Introduccion al hacking ético

1. Introducción

a) ¡Bienvenido al curso!

- Video
  https://platform.thinkific.com/videoproxy/v1/play/butamcuje35bt9cj82og?&autoplay=true&crosstime=147

b) Requisitos antes de empezar

- Video
  https://platform.thinkific.com/videoproxy/v1/play/butbrdmje35bt9cj84vg?&autoplay=true&crosstime=147
- Recomendaciones/Notas

  Descargar :
  Kali Linux o Parrot OS
  Mi tarjeta de red: TP-LINK (TL-WN722N) [Version 1.0]

2. Conceptos básicos

a) Interfaces de red

- Video
  https://platform.thinkific.com/videoproxy/v1/play/butnh43i57dcbr64lit0?&autoplay=true&crosstime=184

b) Tarjetas de red

- Vidéo
  https://platform.thinkific.com/videoproxy/v1/play/butnmhmje35bt9cj8rdg?&autoplay=true&crosstime=89

c) Dirección IP privada/Publica

- Vidéo
  https://platform.thinkific.com/videoproxy/v1/play/buto93ji57dcbr64lka0?&autoplay=true&crosstime=139

d) Direcciones MAC

- Video
  https://platform.thinkific.com/videoproxy/v1/play/butogq3i57dcbr64ll60?&autoplay=true&crosstime=210

3. Vulneración de redes WPA/WPA2 (PSK)

a) Modo monitor

- Video
  https://platform.thinkific.com/videoproxy/v1/play/butpm3uje35bt9cj90d0?&autoplay=true&crosstime=96
- Recomendaciones/Notas
  Material de apoyo
  Modo monitor (concepto) : https://www.acrylicwifi.com/blog/modo-monitor-wifi/#:~:text=El%20modo%20monitor%20es%20el,Beacon)%2C%20Data%20y%20Control.

b) Configuración de la tarjeta de red en modo monitor

- Video
  https://platform.thinkific.com/videoproxy/v1/play/butq9mbi57dcbr64lpag?&autoplay=true&crosstime=418
- Recomendaciones/Notas
  Material de apoyo
  Modo monitor y modo captura nativa:
  https://www.acrylicwifi.com/blog/modo-monitor-wifi/

c) Falsificando nuestra dirección MAC y tips

- Video
  https://platform.thinkific.com/videoproxy/v1/play/butqhori57dcbr64lpr0?&autoplay=true&crosstime=228
- Recomendaciones/Notas
  Material de apoyo
  MAC Adress Spoofing :
  https://wiki.archlinux.org/title/MAC_address_spoofing_(Espa%C3%B1ol)

  Falsificacion de MAC:
  Consigue falsificar tu direccion de MAC. Puedes utilizar como OUI el que quieras, practica!

d) Uso de Airodump para efectuar un análisis del entorno

- Video
  https://platform.thinkific.com/videoproxy/v1/play/butrieri57dcbr64ls1g?&autoplay=true&crosstime=384

- Recomendaciones/Notas

Material de apoyo
Suite de Aircrack-ng – Aircrack :
https://es.wikipedia.org/wiki/Aircrack-ng#:~:text=Aircrack%2Dng%20es%20una%20suite,airbase%2Dng

e) Uso de Airodump para efectuar un análisis del entorno 2

- Video
https://platform.thinkific.com/videoproxy/v1/play/butruruje35bt9cj95l0?&autoplay=true&crosstime=342

- Recomendaciones/Notas

Material de apoyo
Aircrack-ng – Comandos Basicos:
https://yisux.wordpress.com/2009/03/11/aircrack-ng-comandos-basicos-para-ataques-con-clientes-asociados/

f) Modos de filtro con Airodump

- Video
https://platform.thinkific.com/videoproxy/v1/play/bv32u6ri57dcbr65378g?&autoplay=true&crosstime=188

- Recomendaciones/Notas

Material de apoyo
Airodump-ng[Aircrack-ng] modos de uso: https://www.aircrack-ng.org/~~V:/doku.php?id=es:airodump-ng#:~:text=Airodump%2Dng%20se%20usa%20para,y%20obtener%20la%20clave%20WEP.

g) Exportación de evidencias con Airodump

- Video
https://platform.thinkific.com/videoproxy/v1/play/bv3324ri57dcbr6537j0?&autoplay=true&crosstime=191

- Recomendaciones/Notas

Material de apoyo
Airodump-ng [Aircrack-ng] modos de uso: https://www.aircrack-ng.org/~~V:/doku.php?id=es:airodump-ng#:~:text=Airodump%2Dng%20se%20usa%20para,y%20obtener%20la%20clave%20WEP.

h) Conceptos de HandShake

- Video
https://platform.thinkific.com/videoproxy/v1/play/bv33csuje35bt9cjmcig?&autoplay=true&crosstime=287

- Recomendaciones/Notas

Material de apoyo

Concepto de HandShake : https://hacking-etico.com/2013/05/08/redes-wifi-con-wpawpa2inviolables/#:~:text=El%20handshake%20es%2C%20a%20grosso,la%20contrase%C3%B1a%20WiFi%20pero%20cifrada.

i) Ataque de autenticación dirigido

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv33j2ri57dcbr6539b0?&autoplay=true&crosstime=307
- Recomendaciones/Notas

Material de apoyo
Desautenticacion y autenticacion falsa : https://www.google.com/search?q=Ataque+de+de-autenticaci%C3%B3n+aireplay&rlz=1C1GCEA_enES868ES868&oq=Ataque+de+de-autenticaci%C3%B3n+aireplay&aqs=chrome..69i57j33i160.5751j0j7&sourceid=chrome&ie=UTF-8

j) Ataque Deautenticación global (Broadcast MAC Address)

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv33r0ji57dcbr653afg?&autoplay=true&crosstime=347
- Recomendaciones/Notas

Material de apoyo
WiFi de DeAuthentication Attack : https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack

k) Ataque de falsa autenticación

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv341iji57dcbr653b0g?&autoplay=true&crosstime=306
- Recomendaciones/Notas

Material de apoyo
Realizar falsa autenticación con clave compartida: https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack

l) CTS Frame Attack – Secuestro del Ancho de Banda de una red

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv35kb6je35bt9cjmk1g?&autoplay=true&crosstime=245
- Recomendaciones/Notas

Material de apoyo
CTS DoS Mini-HOWTO : ?

m) CTS Frame Attack – Secuestro del Ancho de Banda de una red 2

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv3anqmje35bt9cjn4tg?&autoplay=true&crosstime=787

n) Ataque Beacon Flood Mode

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv3qarqd6nqpp0jbdvhg?&autoplay=true&crosstime=308
- Recomendaciones/Notas
  Material de apoyo
  Beacon Flood Mode Attack : https://mundo-hackers.weebly.com/beacon-flood.html

o) Ataque Disassociation Amok Mode

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv3rooqd6nqpp0jbe4ng?&autoplay=true&crosstime=147
- Recomendaciones/Notas
  Material de apoyo
  Disassociation Amol Mode Attack : https://mundo-hackers.weebly.com/amok-mode---disassociation.html

p) Ataque Michael Shutdown Exploitation – Apagado de un Router en remoto

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv3vqlcerl5cdoalnfg0?&autoplay=true&crosstime=154
- Recomendaciones/Notas
  Material de apoyo
  Michael Shutdown Exploitation : https://mundo-hackers.weebly.com/michael-shutdown-exploitation.html

q) Técnicas pasivas de explotación

- Vidéo
  https://platform.thinkific.com/videoproxy/v1/play/bv409d4erl5cdoalnh50?&autoplay=true&crosstime=150

r) Instalación, compilación y validación del HandShake con Pyrit

- Vidéo
  https://platform.thinkific.com/videoproxy/v1/play/bv42v53jj09frru4617g?&autoplay=true&crosstime=562
- Recomendaciones/Notas
  Material de apoyo
  Uso de Pyrit : https://laquialinux.es/pyrit-descifrar-clave-wpa-con-gpu/

s) Análisis de los paquetes Probe Request

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv4mihcerl5cdoalp9m0?&autoplay=true&crosstime=150
- Recomendaciones/Notas
  Material de apoyo
  Notas inalambricas – Probe Request :
  https://notasinalambricas.wordpress.com/tag/probe-request/

t) Análisis de los paquetes Probe Response

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv4mmlcerl5cdoalpa20?&autoplay=true&crosstime=91
- Recomendaciones/Notas
  Material de apoyo
  Notas inalambricas – Probe Response :
  https://notasinalambricas.wordpress.com/tag/probe-response/

u) Análisis de los paquetes Association Request

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv4mr63jj09frru47jpg?&autoplay=true&crosstime=99
- Recomendaciones/Notas
  Material de apoyo
  Association Request/Response :
  https://mrncciew.com/2014/10/28/802-11-mgmt-association-reqresponse/

v) Análisis de los paquetes Association Response

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv6ds3cerl5cdoalslfg?&autoplay=true&crosstime=99
- Recomendaciones/Notas
  Material de apoyo

Association Request/Response :
https://mrncciew.com/2014/10/28/802-11-mgmt-association-regresponse/

w) Análisis de paquetes Beacon

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv6dv5jjj09frru4b0rg?&autoplay=true&crosstime=99
- Recomendaciones/Notas
  Material de apoyo
  Beacon Frame – wikipedia :
  https://es.wikipedia.org/wiki/Beacon_frame

x) Análisis de paquetes de Autentificación

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv6e0qserl5cdoalsllg?&autoplay=true&crosstime=70

y) Análisis de paquetes de Deautentificación

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv6e4fbjj09frru4b0u0?&autoplay=true&crosstime=135
- Recomendaciones/Notas
  Material de apoyo
  WI-FI Deauthentication Attack : https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack

z) Análisis de paquetes de Desasociación

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv6ec94erl5cdoalsm30?&autoplay=true&crosstime=172
- Recomendaciones/Notas
  Material de apoyo
  Dissasociation Frames : https://mrncciew.com/2014/10/11/802-11-mgmt-deauth-disassociation-frames/

aa) Extracción del Hash en el handShake con AirCrack

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv6elbrjj09frru4b1rg?&autoplay=true&crosstime=223

bb) Fuerza bruta con John para obtener la contraseña de la red

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv6f6kserl5cdoalsndg?&autoplay=true&crosstime=532
- Recomendaciones/Notas
  Material de apoyo
  Cracking Password Hashes with John The Ripper: https://www.tunnelsup.com/getting-started-cracking-password-hashes/

cc) Fuerza bruta con Aircrack para obtener la contraseña de la red

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv6fcdserl5cdoalsnl0?&autoplay=true&crosstime=125
- Recomendaciones/Notas
  Material de apoyo
  Cracking de contrasenas Wifi con AirCrack : https://esgeeks.com/cracking-claves-wifi-con-aircrack-ng/

dd) Proceso de ataque Bettercap

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv6fmi3jj09frru4b390?&autoplay=true&crosstime=268
- Recomendaciones/Notas
  Material de apoyo
  Hack wi-fi Networks with Bettercap: https://null-byte.wonderhowto.com/how-to/hack-wi-fi-networks-with-bettercap-0194422/

ee) Técnicas de aumento de la velocidad de cómputo (Rainbow Table)

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv6ggtserl5cdoalsq10?&autoplay=true&crosstime=248
- Recomendaciones/Notas
  Material de apoyo
  Descifrar contrasenas con las Rainbow Tables : https://www.ionos.es/digitalguide/servidores/seguridad/rainbow-tables/

ff)Cracking con Pyrit

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv72o3kerl5cdoalttd0?&autoplay=true&crosstime=311
- Recomendaciones/Notas
  Material de apoyo
  Cracking with Pyrit : https://null-byte.wonderhowto.com/how-to/crack-wpa-wpa2-wi-fi-passwords-with-pyrit-0196782/

gg) Cracking con Cowpatty

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv7367bjj09frru4c98g?&autoplay=true&crosstime=170
- Recomendaciones/Notas
  Material de apoyo
  Cracking con Cowpatty : https://mundo-hackers.weebly.com/crackingcowpatty.html

hh) Cracking con Airolib

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv73fdbjj09frru4cad0?&autoplay=true&crosstime=292
- Recomendaciones/Notas
  Material de apoyo
  Airolib-ng « El rapido crackeo de WPA/WPA2 » : https://underc0de.org/foro/wireless/airolib-ng-(el-'rapido'-crackeo-de-wpawpa2)/

ii) Creación de una Rainbow Table con GenPMK

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv73jfkerl5cdoalu010?&autoplay=true&crosstime=87

jj) Cracking con Cowpatty frente a una Rainbow Table

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv73nc4erl5cdoalu0dg?&autoplay=true&crosstime=117
- Recomendaciones/Notas
  Material de apoyo
  Utilizando Cowpatty frente a Rainbow Table : https://thehackerway.com/2012/05/17/wireless-hacking-utilizando-cowpatty-y-pyrit-para-optimizar-ataques-por-diccionario-contra-wpawpa2-parte-xv/

kk) Cracking con Pyrit frente a una Rainbow Table

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv73rpjjj09frru4cbqg?&autoplay=true&crosstime=146
- Recomendaciones/Notas
  Material de apoyo
  Cracking con Pyrit frente a Rainbow Table : https://mundo-hackers.weebly.com/cracking-con-pyrit-frente-a-rainbow-table.html

ll) Cracking con Pyrit a través de ataque por base de datos

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv745urjj09frru4ccn0?&autoplay=true&crosstime=244

mm) Técnicas de espionaje

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv7498serl5cdoalu2e0?&autoplay=true&crosstime=116

nn) Uso de Airdecap para el desencriptado de paquetes

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bv74g1kerl5cdoalu3c0?&autoplay=true&crosstime=419
- Recomendaciones/Notas
  Material de apoyo
  MITS en el aire y sin dejar huella: https://www.flu-project.com/2012/09/airdecap-ng-mitm-en-el-aire-y-sin-dejar_30.html#:~:text=airdecap%2Dng%20es%20una%20de,sido%20capturado%20mediante%20airodump%2Dng

oo) Ataques graciosos

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvbq28kerl5cdoam853g?&autoplay=true&crosstime=77

pp) Reemplazado de imágenes web con Xerosploit

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvbq9orjj09frru4mh70?&autoplay=true&crosstime=223
- Recomendaciones/Notas
  Material de apoyo

Man in the Middle con Xerosploit : https://sospedia.net/man-in-the-middle-con-xerosploit/#:~:text=La%20herramienta%20Xerosploit%20es%20un,de%20nuestro%20equipo%20al%20router

Ejercicio de Drifnet:
En base a lo visto en la clase anterior, intenta ejecutar el ataque Drifnet para capturar las imágenes de navegación de un usuario seleccionado.
PD: Para que este ataque funcione es necesario cofigurar ciertas cosas previamente.

qq) Ataque de ipo Evil Twin

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvbuphjjj09frru4n070?&autoplay=true&crosstime=243
- Recomendaciones/Notas
  Material de apoyo
  Ataque Evil Twin : https://diegoaltf4.com/evil-twin/

rr)Evil Twin – configurando nuestro archivo de configuración DHCPD

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvc7iukerl5cdoam91l0?&autoplay=true&crosstime=219

ss) EvilTwin – Descarga y uso de plantilla

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvc7r5jjj09frru4ne0g?&autoplay=true&crosstime=149

tt) EvilTwin – creación de base de datos en MYSQL

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvcigfserl5cdoama19g?&autoplay=true&crosstime=297

uu) EvilTwin – Montando el punto de acceso con Airbase

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvcirb3jj09frru4oem0?&autoplay=true&crosstime=177

vv) EvilTwin – Definicion de reglas con iptables y creación de interfaces de red

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvcj5n4erl5cdoama3bg?&autoplay=true&crosstime=388
- Recomendaciones/Notas
  Material de apoyo
  Tutorial basico de iptables en Linux :
  https://www.linuxito.com/seguridad/793-tutorial-basico-de-iptables-en-linux
  Iptables – Manual práctico:
  http://redesdecomputadores.umh.es/iptables.htm

ww) EvilTwin – Desplegando finalmente el ataque

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvcjb63jj09frru4ogdg?&autoplay=true&crosstime=165

xx) Uso de mi herramienta evilTrust para robo de credenciales en redes sociales

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvcjqikerl5cdoama54g?&autoplay=true&crosstime=259
- Recomendaciones/Notas
  Material de apoyo
  Enlace de la herramienta : https://github.com/s4vitar/evilTrust

yy) Ataque a redes sin clientes

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvckf4serl5cdoama6e0?&autoplay=true&crosstime=73

zz) Ataque desde Bettercap

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvcklfjjj09frru4oj50?&autoplay=true&crosstime=86
- Recomendaciones/Notas
  Material de apoyo
  Bettercap - Herramienta

aaa) Ataque via hcxdumptool

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvckou3jj09frru4ojdg?&autoplay=true&crosstime=92

- Recomendaciones/Notas

  Material de apoyo
  Repositorio : https://github.com/ZerBea/hcxdumptool

bbb) Uso de hcxdumptool y obtención de la contraseña

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvckveserl5cdoama7ng?&autoplay=true&crosstime=225

ccc) Ataques a redes ocultas - ¿Cómo descubrir y comprometer una red oculta?

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvd42gjjj09frru4pgn0?&autoplay=true&crosstime=107
- Recomendaciones/Notas

  Material de apoyo
  Obteniendo nombre de red Wifi oculta :
  https://youtu.be/aaKTtROzR8E

ddd) Ataques Datáfonos

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvd4tkbjj09frru4pk20?&autoplay=true&crosstime=86

eee) Uso del reloj DeAuther – DSTIKE

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvd52v3jj09frru4pl1g?&autoplay=true&crosstime=74

fff) Ataques por WPS

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvd4p7rjj09frru4pjgg?&autoplay=true&crosstime=372
- Recomendaciones/Notas

  Material de apoyo
  Rompiendo redes inalambricas con WPS :
  https://www.dragonjar.org/rompiendo-redes-inalambricas-wpa-y-wpa2-con-wps-en-segundos.xhtml

ggg) Redes WEP – Ataques comunes

- Video
  https://platform.thinkific.com/videoproxy/v1/play/bvd5kfcerl5cdoamb9k0?&autoplay=true&crosstime=233

- Recomendaciones/Notas
  Material de apoyo
  Mi gui adel OSWP :