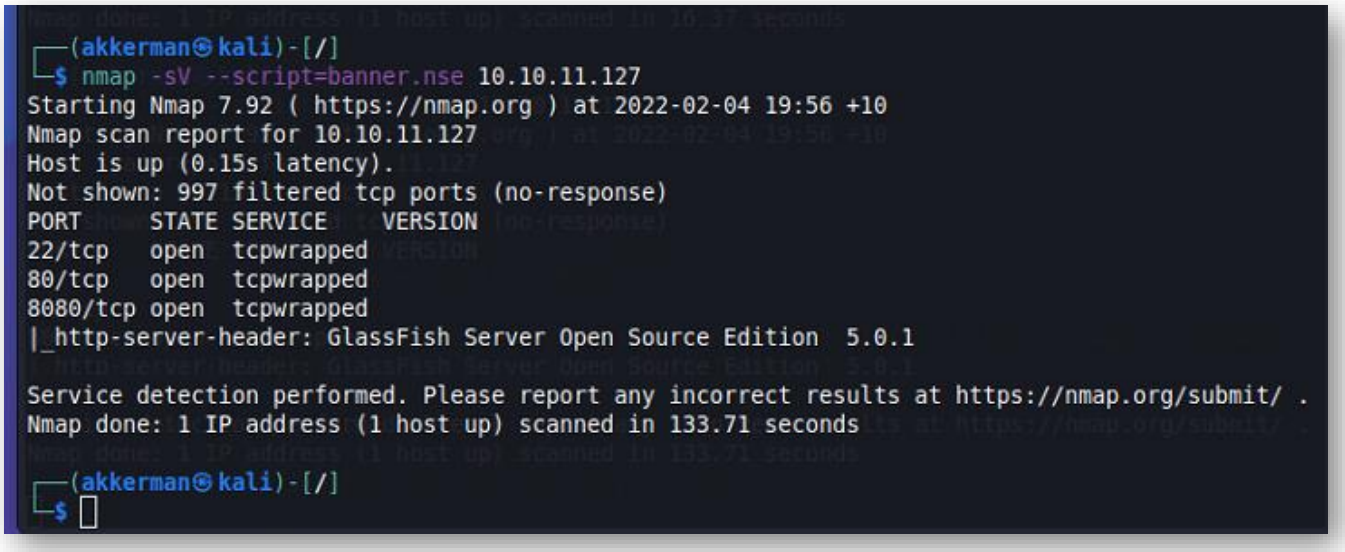
Скрипты:

Этот скрипт будет пытаться определить логин и пароль от FTP на удаленном узле.



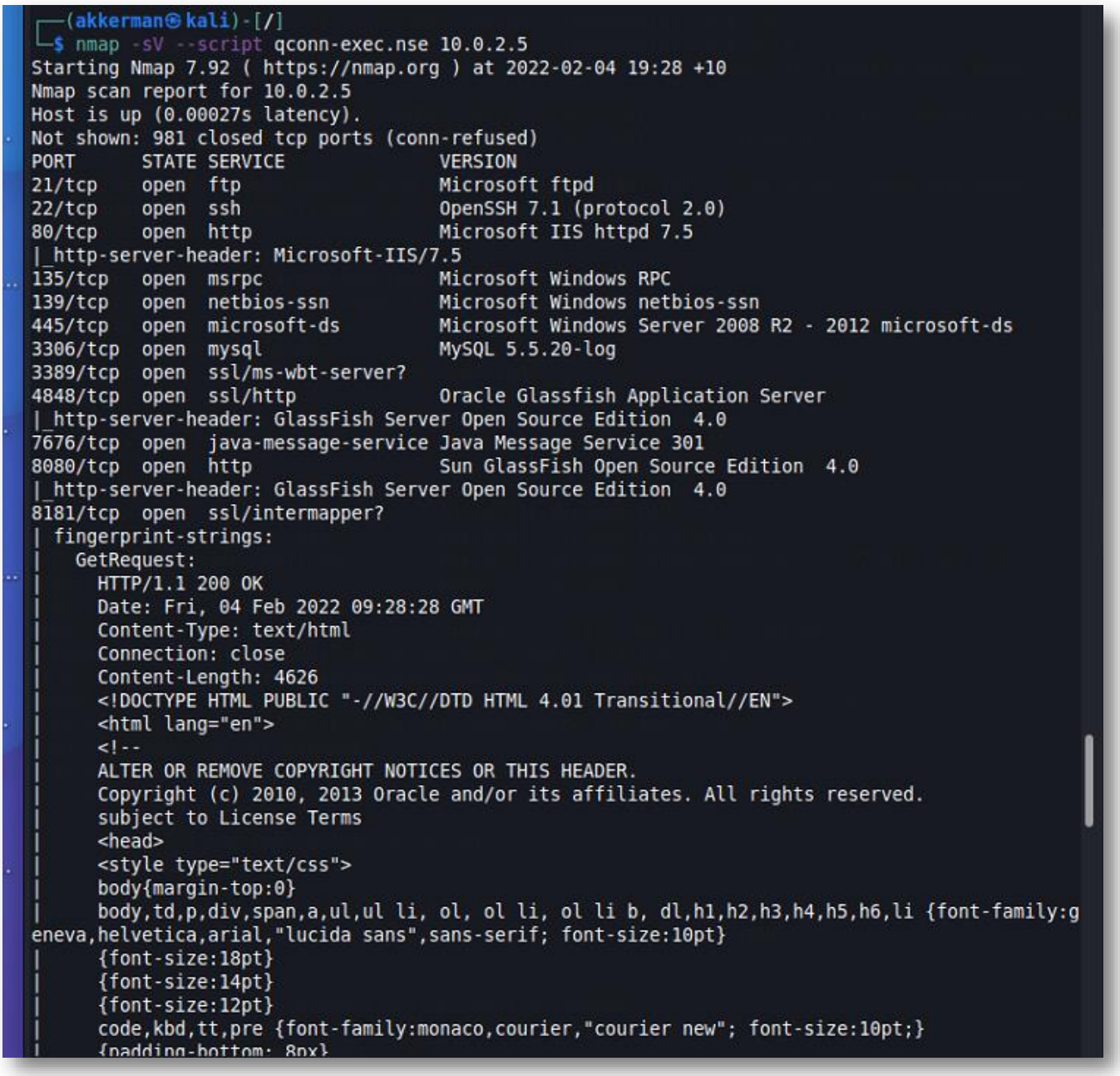
Простой захват баннеров, который подключается к открытому TCP-порту и распечатывает все, что отправляется службой прослушивания, в течение пяти секунд.

Баннер будет обрезан, чтобы поместиться в одну строку, но для каждого увеличения уровня детализации, запрошенного в командной строке, может быть напечатана дополнительная строка.



Пытается определить, позволяет ли слушающий демон QNX QCONN неавторизованным пользователям выполнять произвольные команды операционной системы.

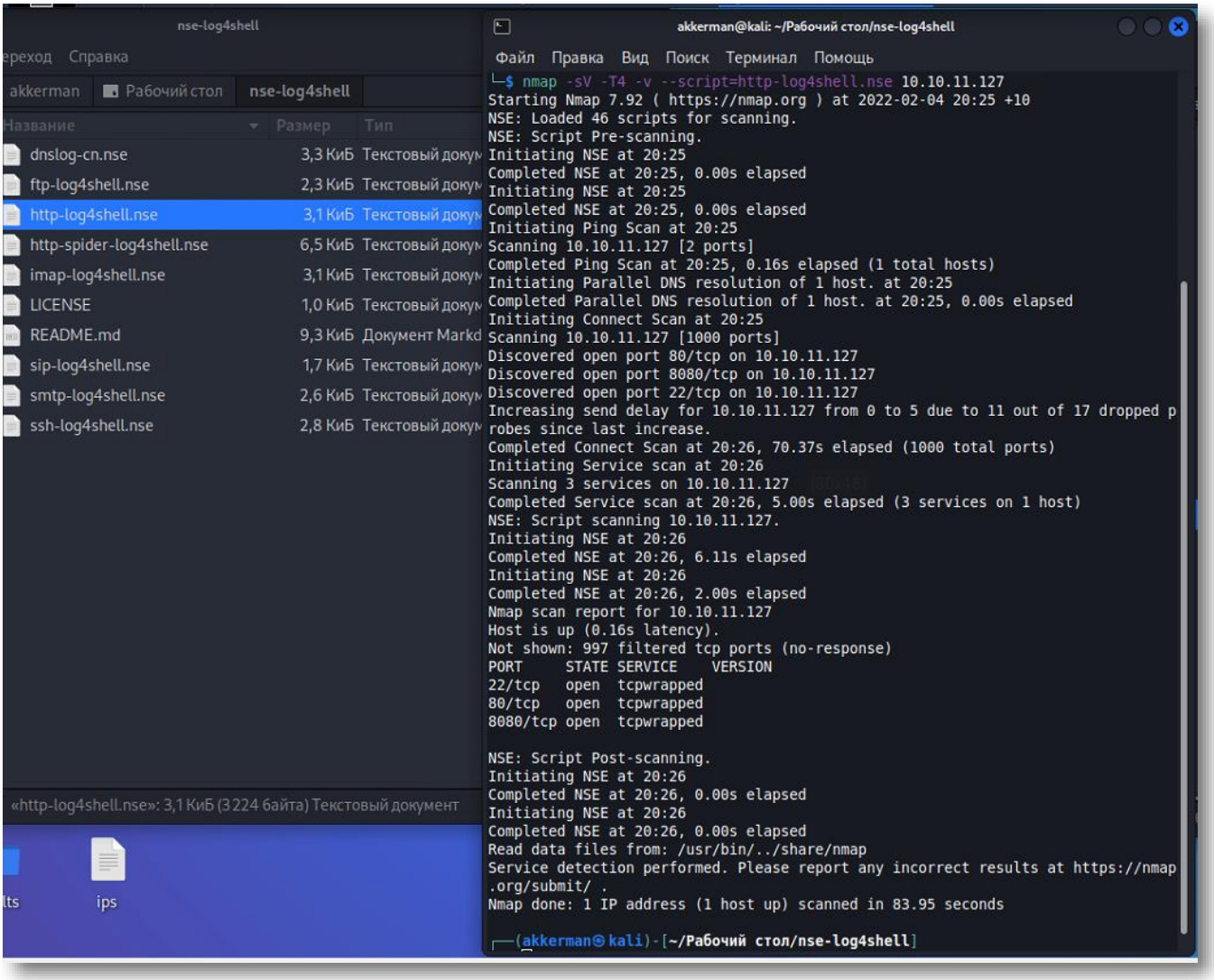
QNX — это коммерческая Unix-подобная операционная система реального времени, предназначенная в первую очередь для рынка встраиваемых систем. Демон QCONN — это поставщик услуг, обеспечивающий поддержку удаленных компонентов IDE, например профилирование системной информации



Ответвление сценария dns-перебора, включенного в nmap, который пытается перечислить имена хостов путем перебора, угадывая общие поддомены. Эта версия позволяет предоставлять список распознавателей, чтобы каждый поток мог запрашивать отдельный DNS-сервер и избегать потенциальных ограничений скорости.

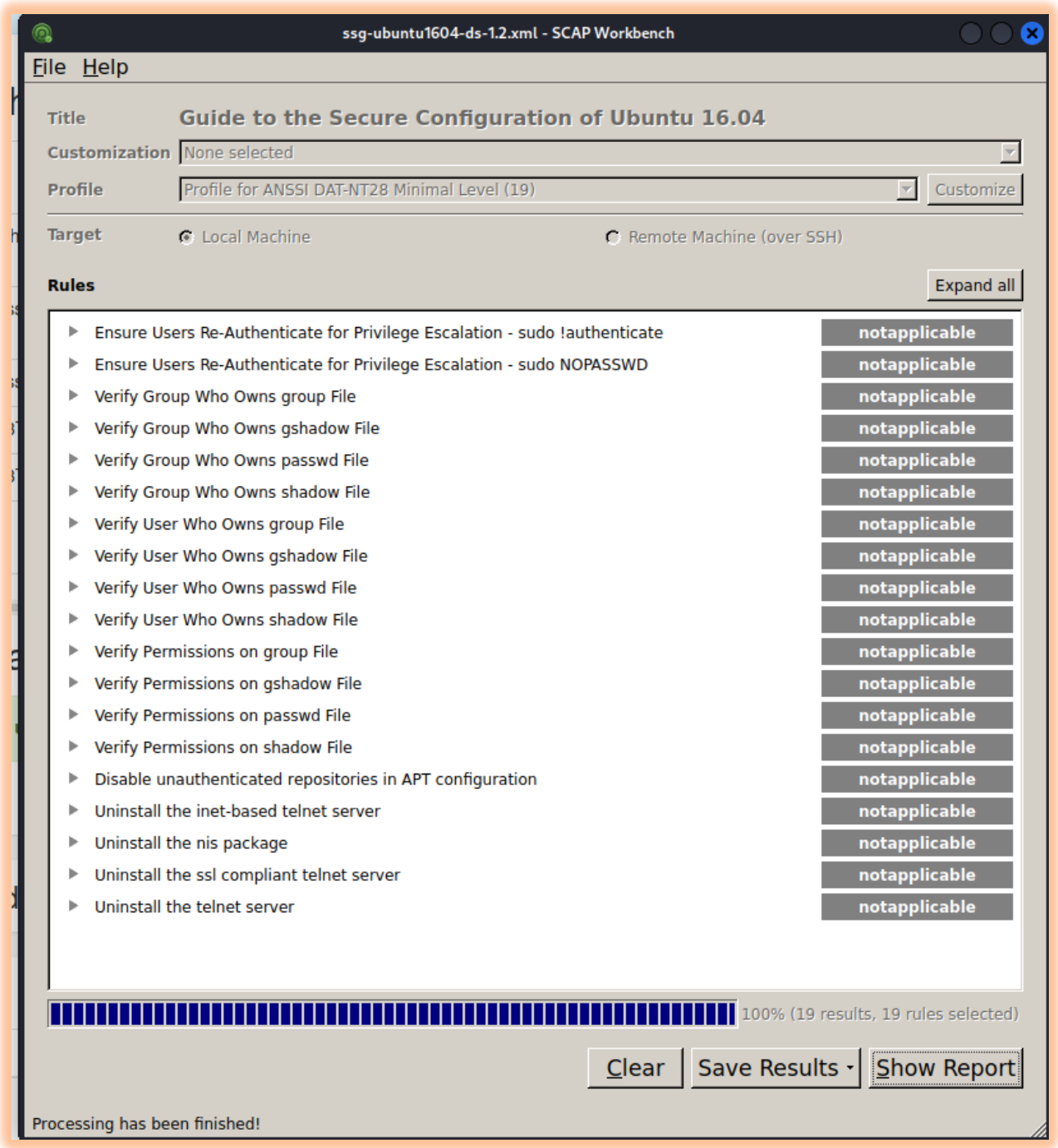
```
Nmap done: 1 IP address (1 host up) scanned in 133.71 seconds

┌──(akkerman㉿kali)-[/]
└─$ nmap -sV --script=dns-brute2.nse 10.10.11.127
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-04 20:10 +10
Nmap scan report for 10.10.11.127
Host is up (0.16s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Werkzeug httpd 1.0.1 (Python 2.7.17)
8080/tcp open  http    Sun GlassFish Open Source Edition  5.0.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_dns-brute2: Can't guess domain of "10.10.11.127"; use dns-brute2.domain script argument.

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 145.94 seconds

┌──(akkerman㉿kali)-[/]
└─$
```

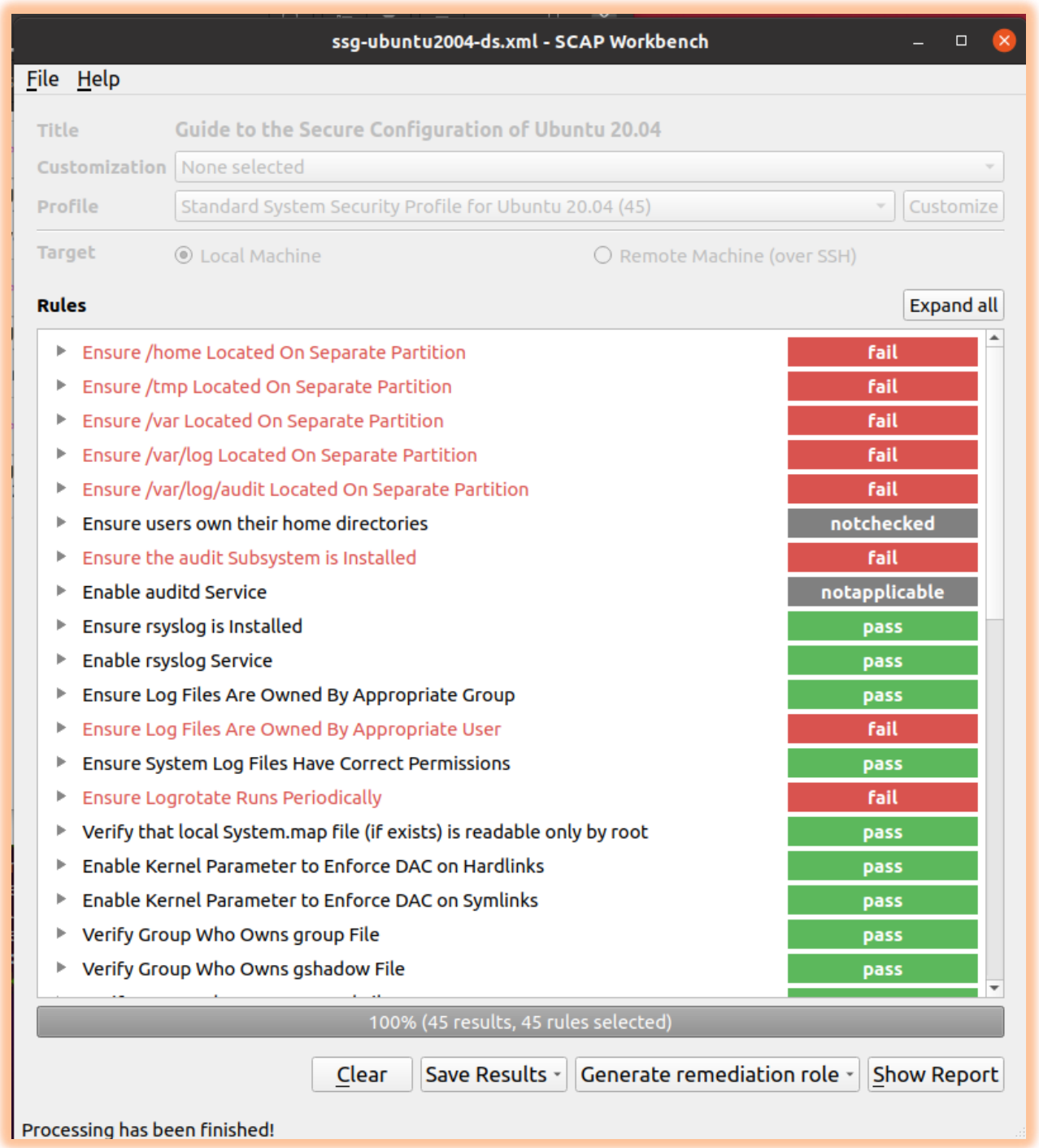
Сценарии Nmap NSE для проверки на наличие уязвимостей log4shell или LogJam (CVE-2021-44228). Сценарии NSE проверяют наиболее популярные открытые сервисы в Интернете.

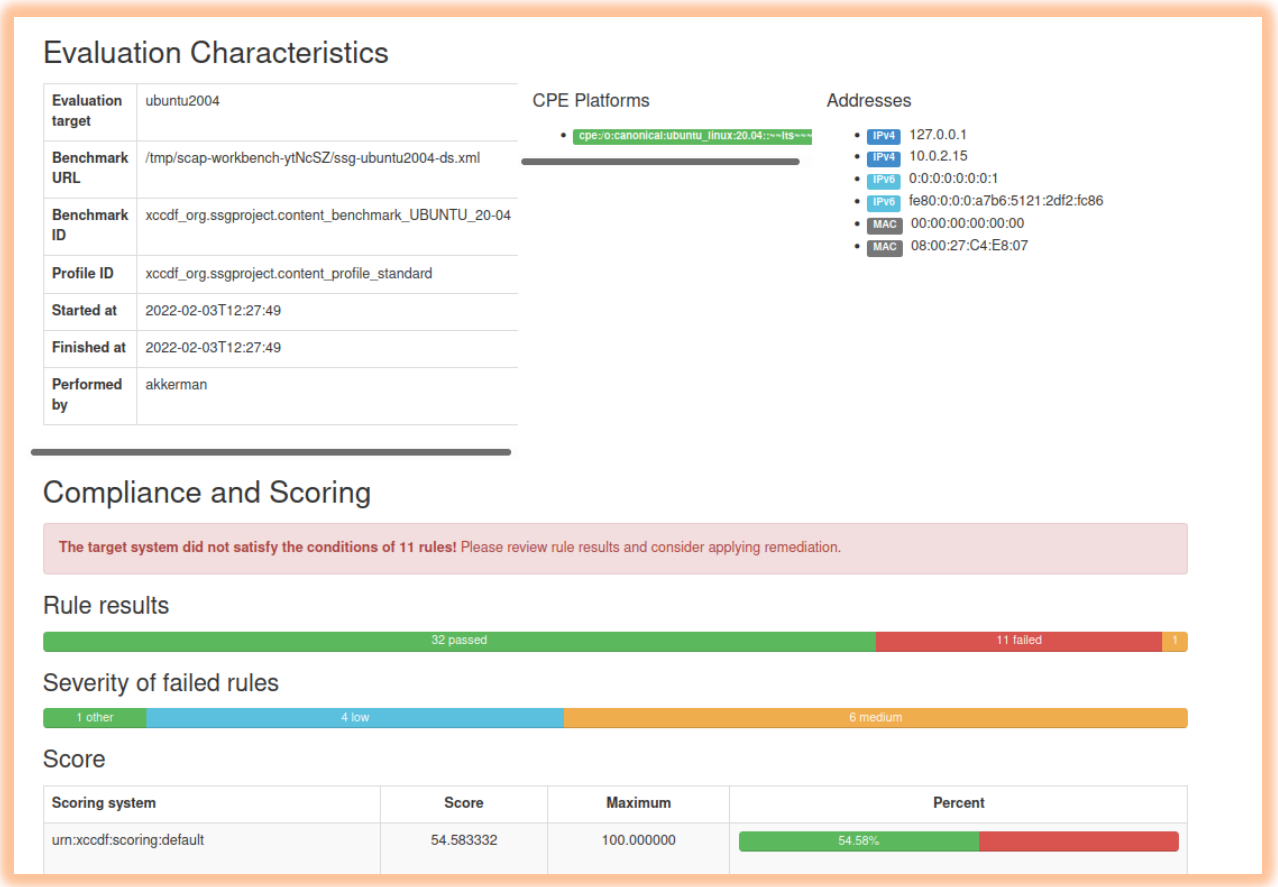


5. OPENSCAP

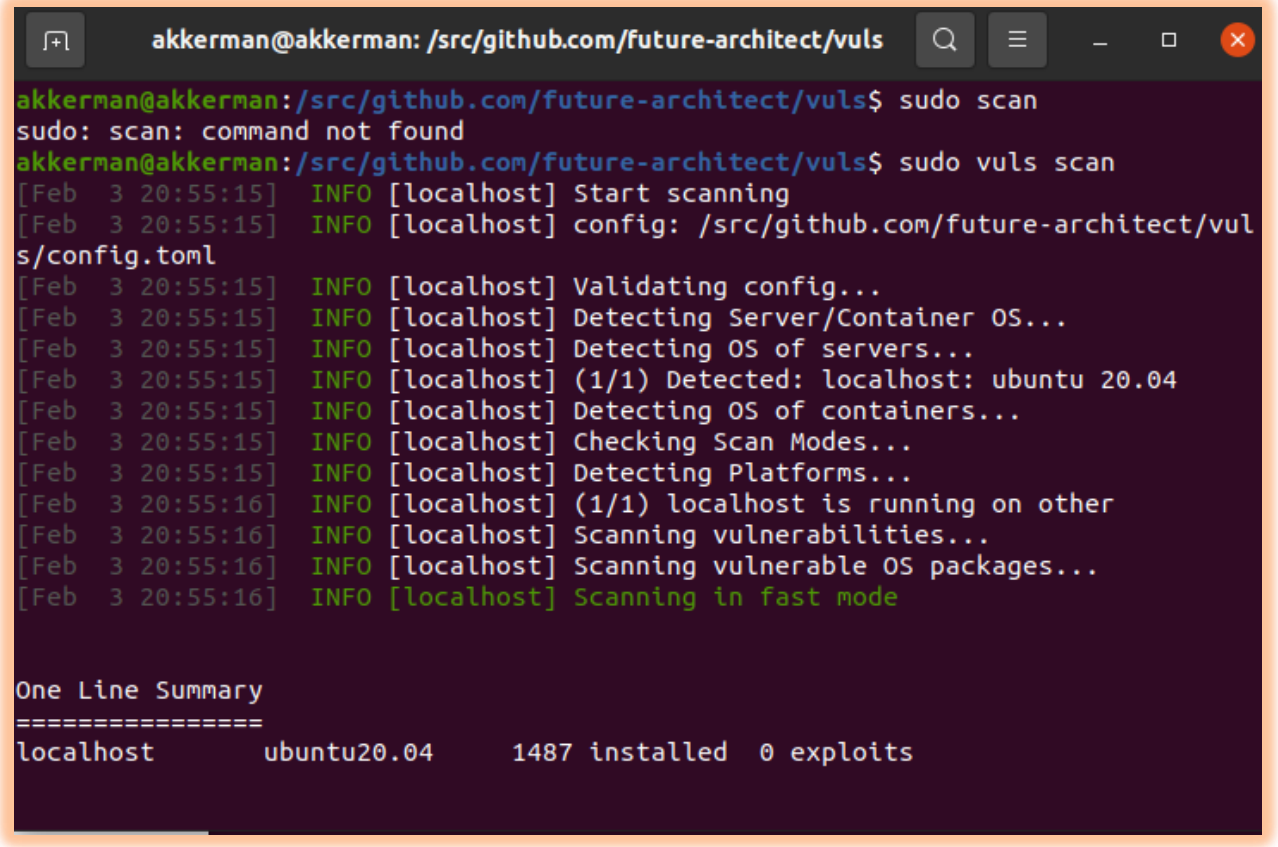
```
==== Inbuilt CPE names ====
Red Hat Enterprise Linux - cpe:/o:redhat:enterprise_linux
Red Hat Enterprise Linux 5 - cpe:/o:redhat:enterprise_linux:5
Red Hat Enterprise Linux 6 - cpe:/o:redhat:enterprise_linux:6
Red Hat Enterprise Linux 7 - cpe:/o:redhat:enterprise_linux:7
Oracle Linux 5 - cpe:/o:oracle:linux:5
Oracle Linux 6 - cpe:/o:oracle:linux:6
Oracle Linux 7 - cpe:/o:oracle:linux:7
Community Enterprise Operating System 5 - cpe:/o:centos:centos:5
Community Enterprise Operating System 6 - cpe:/o:centos:centos:6
Community Enterprise Operating System 7 - cpe:/o:centos:centos:7
Scientific Linux 5 - cpe:/o:scientificlinux:scientificlinux:5
Scientific Linux 6 - cpe:/o:scientificlinux:scientificlinux:6
Scientific Linux 7 - cpe:/o:scientificlinux:scientificlinux:7
Fedora 16 - cpe:/o:fedoraproject:fedora:16
Fedora 17 - cpe:/o:fedoraproject:fedora:17
Fedora 18 - cpe:/o:fedoraproject:fedora:18
Fedora 19 - cpe:/o:fedoraproject:fedora:19
Fedora 20 - cpe:/o:fedoraproject:fedora:20
Fedora 21 - cpe:/o:fedoraproject:fedora:21
Fedora 22 - cpe:/o:fedoraproject:fedora:22
Fedora 23 - cpe:/o:fedoraproject:fedora:23
Fedora 24 - cpe:/o:fedoraproject:fedora:24
Fedora 25 - cpe:/o:fedoraproject:fedora:25
Fedora 26 - cpe:/o:fedoraproject:fedora:26
Fedora 27 - cpe:/o:fedoraproject:fedora:27
Fedora 28 - cpe:/o:fedoraproject:fedora:28
SUSE Linux Enterprise all versions - cpe:/o:suse:sle
SUSE Linux Enterprise Server 10 - cpe:/o:suse:sles:10
SUSE Linux Enterprise Desktop 10 - cpe:/o:suse:sled:10
SUSE Linux Enterprise Server 11 - cpe:/o:suse:linux_enterprise_server:11
SUSE Linux Enterprise Desktop 11 - cpe:/o:suse:linux_enterprise_desktop:11
SUSE Linux Enterprise Server 12 - cpe:/o:suse:sles:12
SUSE Linux Enterprise Desktop 12 - cpe:/o:suse:sled:12
openSUSE 11.4 - cpe:/o:opensuse:opensuse:11.4
openSUSE 13.1 - cpe:/o:opensuse:opensuse:13.1
openSUSE 13.2 - cpe:/o:opensuse:opensuse:13.2
openSUSE 42.1 - cpe:/o:novell:leap:42.1
openSUSE 42.2 - cpe:/o:novell:leap:42.2
openSUSE All Versions - cpe:/o:opensuse:opensuse
Red Hat Enterprise Linux Optional Productivity Applications - cpe:/a:redhat:rhel_productivity
Red Hat Enterprise Linux Optional Productivity Applications 5 - cpe:/a:redhat:rhel_productivity:5
Wind River Linux all versions - cpe:/o:windriver:wrlinux
Wind River Linux 8 - cpe:/o:windriver:wrlinux:8
```

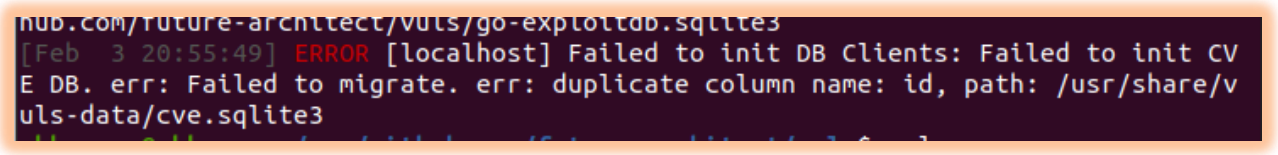

ssg-ubuntu1604-ds-1.2.xml - SCAP Workbench
File Help
Title
Guide to the Secure Configuration of Ubuntu 16.04
Customization
None selected
Profile
Profile for ANSSI DAT-NT28 Minimal Level (19)
Customize
Target
Local Machine
Remote Machine (over SSH)
Rules
Expand all
Ensure Users Re-Authenticate for Privilege Escalation - sudo !authenticate
Ensure Users Re-Authenticate for Privilege Escalation - sudo NOPASSWD
Verify Group Who Owns group File
Verify Group Who Owns gshadow File
Verify Group Who Owns passwd File
Verify Group Who Owns shadow File
Verify User Who Owns group File
Verify User Who Owns gshadow File
Verify User Who Owns passwd File
Verify User Who Owns shadow File
Verify Permissions on group File
Verify Permissions on gshadow File
Verify Permissions on passwd File
Verify Permissions on shadow File
Disable unauthenticated repositories in APT configuration
Uninstall the inet-based telnet server
Uninstall the nis package
Uninstall the ssl compliant telnet server
Uninstall the telnet server
notapplicable
100% (19 results, 19 rules selected)
Clear
Save Results
Show Report
Processing has been finished!


ssg-ubuntu2004-ds.xml - SCAP Workbench
File Help
Title Guide to the Secure Configuration of Ubuntu 20.04
Customization None selected
Profile Standard System Security Profile for Ubuntu 20.04 (45) Customize
Target Local Machine Remote Machine (over SSH)
Rules Expand all
Ensure /home Located On Separate Partition fail
Ensure /tmp Located On Separate Partition fail
Ensure /var Located On Separate Partition fail
Ensure /var/log Located On Separate Partition fail
Ensure /var/log/audit Located On Separate Partition fail
Ensure users own their home directories notchecked
Ensure the audit Subsystem is Installed fail
Enable auditd Service notapplicable
Ensure rsyslog is Installed pass
Enable rsyslog Service pass
Ensure Log Files Are Owned By Appropriate Group pass
Ensure Log Files Are Owned By Appropriate User fail
Ensure System Log Files Have Correct Permissions pass
Ensure Logrotate Runs Periodically fail
Verify that local System.map file (if exists) is readable only by root pass
Enable Kernel Parameter to Enforce DAC on Hardlinks pass
Enable Kernel Parameter to Enforce DAC on Symlinks pass
Verify Group Who Owns group File pass
Verify Group Who Owns gshadow File pass
100% (45 results, 45 rules selected)
Clear Save Results Generate remediation role Show Report
Processing has been finished!

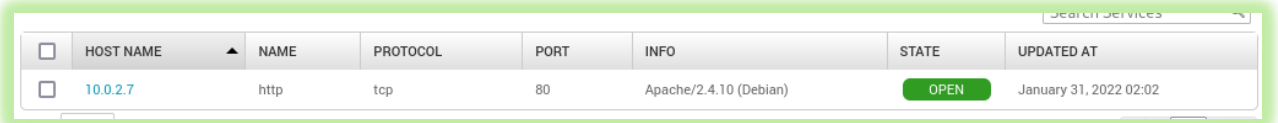

Evaluation Characteristics
Evaluation target
ubuntu2004
Benchmark URL
/tmp/scap-workbench-ytNcSZ/ssg-ubuntu2004-ds.xml
Benchmark ID
xccdf_org.ssgproject.content_benchmark_UBUNTU_20-04
Profile ID
xccdf_org.ssgproject.content_profile_standard
Started at
2022-02-03T12:27:49
Finished at
2022-02-03T12:27:49
Performed by
akkerman
CPE Platforms
Addresses
IPv4 127.0.0.1
IPv4 10.0.2.15
IPv6 0:0:0:0:0:0:0:1
IPv6 fe80:0:0:0:a7b6:5121:2df2:fc86
MAC 00:00:00:00:00:00
MAC 08:00:27:C4:E8:07
Compliance and Scoring
The target system did not satisfy the conditions of 11 rules! Please review rule results and consider applying remediation.
Rule results
32 passed
11 failed
Severity of failed rules
1 other
4 low
6 medium
Score
Scoring system
Score
Maximum
Percent
urn:xccdf:scoring:default
54.583332
100.000000
54.58%

6. VULS

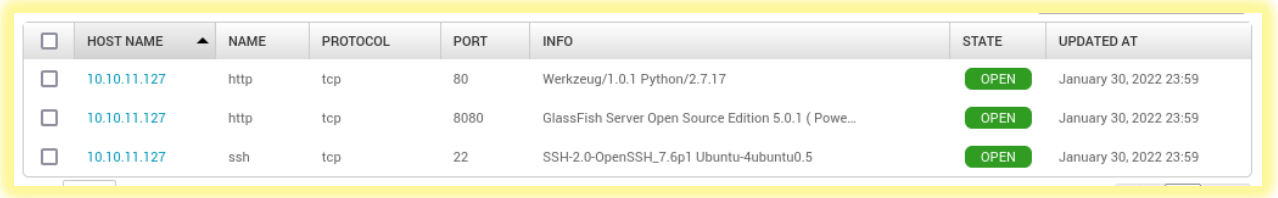

akkerman@akkerman: /src/github.com/future-architect/vuls
akkerman@akkerman:/src/github.com/future-architect/vuls$ sudo scan
sudo: scan: command not found
akkerman@akkerman:/src/github.com/future-architect/vuls$ sudo vuls scan
[Feb 3 20:55:15] INFO [localhost] Start scanning
[Feb 3 20:55:15] INFO [localhost] config: /src/github.com/future-architect/vuls/config.toml
[Feb 3 20:55:15] INFO [localhost] Validating config...
[Feb 3 20:55:15] INFO [localhost] Detecting Server/Container OS...
[Feb 3 20:55:15] INFO [localhost] Detecting OS of servers...
[Feb 3 20:55:15] INFO [localhost] (1/1) Detected: localhost: ubuntu 20.04
[Feb 3 20:55:15] INFO [localhost] Detecting OS of containers...
[Feb 3 20:55:15] INFO [localhost] Checking Scan Modes...
[Feb 3 20:55:15] INFO [localhost] Detecting Platforms...
[Feb 3 20:55:16] INFO [localhost] (1/1) localhost is running on other
[Feb 3 20:55:16] INFO [localhost] Scanning vulnerabilities...
[Feb 3 20:55:16] INFO [localhost] Scanning vulnerable OS packages...
[Feb 3 20:55:16] INFO [localhost] Scanning in fast mode
One Line Summary
localhost ubuntu20.04 1487 installed 0 exploits



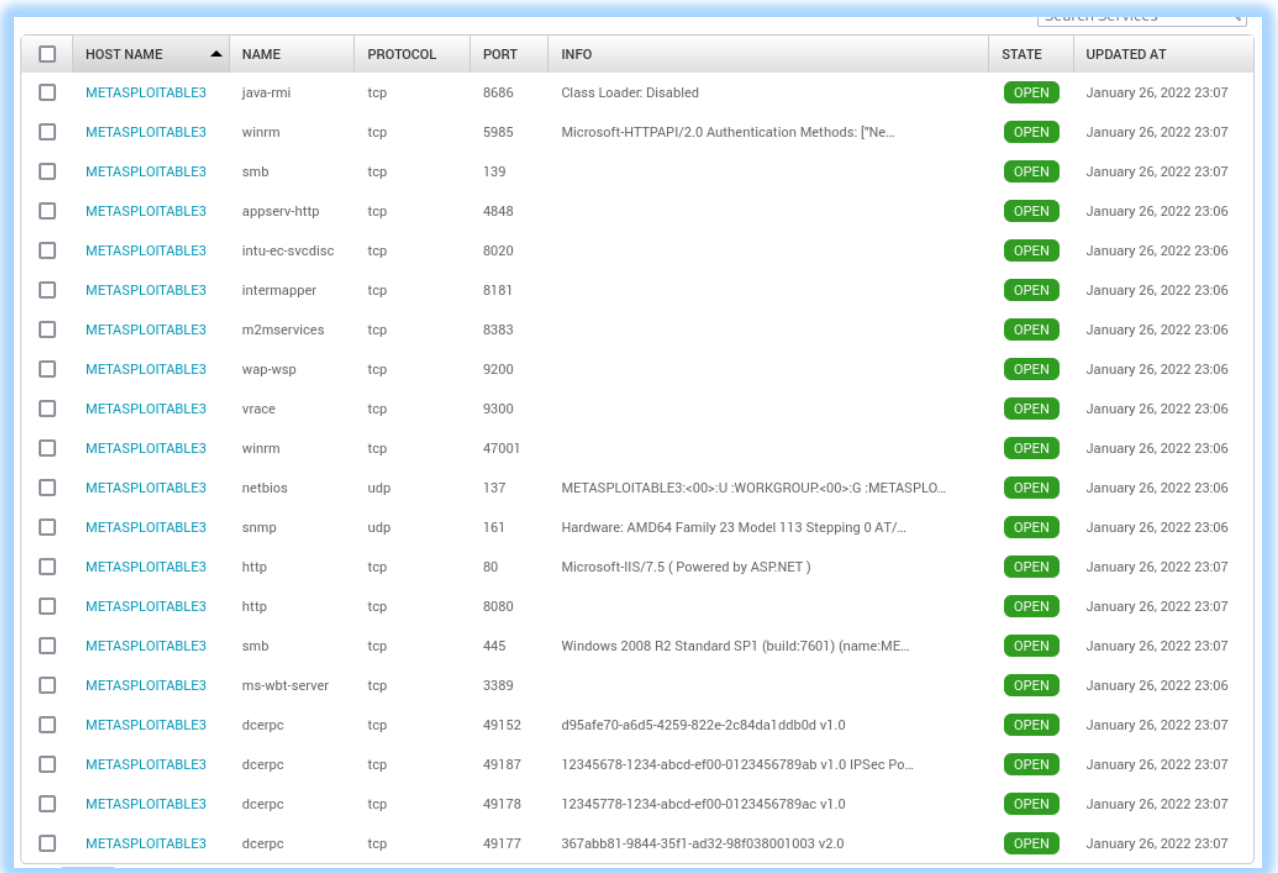
7. Metasploit Pro Scanner



HOST NAME	NAME	PROTOCOL	PORT	INFO	STATE	UPDATED AT
10.0.2.7	http	tcp	80	Apache/2.4.10 (Debian)	OPEN	January 31, 2022 02:02



HOST NAME	NAME	PROTOCOL	PORT	INFO	STATE	UPDATED AT
10.10.11.127	http	tcp	80	Werkzeug/1.0.1 Python/2.7.17	OPEN	January 30, 2022 23:59
10.10.11.127	http	tcp	8080	GlassFish Server Open Source Edition 5.0.1 (Powe...	OPEN	January 30, 2022 23:59
10.10.11.127	ssh	tcp	22	SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.5	OPEN	January 30, 2022 23:59



HOST NAME	NAME	PROTOCOL	PORT	INFO	STATE	UPDATED AT
METASPLOITABLE3	java-rmi	tcp	8686	Class Loader: Disabled	OPEN	January 26, 2022 23:07
METASPLOITABLE3	winrm	tcp	5985	Microsoft-HTTPAPI/2.0 Authentication Methods: ["Ne...	OPEN	January 26, 2022 23:07
METASPLOITABLE3	smb	tcp	139		OPEN	January 26, 2022 23:07
METASPLOITABLE3	appserv-http	tcp	4848		OPEN	January 26, 2022 23:06
METASPLOITABLE3	intu-ec-svcdisc	tcp	8020		OPEN	January 26, 2022 23:06
METASPLOITABLE3	intermapper	tcp	8181		OPEN	January 26, 2022 23:06
METASPLOITABLE3	m2mservices	tcp	8383		OPEN	January 26, 2022 23:06
METASPLOITABLE3	wap-wsp	tcp	9200		OPEN	January 26, 2022 23:06
METASPLOITABLE3	vrace	tcp	9300		OPEN	January 26, 2022 23:06
METASPLOITABLE3	winrm	tcp	47001		OPEN	January 26, 2022 23:06
METASPLOITABLE3	netbios	udp	137	METASPLOITABLE3:<00>:U :WORKGROUP:<00>:G :METASPLO...	OPEN	January 26, 2022 23:06
METASPLOITABLE3	snmp	udp	161	Hardware: AMD64 Family 23 Model 113 Stepping 0 AT/...	OPEN	January 26, 2022 23:06
METASPLOITABLE3	http	tcp	80	Microsoft-IIS/7.5 (Powered by ASP.NET)	OPEN	January 26, 2022 23:07
METASPLOITABLE3	http	tcp	8080		OPEN	January 26, 2022 23:07
METASPLOITABLE3	smb	tcp	445	Windows 2008 R2 Standard SP1 (build:7601) (name:ME...	OPEN	January 26, 2022 23:07
METASPLOITABLE3	ms-wbt-server	tcp	3389		OPEN	January 26, 2022 23:06
METASPLOITABLE3	dcerpc	tcp	49152	d95afe70-a6d5-4259-822e-2c84da1ddb0d v1.0	OPEN	January 26, 2022 23:07
METASPLOITABLE3	dcerpc	tcp	49187	12345678-1234-abcd-ef00-0123456789ab v1.0 IPSec Po...	OPEN	January 26, 2022 23:07
METASPLOITABLE3	dcerpc	tcp	49178	12345778-1234-abcd-ef00-0123456789ac v1.0	OPEN	January 26, 2022 23:07
METASPLOITABLE3	dcerpc	tcp	49177	367abb81-9844-35f1-ad32-98f038001003 v2.0	OPEN	January 26, 2022 23:07

Вывод

Было проведено сканирование 3х различных виртуальных машин. Наибольшее количество уязвимостей было обнаружено на Windows Server 2008 из пакета metasploitable 3. Наиболее структурированной и ультимативной программой оказалась

Nessus Pro, впрочем OpenVas тоже нашёл много уязвимостей. В качестве векторов атаки, доступны несколько вариантов:

1. Windows Server
    a. Атака через IIS-HTTP на 80 порту(HTTP)
    b. Атака через MySQL на порту 3306(TCP)
    c. Атака через SSH на порту 22
2. Fingerprint
    a. Открытые порты 22,80,8080
3. HACKERHOUSE
    a. Поддержка Debian 8.0 закончилась в 18 году, можно воспользоваться уязвимостью