# Analisi delle vulnerabilità: Porte della metasploitable

## scanner:

L'obiettivo dell'esercizio è quello di fornire una **Vulnerability Assessment** (Valutazione delle vulnerabilità) che non è altro di una revisione manuale e quindi più approfondita della **Vulnerability Scanner** (Scanner di vulnerabilità) è uno strumento software automatizzato che esegue una scansione di un sistema o di una rete alla ricerca di vulnerabilità conosciute. Quindi si unisce la scansione automatica con l'analisi manuale per valutare la sicurezza di sistema con le specifiche di una determinata azienda e gestire la gravità del pericolo per una eventuale pianificazione delle soluzioni o penetration test.

## Vulnerability Scanner

### a) Passaggi vulnerability scanner

Come strumento di scanner andremo ad utilizzare Nessus, come da prassi è uno strumento che va sempre aggiornato periodicamente per avere dei database sempre fornito dei nuovi controlli.
**Nessus** è uno strumento molto usato essendo potente e semplice da usare ci fornisce molte opzioni di utilizzo dei quali i passaggi principali sono:

1) **port scanning**
2) **service detection**
3) **ricerca nel vulnerability database**
4) **test**

### b) Architettura Nessus

Nessus ha due componenti principali: un server e un client.

1) Il client: configura le scansioni per determinare i target ip e le modalità di scansione e test.
2) Il server: si occupa di effettuare i test sugli obiettivi specificati dal client.
3) Al termine delle scansioni il server confronta le risposte con il proprio database di vulnerabilità.

### c) Struttura della rete

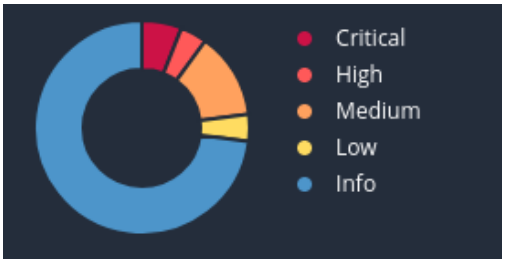
All'interno di una **rete interna** andremo ad utilizzare Nessus con il sistema operativo Kali, per analizzare le vulnerabilità di sicurezza delle porte della macchina metasploitable presente all'interno della stessa rete interna, all'epicentro della quale troviamo la Pfsense che definisce i collegamenti con le macchine interessate.

# Vulnerability Assessment

## a) report vulnerability scanner

al termine del vulnerability scanner il programma automatizzato ci restituirà un report delle valutazioni grazie all'utilizzo del database delle vulnerabilità, elencando quali vulnerabilità sono più critiche divise per colore di priorità, troviamo i parametri:

- Critical
- High
- Medium
- Low
- Info

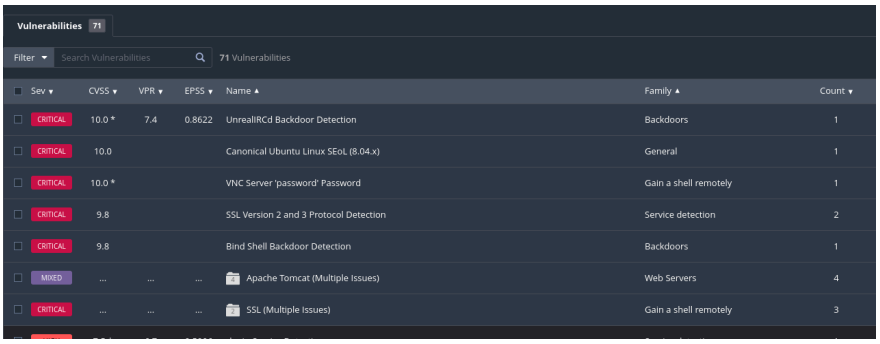



Il report che andremo ad analizzare contiene:

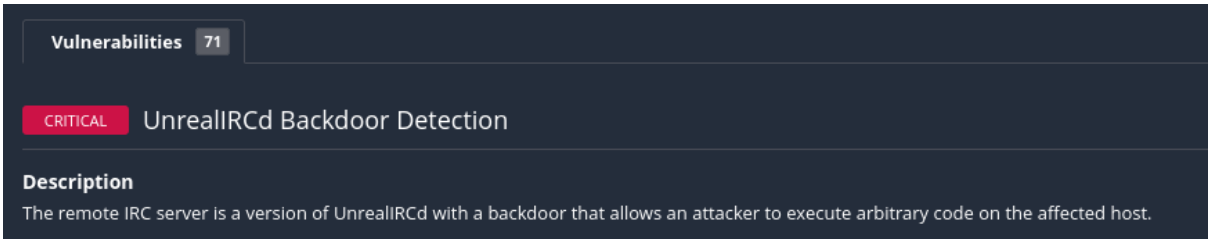
- Una soluzione.
- Fattore rischio.
- Score nel sistema CVSS.
- Informazioni sul plugin di Nessus che ha identificato la vulnerabilità.

## b) Nessus

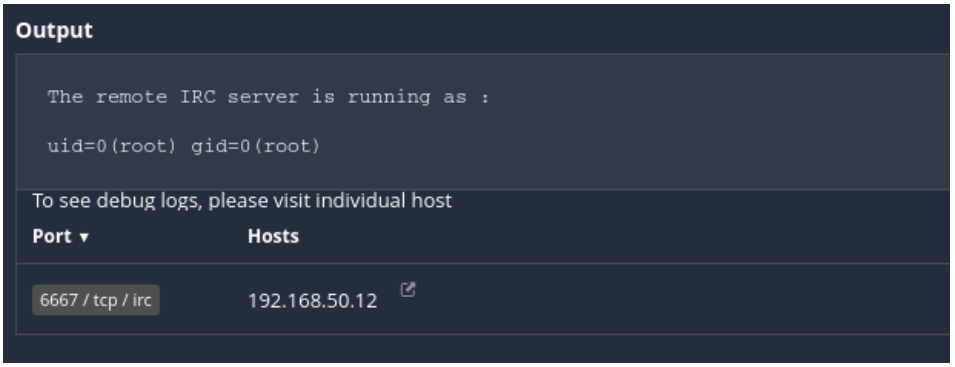
Andando a esaminare quella che è la scansione delle vulnerabilità che abbiamo trovato su metasploitable troviamo la il seguente risultato:




## b0) Rilevamento backdoor UnrealIRCd

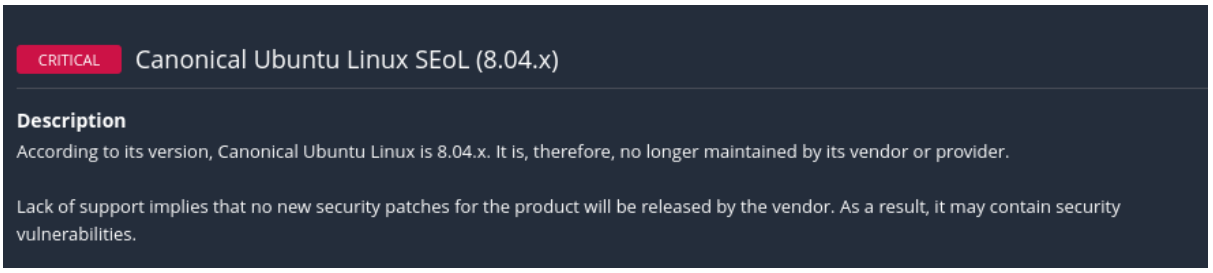



**descrizione:** ci dice che Il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente a un aggressore di eseguire codice arbitrario sull'host interessato. Più nel dettaglio è una versione di molto tempo fa e la backdoor consente a chiunque di eseguire qualsiasi comando con i privilegi dell'utente indipendentemente dalle restrizioni. di fatto è una vulnerabilità estremamente pericolosa a cui diamo estrema priorità.

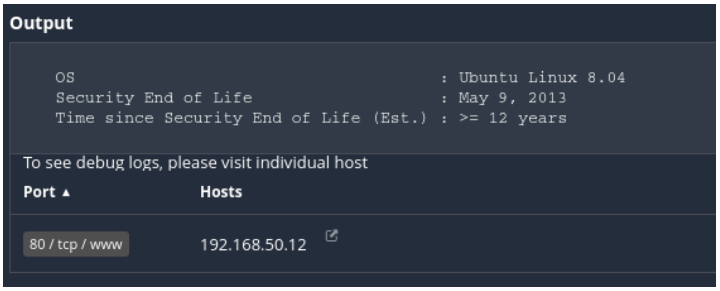



**soluzione:** infatti consiglia di Scaricare nuovamente il software e verificarlo utilizzando i checksum MD5/SHA1 pubblicati e reinstallarlo.

## b1) Canonical Ubuntu Linux SEoL (8.04.x)

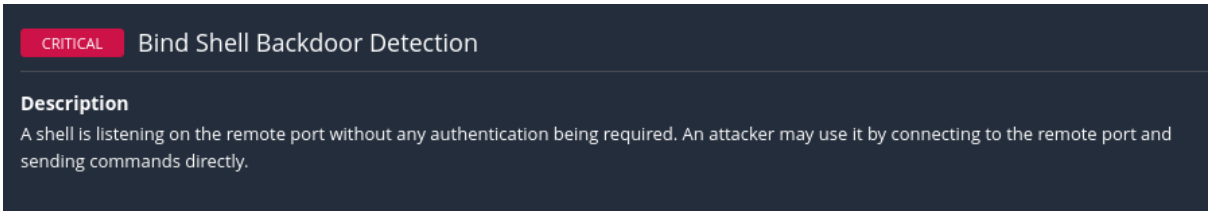



**descrizione:** in quest'altra vulnerabilità critica ci dice che la versione di Canonical Ubuntu Linux versione 8.04.x, non è più supportata dal suo fornitore, ciò implica che questa versione non è più all'avanguardia per la sicurezza e potrebbe essere fonte di molte vulnerabilità.




**soluzione:** quindi ci consiglia di aggiornare Canonical Ubuntu Linux con una versione attualmente supportata.

## b2)Bind Shell Backdoor Detection




**descrizione:** qui ci avverte di una shell che è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Quindi un aggressore può utilizzarla connettendosi alla porta remota e inviando comandi direttamente.


**soluzione:** ci consiglia di verificare se l'host remoto è stato compromesso e reinstallare il sistema se necessario.

## Conclusione

Il Vulnerability Assessment è una parte essenziale della fase di raccolta informazioni del Penetration Testing, è la parte dove si unisce l’automazione della macchina con la manualità del hacker e ottenere un risultato estremamente dettagliato delle vulnerabilità di interesse.
Al termine di questa fase avremo un quadro generale completo della struttura e delle vulnerabilità del nostro target, non che l’inizio della fase successiva, il vero e proprio attacco.