

"Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for."

("Si, soy un criminal. Mi crimen es la curiosidad, juzgar a la gente por lo que dice y piense, no por su aspecto. Mi crimen es superarte, algo por lo que nunca me vas a perdonar.")

Extraido del Manifiesto Hacker,
The Mentor, 1986

Guía de la Presentación (Buanzo's Memory Pointers)

Primera Parte -- Nmap

- **¿Qué es Nmap?**
- **Groso, pero... ¿Para qué me sirve?**
- **Y qué, yo te cambio el SSH de puerto...**
- **Ejemplos Prácticos**

Segunda Parte – Nmap Scripting Engine

- **¿Qué es el NSE?**
- **¿Qué es LUA?**
- **¿Para qué puede servir?**
- **¿Cómo se crea un script NSE?**
- **A ver, mostrame un par de scripts...**

- **Ronda de Preguntas y Respuestas**
- **Agradecimientos**

¿Qué es Nmap?

"Nmap es, ante todo, Software Libre."

Los servicios funcionan en puertos. Los puertos se ven en direcciones IP, las direcciones IP se encuentran en equipos, los equipos están detrás de firewalls, y en el medio hay muchos routers. Y después, vos.

Nmap es la aplicación que utilizás para descubrir muchos detalles de todo eso.

Más sencillamente, Nmap es un analizador de puertos y servicios.

Groso, pero... ¿Para qué me sirve?

Sirve para saber que tipo de software se encuentra escuchando conexiones detrás de cada combinación IP/puerto, si desde nuestro punto de vista está filtrado o no.

Nos permite conocer la potencial versión del software, e incluso adivinar el sistema operativo remoto, con lo que la selección de que exploits utilizar se simplifica.

Con las últimas mejoras, como el Qscan, permite realizar análisis muy avanzados, lográndose determinar NATs, Firewalling, Proxies Transparentes.

Nmap incluso permite realizar sondeos via proxies.

Y qué, yo te cambio el SSH de puerto...

!¿Y a mi qué!? ESO van a responder ustedes, porque Nmap NO se basa en el número de puerto para detectar el servicio, sino que realiza pruebas concretas: utiliza cada protocolo en cada puerto y analiza las respuestas.

De esta manera, Nmap ayuda a que la seguridad que se implemente no sea mediante obscuridad.

Ejemplos Prácticos

* Descubrir OS y Software remoto

- Sólo en puertos 22,25 y 80:

```
nmap -A -p 22,25,80 $OBJETIVO
```

- Según nmap-services:

```
nmap -A -F $OBJETIVO
```

- En un rango de IP:

```
nmap -A -F 24.232.150.0/32
```

(Si hay tiempo, ejemplos durante la charla según indiquen los asistentes).

¿Qué es el NSE?

Es, literalmente, el motor de scripting integrado a Nmap, y que permite agregar funcionalidad interactiva avanzada.

Esto significa que Nmap, gracias al NSE, puede realizar tareas que solo Nessus y Metasploit brindaban.

Por ejemplo, se podría hacer un script que se ejecute sólo si el puerto 80 o un servicio web es descubierto, y realizar alguna tarea puntual, como determinar la versión de PHP instalada.

¿Qué es LUA?

LUA es un lenguaje diseñado para ser embebido en otras aplicaciones, para extender la funcionalidad de las mismas. (Y no pregunten por NASL!)

```
function explode(d,p)
local t,ll,l
t={}
ll=0
  while true do
    l=string.find(p,d,ll+1,true) -- comentario
    if l~=nil then
      table.insert(t, string.sub(p,ll,l-1))
      ll=l+1
    else
      table.insert(t, string.sub(p,ll))
      break
    end
  end
end
return t
end
```

¿Para qué puede servir?

- * **Exploits automatizados / inteligentes**
- * **Obtener información de los servicios remotos**
- * **Encontrar errores de configuración**
- * **Realizar pruebas de stress**
- * **Monitorear estado de servicios**
- * **Cruzar información obtenida con fuentes externas (whois, axfr, traceroute, etc)**
- * **Enviar alertas por mail, SMS**
- * **Cualquier cosa, bah.**

¿Cómo se crea un script NSE?

Ante todo, lo principal es basarse en un script ya existente, para evitar tener que aprender de cero algunas “particularidades” de LUA, y para no reinventar la rueda.

Luego, un script NSE debe definir las siguientes constantes y funciones:

CONSTANTES: id, description y tag.

FUNCIONES: portrule y action

La función portrule devuelve TRUE sólomente si el script debe ser ejecutado.

La función action es el script en sí, y devolverá un mensaje que será mostrado junto con el id, siempre y cuando portrule haya indicado TRUE.

¿Cómo se crea un script NSE?

```
id="Open Proxy Test"  
description="Test if remote proxy is open to usage"  
tags = {"intrusive"}  
  
portrule = function(host, port)  
  if (  
    port.number == 3128 or  
    port.number == 8080 or  
    port.service == "http-proxy" or  
    port.service == "squid-proxy"  
    ) and port.protocol == "tcp"  
  then  
    return true  
  else  
    return false  
  end  
end  
end
```

¿Cómo se crea un script NSE?

```
action = function(host, port)
local socket = nmap.new_socket()
local retval = ""

socket:connect(host.ip, port.number, port.protocol)
socket:send("GET http://www.google.com HTTP[...]")

status, result = socket:receive_lines(1)
if (status == false) or (result == "TIMEOUT") then
[...]
else
[...]
retval = "Open Proxy Found"
end

socket:close()
return retval
end
```



Y ahora, algo práctico antes de terminar

Agradecimientos

A mi hijo Damián.

A mi futura esposa, Erica.

A Karmax.

A 2600, por la frecuencia.

A todos los que hicieron posible que yo esté acá.

**(Y, ya que estamos a la SC2_SK,
por tantas batallas juntos!)**

Y especialmente a...

USTEDES por no asesinarme durante...

ni despues....

de esta charla.

¡Adios!

Arturo 'Buanzo' Busleiman
www.buanzo.com.ar
www.vivamoslavida.com.ar
buanzo@buanzo.com.ar

