Listado de prácticas sobre temas de seguridad

Conexión entre Windows, Linux y Android

- https://www.jesusninoc.com/02/25/creating-reverse-shell/
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-01-08.md
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-01-09.md
- https://www.jesusninoc.com/11/12/enviar-un-video-mp4-entre-dos-linux-mediante-netcat/

Servidores web

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-02-14.md
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-02-18.md
- https://twitter.com/JaneScott_/status/1011824778808717312
- https://gist.github.com/jesusninoc/9efe81d90fbb1adf8212686b62de2b7c

---

Android

- https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector

---

Embed a Metasploit Payload in an Original .Apk

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-01-10.md
- https://null-byte.wonderhowto.com/how-to/embed-metasploit-payload-original-apk-file-part-2-do-manually-0167124/

Ejecutar un comando remotamente en un equipo con PowerShell

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-01-14.md
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-01-15.md
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-01-16.md
- https://www.jesusninoc.com/10/07/crear-un-cliente-y-un-servidor-tcpip-con-powershell/
- https://www.jesusninoc.com/03/08/psexec/

```
psexec \\dnsname-or-ip reg add
```

```
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Policies\System" /v EnableLUA /t REG_DWORD /d 0 /f
```

Uso de DLL

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-01-29.md
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-01-30.md
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-01-31.md
- https://www.jesusninoc.com/11/28/crear-compilar-y-ejecutar-una-dll-con-microsoft-visual-c-que-abre-notepad-desde-powershell/
- https://github.com/jesusninoc/ClasesISO/blob/master/2019-04-04.md
- https://www.jesusninoc.com/02/05/crear-un-usuario-local-con-contrasena-en-windows-10/
- https://www.jesusninoc.com/11/29/crear-compilar-y-ejecutar-una-dll-con-microsoft-visual-c-que-crear-un-usuario-desde-powershell/
- https://www.jesusninoc.com/01/27/comprobar-si-ha-cambiado-algun-fichero-utilizando-la-funcion-hash-sha1/
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-02-05.md
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-02-09.md
- https://www.endgame.com/blog/technical-blog/ten-process-injection-techniques-technical-survey-common-and-trending-process
- https://github.com/fdiskyou/injectAllTheThings

Enviar informacion sobre equipos utilizando un servidor web

- https://www.jesusninoc.com/12/02/obtener-serial-de-windows-con-powershell/
- https://www.jesusninoc.com/10/21/almacenar-entradas-cache-dns-en-un-fichero/
- https://github.com/1N3/PowerExfil

Uncover Tiny URLs

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-03-08.md

---

DOS

- https://gist.github.com/steakknife/1865841
- https://github.com/NewEraCracker/LOIC

BoNeSi: simular una botnet para pruebas DDoS

- https://www.hackplayers.com/2018/12/bonesi-simular-una-botnet-para-pruebas-ddos.html

TOR

- https://www.jesusninoc.com/02/01/crear-un-dominio-onion/
- https://www.hacklooking.cl/2019/01/13/kali-linux-tor-desde-tu-navegador-y-sin-instalar-nada/

Control y notificaciones

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-02-12.md#control

Análisis de paquetes

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-02-07.md
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-02-11.md
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-02-20.md

¿Qué podemos analizar en la red con Wireshark?

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-02-21.md

Modificar UDP

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-01-17.md

- https://www.jesusninoc.com/12/29/server-and-client/
- https://www.jesusninoc.com/03/19/modificar-datagramas-udp-con-softperfect-network-protocol-analyzer/

Virus y antivirus

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-01-24.md
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-01-28.md
- https://github.com/jesusninoc/Seguridad/blob/master/Una%20aproximaci%C3%B3n%20a%20los%20virus%20en%20PowerShell.md
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-02-19.md#antivirus

Hash parcial

- https://github.com/jesusninoc/PowerShell/blob/master/Seguridad/Realizar%20hashes%20parciales%20sobre%20un%20fichero.ps1

Web Application Penetration Testing Course URLs.docx

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-02-04.md
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-02-05.md

- https://paper.tuisec.win/detail/eeb64a1fb983f6a

Acercarse al objetivo

- https://github.com/jesusninoc/ClasesISO/blob/master/2018-03-01.md

Ataque paso a paso

- https://github.com/jesusninoc/ClasesISO/blob/master/2018-03-01.md

Fallos posibles

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-02-14.md

Introduccion a OWASP Top Ten 2017

- https://www.jesusninoc.com/12/29/introduccion-a-owasp-top-ten-2017/

PowerShell for Pentesters

- http://www.securitytube-training.com/online-courses/powershell-for-pentesters/index.html
- https://github.com/salu90/PSFPT

AutoRDPwn – La guía definitiva

- https://darkbyte.net/autordpwn-la-guia-definitiva/

Powercat

- https://0xword.com/es/libros/69-pentesting-con-powershell.html

PowerTools

- https://0xword.com/es/libros/69-pentesting-con-powershell.html

Posh-SecMod

- https://0xword.com/es/libros/69-pentesting-con-powershell.html

PowerSploit

- https://0xword.com/es/libros/69-pentesting-con-powershell.html

Nishang

- https://0xword.com/es/libros/69-pentesting-con-powershell.html

---

Keylogger

- https://www.jesusninoc.com/03/11/keylogger-sencillo-con-powershell/
- https://www.jesusninoc.com/07/16/transfer-keylogger-log-file-between-server-and-client-sockets-tcp/
- http://powershell.com/cs/blogs/tips/archive/2015/12/09/creating-simple-keylogger.aspx
- https://github.com/vacmf/powershell-scripts/blob/master/powershell-keylogger.ps1
- https://www.jesusninoc.com/04/30/enviar-datos-a-un-formulario-de-google-docs-desde-powershell-deducir-los-parametros-que-se-envian-por-post/

Análisis forense

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-02-07.md

Metadatos

- https://www.jesusninoc.com/01/01/extraer-coordenadas-gps-de-imagenes-con-powershell/

Fuerza

- https://github.com/jesusninoc/Seguridad/tree/master/GetPost
- https://github.com/jesusninoc/Seguridad/tree/master/Fuer

zaBruta

Fuerza bruta y ofuscación

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-02-20.md
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-02-21.md
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-02-25.md
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-01-11.md
- https://github.com/CBHue/PyFuscation

Certificados

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-02-26.md

---

Enviar una contraseña utilizando un servidor web

- https://www.jesusninoc.com/02/11/hacking-wifi-with-powershell/

Password cracker

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-02-08.md

Hash

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-02-05.md

Colisiones

- https://www.jesusninoc.com/02/24/poc-para-detectar-colision-en-sha1-con-powershell/
- http://www.codeproject.com/Questions/458694/Proving-MD-Collision-with-Csharp

Criptografía con PowerShell

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-01-18.md

Cifrado sencillo

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-01-30.md

---

Shellcode

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-02-08.md
- https://gist.github.com/Arno0x/17d1705ecfc945088579c84994a652d3

Infección de procesos en Linux

- https://www.tarlogic.com/blog/infeccion-procesos-linux-parte-i/

XSS

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-03-07.md
- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-02-12.md

LFI/RFI

- https://www.hackingarticles.in/beginner-guide-file-inclusion-attack-lfirfi/
- https://www.hackingarticles.in/smtp-log-poisioning-through-lfi-to-remote-code-exceution/

CAPTCHA

- https://www.jesusninoc.com/01/06/resolver-el-captcha-de-amazon/
- https://www.jesusninoc.com/01/05/descargar-la-imagen-del-captcha-de-amazon/
- https://www.jesusninoc.com/02/09/aclarar-una-imagen-utilizando-imagemagick-y-convertir-a-texto-con-tesseract/

Reverse engineering

- https://www.jesusninoc.com/11/20/apktool/
- https://www.jesusninoc.com/02/09/crear-compilar-generar-y-ejecutar-un-jar-de-java-que-ejecuta-un-cmdlet-de-powershell-utilizando-runtime/

Manipulación de ficheros PDF

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-03-06.md
- https://www.jesusninoc.com/08/17/crear-un-pdf-utilizando-powershell/
- https://www.jesusninoc.com/02/17/crear-un-fichero-pdf-con-un-script-embebido-de-javascript/

JavaScript embebido

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-02-26.md

---

Introducción al exploiting

- https://ironhackers.es/tutoriales/introduccion-al-exploiting-parte-1-stack-0-2-protostar/
- https://ironhackers.es/tutoriales/introduccion-al-exploiting-parte-2-stack-3-4-protostar/

Reconocimiento

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-01-24.md#reconocimiento-recolectar-informaci%C3%B3n
- https://noticiasseguridad.com/tutoriales/the-harvester-busque-a-los-empleados-que-trabajan-en-una-empresa/

Análisis de un dispositivo USB

- https://www.jesusninoc.com/05/01/usbpcap-usb-packet-capture-for-windows/
- https://hacking-etico.com/2016/03/10/analisis-usb-wireshark-parte-2

Hardware

- https://www.hackerarsenal.com/collections/frontpage/products/wimonitor
- https://shop.hak5.org/collections/all
- http://www.keelog.com/es/

WIFI

- http://rubyfu.net/content/module_0x3__network_kung_fu/ssid_finder.html
- https://www.jesusninoc.com/10/16/enviar-paquetes-de-desasociacion-con-aireplay-ng-a-un-cliente-que-actualmente-esta-asociado-con-un-punto-de-acceso-en-linux-

realizando-una-conexion-ssh-desde-powershell-en-windows/

USB Rubber Ducky

- https://shop.hak5.org/products/usb-rubber-ducky-deluxe
- https://www.jesusninoc.com/03/09/scripts-en-rubber-ducky-parte-1/
- https://www.jesusninoc.com/03/20/scripts-en-rubber-ducky-parte-2/
- https://www.jesusninoc.com/ducky-scripts/

Ejecutar aplicaciones desde lenguajes de programación

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-02-13.md

Metasploit

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2018-02-26.md

---

Awesome Red Teaming

- https://github.com/jesusninoc/ClasesSeguridad/blob/master/2019-01-23.md
- https://github.com/yeyintminthuhtut/Awesome-Red-Teaming
- https://github.com/Mr-Un1k0d3r/RedTeamPowershellScripts

Proxy

- https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- https://www.zaproxy.org/
- https://mitmproxy.org/

Manipulación QR

- https://www.jesusninoc.com/05/27/crear-codigo-qr-para-una-ubicacion-gps/
- https://www.jesusninoc.com/05/23/crear-codigo-qr-para-la-conexion-wifi/
- https://www.jesusninoc.com/06/01/crear-y-leer-un-codigo-qr-con-un-comando-en-bash-mediante-wsl-desde-powershell/
- https://www.jesusninoc.com/06/05/crear-un-servidor-web-con-un-servicio-que-permita-leer-un-codigo-qr-desde-powershell/

Macros

- https://social.technet.microsoft.com/Forums/windowsserver/en-US/4425e609-1353-4b03-b9d9-ed4a3bc5e365/running-an-excel-macro-from-powershell?forum=winserverpowershell
- https://www.blackhillsinfosec.com/phishing-with-powerpoint/
- https://community.idera.com/database-tools/powershell/powertips/b/tips/posts/invoking-excel-macros-from-powershell

Bounty Write-up (HTB)

- https://medium.com/ctf-writeups/bounty-write-up-htb-9b01c934dfd2