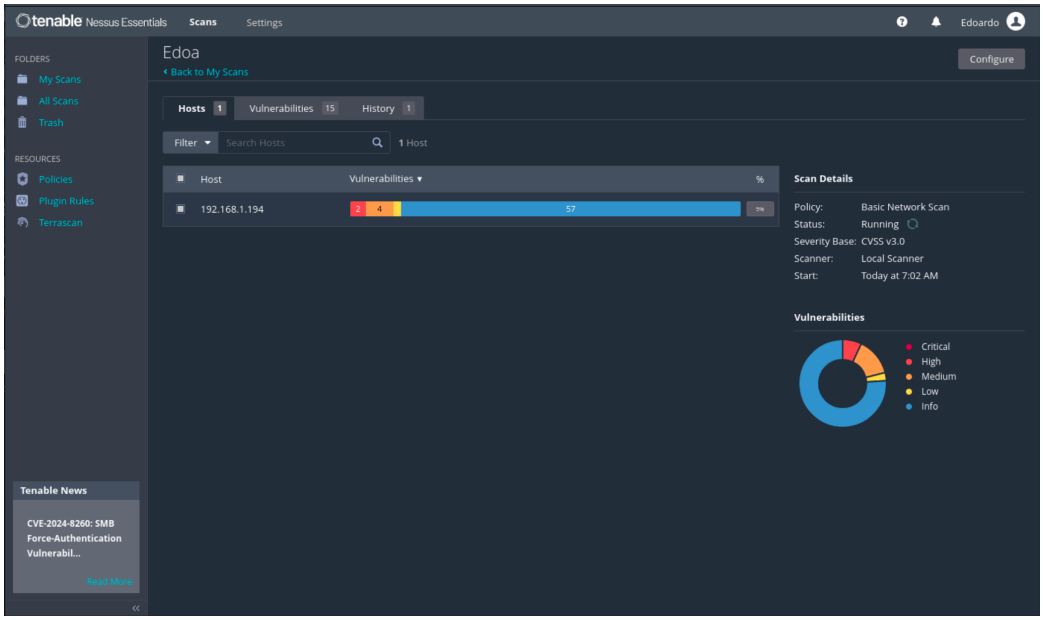
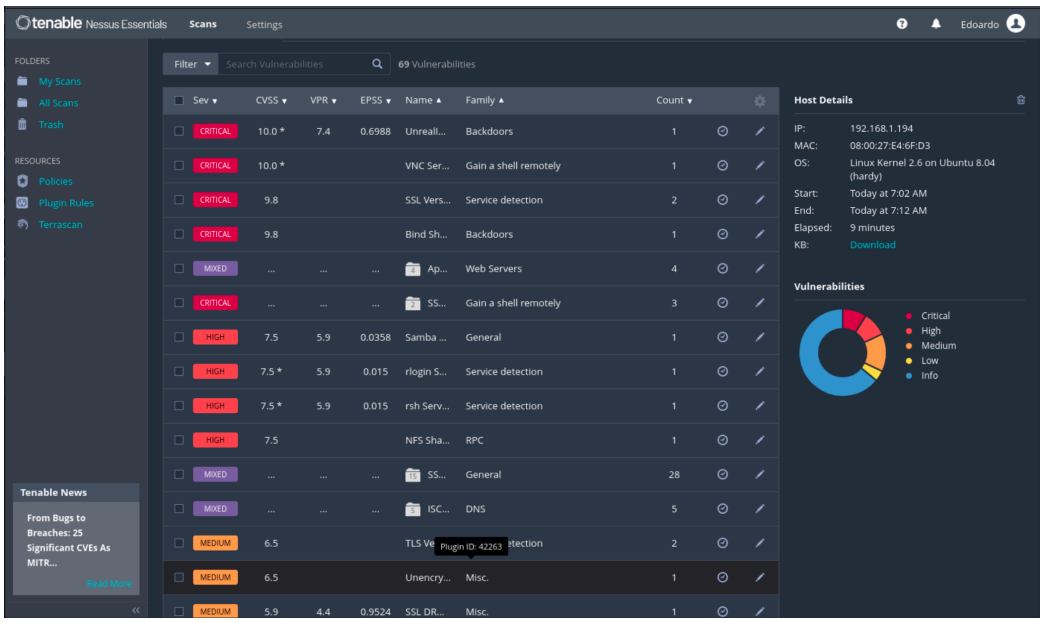
Introduzione
L'obbiettivo di questo esercizio è stato effettuare un vulnerability Scanning sulla macchina Metasploitable utilizzando lo strumento Nessus. Durante l'esecuzione, ho monitorato il progresso e ho atteso il completamento della scansione, assicurandomi che tutte le porte specificate fossero analizzate. La scansione ha impiegato un tempo ragionevole, fornendo risultati dettagliati.

Una volta raggiunta l'interfaccia web per la configurazione della scansione ho selezionato una delle scansioni predefinite, in questo caso "Basic Network Scan", in alternativa, si potrebbe pensare di scegliere «Advanced Scan» e configurare manualmente tutte le «policy» della nostra scansione.
Nella sezione "Basic" sono stati inserite le informazioni generali come il nome e il target, nello specifico l'indirizzo IP della macchina di Metasploitable: 192.168.1.194.
Nella sezione "discovery" invece è stato inserita la modalità del Port scanner, dove si può scegliere uno di default "port scan common ports o all ports" oppure optare per una configurazione custom, in questo caso è stato scelto "all ports"

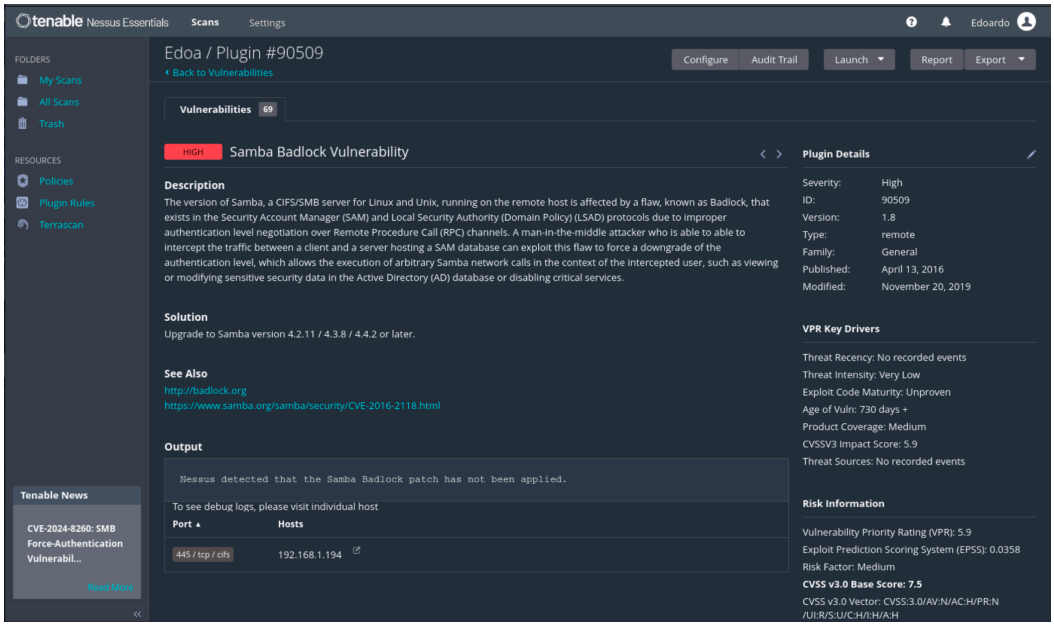




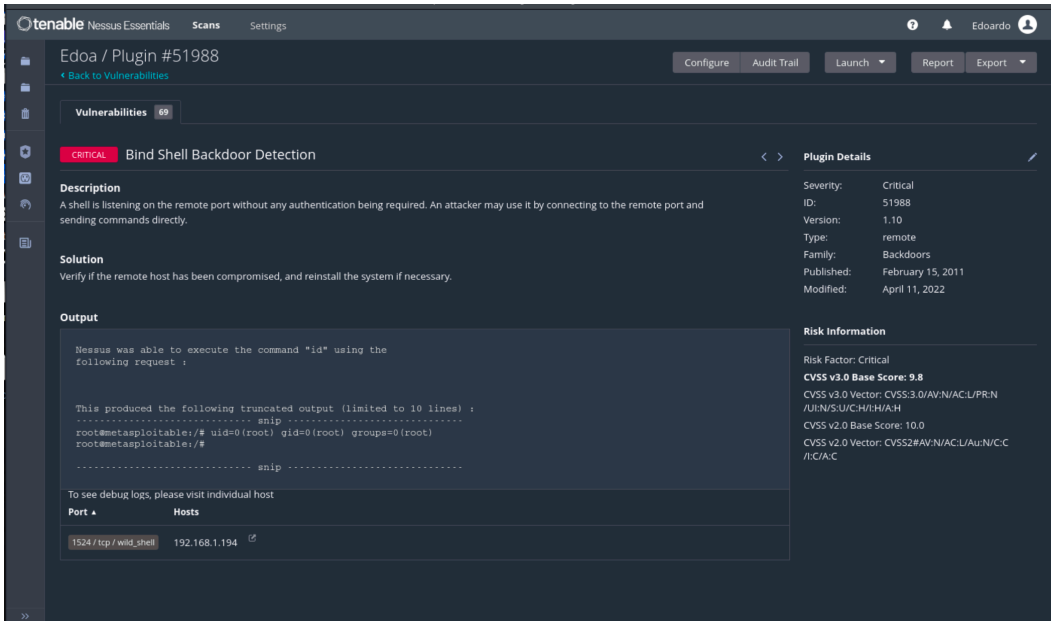
La prima informazione contenuta nel report è una vista sulle vulnerabilità trovate divise per colore / priorità: Critical, High, Medium, Low, Info.

5 VULNERABILITA’

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto ha un difetto, noto come Badlock. Un utente malintenzionato man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete.



il server IRC remoto è una versione. di unrealRCd con una backdoor che consente a un utente malintenzionato di eseguire codice arbitrario sull'host interessato



Il servizio SMTP remoto contiene un difetto software che potrebbe consentire a un utente malintenzionato da remoto e senza autenticazione di inserire comandi durante la fase del protocollo di testo in chiaro che verranno poi eseguiti durante nella fase del protocollo di testo cifrato.
Uno sfruttamento riuscito potrebbe consentire a un utente malintenzionato di rubare l'e-mail di una vittima o il SAL associato (Simple Authentication and Security Layer)