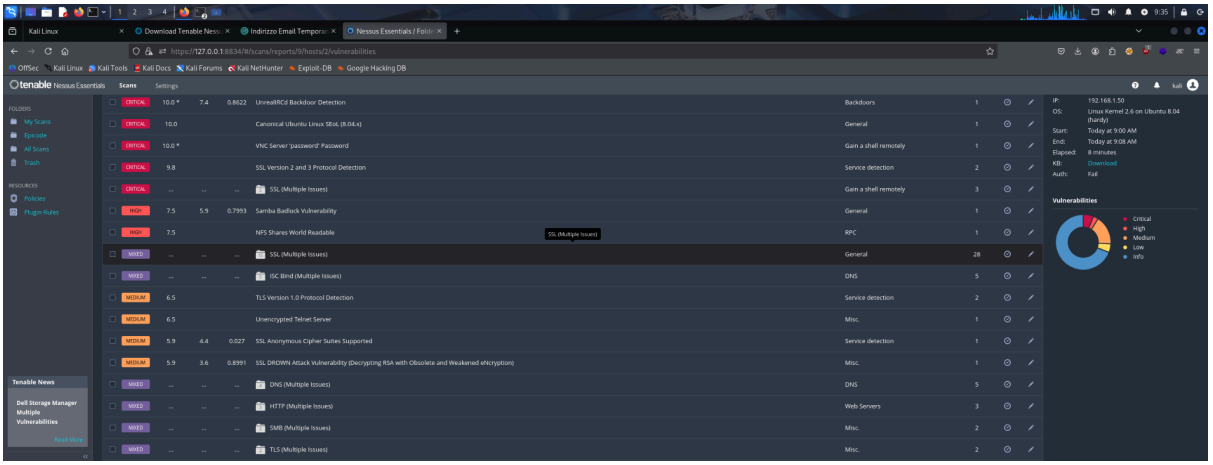
Scansione di Metasploitable con Nessus



Executive Summary

Questo report documenta i risultati di un Vulnerability Assessment condotto tramite Tenable Nessus Essentials su un sistema Linux legacy. L'analisi ha evidenziato un livello di rischio critico, con vulnerabilità che consentono la compromissione remota completa del sistema. Il documento fornisce inoltre una spiegazione tecnica del rilevamento di porte non esplicitamente incluse nel range di scansione configurato.

Obiettivi e ambito dell'analisi

L'obiettivo dell'attività era valutare la postura di sicurezza del sistema target attraverso una scansione non autenticata. Il test è stato eseguito esclusivamente a fini didattici, senza sfruttamento attivo delle vulnerabilità identificate.

Metodologia

1. Strumento utilizzato: Tenable Nessus Essentials
2. Tipologia di scansione: Basic Network Scan
3. Protocollo di scansione: TCP
4. Port scanning: limitato a porte selezionate
5. Autenticazione: non utilizzata

Informazioni sul sistema analizzato

Indirizzo IP: 192.168.1.50
Sistema operativo rilevato: Linux Kernel 2.6 su Ubuntu 8.04 (Hardy)
Tipologia sistema: Host Linux legacy
Durata scansione: 8 minut

Analisi delle vulnerabilità critiche

1. UnrealIRCd Backdoor (Critical)
   La presenza di una versione compromessa di UnrealIRCd introduce una backdoor che consente l'esecuzione remota di comandi con i privilegi del servizio. L'impatto è classificabile come compromissione totale del sistema, rendendo questa vulnerabilità una delle più gravi rilevate.

2. VNC con password di default (Critical)
   Il servizio VNC risulta configurato con credenziali deboli o di default. Un attaccante può ottenere accesso remoto all'interfaccia grafica del sistema, con potenziale escalation dei privilegi.
3. Protocolli SSL obsoleti (Critical)
   Il supporto a SSLv2 e SSLv3 espone il sistema ad attacchi crittografici noti, tra cui POODLE e DROWN, che compromettono la riservatezza delle comunicazioni.

Vulnerabilità ad alto e medio rischio

1. Samba Badlock: rischio di attacchi Man-in-the-Middle sul protocollo SMB.
2. TLS 1.0 abilitato: protocollo deprecato.
3. Telnet non cifrato: esposizione delle credenziali in chiaro.

Analisi del rilevamento di porte non configurate

Il rilevamento di vulnerabilità associate a porte non esplicitamente incluse nel port range è attribuibile all'architettura plugin-based di Nessus. Una volta identificato un servizio principale, alcuni plugin analizzano porte dinamiche o secondarie dichiarate dal servizio stesso, senza eseguire un port scan tradizionale.

Raccomandazioni

1. Aggiornamento o dismissione del sistema operativo legacy
2. Disabilitazione dei servizi non necessari.
3. Rimozione di protocolli e cifrari obsoleti.
4. Applicazione delle best practice di hardening.

Conclusioni finali

Il sistema analizzato presenta una superficie di attacco estremamente ampia e non è idoneo all'utilizzo in un contesto produttivo. Le vulnerabilità individuate dimostrano l'importanza di un corretto processo di vulnerability management.