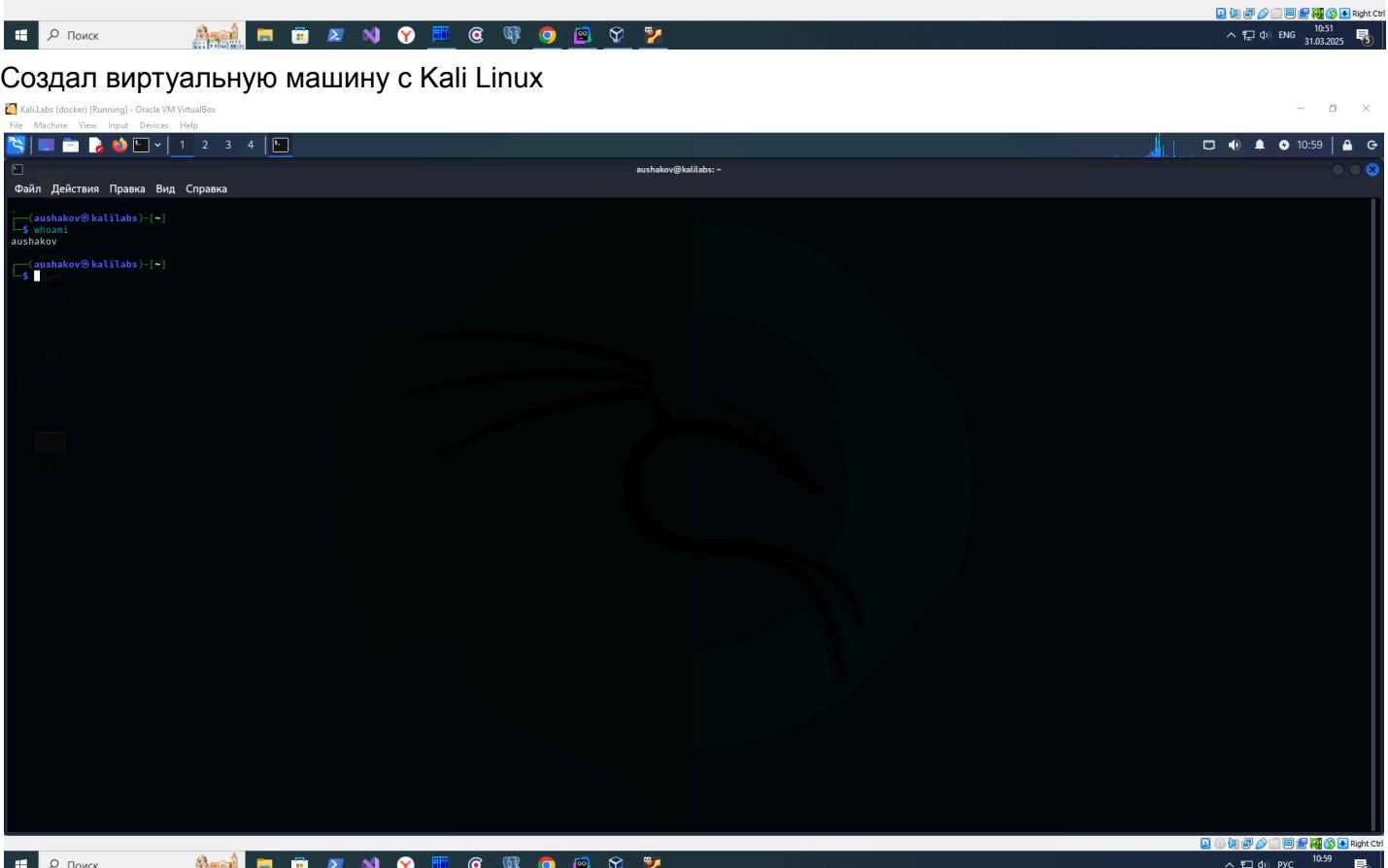
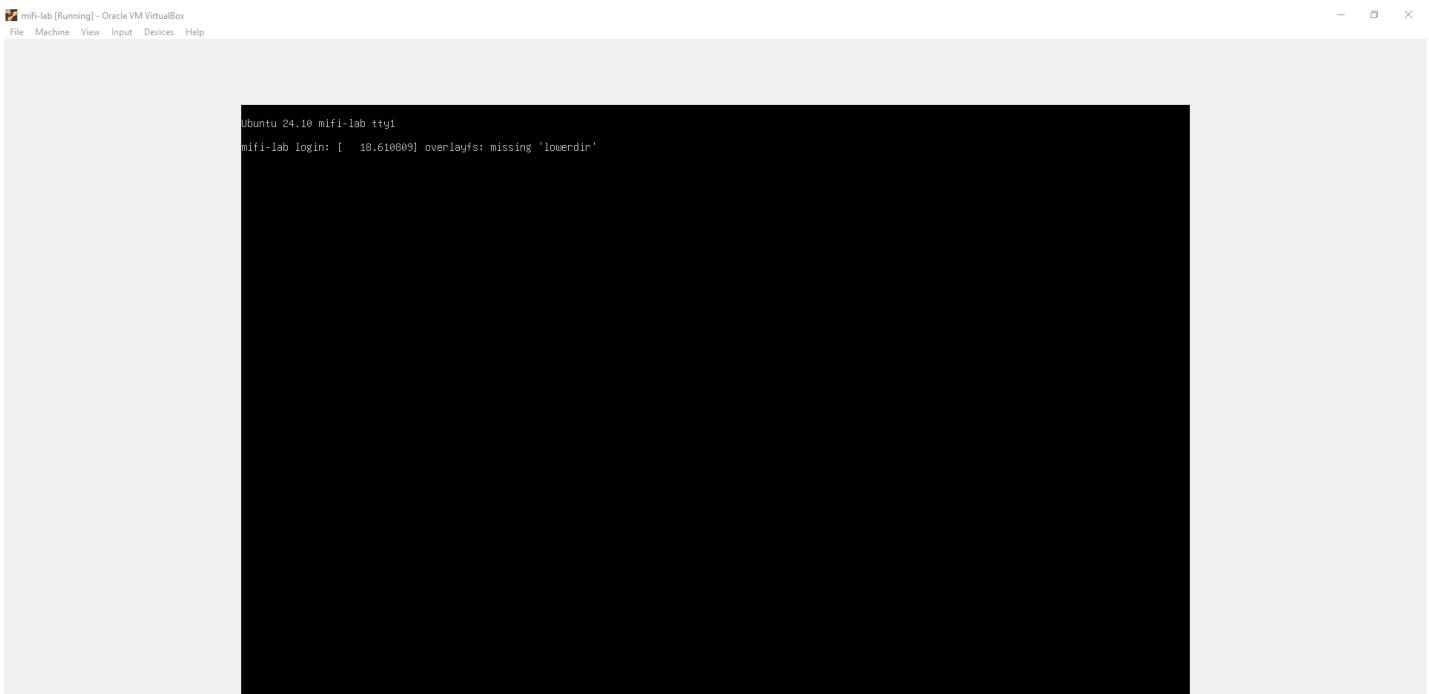
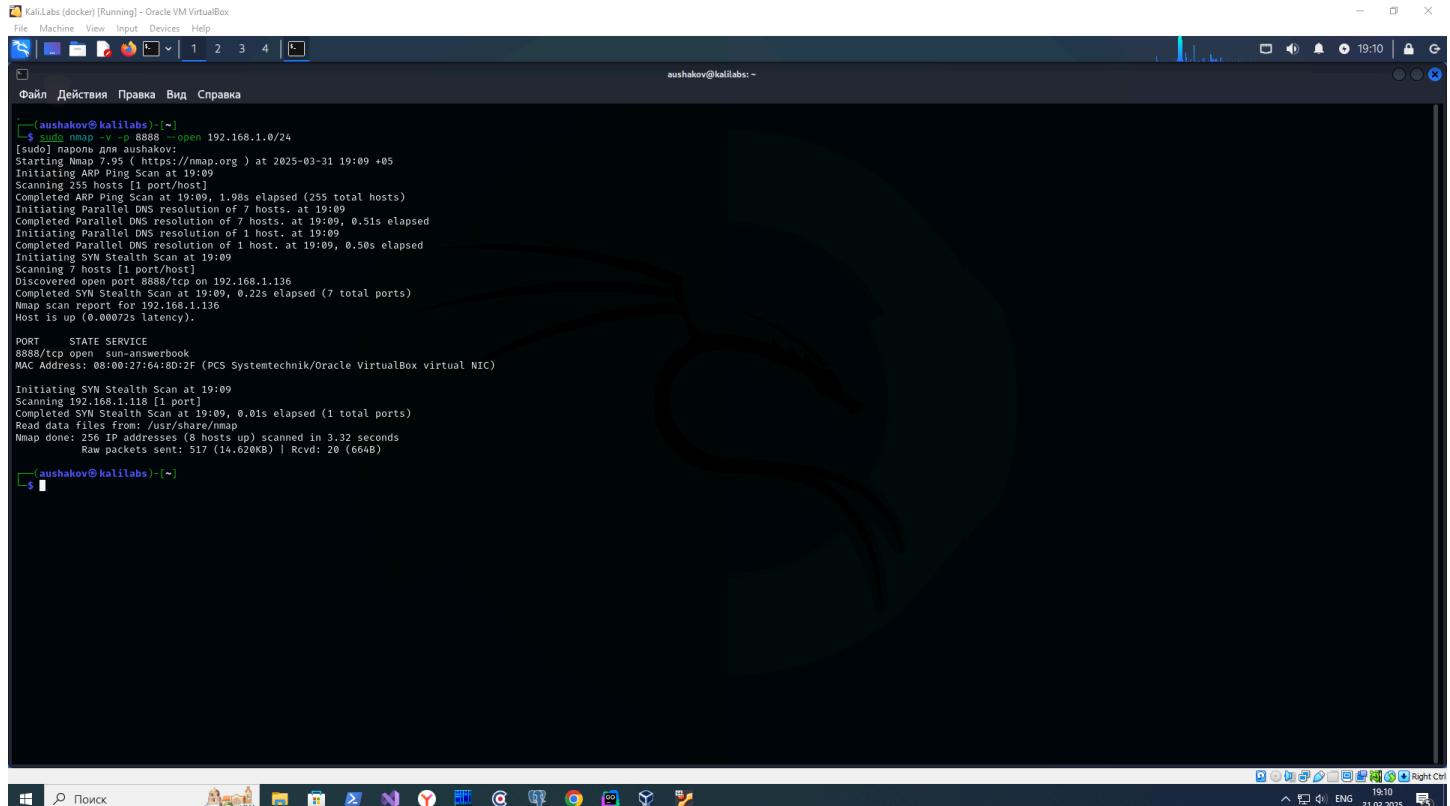


Запустил виртуальную машину с уязвимостями (я буду использовать не только виртуальную машину с уязвимостями, развернутую локально, но и ее удаленно развернутый экземпляр, т.к. часть уязвимостей легче определяется на ней почему то)



Определяю ip-адрес машины с уязвимостями:



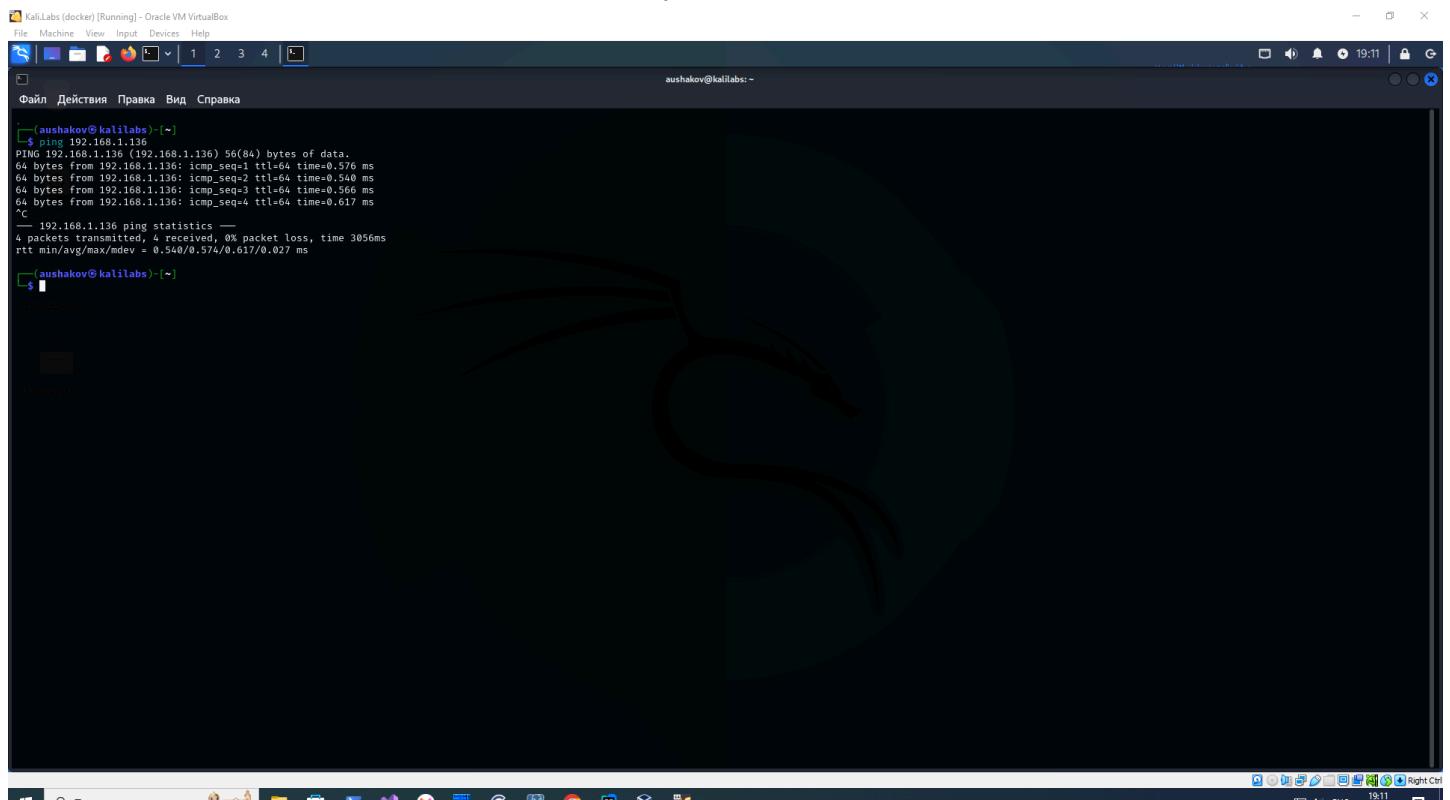
```
(ausakov㉿kalilabs) [~]
$ sudo nmap -v -p 8888 --open 192.168.1.0/24
[sudo] пароль для ausakov:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-31 19:09 +05
Initiating ARP Ping Scan at 19:09
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 19:09, 1.98s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 7 hosts. at 19:09
Completed Parallel DNS resolution of 7 hosts. at 19:09, 0.51s elapsed
Initiating Parallel DNS resolution of 1 host. at 19:09
Completed Parallel DNS resolution of 1 host. at 19:09, 0.50s elapsed
Initiating SYN Stealth Scan at 19:09
Scanning 7 hosts [1 port/host]
Disclosed open port 8888/tcp on 192.168.1.136
Completed SYN Stealth Scan at 19:09, 0.22s elapsed (7 total ports)
Nmap scan report for 192.168.1.136
Host is up (0.00072s latency).

PORT      STATE SERVICE
8888/tcp  open  sun-answerbook
MAC Address: 08:00:27:64:BD:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Initiating SYN Stealth Scan at 19:09
Scanning 192.168.1.118 [1 port]
Completed SYN Stealth Scan at 19:09, 0.01s elapsed (1 total ports)
Read data from /root/share/nmap
Nmap done: 256 IP addresses (8 hosts up) scanned in 3.32 seconds
  Raw packets sent: 517 (14.620KB) | Rcvd: 29 (664B)
```

Для этого я использую следующую команду: nmap -v -p 8888 --open 192.168.1.0/24. Видно, что ip-адрес машины с уязвимостями следующий: 192.168.1.136.

Можно еще проверить, что данная машина пингуется:



```
(ausakov㉿kalilabs) [~]
$ ping 192.168.1.136
PING 192.168.1.136 (192.168.1.136) 56(84) bytes of data.
64 bytes from 192.168.1.136 icmp_seq=1 ttl=64 time=0.576 ms
64 bytes from 192.168.1.136 icmp_seq=2 ttl=64 time=0.540 ms
64 bytes from 192.168.1.136 icmp_seq=3 ttl=64 time=0.566 ms
64 bytes from 192.168.1.136 icmp_seq=4 ttl=64 time=0.617 ms
```
--- 192.168.1.136 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3056ms
rtt min/avg/max/mdev = 0.540/0.574/0.617/0.027 ms
```

Сначала, я проверю уязвимости с помощью nmap - я буду использовать nse (nmap scripting engine) функции с категорией vuln:

```
KaliLabs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[File] [Действия] [Правка] [Вид] [Справка]
[auschakov@kallabs: ~]
[s] auschakov@kallabs: ~
$ sudo nmap -p 22,631,2000,4712,6123,8080,8988,8443,8888 --script vuln 192.168.1.136
Starting Nmap 7.95 (https://nmap.org) at 2025-04-02 00:17 +05
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 00:17
NSE Timing: About 40.00% done; ETC: 00:18 (0:00:48 remaining)
Completed NSE at 00:18. 34.02s elapsed
Completed NSE at 00:18. 0.00s elapsed
Pre-scan script results:
| broadcast-avahi-dos:
| Discovered hosts:
| 224.0.0.254
| [REDACTED] UDP avahi socket Dos (CVE-2011-1002).
| Hosts are all up (not vulnerable).
Initiating ARP Ping Scan at 00:18
Scanning 192.168.1.136 [1 port]
Completed ARP Ping Scan at 00:18, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:18
Completed Parallel DNS resolution of 1 host. at 00:18, 0.05s elapsed
Initiating NSE at 00:18
Scanning 192.168.1.136 [18 ports]
Discovered open port 22/tcp on 192.168.1.136
Discovered open port 8880/tcp on 192.168.1.136
Discovered open port 8888/tcp on 192.168.1.136
Discovered open port 631/tcp on 192.168.1.136
Discovered open port 8080/tcp on 192.168.1.136
Discovered open port 843/tcp on 192.168.1.136
Discovered open port 6123/tcp on 192.168.1.136
Discovered open port 4712/tcp on 192.168.1.136
Discovered open port 8443/tcp on 192.168.1.136
Discovered open port 3000/tcp on 192.168.1.136
Completed SYN Stealth Scan at 00:18, 0.03s elapsed (10 total ports)
NSE: Script scanning 192.168.1.136.
Initiating all open ports NSE at 00:18
Completed NSE at 00:21, 220.09s elapsed
Initiating NSE at 00:21
Completed NSE at 00:21, 0.02s elapsed
Nmap scan report for 192.168.1.136
Host is up (0.001ms latency).

PORT STATE SERVICE
22/tcp open ssh
631/tcp open ipp
|_http-aspn...-debug: ERROR: Script execution failed (use -d to debug)
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE-CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.

Disclosure date: 2009-09-17
References:
 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
 http://ha.ckers.org/slowloris/
| http-enum:
| /robots.txt: Robots file
| /classes/: Potentially interesting folder
| /es/: Potentially interesting folder
| /help/: Potentially interesting folder
| /javadoc/: Potentially interesting folder
3000/tcp open http-proxy
4712/tcp open unknown
6123/tcp open backup-express
8080/tcp open http-proxy
|_http-iis-webdav-vuln: WebDAV is DISABLED. Server is not currently vulnerable.
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE-CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.

Disclosure date: 2009-09-17
References:
 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
 http://ha.ckers.org/slowloris/
8081/tcp open blackice-icecap
8088/tcp open http-alt
| http-aspn...-debug:
| status: DEBUG is enabled
8443/tcp open https-alt
| ssl-ccs-injection:
| VULNERABLE:
```

```
KaliLabs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[File] [Действия] [Правка] [Вид] [Справка]
[auschakov@kallabs: ~]
[s] auschakov@kallabs: ~
$ Completed NSE at 00:21, 0.02s elapsed
Nmap scan report for 192.168.1.136
Host is up (0.001ms latency).

PORT STATE SERVICE
22/tcp open ssh
631/tcp open ipp
|_http-aspn...-debug: ERROR: Script execution failed (use -d to debug)
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE-CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.

Disclosure date: 2009-09-17
References:
 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
 http://ha.ckers.org/slowloris/
| http-enum:
| /robots.txt: Robots file
| /classes/: Potentially interesting folder
| /es/: Potentially interesting folder
| /help/: Potentially interesting folder
| /javadoc/: Potentially interesting folder
3000/tcp open http-proxy
4712/tcp open unknown
6123/tcp open backup-express
8080/tcp open http-proxy
|_http-iis-webdav-vuln: WebDAV is DISABLED. Server is not currently vulnerable.
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE-CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.

Disclosure date: 2009-09-17
References:
 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
 http://ha.ckers.org/slowloris/
8081/tcp open blackice-icecap
8088/tcp open http-alt
| http-aspn...-debug:
| status: DEBUG is enabled
8443/tcp open https-alt
| ssl-ccs-injection:
| VULNERABLE:
```

```

Kali.Labs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Machine View Input Devices Help
aushakov@kalilabs: ~

Файл Действия Правка Вид Справка
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http://ha.ckers.org/slowloris/
8081/tcp open blackice-icecap
8088/tcp open radan-ntp
| http-aspnet-debug:
|_ status: DEBUG is enabled
8443/tcp open https-alt
|_ http-aspnet-debug:
|_ VULNERABLE:
SSL/TLS MITM vulnerability (CCS Injection)
State: VULNERABLE
Risk factor: High
OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
does not properly restrict processing of ChangeCipherSpec messages,
which allows man-in-the-middle attackers to trigger use of a zero
length master key in certain OpenSSL-to-OpenSSL communications, and
consequently hijack sessions or obtain sensitive information, via
a crafted TLS handshake, aka the "CCS Injection" vulnerability.

References:
http://www.openssl.org/news/secadv_2014-0605.txt
https://www.cvedetails.com/cve/2014-0224
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
ssl-heartbleed:
| VULNERABLE:
The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption.
State: VULNERABLE
Risk factor: High
OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.

References:
http://www.openssl.org/news/secadv_20140407.txt
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
https://www.cvedetails.com/cve/2014-0160/
8888/tcp open http-aspnet-debug
MAC Address: 08:00:27:64:BD:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

NSE: Script Post-scanning.
Initiating NSE at 00:21
Completed NSE at 00:21 0.00s elapsed
Initiating NSE at 00:21
Completed NSE at 00:21 0.00s elapsed
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 254.38 seconds
Raw packets sent: 11 (468B) | Rcvd: 11 (468B)

[aushakov@kalilabs] ~

```

Для этого я использую следующую команду:

```
nmap -v -p 22,631,3000,4712,6123,8080,8081,8088,8443,8888 --script vuln 192.168.1.136
```

Я получаю следующий результат о найденных уязвимостях (продублировал информацию со скриншота выше):

```

PORT STATE SERVICE
22/tcp open ssh
631/tcp open ipp
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
| http-slowloris-check:
|_ VULNERABLE:
Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.

| Disclosure date: 2009-09-17
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http://ha.ckers.org/slowloris/
| http-enum:
| /robots.txt: Robots file

```

```
| /classes/: Potentially interesting folder
| /es/: Potentially interesting folder
| /help/: Potentially interesting folder
|_ /printers/: Potentially interesting folder
3000/tcp open ppp
4712/tcp open unknown
6123/tcp open backup-express
8080/tcp open http-proxy
|_http-iis-webdav-vuln: WebDAV is DISABLED. Server is not currently vulnerable.
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.

| Disclosure date: 2009-09-17
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_ http://ha.ckers.org/slowloris/
8081/tcp open blackice-icecap
8088/tcp open radan-http
| http-aspnet-debug:
|_ status: DEBUG is enabled
8443/tcp open https-alt
| ssl-ccs-injection:
| VULNERABLE:
| SSL/TLS MITM vulnerability (CCS Injection)
| State: VULNERABLE
| Risk factor: High
| OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
| does not properly restrict processing of ChangeCipherSpec messages,
| which allows man-in-the-middle attackers to trigger use of a zero
| length master key in certain OpenSSL-to-OpenSSL communications, and
| consequently hijack sessions or obtain sensitive information, via
| a crafted TLS handshake, aka the "CCS Injection" vulnerability.

| References:
| http://www.openssl.org/news/secadv_20140605.txt
| http://www.cvedetails.com/cve/2014-0224
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
| ssl-heartbleed:
| VULNERABLE:
| The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It
| allows for stealing information intended to be protected by SSL/TLS encryption.
```

| State: VULNERABLE  
| Risk factor: High  
| OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.  
| References:  
| [http://www.openssl.org/news/secadv\\_20140407.txt](http://www.openssl.org/news/secadv_20140407.txt)  
| <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160>  
| <http://cvedetails.com/cve/2014-0160/>  
| 8888/tcp open sun-answerbook

На следующем шаге, я буду искать уязвимости с помощью nuclei  
Устанавливаю nuclei

```

aushakov@kali:~$ sudo apt install golang-go -y
Следующие пакеты устанавливались автоматически и больше не требуется:
 firebird3.0-common libcapstone4 libflac12t64 libgles-dev libgtksourceview-3.0-common libmsgraph-0-1 libtag1v5 libx265-209 python3-setproctitle
 firebird3.0-common-doc libconfig++9v5 libfmt9 libgles1 libgtksourceviewmm-3.0-0v5 libpaper1 libtag1v5-vanilla libopenjdk-23-jre ruby-zeitwerk
 libffio1 libconfig9 libgeo3d.13.0 libglvnd-core-dev libjumbo2 libqt5sensor5 libtagc0 libopenjdk-23-jre-headless ruby3.1
 libcurl++19 libdirectfb-1.7-7t64 libgl1-mesa-dev libglvnd-dev libjxl10.9 libqt5webkit5 libumwind-19 python3-appdirs ruby3.1-dev
 libcurl++abi1-19 libegl1 libglapi-mesa libgtksourceview-3.0-1 libmbcrypto7t64 libsuperlu6 libwebrtc-audio-processing1 python3-ntlm-auth ruby3.1-doc
 Для их удаления используйте <sudo apt autoremove>.

Установка:
 golang-go

Установка зависимостей:
 golang-1.24-go golang-1.24-src golang-src libpkgsconf3 pkgconf pkgconf-bin

Предлагаемые пакеты:
 bzr | brz mercurial

Сводка:
 Обновление: 0, Установка: 7, Удаление: 0, Пропуск обновления: 118
 Объем загрузки: 50,0 МБ
 Требуемое пространство: 259 МБ / 27,4 GB доступно

Пон:2 http://mirror.trunetwork.ru/kali kali-rolling/main amd64 golang/main amd64 golang-1.24-go amd64 1.24.1-1 [28,6 MB]
Пон:1 http://mirror.trunetwork.ru/kali kali-rolling/main all 1.24.1-1 [21,2 MB]
Пон:6 http://mirror.acmcsa.com/kali kali-rolling/main amd64 pkgsconf-bin amd64 1.8.1-4 [30,2 kB]
Пон:3 http://http.kali.org/kali kali-rolling/main amd64 golang-src all 2:1.24-2 [5 136 B]
Пон:4 http://http.kali.org/kali kali-rolling/main amd64 libpkgsconf3 amd64 1.8.1-4 [26,2 kB]
Пон:5 http://kali.download/Kali kali-rolling/main amd64 libpkgsconf3 amd64 1.8.1-4 [36,4 kB]
Пон:7 http://kali.download/Kali kali-rolling/main amd64 pkgsconf amd64 1.8.1-4 [26,2 kB]
Получено 50,0 МБ за 31с (1 612 kB/s)
Выбор ранее не выбранного пакета golang-1.24-src.
(Чтение базы данных ... на данный момент установлены 440717 файлов и каталогов.)
Подготовка к распаковке .../0-golang-1.24-1_all.deb ...
Распаковывается golang-1.24-1_all.deb ...
Выбор ранее не выбранного пакета golang-1.24-go.
Подготовка к распаковке .../1-golang-1.24-go_1.24.1-1_amd64.deb ...
Распаковывается golang-1.24-go (1.24.1-1) ...
Выбор ранее не выбранного пакета golang-src.
Подготовка к распаковке .../2-golang-src_233a1.24-2_all.deb ...
Распаковывается golang-src (2:1.24-2) ...
Выбор ранее не выбранного пакета golang-go:amd64.
Подготовка к распаковке .../3-golang-go_233a1.24-2_amd64.deb ...
Распаковывается golang-go:amd64 (2:1.24-2) ...
Выбор ранее не выбранного пакета libpkgsconf3:amd64.
Подготовка к распаковке .../4-libpkgsconf3:amd64.deb ...
Распаковывается libpkgsconf3:amd64 (1.8.1-4) ...
Выбор ранее не выбранного пакета libpkgsconf-bin.
Подготовка к распаковке .../5-pkgsconf-bin_1.8.1-4_amd64.deb ...
Распаковывается pkgsconf-bin (1.8.1-4) ...
Выбор ранее не выбранного пакета pkgsconf:amd64.
Подготовка к распаковке .../6-pkgsconf_1.8.1-4_amd64.deb ...

```

Kali.Labs (docker) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Файл Действия Правка Вид Справка

```
(ausshakov㉿kalilabs) ~
$ go version
go version go1.24.1 linux/amd64
(ausshakov㉿kalilabs) ~
$
```

Kali.Labs (docker) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Файл Действия Правка Вид Справка

```
(ausshakov㉿kalilabs) ~
$ go install github.com/projectdiscovery/nuclei/v3/cmd/nuclei@latest
go: downloading github.com/projectdiscovery/nuclei v1.1.7
go: downloading github.com/projectdiscovery/nuclei/v3 v3.4.1
go: downloading github.com/projectdiscovery/gojson v0.1.0
go: downloading github.com/projectdiscovery/logger v1.1.49
go: downloading github.com/projectdiscovery/interacts v1.2.4
go: downloading github.com/projectdiscovery/utils v0.4.15
go: downloading github.com/cnfs/structhash v0.0.0-20201127153200-e1b16c1ebc08
go: downloading github.com/google/shlex v0.0.0-20191202100458-e7afc7fbc510
go: downloading github.com/pkg/errors v0.9.1
go: downloading github.com/projectdiscovery/xss v2.0.1-20250106191152-7588d65b2ba8
go: downloading gopkg.in/yaml.v3 v3.0.1
go: downloading github.com/google/uuid v1.6.0
go: downloading github.com/json-iterator/go v1.1.12
go: downloading github.com/projectdiscovery/asnmap v1.1.1
go: downloading github.com/projectdiscovery/retryablehttp-go v1.0.102
go: downloading github.com/rs/xid v1.5.0
go: downloading github.com/urfave/cli v2.2.2.v1 v1.0.0
go: downloading github.com/elektrohomas/chroma v0.10.0
go: downloading github.com/go-playground/validator/v10 v10.14.1
go: downloading github.com/llogarosgru/aurora v2.0.3+incompatible
go: downloading github.com/projectdiscovery/hmap v0.0.85
go: downloading github.com/projectdiscovery/htpx v1.6.10
go: downloading github.com/projectdiscovery/ratelimit v0.0.77
go: downloading github.com/projectdiscovery/uncover v1.0.10
go: downloading github.com/projectdiscovery/tlsnextserver/v3 v3.2.1
go: downloading gopkg.in/yaml.v2 v2.4.0
go: downloading gopkg.in/charbracelet/glamour v0.8.0
go: downloading gopkg.in/olekukonko/tablewriter v0.0.5
go: downloading github.com/invopop/jsonschema v0.12.0
go: downloading github.com/knetic/govalue v3.0.1-20171022003610-9aa49832a739+incompatible
go: downloading github.com/miekg/dns v1.1.0
go: downloading github.com/projectdiscovery/dsl v0.3.21
go: downloading github.com/cespare/xxhash v1.1.0
go: downloading github.com/projectdiscovery/fastdialer v0.4.0
go: downloading github.com/projectdiscovery/rawhttp v0.1.99
go: downloading github.com/projectdiscovery/useragent v0.0.97
go: downloading go.uber.org/multierr v1.11.0
go: downloading github.com/http2go/http2go
go: downloading github.com/projectdiscovery/yaml/doc-go v1.0.6
go: downloading gopkg.in/segmentio/ksuid v1.0.4
go: downloading golang.org/xfer v0.29.0
go: downloading github.com/asaskevich/govalidator v0.0.0-20230301143203-a9d515a09cc2
go: downloading github.com/DataDog/gostackparse v0.6.0
go: downloading github.com/mattn/go-isatty v0.0.20
go: downloading github.com/miekg/fingerprint v0.9.5
go: downloading github.com/microcosm-cc/blueprint v1.0.27
go: downloading github.com/saintfish/charset v0.0.0-20230101081208-5e3ef4b5456d
go: downloading github.com/cheesaaa/gb/v3 v3.1.4
go: downloading github.com/google/go-github/v30 v30.1.0
go: downloading github.com/google/go-github v17.0.0+incompatible
go: downloading github.com/minio/selfupdate v0.6.1-0.20230907112617-f11e74f84ca7
```

A screenshot of a Kali Linux desktop environment. The terminal window at the bottom shows the command line interface. The user has run the command 'nuclei -version' and received output indicating the Nuclei Engine Version is v3.4.1, and the Nucl ei Config Directory, Cache Directory, and PDPC Directory are all set to '/home/aus hakov'. The terminal window has a dark background with light-colored text. The top of the screen shows the Kali Labs (docker) [Running] - Oracle VM VirtualBox window title, along with standard window controls like minimize, maximize, and close. The system tray on the right shows icons for battery, signal strength, and system status.

A screenshot of a Kali Linux desktop environment. The top bar shows various application icons and system status. A terminal window is open in the foreground, displaying the command 'git clone https://github.com/projectdiscovery/nuclei-templates.git \${go env GOPATH}/src/github.com/projectdiscovery/nuclei-templates' and its execution results. Below the terminal, there's a decorative graphic of a hand holding a stylized 'n'. The bottom bar contains the standard Windows-style taskbar with icons for search, file explorer, and other applications.

Запускаю nuclei для сервиса на порту 22/tcp (OpenSSH 9.7p1)

Для этого я использую следующую команду:

```
nuclei -u 158.160.26.20:22 -t ./nuclei-templates
```

Для сервиса на данном порту уязвимостей не обнаружено

Запускаю nuclei для сервиса на порту 631/tcp (CUPS 2.4)

Kali.Labs (docker) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

aushakov@kaililabs: ~

Файл Действия Правка Вид Справка

```
$ nuclei -u 192.168.1.136:631 -t ./nuclei-templates
```

v3.4.1

projectdiscovery.io

```
[INFO] Current nuclei version: v3.4.1 (latest)
[INFO] Current nuclei-templates version: v10.1.6 (latest)
[WRN] Scan results upload to cloud is disabled.
[INFO] New templates added in latest release: 78
[INFO] Templates loaded for current scan: 7830
[INFO] Executing 7641 signed templates from projectdiscovery/nuclei-templates
[INFO] Using 192.168.1.136 as target for scan. Use with caution.
[INFO] Targets loaded for current scan: 1
[INFO] Running httpx on input host
[INFO] Found 1 URL from httpx
[INFO] Templates clustered: 1716 (Reduced 1613 Requests)
[INFO] Using Interactsh Server: oast.me
[CVE-2024-47176] [javascript] [high] 192.168.1.136:631 ["CUPS/2.4.2 (Linux 6.11.0-21-generic; x86_64) IPP/2.0"]
```

Для этого я использую следующую команду:

```
nuclei -u 158.160.26.20:631 -t ./nuclei-templates
```

В результате обнаружена следующая уязвимость (продублировал информацию со скриншота выше):

[CVE-2024-47176] [javascript] [high] 192.168.1.136:631 ["CUPS/2.4.2 (Linux 6.11.0-21-generic; x86\_64)  
IPP/2.0"]

Запускаю nuclei для сервиса на порту 3000/tcp (Grafana http)

Для этого я использую следующую команду:

nuclei -u 158.160.26.20:3000 -t ./nuclei-templates

В результате выводится следующая информация и обнаружена следующая уязвимость (продублировал информацию со скриншота выше):

[cookies-without-secure] [javascript] [info] 158.160.26.20:3000 ["redirect\_to"]

[grafana-file-read] [http] [high] http://158.160.26.20:3000/public/plugins/canvas/../../../../../../../../conf/default.ini  
[pluginSlug="canvas"]

[CVE-2021-437981 [http] [high]]

Задускаю nucleus для сервиса на порту 4712/tcp (неопределенный сервис)

```
KaliLabs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[1 2 3 4] aushakov@kallilabs: ~
Файл Действия Правка Вид Справка
(aushakov@kallilabs) [~]
$ nuclei -u 158.160.26.20:4712 -t ./nuclei-templates
 _/ \
 / _v_/_/ _/_v_/_/ \
/ _/_/_/_/_/_/_/_/
 v3.4.1
projectdiscovery.io

[INF] Current nuclei version: v3.4.1 (Latest)
[INF] Current nuclei-templates version: v10.1.6 (Latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 78
[INF] Templates loaded for current scan: 7830
[INF] Executing 7641 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 189 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running https on input host
[INF] Found 0 URL from httpx
[INF] Templates clustered: 1716 (Reduced 1613 Requests)
[INF] Using Interactsh Server: oast.site
[INF] No results found. Better luck next time!
(aushakov@kallilabs) [~]
$
```

Для этого я использую следующую команду:

`nuclei -u 158.160.26.20:4712 -t ./nuclei-templates`

Для сервиса на данном порту уязвимостей не обнаружено

Запускаю nuclei для сервиса на порту 6123/tcp (Apache Spark)

```
KaliLabs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[1 2 3 4] aushakov@kallilabs: ~
Файл Действия Правка Вид Справка
(aushakov@kallilabs) [~]
$ nuclei -u 158.160.26.20:6123 -t ./nuclei-templates
 _/ \
 / _v_/_/ _/_v_/_/ \
/ _/_/_/_/_/_/_/_/
 v3.4.1
projectdiscovery.io

[INF] Current nuclei version: v3.4.1 (Latest)
[INF] Current nuclei-templates version: v10.1.6 (Latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 78
[INF] Templates loaded for current scan: 7830
[INF] Executing 7641 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 189 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running https on input host
[INF] Found 0 URL from httpx
[INF] Templates clustered: 1716 (Reduced 1613 Requests)
[INF] Using Interactsh Server: oast.site
[INF] No results found. Better luck next time!
(aushakov@kallilabs) [~]
$
```

20.23 ENG 02.04.2025 Right Ctrl

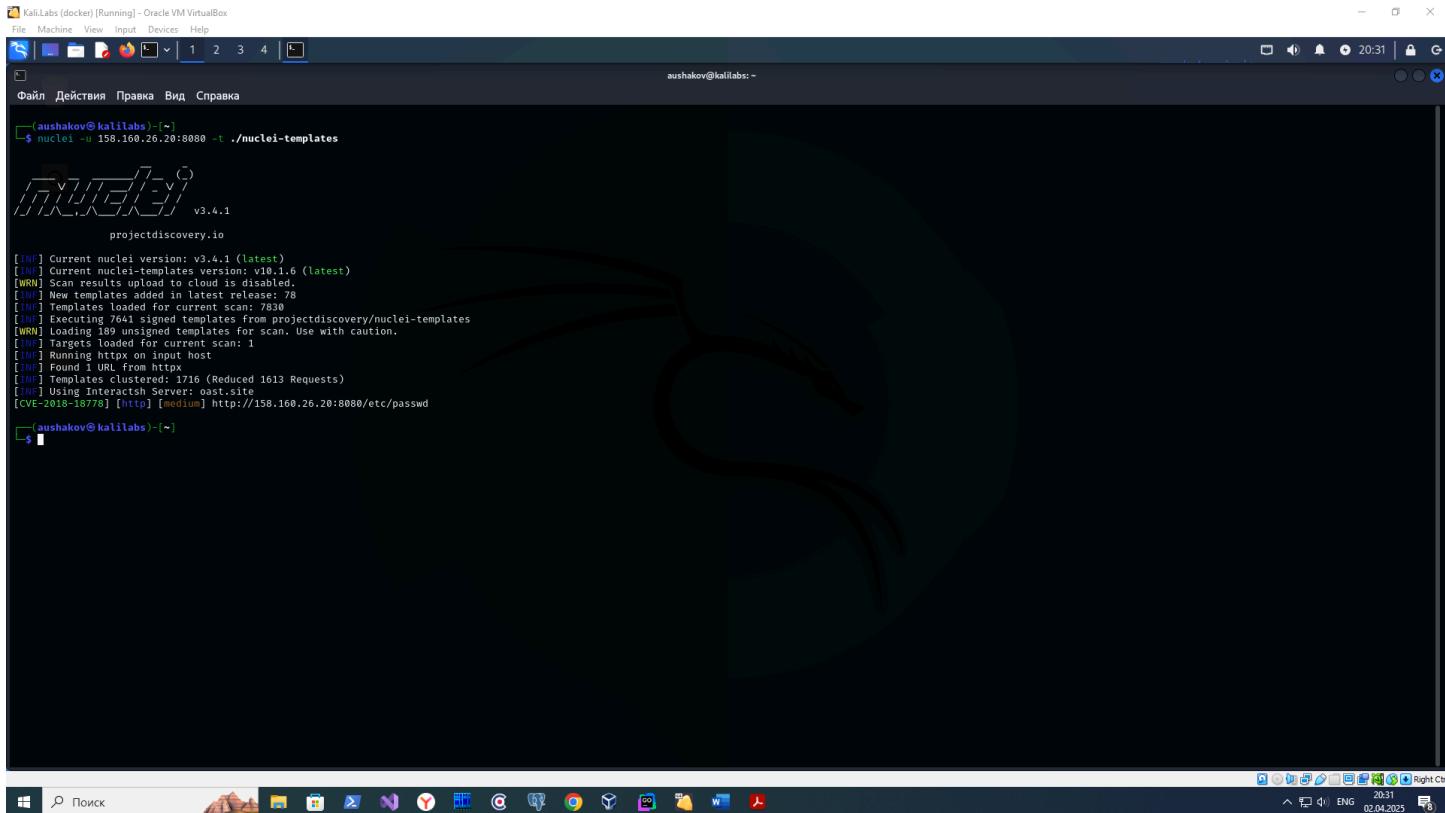
20.27 ENG 02.04.2025 Right Ctrl

Для этого я использую следующую команду:

nuclei -u 158.160.26.20:6123 -t ./nuclei-templates

Для сервиса на данном порту уязвимостей не обнаружено

Запускаю nuclei для сервиса на порту 8080/tcp (mini\_httpd 1.29)



```
KaliLabs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[File] [Machine] [View] [Input] [Devices] [Help]
1 2 3 4 []
aushakov@kalilabs: ~
(aushakov@kalilabs)~$ nuclei -u 158.160.26.20:8080 -t ./nuclei-templates
v3.4.1
projectdiscovery.io
[INFO] Current nuclei version: v3.4.1 (latest)
[INFO] Current nuclei-templates version: v10.1.6 (latest)
[WRN] Scan results upload to cloud is disabled.
[INFO] New templates added in latest release: 78
[INFO] Template loader for current scan: 7830
[INFO] Executing 764 signed templates from projectdiscovery/nuclei-templates
[WRN] Using unverified templates for scan. Use with caution.
[INFO] Targets loaded for current scan: 1
[INFO] Running httpx on input host
[INFO] Found 1 URL from httpx
[INFO] Templates clustered: 1716 (Reduced 1613 Requests)
[INFO] Using Intercept Server: oast.site
[CVE-2018-18778] [http] [medium] http://158.160.26.20:8080/etc/passwd
(aushakov@kalilabs)~$
```

Для этого я использую следующую команду:

nuclei -u 158.160.26.20:8080 -t ./nuclei-templates

В результате обнаружена следующая уязвимость (продублировал информацию со скриншота выше):

[CVE-2018-18778] [http] [medium] http://158.160.26.20:8080/etc/passwd

Запускаю nuclei для сервиса на порту 8081/tcp (icecap)

```
KaliLabs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[] 1 2 3 4 []
Файл Действия Правка Вид Справка
(aushakov@kalilabs) ~
$ nuclei -u 158.160.26.20:8081 -t ./nuclei-templates
[/ \] v3.4.1
projectdiscovery.io

[INFO] Current nuclei version: v3.4.1 (latest)
[INFO] Current nuclei-templates version: v10.1.6 (latest)
[WRN] Scan results upload to cloud is disabled.
[INFO] New templates added in latest release: 78
[INFO] Templates loaded for current scan: 7830
[INFO] Executing 7641 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 189 unsigned templates for scan. Use with caution.
[INFO] Targets loaded for current scan: 1
[INFO] Running httpx on input host
[INFO] Found 0 URL from httpx
[INFO] Templates clustered: 1716 (Reduced 1613 Requests)
[INFO] Using Interactsh Server: oast.pro
[INFO] No results found. Better luck next time!

(aushakov@kalilabs) ~
$
```

Для этого я использую следующую команду:

```
nuclei -u 158.160.26.20:8081 -t ./nuclei-templates
```

Для сервиса на данном порту уязвимостей не обнаружено

Запускаю nuclei для сервиса на порту 8088/tcp (Apache httpd 2.4.62)

```
KaliLabs (docker) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[] 1 2 3 4 []
Файл Действия Правка Вид Справка
(aushakov@kalilabs) ~
$ nuclei -u 158.160.26.20:8088 -t ./nuclei-templates
[/ \] v3.4.1
projectdiscovery.io

[INFO] Current nuclei version: v3.4.1 (latest)
[INFO] Current nuclei-templates version: v10.1.6 (latest)
[WRN] Scan results upload to cloud is disabled.
[INFO] New templates added in latest release: 78
[INFO] Templates loaded for current scan: 7830
[INFO] Loading 189 unsigned templates for scan. Use with caution.
[INFO] Executing 7641 signed templates from projectdiscovery/nuclei-templates
[INFO] Targets loaded for current scan: 1
[INFO] Running httpx on input host
[INFO] Found 0 URL from httpx
[INFO] Templates clustered: 1716 (Reduced 1613 Requests)
[INFO] Using Interactsh Server: oast.online
[INFO] No results found. Better luck next time!

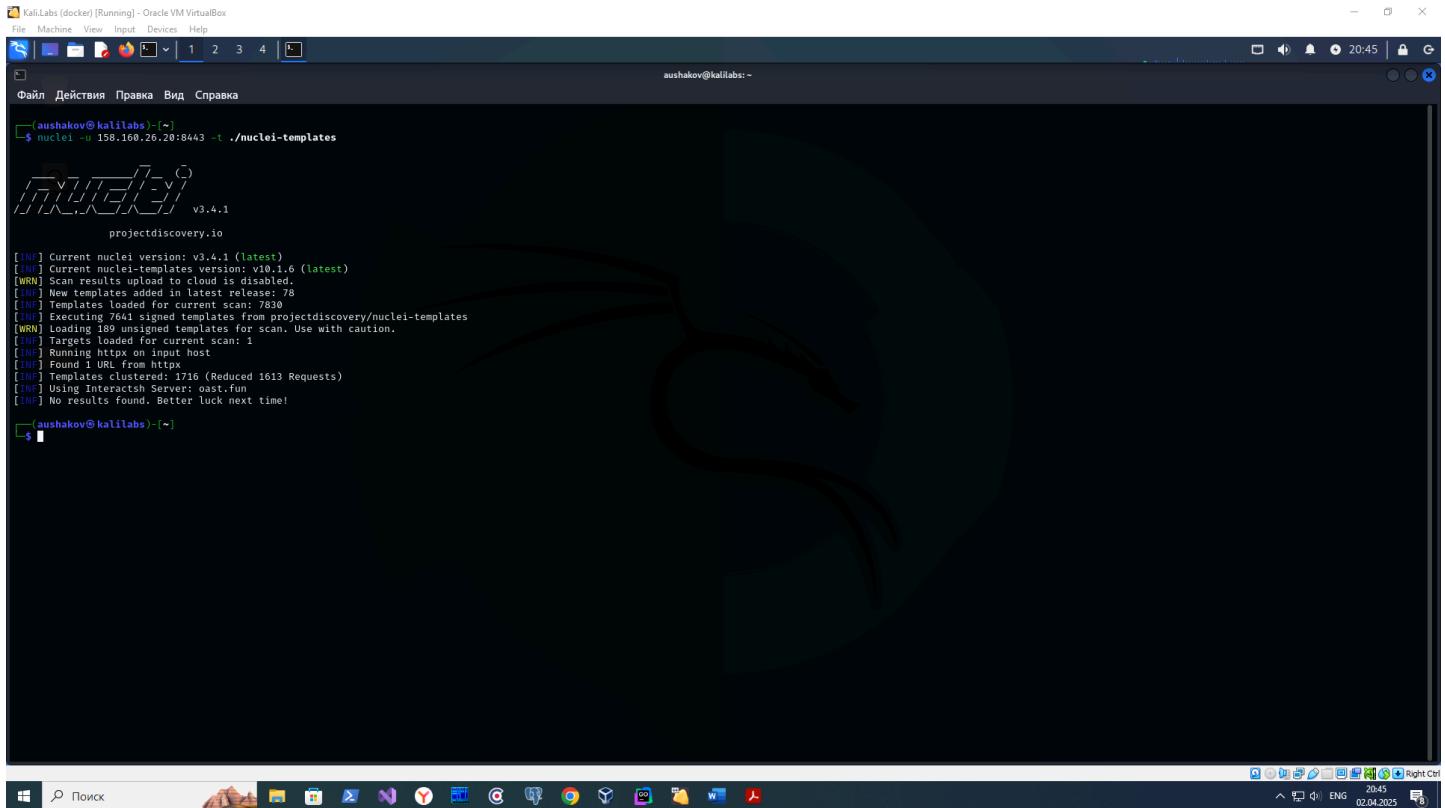
(aushakov@kalilabs) ~
$
```

Для этого я использую следующую команду:

```
nuclei -u 158.160.26.20:8088 -t ./nuclei-templates
```

Для сервиса на данном порту уязвимостей не обнаружено

Запускаю nuclei для сервиса на порту 8443/tcp (nginx 1.11.13)



```
(aushakov㉿kalilabs) -[~]
$ nuclei -u 158.160.26.20:8443 -t ./nuclei-templates
v3.4.1
projectdiscovery.io

[INFO] Current nuclei version: v3.4.1 (latest)
[INFO] Current nuclei-templates version: v10.1.6 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 78
[INF] Templates loaded for current scan: 7830
[INF] Executing 141 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 189 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Template clustered: 1716 (Reduced 1613 Requests)
[INF] Using Interactsh Server: post.fuN
[INF] No results found. Better luck next time!

(aushakov㉿kalilabs) -[~]
$
```

command

```
nuclei -u 158.160.26.20:8443 -t ./nuclei-templates
```

Для сервиса на данном порту уязвимостей не обнаружено

Запускаю nuclei для сервиса на порту 8888/tcp (Jetty)

```
(aushakov㉿kaliLabs) -~$ nuclei -u 158.160.26.20:8888 -t ./nuclei-templates
v3.4.1
projectdiscovery.io

[INFO] Current nuclei version: v3.4.1 (latest)
[INFO] Current nuclei-templates version: v10.1.6 (latest)
[WRN] Scan results upload to cloud is disabled.
[INFO] New templates added in latest release: 7830
[INFO] Templates loaded for current scan: 7830
[INFO] Executing 7641 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 189 unsigned templates for scan. Use with caution.
[INFO] Targets loaded for current scan: 1
[INFO] Running on http://158.160.26.20:8888
[INFO] Found 1 URLS from http://
[INFO] Templates clustered: 171 (Reduced 1613 Requests)
[INFO] Using Interceptor Server: oast.fun
[http-missing-security-headers:strict-transport-security] [http] [info] http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:x-content-type-options] [http] [info] http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:clear-site-data] [http] [info] http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:content-security-policy] [http] [info] http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:permissions-policy] [http] [info] http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:x-frame-options] [http] [info] http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:referrer-policy] [http] [info] http://158.160.26.20:8888/unified-console.html
[apache-druid-unauth] [http] [low] http://158.160.26.20:8888/unified-console.html
[fingerprinthub-web-fingerprints:apache-druid] [http] [info] http://158.160.26.20:8888/unified-console.html
```

Для этого я использую следующую команду:

```
nuclei -u 158.160.26.20:8888 -t ./nuclei-templates
```

В результате выводится следующая информация (продублировал информацию со скриншота выше):

```
[http-missing-security-headers:strict-transport-security] [http] [info]
http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:x-content-type-options] [http] [info]
http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:clear-site-data] [http] [info] http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info]
http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:cross-origin-opener-policy] [http] [info]
http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:cross-origin-resource-policy] [http] [info]
http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:content-security-policy] [http] [info]
http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:permissions-policy] [http] [info]
http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:x-frame-options] [http] [info]
http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info]
http://158.160.26.20:8888/unified-console.html
[http-missing-security-headers:referrer-policy] [http] [info] http://158.160.26.20:8888/unified-console.html
[apache-druid-unauth] [http] [low] http://158.160.26.20:8888/unified-console.html
[fingerprinthub-web-fingerprints:apache-druid] [http] [info] http://158.160.26.20:8888/unified-console.html
```

Давайте рассмотрим возможные уязвимости исходя из информации о версии установленных сервисов (только для тех сервисов, для которых поиск информации об их версии вернул какой-либо результат с помощью `ptar` - в противном случае мы получим слишком много разных CVE для всех возможных версий сервисов); при этом стоит упомянуть, что скорее всего этот список не полон.

#### 1. OpenSSH 9.7p1:

Уязвимость CVE-2006-5051: На сервере OpenSSH (`sshd`) от версии 8.5p1 до версии 9.7p1 существует состояние гонки обработчиков сигналов в OpenSSH, которое позволяет удаленным злоумышленникам вызывать отказ в обслуживании (сбой) и, возможно, выполнять произвольный код, если включена аутентификация GSSAPI, через неуказанные векторы атаки, которые приводят к двойному освобождению памяти.

#### 2. CUPS 2.4

Уязвимость CVE-2024-47176: связана с CUPS (Common Unix Printing System), который используется для управления принтерами в Unix-подобных системах. Эта уязвимость (но только совместно с другими уязвимостями, такими, как CVE-2024-47076, CVE-2024-47175, and CVE-2024-47177) позволяет злоумышленникам выполнять произвольный код на сервере, используя уязвимости в обработке запросов к серверу печати.

Уязвимость CVE-2023-4504: Из-за сбоя проверки длины, предоставленной созданным злоумышленником документом PPD PostScript, CUPS и `libppd` подвержены переполнению буфера кучи и возможному выполнению кода.

Уязвимость CVE-2023-32324: В версиях 2.4.2 и более ранних уязвимость переполнения буфера кучи позволяет удаленному злоумышленнику запустить атаку типа «отказ в обслуживании» (DoS). Уязвимость переполнения буфера в функции `'format_log_line'` может позволить удаленным злоумышленникам вызвать DoS в уязвимой системе. Эксплуатация уязвимости может быть вызвана, когда файл конфигурации `'cupsd.conf'` устанавливает значение `'loglevel'` на `'DEBUG'`.

#### 3. mini\_httpd 1.29

Уязвимость CVE-2018-18778: Реализация ACME (протокол автоматизированной среды управления сертификатами) `mini_httpd` до версии 1.30 позволяет удаленным пользователям читать произвольные файлы.

#### 4. Apache httpd 2.4.62

Уязвимость CVE-2025-31492: `mod_auth_openidc` — это сертифицированный OpenID модуль аутентификации и авторизации для HTTP-сервера Apache 2.x, реализующий функциональность OpenID Connect Relying Party. До версии 2.4.16.11 ошибка в `mod_auth_openidc` приводила к раскрытию защищенного контента неавтентифицированным пользователям. Условиями раскрытия являются POST-запрос `OIDCProviderAuthRequestMethod`, действительная учетная запись и отсутствие шлюза уровня приложения (или балансировщика нагрузки и т. д.), защищающего сервер. Когда вы запрашиваете защищенный ресурс, ответ включает в себя статус HTTP, заголовки HTTP, предполагаемый ответ (самостоятельно отправляемая форма) и защищенный

ресурс (без заголовков). Это пример запроса защищенного ресурса, включая все возвращаемые данные. В случае, когда mod\_auth\_openidc возвращает форму, он должен вернуть OK из check\_userid, чтобы не перейти по пути ошибки в httpd. Это означает, что httpd попытается выдать защищенный ресурс. oidc\_content\_handler вызывается рано, что дает возможность предотвратить нормальный вывод, выдаваемый httpd. У oidc\_content\_handler есть ряд проверок, когда он вмешивается, но он не проверяет этот случай, поэтому обработчик возвращает DECLINED. Следовательно, httpd добавляет защищенное содержимое к ответу.

## 5. nginx 1.11.13

Уязвимость CVE-2017-7529: Версии Nginx с 0.5.6 по 1.13.2 включительно уязвимы к целочисленному переполнению в модуле фильтра диапазона nginx, что приводит к утечке потенциально конфиденциальной информации, вызванной специально созданным запросом.

Уязвимость CVE-2017-20005: В NGINX до версии 1.13.6 происходит переполнение буфера для годов, превышающих четыре цифры, как показано на примере файла с датой изменения в 1969 году, который вызывает целочисленное переполнение (или ложную дату изменения в далеком будущем) при обнаружении его модулем автоиндексации.

Попробую проверить наличие этих конкретных уязвимостей с помощью nuclei (или с помощью других утилит, для которых смогу что-либо найти, т.к. с нуля написать самому - это достаточно сложно):

### CVE-2006-5051:

Scanning for open SSH connections (regardless of port) reporting hostname, openssh versions and vulnerabilities

Background

On July 1, 2024, a new OpenSSH unauthenticated remote code execution (RCE) vulnerability dubbed regresSHion was reported, affecting glibc-based Linux systems. This vulnerability, identified as CVE-2024-6387, allows remote attackers to execute arbitrary code as root due to a signal handler race condition in sshd.

This vulnerability, if exploited, could lead to full system compromise, where an attacker can execute arbitrary code with the highest privileges, resulting in a complete system takeover, installation of malware, data manipulation, and the creation of backdoors for persistent access. It could facilitate network propagation, allowing attackers to use a compromised system as a foothold to traverse and exploit other vulnerable systems within the organization.

Versions Affected

Languages

Python 100.0%

```
(aushakov㉿kalilabs) [~/custom]
$ git clone https://github.com/David-M-Berry/openssh-cve-discovery.git
Клонирование в «openssh-cve-discovery»...
remote: Enumerating objects: 29, done.
remote: Counting files: 100% (29/29), done.
remote: Compressing objects: 100% (26/26), done.
remote: Total 26 (delta 11), reused 0 (delta 0), pack-reused 0 (from .)
Получение объектов: 100% (26/26), 23.64 Кб | 361.00 Кб/с, готово.
Определение изменений: 100% (13/13), готово.
```

```
(aushakov㉿kalilabs) [~/custom]
$ sudo ./my-venv/bin/python3 ./openssh-cve-discovery/openssh-cve-discovery.py --cidr 158.160.26.20/32
Scanning started at: 2025-04-08 23:59:07.709401
Total Hosts to scan: 1
Host: 158.160.26.20, Port: 22, OpenSSH Version: OpenSSH 9.6p1 Ubuntu 3ubuntu13.8, Vulnerability: Vulnerable to regressHion
Scanning completed at: 2025-04-08 23:59:22.474697
Duration: 0:00:14.765296
```

Для поиска этой уязвимости был найден отдельный питон скрипт на github в репозитории David-M-Berry/openssh-cve-discovery. Из результатов сканирования видно, что уязвимость была найдена.

CVE-2023-4504:

**CVE-2023-47504-POC**

Exploit for CVE-2023-47504. According to NIST, this vulnerability should allow unauthenticated users to access functionalities in the Elementor Website Builder Plugin. Based on my research into the vulnerability, and also judging by the URL from Patchstack that describes the vulnerability: [https://patchstack.com/database/vulnerability/elementor/wordpress-elementor-plugin-3-16-4-contributor-arbitrary-attachment-read-vulnerability?\\_s\\_id=cve](https://patchstack.com/database/vulnerability/elementor/wordpress-elementor-plugin-3-16-4-contributor-arbitrary-attachment-read-vulnerability?_s_id=cve), I recon this is actually requires credentials for at least a subscriber account. Also, for the exploit to work one needs access to the `wp-config.php` file of the target website.

**Requirements**

1. Credentials for at least a subscriber account
2. Access to `wp-config.php`
3. Authorization to exploit the website ;)

**Usage**

1. Proxy your traffic to burp, or use the browser's developers tool to intercept requests;

На github в репозитории `davidxbors/CVE-2023-47504-POC` есть РОС для эксплуатации этой уязвимости. При желании, конечно, можно воспользоваться и им для проверки наличия уязвимости, но кажется, что это будет не совсем корректно и безопасно.

## CVE-2023-32324:

**CVE-2023-32315**

Tool for CVE-2023-32315 exploitation

**Features:**

- Scans single or bulk targets from txt files
- Utilizes multiprocessing for faster scanning
- Automatic login capability

**Installation:**

- Make sure you're in this repo's directory and have python3 installed
- Install required packages using:

```
pip install -r requirements.txt
```

На github в репозитории `gibran-abdillah/CVE-2023-32315` есть утилита для эксплуатации этой уязвимости. При желании, конечно, можно воспользоваться и им для проверки наличия уязвимости, но кажется, что это будет не совсем корректно и безопасно.

## CVE-2017-7529:

The screenshot shows a Windows desktop environment. At the top, there is a taskbar with various icons. In the center, a Microsoft Edge browser window is open, displaying the file `CVE-2017-7529.yaml` from the `ping-0day/templates` repository on GitHub. The code content is as follows:

```
1 id: CVE-2017-7529
2
3 info:
4 name: Nginx Remote Integer Overflow
5 author: medbsq
6 severity: medium
7
8 # https://www.cvebase.com/cve/2017/7529
9 requests:
10 - method: GET
11 path:
12 - "{{{BaseUrl}}}/"
13 headers:
14 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3984.0 Safari/537.36
15 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
16 Range: bytes=17206,-922337203685475892
17 matchers-condition: and
18 matchers:
19 - type: word
20 words:
21 - "Server: nginx"
22 - "Content-Range"
23 condition: and
24 part: header
25 - type: status
26 status:
27 - 206
```

Below the browser, a terminal window is open in a KaliLabs Docker container. The terminal prompt is `aushakov@kalilabs:~/custom`. The user has run the command `git clone https://github.com/ping-0day/templates.git`, which is cloning the repository into the `~/custom` directory. The output of the command shows the progress of cloning the repository, including object enumeration, counting, compressing, and finalizing the clone.

```
[aushakov@kalilabs:~/custom]$ git clone https://github.com/ping-0day/templates.git
Клонирование в «templates»...
remote: Enumerating objects: 4596, done.
remote: Counting objects: 100% (4596/4596), done.
remote: Compressing objects: 100% (3062/3062), done.
remote: Total 4596 (delta 1513), reused 4596 (delta 1513), pack-reused 0 (from 0)
Получение объектов: 100% (4596/4596), 1.67 Мб | 3.62 Мб/с, готово.
Определение изменений: 100% (1513/1513), готово.
```

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal title is '(aushakov㉿kali: ~/custom)'. The command entered is 'nuclei -v -u 158.160.26.20:8443 -t ./templates/CVE-2017-7529.yaml'. The output of the command is displayed below:

```
[VER] Started metrics server at localhost:9092
[WRN] Found 1 templates loaded with deprecated protocol syntax, update before v3 for continued support.
[INF] Current template version: v3.0.1.6 (latest)
[INF] Current nuclei-templates version: v3.0.1.6 (latest)
[WRN] Scan results upload to Cloud is disabled.
[INF] New templates added in latest release: 78
[INF] Templates loaded for current scan: 1
[WRN] Loading 1 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on default host
[INF] Found 1 targets from httpx
[VER] CVE-2017-7529| Sent HTTP request to https://158.160.26.20:8443
[INF] No results found. Better luck next time!
```

На github в репозитории ping-0day/templates есть шаблон для nuclei для нахождения этой уязвимости. Однако при его использовании этого шаблона, найти эту уязвимость не удалось.

**CVE-2017-7529** Public

main 1 Branch 0 Tags

Go to file Add file Code

**Shehzadcyber** Update [CVE-2017-7529.py](#) 380419f · 3 years ago 7 Commits

[CVE-2017-7529.py](#) Update [CVE-2017-7529.py](#) 3 years ago

[README.md](#) Update [README.md](#) 3 years ago

**README**

## CVE-2017-7529

Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.

### Installation

```
$ git clone https://github.com/Shehzadcyber/CVE-2017-7529.git
$ cd CVE-2017-7529
```

### Usage

```
$ python3 CVE-2017-7529.py URL
$ python3 CVE-2017-7529.py https://target.com/
```

**About**

Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.

Readme Activity 7 stars 1 watching 0 forks Report repository

**Releases**

No releases published

**Packages**

No packages published

**Languages**

Python 100.0%

На github в репозитории Shehzadcyber/CVE-2017-7529 есть утилита для эксплуатации этой уязвимости. При желании, конечно, можно воспользоваться и им для проверки наличия уязвимости, но кажется, что это будет не совсем корректно и безопасно.

Найденные уязвимости с помощью nmap и nuclei:

1. Сервис на порту 22/tcp (OpenSSH 9.7p1) - CVE-2006-5051.

Уязвимость CVE-2006-5051: На сервере OpenSSH (sshd) от версии 8.5p1 до версии 9.7p1 существует состояние гонки обработчиков сигналов в OpenSSH, которое позволяет удаленным злоумышленникам вызывать отказ в обслуживании (сбой) и, возможно, выполнять произвольный код, если включена аутентификация GSSAPI, через неуказанные векторы атаки, которые приводят к двойному освобождению памяти.

Метрика:

- Вектор CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
- Оценка 8.1 HIGH

Краткое описание уязвимости:

- Тип уязвимости: Удаленное выполнение кода.
- Компонент: OpenSSH (sshd) от версии 8.5p1 до версии 9.7p1.
- Проблема: из-за наличия состояния гонки обработчиков сигналов в OpenSSH, удаленный злоумышленник может вызвать отказ в обслуживании (сбой) и, возможно, выполнить произвольный код.
- Последствия: Это может позволить злоумышленнику получить доступ к системе, модифицировать или удалять файлы, а также выполнять другие вредоносные действия.

2. Сервис на порту 631/tcp (CUPS 2.4 сервис) - CVE-2024-47176.

Уязвимость CVE-2024-47176 связана с CUPS (Common Unix Printing System), который используется для управления принтерами в Unix-подобных системах. Эта уязвимость (но только совместно с другими уязвимостями, такими, как CVE-2024-47076, CVE-2024-47175, and CVE-2024-47177) позволяет злоумышленникам выполнять произвольный код на сервере, используя уязвимости в обработке запросов к серверу печати.

Метрика:

- Вектор CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
- Оценка 5.3 MEDIUM

Краткое описание уязвимости:

- Тип уязвимости: Удаленное выполнение кода.
- Компонент: CUPS (версия, подверженная уязвимости).
- Проблема: Злоумышленник может отправить специально сформированный запрос к серверу CUPS, что может привести к выполнению произвольного кода с правами пользователя, под которым работает CUPS.
- Последствия: Это может позволить злоумышленнику получить доступ к системе, модифицировать или удалять файлы, а также выполнять другие вредоносные действия.

3. Сервис на порту 631/tcp (CUPS 2.4 сервис) - CVE-2007-6750.

Уязвимость CVE-2007-6750 связана с серверами Apache HTTP Server 1.x и 2.x, в которых злоумышленник может вызвать DoS (отказ в работе демона) с помощью HTTP-запросов, разбитых на части.

Метрика:

- Вектор CVSS 2.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
- Оценка 5.0 MEDIUM

Краткое описание уязвимости:

- Тип уязвимости: DoS.
- Компонент: сервер Apache HTTP Server 1.x или 2.x
- Проблема: Злоумышленник может вызвать DoS (отказ в работе демона) с помощью HTTP-запросов, разбитых на части.
- Последствия: недоступность сервиса

#### 4. Сервис на порту 3000/tcp (Grafana http) - CVE-2021-43798

Уязвимость CVE-2021-43798 связана с Grafana с версии 8.0.0-beta1 по 8.3.0 (за исключением исправленных версий); существует возможность обхода каталогов, что позволяет получить доступ к локальным файлам. Уязвимый URL имеет следующий вид: "<grafana\_host\_url>/public/plugins/pluginID/", где pluginID - идентификатор плагина для любого установленного плагина.

Метрика:

- Вектор CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
- Оценка 7.5 HIGH

Краткое описание уязвимости:

- Тип уязвимости: Удаленный доступ к локальной файловой системе.
- Компонент: Grafana с версии 8.0.0-beta1 по 8.3.0
- Проблема: Злоумышленник может обойти каталоги локальной файловой системы с помощью уязвимого URL, который имеет следующий вид: "<grafana\_host\_url>/public/plugins/pluginID/", где pluginID - идентификатор плагина для любого установленного плагина.
- Последствия: нарушение конфиденциальности.

#### 5. Сервис на порту 8080/tcp (mini\_httpd 1.29 23May2018) - CVE-2018-18778

Уязвимость CVE-2018-18778: Реализация ACME (протокол автоматизированной среды управления сертификатами) mini\_httpd до версии 1.30 позволяет удаленным пользователям читать произвольные файлы.

Метрика:

- Вектор CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
- Оценка 6.5 MEDIUM

Краткое описание уязвимости:

- Тип уязвимости: Удаленный доступ к локальной файловой системе.
- Компонент: mini\_httpd до версии 1.30

- Проблема: Злоумышленник может читать произвольные файлы, расположенные в локальной файловой системе.
- Последствия: нарушение конфиденциальности.

## 6. Сервис на порту 8080/tcp (mini\_httpd 1.29 23May2018) - CVE-2007-6750

Уязвимость CVE-2007-6750 связана с серверами Apache HTTP Server 1.x и 2.x, в которых злоумышленник может вызвать DoS (отказ в работе демона) с помощью HTTP-запросов, разбитых на части.

Метрика:

- Вектор CVSS 2.0 (AV:N/AC:L/Au:N/C:N/I:N/A:P)
- Оценка 5.0 MEDIUM

Краткое описание уязвимости:

- Тип уязвимости: DoS.
- Компонент: сервер Apache HTTP Server 1.x или 2.x
- Проблема: Злоумышленник может вызвать DoS (отказ в работе демона) с помощью HTTP-запросов, разбитых на части.
- Последствия: недоступность сервиса

## 7. Сервис на порту 8443/tcp (nginx 1.11.13) - CVE-2007-6750

Уязвимость CVE-2007-6750: OpenSSL до версии 0.9.8za, 1.0.0 до версии 1.0.0m и 1.0.1 до версии 1.0.1h не ограничивает обработку сообщений ChangeCipherSpec должным образом, что позволяет злоумышленникам, использующим метод “man-in-the-middle”, инициировать использование мастер ключа нулевой длины в определенных OpenSSL-OpenSSL соединениях и, следовательно, перехватывать сеансы или получать конфиденциальную информацию с помощью специально созданного рукопожатия TLS, также известного как уязвимость “CCS Injection”.

Метрика:

- Вектор CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
- Оценка 7.4 HIGH

Краткое описание уязвимости:

- Тип уязвимости: “CCS Injection” в OpenSSL-OpenSSL соединениях.
- Компонент: OpenSSL до версии 0.9.8za, 1.0.0 до версии 1.0.0m и 1.0.1 до версии 1.0.1h
- Проблема: Злоумышленник может перехватывать сеансы OpenSSL или получать конфиденциальную информацию с помощью специально созданного рукопожатия TLS.
- Последствия: нарушение конфиденциальности и целостности при передаче информации.

## 8. Сервис на порту 8443/tcp (nginx 1.11.13) - CVE-2014-0160

Уязвимость CVE-2014-0160: Реализации TLS и DTLS в OpenSSL 1.0.1 до версии 1.0.1g некорректно обрабатывают пакеты Heartbeat Extension, что позволяет удаленным злоумышленникам получать конфиденциальную информацию из памяти процесса с помощью специально созданных пакетов, которые вызывают повторное чтение буфера.

Метрика:

- Вектор CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
- Оценка 7.5 HIGH

Краткое описание уязвимости:

- Тип уязвимости: получение конфиденциальной информации из памяти процесса.
- Компонент: OpenSSL 1.0.1 до версии 1.0.1g
- Проблема: Удаленный злоумышленник может получить конфиденциальную информацию из памяти процесса с помощью специально созданных пакетов Heartbeat Extension.
- Последствия: нарушение конфиденциальности информации.

## 9. Сервис на порту 8888/tcp (Jetty)

nuclei показывает, что для данного сервиса сработал шаблон с идентификатором apache-druid-unauth и низким уровнем критичности. По этому идентификатору легко ищется сам шаблон, однако какой-то вменяемой информации найти не удалось. Но поскольку у данной потенциальной уязвимости нет CVE, то можно предположить, что ее критичность достаточно низкая.