



BugCon
security conferences

Nmap Script Engine

Hugo González



<http://creativecommons.org/licenses/by/2.5/mx/>



Alguien NO sabe que es NMAP ???????



Para que sirve nmap

- Software libre !!!!
- Sirve para saber que tipo de software está escuchando conexiones en cada combinación de IP/puerto
- Nos permite conocer la potencial versión de software, adivinar el SO remoto ... buscar vulnerabilidades específicas.
- Realizar análisis avanzados ...
- Incluso identifica software en puertos no convencionales



Ejemplos

- `nmap 192.168.9.41`
- `nmap -p 80,22,23 192.168.9.41`
- `nmap 192.168.9.0/24`
- `nmap 192.168.0.0/16`
- `nmap -A -T4 192.168.9.0/24`
- `nmap -F 192.168.9.0/24`
- `nmap -PN 192.168.9.0/24`
- `man nmap`



Nmap 5.00

- Nueva versión liberada en Julio
- Mayor revisión desde 1997
- Mejoras en el desempeño *
- Más scripts ;)
- Ncat
- Ndiff
- Zenmap
- ** el libro, Nmap Network Scanning



Mejor desempeño

- Se limitó el número de puertos determinados para los escaneos rápidos a 1000 y a 100
- <http://nmap.org/5/#changes-performance>



Ncat

- Reimplementación de ncat
incluye IPv6, SSL, NAT traversal, port redirection, y más



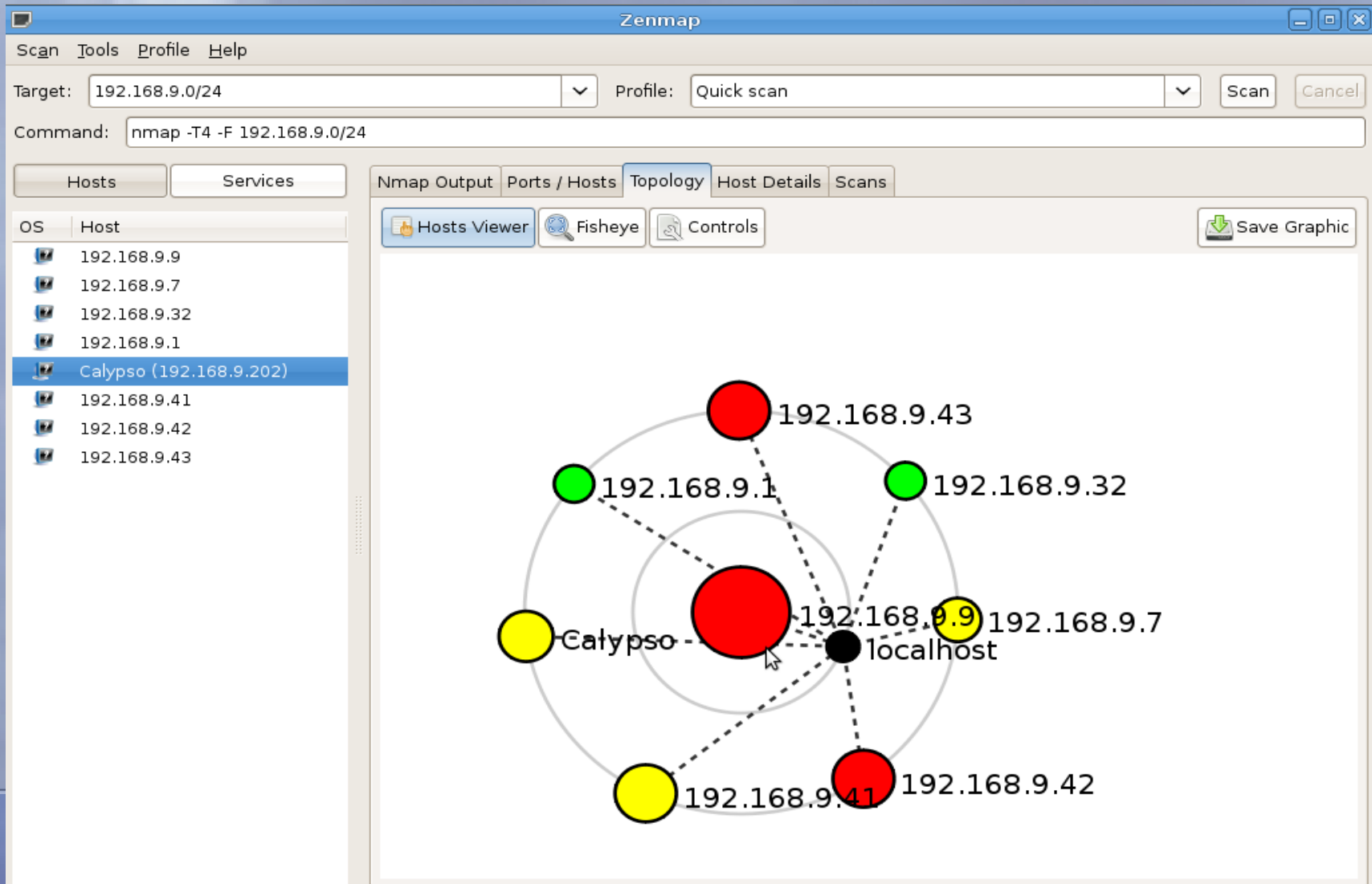
Ndiff

- Basado en el popular diff, este sirve para encontrar diferencias entre escaneos, pudiendo automatizar la verificación de redes o hosts

```
hugo@Atenea:~/proyectos/nmap-5.00/ndiff$ ndiff test-scans/single.xml test-scans/
simple.xml
Wed Sep  3 21:04:31 2008 -> Wed Sep  3 20:49:34 2008
scanme.nmap.org (64.13.134.52):
  -25/tcp closed smtp
  -53/tcp open domain
  -70/tcp closed gopher
  -80/tcp open http
  +113/tcp closed auth
  The following 95 tcp ports changed state from filtered to unknown:
    1-21,23-24,26-52,54-69,71-79,81-100
hugo@Atenea:~/proyectos/nmap-5.00/ndiff$
```

Zenmap

- Interface gráfica para nmap ...



The screenshot displays the Zenmap application window. The title bar reads "Zenmap". The menu bar includes "Scan", "Tools", "Profile", and "Help". The main interface is divided into several sections:

- Target and Profile:** Target is set to "192.168.9.0/24" and Profile is "Quick scan". Buttons for "Scan" and "Cancel" are visible.
- Command:** The command field contains "nmap -T4 -F 192.168.9.0/24".
- Hosts List:** A table on the left shows the results of the scan. The "Calypso" host is selected.
- Topology View:** The main area shows a network diagram with nodes and connections.

OS	Host
<input checked="" type="checkbox"/>	192.168.9.9
<input checked="" type="checkbox"/>	192.168.9.7
<input checked="" type="checkbox"/>	192.168.9.32
<input checked="" type="checkbox"/>	192.168.9.1
<input checked="" type="checkbox"/>	Calypso (192.168.9.202)
<input checked="" type="checkbox"/>	192.168.9.41
<input checked="" type="checkbox"/>	192.168.9.42
<input checked="" type="checkbox"/>	192.168.9.43

The network topology diagram shows a central node labeled "Calypso" (red circle) connected to several other nodes: "localhost" (black circle), "192.168.9.9" (yellow circle), "192.168.9.41" (yellow circle), "192.168.9.42" (red circle), "192.168.9.43" (red circle), "192.168.9.1" (green circle), and "192.168.9.32" (green circle). Dashed lines represent connections between these nodes.



NSE

- Es una característica flexible y poderosa, permite a los usuarios crear y compartir “sencillos” scripts para realizar tareas específicas
- Estos son ejecutados en paralelo con la velocidad y eficiencia que se espera de nmap
- Se incluyen muchos scripts con Nmap ...
 - safe, intrusive, malware, version, discovery, vuln, auth, and default
- Estos scripts pueden dañar tu sistema, evitar ejecutar scripts de terceros ...



Probando “no intrusive”

```
Starting Nmap 5.00 ( http://nmap.org ) at 2009-08-12 18:32 CDT
Interesting ports on 192.168.7.55:
Not shown: 990 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
|_ banner: 220 Microsoft FTP Service
80/tcp    open  http
|_ html-title: Cat\xEllogo de Libros *
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
1038/tcp   open  unknown
1039/tcp   open  unknown
1433/tcp   open  ms-sql-s
3389/tcp   open  ms-term-serv

Host script results:
| smb-security-mode: User-level authentication
| SMB Security: Challenge/response passwords supported
|_ SMB Security: Message signing not supported
| smb-os-discovery: Windows Server 2003 3790 Service Pack 2
| LAN Manager: Windows Server 2003 5.2
| Name: UPSLP\CID
|_ System time: 2009-08-12 18:33:27 UTC-5
|_ nbstat: NetBIOS name: CID, NetBIOS user: <unknown>, NetBIOS MAC: 00:11:25:54:
fe:78

Nmap done: 1 IP address (1 host up) scanned in 44.72 seconds
hugo@Atenea:~/proyectos/nmap-5.00$
```



Ejemplos

- `nmap --script "not intrusive" target`
- `nmap --script "default or safe"`
- `nmap --script "default and safe"`
- `nmap --script "(default or safe or intrusive) and not http-*`
-



Sirve para ...

- Desarrollar scripts para puertos específicos ...
- Los scripts están desarrollados en LUA !?!?!?
- Ya existen librerías que facilitan el desarrollo

* base64

* bin

* bit

* comm

* datafiles

* dns

* http

* imap

* ipOps

* listop

* match

* msrpc

* msrpcperformance

* msrpctypes

* netbios

* nmap

* nsedebug

* openssl

* packet

* pcre

* pop3

* shortport

* smb

* smbauth

* snmp

* ssh1

* ssh2

* stdnse

* strbuf

* strict

* tab

* unpwdb

* url



O sea ...

- Con NSE puedo hacer cosas “parecidas” a metasploit o nessus ...
- No solo escanear, sino detectar vulnerabilidades ...
- O bien detectar malware
 - smtp en otros puertos
 - conficker
- Incluso ... explotarlas



Como hago un script ???

- Basicamente tenemos dos partes ...
- Constantes
 - Id
 - description
 - category
- Y tenemos 2 funciones principales
 - portrule
 - Action
- **Iniciar con un script ya desarrollado**



Constantes

```
description = [[  
Checks if a VNC server is vulnerable to the RealVNC  
authentication bypass  
(CVE-2006-2369).  
]]  
author = "Brandon Enright <bmenrigh@ucsd.edu>"  
license = "Same as Nmap--See http://nmap.org/book/man-legal.html"  
  
categories = {"default", "vuln"}  
  
require "shortport"
```



Funciones

```
portrule = shortport.port_or_service(5900, "vnc")
```

```
action = function(host, port)
```

```
  local socket = nmap.new_socket()
```

```
  local result
```

```
  local status = true
```

```
  socket:connect(host.ip, port.number, port.protocol)
```

```
  status, result = socket:receive_lines(1)
```

```
  if (result == "TIMEOUT") then
```

```
    socket:close()
```

```
    return
```

```
  end
```



```
socket:send("RFB 003.008\n")  
status, result = socket:receive_bytes(2)
```

```
if (result == "TIMEOUT") then  
    socket:close()  
    return  
end
```

```
if (result ~= "\001\002") then  
    socket:close()  
    return  
end
```

```
socket:send("\001")  
status, result = socket:receive_bytes(4)
```



```
if (result == "TIMEOUT") then
    socket:close()
    return
end

if (result ~= "\000\000\000\000") then
    socket:close()
    return
end

socket:close()

return "Vulnerable"
end
```



Ejemplo ...



```
description = [[
```

```
Verifica que la contraseña de acceso sea cisco a traves de telnet
```

```
Basado en ftp-anon.nse
```

```
]]
```

```
author = "Hugo Gonzalez <hugo.glez@gmail.com>"
```

```
license = "Same as Nmap--See http://nmap.org/book/man-legal.html"
```

```
categories = {"default", "auth", "safe"}
```

```
require "shortport"
```

```
portrule = shortport.port_or_service(23, "telnet")
```

```
action = function(host, port)
```

```
    local socket = nmap.new_socket()
```

```
    local result
```

```
    local status = true
```

```
    local isdefault = false
```

```
    local err_catch = function()
```

```
        socket:close()
```

```
    end
```



```
local try = nmap.new_try(err_catch)
```

```
socket:set_timeout(5000)
```

```
try(socket:connect(host.ip, port.number, port.protocol))
```

```
try(socket:send("cisco\r\n"))
```

```
try(socket:send("cisco\r\n"))
```

```
while status do
```

```
    status, result = socket:receive_lines(1);
```

```
    if (string.match(result, ">") or string.match(result, "#") )then
```

```
        isdefault = true
```

```
        break
```

```
    end
```

```
end
```

```
socket:close()
```

```
if(isdefault) then
```

```
    return "Password por defecto cisco"
```

```
end
```

```
end
```



Algunos scripts útiles

- # smb-brute.nse
- # smb-check-vulns.nse
- # smb-enum-domains.nse
- # smb-enum-processes.nse
- # smb-enum-sessions.nse
- # smb-enum-shares.nse
- # smb-enum-users.nse
- # smb-os-discovery.nse
- # smb-pwdump.nse
- # smb-security-mode.nse
- # smb-server-stats.nse
- # smb-system-info.nse



Agradecimientos !

- Fyodor y equipo ...
- Organizadores del BugCON ...
 - UPSLP \$\$\$





BugCon

security conferences

Preguntas ?!?!?!?

hugo.gonzalez@upslp.edu.mx

