Esercitazione S5L3

In questa esercitazione vediamo nel dettaglio il funzionamento di un vulnerability scanner e l'analisi dei risultati ottenuti da una scansione di una macchina target.

Nessus: spiegazione

Nessus è un software vulnerability scanner in grado di analizzare in modo dettagliato una macchina. La sua forza è quella di fornirci oltre a dei dati oggettivi anche delle informazioni dettagliate sulla macchina target.

Il funzionamento di Nessus consiste nell'inviare dei pacchetti in grado, in base alle risposte, di determinare:

- ping
- porte aperte
- applicazioni
- registri (aggiornamenti)
- servizi attivi sulle porte aperte
- versioni dei servizi.

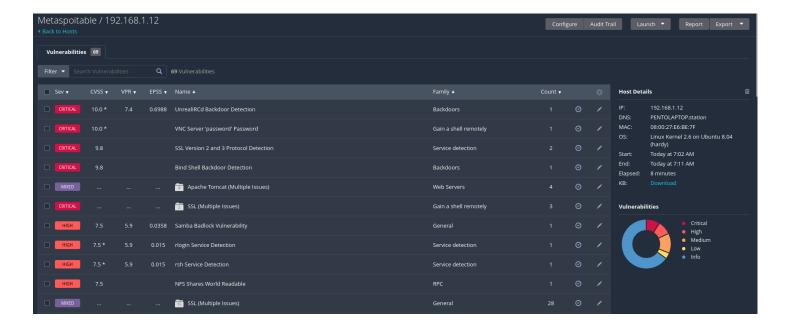
In più, oltre a queste già importanti funzionalità, è in grado di fare una fase di exploit alla macchina. La fase di exploit consiste nell'attaccare la macchina cercando le vulnerabilità. Nessus è anche in grado di dare un report sulle vulnerabilità trovate classificandole per pericolosità. Ovviamente queste fasi possono richiedere un largo utilizzo della banda, in situazioni nel quale le scansioni debbano essere effettuate per conto di un'azienda è bene tener conto di questa informazione e accordarsi per trovare uno o più giorni utili per effettuare i test.

Nessus: funzionamento

Impostando un IP di destinazione (in questo caso ho utilizzato Metaspoitable come target) e eventualmente customizzando la scannerizzazione si può iniziare la scansione. In questo caso ho utilizzato lo scan base.

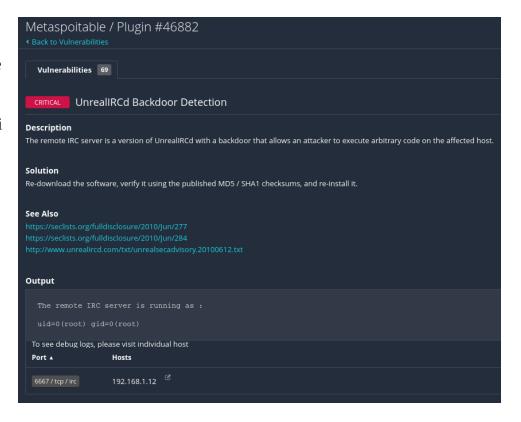
Nessus: risultati

Finita la scansione ho ottenuto il report dello scan e sono state trovate diverse vulnerabilità:

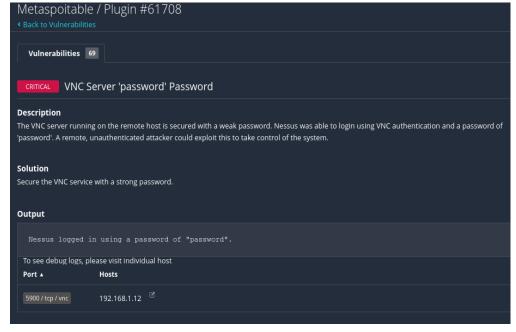


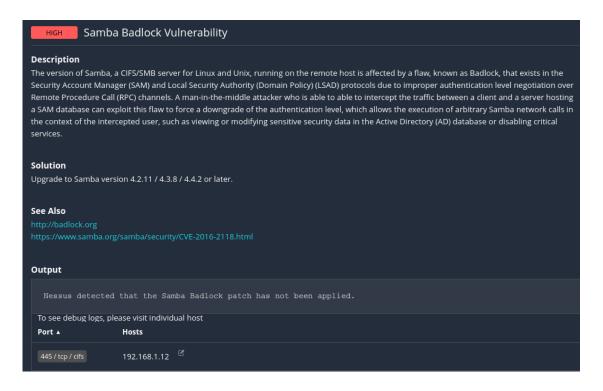
Come si può vedere dall'immagine precedente si ha un elenco di vulnerabilità ordinate per criticità.

Aprendo nel dettaglio una criticità possiamo notare che il software in automatico ci fornisce una descrizione del problema, una soluzione, dei link utili per il dettaglio e la risoluzione del programma, l'output e la porta dove è stata trovata la vulnerabilità.



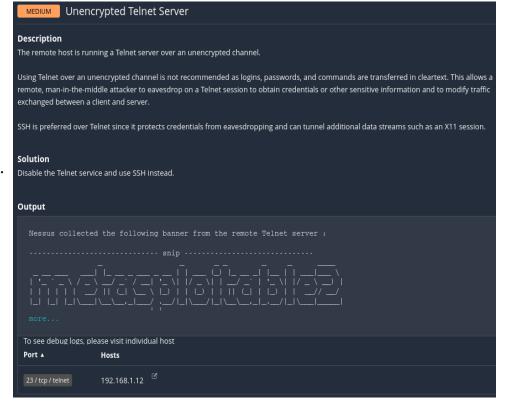
In questo caso ad esempio ci dice ceh il VNC server è protetto da una password molto semplice e ci consiglia di assicurare il VNC server con una password più sicura.





In quest'altro caso invece è stata trovata una vulnerabilità sulla porta 445 e corrisponte al protocollo Samba. La criticità trovata in questo caso è una versione obsoleta del protocollo ed è ovviamente vulnerabile. Ci consiglia quindi l'aggiornamento del protocollo Samba.

Come ultimo caso ho preso in esame una vulnerabilità non critica ma valutata come "MEDIUM" e ci dice che è attivo il servizio Telnet sulla porta 23. Come soluzione ci consiglia di disabilitare il protocollo Telnet e usare il protocollo SSH in sostituzione.



Come si può notare le vulnerabilità vengono classificate più o meno critiche, e questo può farlo automaticamente grazie a una sua tabella o a un suo database dove và a confrontare i risultati ottenuti .