www.uoc.edu

SEGURIDAD EN SISTEMAS OPERATIVOS

Curso Febrero 2020 – Junio 2020

Práctica Final

EXPLOTACIÓN DE SISTEMAS Y HACKING ÉTICO

- Objetivos
- Presentación
- Ejercicios

Objetivos

Los objetivos de esta PEC son:

- Familiarizarse con el entorno de Metasploitable.
- Llevar a cabo la explotación de un sistema Linux y Windows.
- Entender técnicas utilizadas en auditorías internas.
- Manejar la herramienta de auditoría técnica Metasploit.

Presentación

La práctica final de la asignatura presenta tres hitos diferenciados. En los hitos el alumno estudiará formas de vulnerar un sistema operativo, ya sea directamente o a través de una aplicación o servicio de terceros. Previo a la realización de los ejercicios debemos familiarizarnos con el entorno, por lo que se recomienda que se lea información sobre Metasploit.

Familiarizaros con Metasploitable

Hay que descargar la ISO de Metasploitable y utilizar mediante VirtualBox o VMWare. El uso de Metasploitable es sencillo, ya que no hace falta instalarla, solamente con arrancar la máquina virtual con la ISO es suficiente. Metasploitable es un entorno o máquina virtual preparada con diversas vulnerabilidades.

La ISO de Metasploitable la podéis descargar desde la siguiente dirección URL: https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Tenéis más información sobre los requisitos de la máquina y de dónde descargarla en la siguiente dirección URL: https://www.offensive-security.com/metasploit-unleashed/requirements/

Familiarizaros con Metasploit

Para familiarizarse con la herramienta Metasploit os recomendamos que descarguéis el manual sobre la herramienta y lo leáis.

Hitos

La práctica final consta de tres partes:

- El primer hito es conseguir explotar una vulnerabilidad de la máquina Metasploitable. En este hito tenéis que utilizar alguna herramienta que os permita realizar fingerprinting sobre la máquina Metasploitable. En el apartado de ejercicios se detallará más sobre el proceso a realizar en este primer hito.
- El segundo hito consiste en explotar una vulnerabilidad de la herramienta Easy File Management Web Server 5.3 sobre un sistema Windows 7. En el apartado de ejercicios se detallará más sobre el proceso a realizar en este segundo hito.

- El tercer hito consiste en utilizar la técnica Pass the Hash (PtH) en entornos Windows con el objetivo de poder desplazarse lateralmente entre máquinas Windows.

Ejercicios

1. Montar laboratorio práctica final

Vamos a montar un laboratorio para esta práctica final. Para ello debéis descargaros diferentes máquinas:

- Metasploitable. Esta máquina no hay que instalarla, solamente utilizar la ISO con Virtual Box. Se puede descargar desde esta dirección URL: https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
- Windows 7. Se debe obtener una máquina Windows 7, la cual podéis descargar desde DreamSpark o, ya instalada en formato VHD, desde el sitio web Modern IE: https://dev.windows.com/en-us/microsoft-edge/tools/vms/windows/ (Utilizar dos máquinas Windows 7).
- Metasploit Framework. Metasploit está disponible para diferentes entornos (Linux, Windows y OS X). Podéis instalarlo en vuestra máquina Debian. También podéis utilizar una distribución Kali Linux, dónde ya viene instalada: https://www.kali.org/downloads/

2. Explotando vulnerabilidades en Metasploitable

En este hito debéis crear la máquina para Metasploitable y arrancar desde el CD/DVD con la ISO. Es recomendable configurar la red de la máquina Metasploitable de forma que tengáis conectividad con vuestras otras máquinas y con la máquina anfitriona (máquina física).

En esta actividad deberéis responder en la memoria de trabajo a las siguientes preguntas y mostrar el proceso completo que habéis llevado a cabo para obtener las respuestas. La captura de imágenes es algo importante, ya que demostráis cómo habéis ido haciendo el proceso.

a) Fingerprinting sobre la máquina Metasploitable. Utilizar alguna herramienta para llevar a cabo un fingerprinting sobre la máquina Metasploitable. Recopilar todos los puertos y versiones posibles. Se recomienda utilizar herramientas como Nmap y módulos de Metasploit como auxiliary/scanner/portscan/tcp o auxiliary/scanner/ftp/ftp_version y similares. (1 punto)

b) Fijaros en el puerto 21 de la máquina Metasploitable. ¿Qué servicio está corriendo? ¿Qué versión es? ¿Existe alguna vulnerabilidad conocida? (1 Punto)

c) Conseguir ejecutar un payload sobre la máquina Metasploitable a través del puerto 21. ¿Existe un módulo de Metasploit que se aproveche de alguna vulnerabilidad del software que se ejecuta en el puerto 21? Demostrar con imágenes vuestro proceso. Tenéis que conseguir ejecutar código que os devuelva el control sobre la máquina Metasploitable. (1 Punto)

3. Explotación de sistemas Windows

En este segundo hito hay que crear una máquina Windows 10 (https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/) en el entorno virtual. Hay que instalar la siguiente aplicación de terceros denominada FTP Utility (Es importante la versión): https://www.exploit-db.com/exploits/39215.

Esta aplicación es un servidor FTP el cual contiene una vulnerabilidad explotable en sistemas Windows 7/10. Debéis contestar a las siguientes preguntas:

a) Realizar fingerprinting sobre la máquina Windows 10, una vez la herramienta FTP Utility se encuentre en ejecución. ¿Qué versión devuelve vuestro fingerprint sobre FTP Utility? (1 Punto)

b) Detallar el proceso de búsqueda de un módulo de Metasploit que explote la vulnerabilidad. Detallar con imágenes el proceso y demostrar que conseguís acceso a la máquina Windows 10 con la configuración del siguiente payload windows/meterpreter/reverse_tcp. (1,5 Puntos)

c) ¿Qué diferencia hay entre una conexión de tipo reverse y de tipo bind en un payload? Realiza una explotación dónde se vea y configure un Meterpreter de tipo reverse y otro de tipo bind. (1 Punto)

4. Bypass UAC & AMSI en Windows 10

En este apartado hay que trabajar dos conceptos. El bypass de UAC y el bypass de AMSI.

En el primer caso trabajaremos el concepto de bypass UAC. Se debe investigar:

a) ¿Qué es un bypass de UAC? ¿Qué permite? (0,5 puntos)

Ahora, vamos a trabajar el concepto de manera práctica en Windows 10. Existe una técnica llamada Bypass UAC Environment Injection. Se logra realizar un bypass de UAC sin necesidad de subir un fichero EXE o DLL a disco. Todo consiste en la manipulación de hives de registro.

La idea es sencilla: las variables de entorno que el usuario tiene en su sesión son almacenadas en HKLM y HKCU (dependiendo de si son variables de entorno globales o locales de cada usuario). Hay una tarea programada en Windows 10, las cuales se ejecutan en nivel de integridad alto en Windows, es decir, con privilegio. Aquí tenemos una imagen de ello.

```
PS C:\Users\IEUser> Get-ScheduledTask silentcleanup

TaskPath                                    TaskName                    State
--------                                    --------                    -----
\Microsoft\Windows\DiskCleanup\             SilentCleanup               Ready


PS C:\Users\IEUser> $tarea = Get-ScheduledTask silentcleanup
PS C:\Users\IEUser> $tarea | Get-Member


   TypeName: Microsoft.Management.Infrastructure.CimInstance#Root/Microsoft/Windows/TaskScheduler/MSFT_ScheduledTask

Name                      MemberType     Definition
----                      ----------     ----------
Clone                     Method         System.Object ICloneable.Clone()
Dispose                   Method         void Dispose(), void IDisposable.Dispose()
Equals                    Method         bool Equals(System.Object obj)
GetCimSessionComputerName Method         string GetCimSessionComputerName()
GetCimSessionInstanceId   Method         guid GetCimSessionInstanceId()
GetHashCode               Method         int GetHashCode()
GetObjectData             Method         void GetObjectData(System.Runtime.Serialization.SerializationInfo info, Sys...
GetType                   Method         type GetType()
ToString                  Method         string ToString()
Actions                   Property       CimInstance#InstanceArray Actions {get;set;}
Author                    Property       string Author {get;set;}
Date                      Property       string Date {get;set;}
Description               Property       string Description {get;set;}
Documentation             Property       string Documentation {get;set;}
Principal                 Property       CimInstance#Instance Principal {get;set;}
PSComputerName            Property       string PSComputerName {get;}
SecurityDescriptor        Property       string SecurityDescriptor {get;set;}
Settings                  Property       CimInstance#Instance Settings {get;set;}
Source                    Property       string Source {get;set;}
TaskName                  Property       string TaskName {get;}
TaskPath                  Property       string TaskPath {get;}
Triggers                  Property       CimInstance#InstanceArray Triggers {get;set;}
URI                       Property       string URI {get;}
Version                   Property       string Version {get;set;}
State                     ScriptProperty System.Object State {get=[Microsoft.PowerShell.Cmdletization.GeneratedTypes...


PS C:\Users\IEUser> $tarea.Principal


DisplayName         :
GroupId             : Users
Id                  : Authenticated Users
LogonType           : Group
RunLevel            : Highest
UserId              :
ProcessTokenSidType : Default
RequiredPrivilege   :
PSComputerName      :
```

Como se puede ver en la siguiente imagen, la variable de entorno precede al resto de la instrucción, por lo que se puede inyectar ahí la instrucción que queramos. En el momento que invoquemos a la tarea programada se ejecutará la instrucción que a nosotros nos interese, es decir, la que albergue la variable de entorno que depende de la rama HKCU.

```
PS C:\Users\IEUser> $tarea.Actions


Id               :
Arguments        : /autoclean /d %systemdrive%
Execute          : %windir%\system32\cleanmgr.exe
WorkingDirectory :
PSComputerName   :
```

Tened en cuenta que las variables de entorno de usuario se almacenan en HKCU:\Environment. Por lo que si creáis la variable de entorno "windir" en esa ruta del registro podréis ejecutar lo que queráis y con privileigio. Ahí está el secreto del bypass de UAC.

b) Detallar el proceso para conseguir el bypass de UAC en Windows 10 utilizando la técnica. Explicad el paso a paso. Se valorará positivamente el paso a paso y los enlaces de referencia de lo que hayáis investigado. (1,5 puntos)

Por último, vamos a trabajar el concepto de bypass de AMSI.

c) Investigad diferentes formas de hacer un bypass de AMSI. Podéis explicar los AMSI "classics", herramientas como Invoke-Obfuscation o la técnica Patch AMSI ScanBuffer = 0. Se recomienda ésta última. Explicad y haced la ejecución de unas técnicas. El resultado esperado es que cuando ejecutemos la instrucción "amsiutils" en una powershell nos salga habilitado y después de aplicar el bypass y ejecutemos de nuevo "amsiutils" nos salga no habilitado (1 punto).

ANTES:

```
PS C:\Users\IEUser> amsiutils
At line:1 char:1
+ amsiutils
+ ~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\IEUser>
```

DESPUES BYPASS:

```
PS C:\Users\IEUser\Desktop> amsiutils
amsiutils : The term 'amsiutils' is not recognized as the name of a cmdlet, function, script file, or
operable program. Check the spelling of the name, or if a path was included, verify that the path is
correct and try again.
At line:1 char:1
+ amsiutils
+ ~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (amsiutils:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
```

Indicaciones para la PEC

Existen preguntas que pueden responderse de múltiples formas distintas, simplemente elegid y comentad aquella que se haya utilizado.

Procurad que las respuestas sean lo más concretas posible. No os extendáis.

El documento que enviéis al buzón no debe exceder las 14 páginas máximo. Se recomienda que utilicéis formato PDF para la entrega.

Entrega

Depositaréis en las respuestas del enunciado de la PEC en el área destinada a tal fin. Adjuntad toda la práctica en un solo documento, en formato PDF. En caso de que necesitéis adjuntar documentos adicionales, entonces enviadlos dentro de un fichero comprimido (zip, rar, 7z, tgz…).