SIS

PROF. ROSELLI SERGIO

DOCENTE DI LAB. INFORMATICA , SISTEMI E RETI

KALI LINUX e RASPBERRY PY :
ACCOPPIATA PER LA SICUREZZA INFORMATICA E IL CYBER HACKING

In questa guida vedremo come con un **Raspberry Pi** ed il sistema operativo **Kali Linux** sia possibile realizzare una station da poter utilizzare in operazioni come :

- Man-In-The-Middle (MITM);
- Attack Wireless Network.
- Sniffer;

Dobbiamo installare sul Raspeberry Pi una distribuzione di Kali Linux, ottenendo in questo modo un dispositivo al quale collegarci da remoto e poter eseguire uno degli attacchi prescelti (ovviamente a scopo didattico). L'immagine di Kali linux per processori ARM è già ottimizzata per Raspeberry Pi.

NOTA
Se utilizziamo una delle ultime versioni di Raspeberry, non avremo bisogno di schede Wi-Fi USB, in quanto già istallata sul dispositivo.

CONFIGURAZIONE HARDWARE

Digitiamo quindi da terminale il comando:

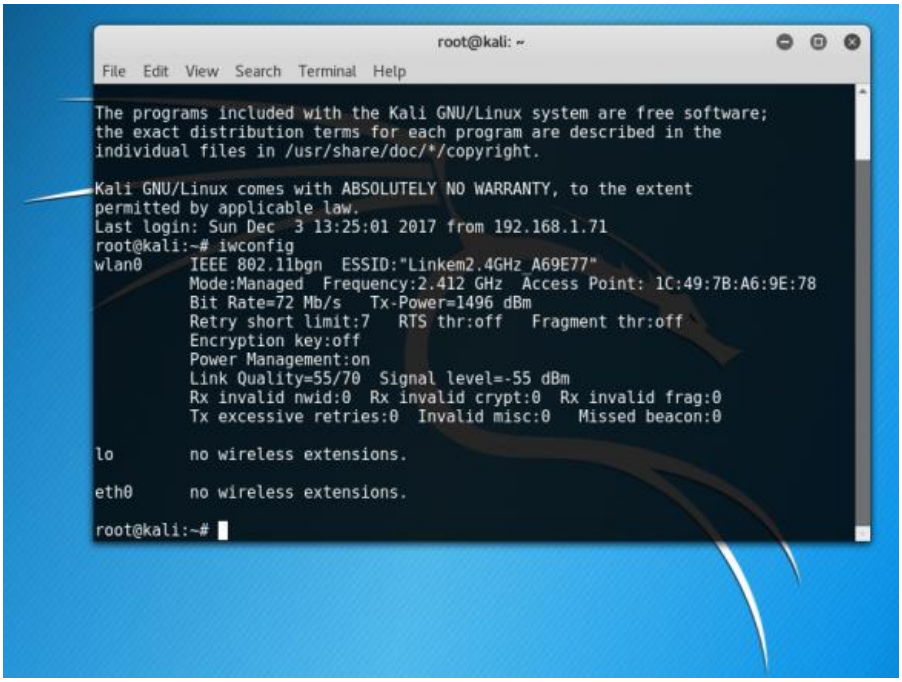
```
iwconfig
```

Attiviamo quindi la scheda Wi-Fi se spenta :

```
ifconfig wlan0 up
```

di seguito cosa apparirà a video

Figura 1

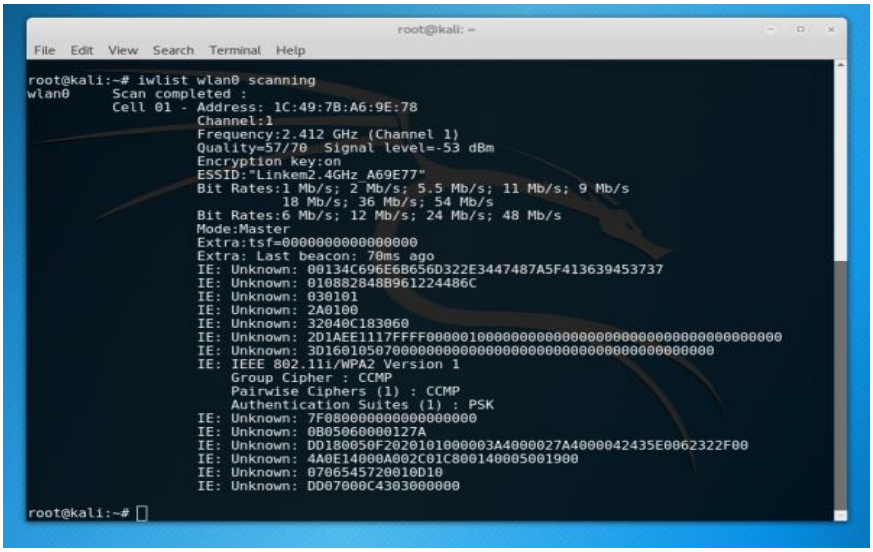


INDIRIZZO DI POSTA ELETTRONICA

Siamo pronti per eseguire una scansione alla ricerca di reti Wi-Fi nelle vicinanze. Digitiamo da terminale il comando:

iwlist wlan0 scanning

Figura 2. Scansione delle reti disponibili



Il comando digitato mostrerà il SSID ed il MAC Address associato ai punti di accesso trovati. Nel nostro caso, è stata trovata una rete wireless *Lab* con indirizzo MAC *1C:49:7B:A6:9E:78*. Prendiamo nota delle informazioni, ci serviranno in seguito.

AVVIO SERVIZIO "SECURE SHELL" (SSH)

Il servizio **Secure Shell** (**SSH**) è importante se vogliamo avere l'accesso al Raspeberry Pi da postazione remota. (È il modo più comune per gestire in remoto sistemi Linux, mediante la riga di comando) in questo modo l'interfaccia grafica di Kali Linux non sarà necessaria.

Verifichiamo se sul nostro Kali il servizio SSH è installato ed attivo :

```
service --status-all
```

Figura 3. Verifica stato di SSH

Se nella prima colonna è presente un "+" allora il servizio SSH è installato ed attivo, diversamente sarà necessario installare il server OpenSSH.

Per installare il server OpenSSH, digitiamo il comando:

```
apt-get install openssh-server
```

Terminata l'istallazione, sarà necessario avviare i servizi SSH :

```
service ssh start
```

Abbiamo terminato, il nostro Raspeberry ora è pronto per l'uso.

Ecco alcuni degli strumenti e tool di cyber security ed hacking che possono essere utilizzati con il raspberry pi 3 e kali linux:

nmap: tool di sicurezza basico ma molto potente. Si tratta di un programma nativo, già presente all'interno della distribuzione kali linux. Nmap è un network security scanner che esercita la funzione di port scanning all'interno di qualsiasi macchina server. Lanciando e indirizzando questo programma verso un server specifico si avrà la possibilità di inviare una richiesta icmp ad ogni porta ed ottenere in output la lista delle porte ed il loro stato effettivo (aperta/chiusa).
Ncrack: altro programma nativo di kali linux, ma molto più potente. Questo tool è stato creato appositamente per poter permettere alla aziende di testare i propri server e verificare se questi sono a prova di hacker oppure se hanno qualche falla. E' inutile dire che molti utenti lo utilizzano per scopi totalmente diversi da quelli per il quale è stato progettato. Richiede l'esecuzione a riga di comando, permettendo di forzare l'accesso ad una qualsiasi porta aperta del server bersaglio, ammesso che ce ne sia qualcuna aperta ed utilizzabile).

Metasploit: programma nativo di kali linux, è uno dei tool più potenti che un esperto informatico dovrà conoscere e saper utilizzare. Questo tool è un archivio di exploit dai differenti funzionamenti ed anche una risorsa fondamentale per imparare qualcosa di sicurezza informatica. L'utilizzo degli exploit è vastissima, imparare ad utilizzare gli exploit presenti in metasploit è importantissimo per chi vuole imparare ad adattarsi in diverse situazioni e raggiungere determinati obiettivi ;)

Armitage: è utile per l'utente, che vuole risparmiare tempo e fatica. Il programma è anche lui nativo di kali linux e permette di visualizzare, dopo aver correttamente configurato, un interfaccia grafica comoda che racchiude le funzioni testuali citate prima (ncrack, nmap, metasploit) e molte altre che possono essere utilizzate dunque in maniera più semplice. Non è comunque da sottovalutare.

Openvas: altro programma importante che permette all'utente di analizzare ogni angolo delle lan bersaglio, locali e remote mettendone in vista le vulnerabilità. Questo programma come armitage include un interfaccia grafica elementare.

INDIRIZZO DI POSTA ELETTRONICA

CONCLUSIONI

Abbiamo configurato un Raspeberry Pi in modo da trasformarlo in un piccolo e potente dispositivo di hacking che potrebbe essere utilizzato come “falso” punto di accesso Wi-Fi, oppure per effettuare un attacco Man in the Middle o ancora “sniffare” pacchetti di una connessione.

Con pochi euro, un perfetto sconosciuto potrebbe impadronirsi di password, dati di carte di credito, numeri telefonici, credenziali, indirizzi di posta elettronica e molto altro. Questo articolo ha lo scopo di sensibilizzare gli utenti a diffidare di connessioni libere di cui non si conosce il reale gestore.

Nota: questo articolo ha uno scopo educativo, tutti i test sono stati eseguiti in ambiente di laboratorio. Eventuali tentativi di replica su siti web o indirizzi IP pubblici costituiscono reato informatico.

INDIRIZZO DI POSTA ELETTRONICA