KALI PURPLE

LA VERSIONE DEFENSIVE DELLA OFFENSIVE

ETHICAL® HACKER ITALIANI

KALI PURPLE ed il suo modello

Kali ha basato la sua versione Purple sul framework di sicurezza del NIST (National Institute of Standards and Technology)

Identificazione – Processi Critici, Flussi di Informazioni, Inventario Hw e Sw, Policies, Minacce, Vulnerabilità e Rischi

Protezione – Management dell'accesso ai dati, Protezione dei devices, Training degli utenti, Backup regolari

Rilevamento – Processi di rilevamento, Monitor dei logs, Analisi dei flussi, impatto degli eventi.

Risposta – Test dei piani di risposta, Certezza che funzionino, coordinamento con le parti interne ed esterne

Recupero – Comunicazioni con interni ed esterni, Concretezza dei piani di recovery e controllo della reputazione dell'azienda.

Installiamo Pentbox

WGET HTTP://DOWNLOADS.SOURCEFORGE.NET/PROJECT/PENTBOX18REALISED/PENTBOX-1.8.TAR.GZ

TAR XVFZ PENTBOX-1.8.TAR.GZ

CD PENTBOX-1.8

./PENTTBOX.RB

Il Network TAP Passivo

HTTPS://WWW.INSTRUCTABLES.COM/MAKE-A-PASSIVE-NETWORK-TAP/

HTTPS://RINGTAIL.CH/PRODUCTS/NETSPLIT-PASSIVE-ETHERNET-TAP

Installare PcapXray

GIT-CLONE HTTPS://GITHUB.COM/SRINIVAS11789/PCAPXRAY.GIT

CD PCAPXRAY

TO INSTALL THE REQUIREMENTS: PIP INSTALL -R REQUIREMENTS.TXT

TO RUN : PYTHON SOURCE/MAIN.PY

FcrackZIP

ILCOMANDO PER CRACCARE UNA PASSWORD DI 6 CARATTERI IN PURE BRUTE È QUESTO

FCRACKZIP -V -U -B -C 'AA1' -MIN 6 -MAX 6 /PERCORSO/ARCHIVIO.ZIP

SAMDUMP

SAMDUMP2 //HOSTNAME/C$/WINDOWS/SYSTEM32/CONFIG/SYSTEM
//HOSTNAME/C$/WINDOWS/SYSTEM32/CONFIG/SAM -U USERNAME -P PASSWORD > DUMP.TXT

Installiamo GVM

Greenbone

1 Installiamo la piattaforma

sudo apt install gvm

2 Inizializziamo GVM

sudo gvm-setup

ATTENZIONE A PRENDERE LA PASSWORD CREATA PER IL LOGIN

3 Controlliamo i servizi

sudo gvm-check-setup

4 Aggiorniamo i feed

sudo gvm-feed-update

5 Ci connettiamo al https://127.0.0.1:9392

Quando facciamo ripartire il Sistema, per far partire GVM dobbiamo digitare

sudo gvm-start