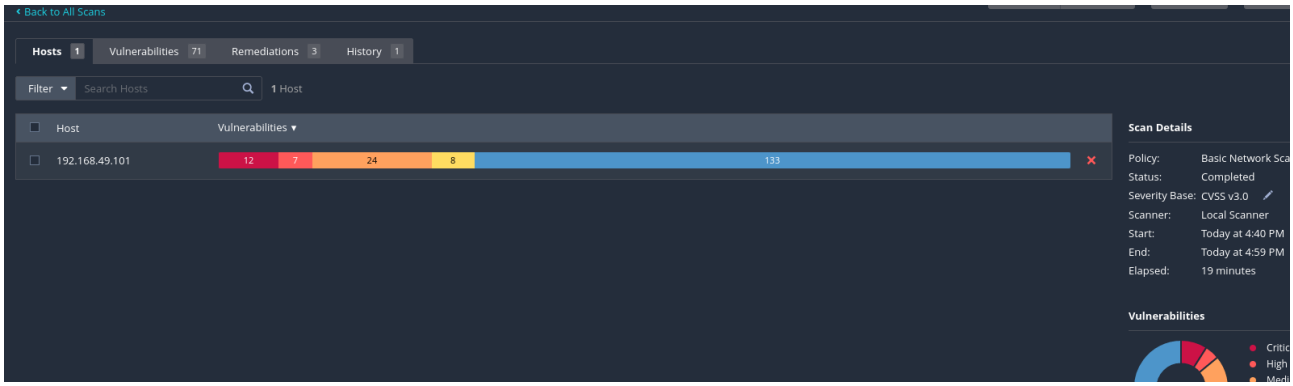
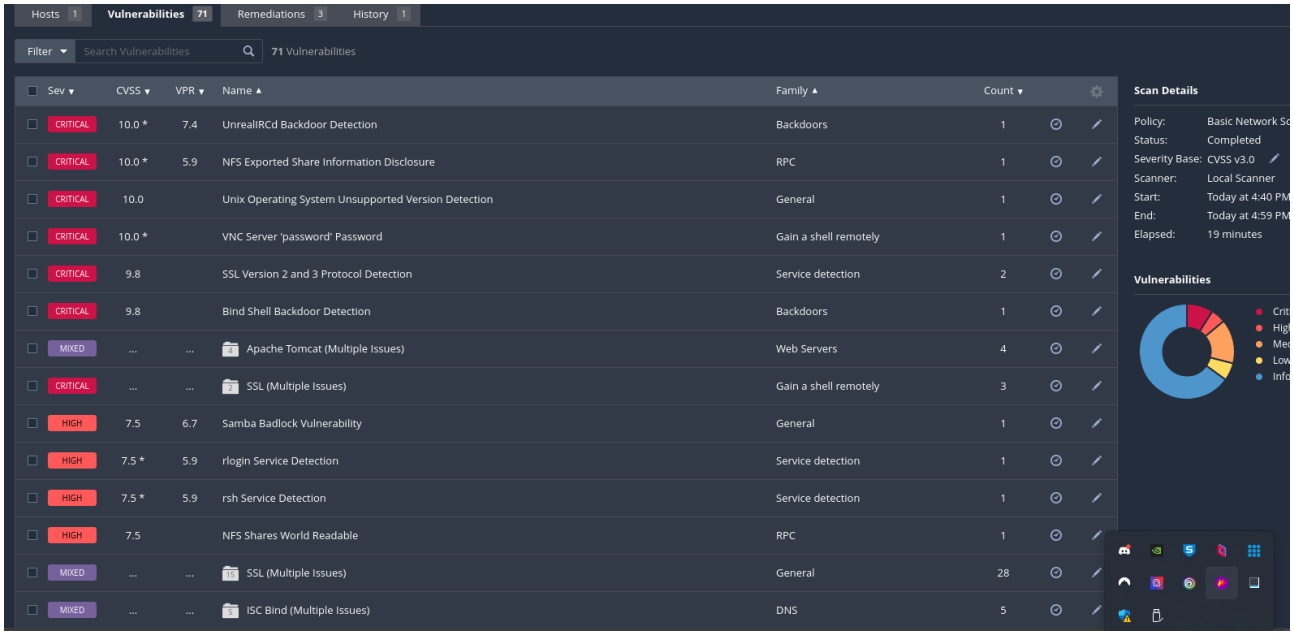
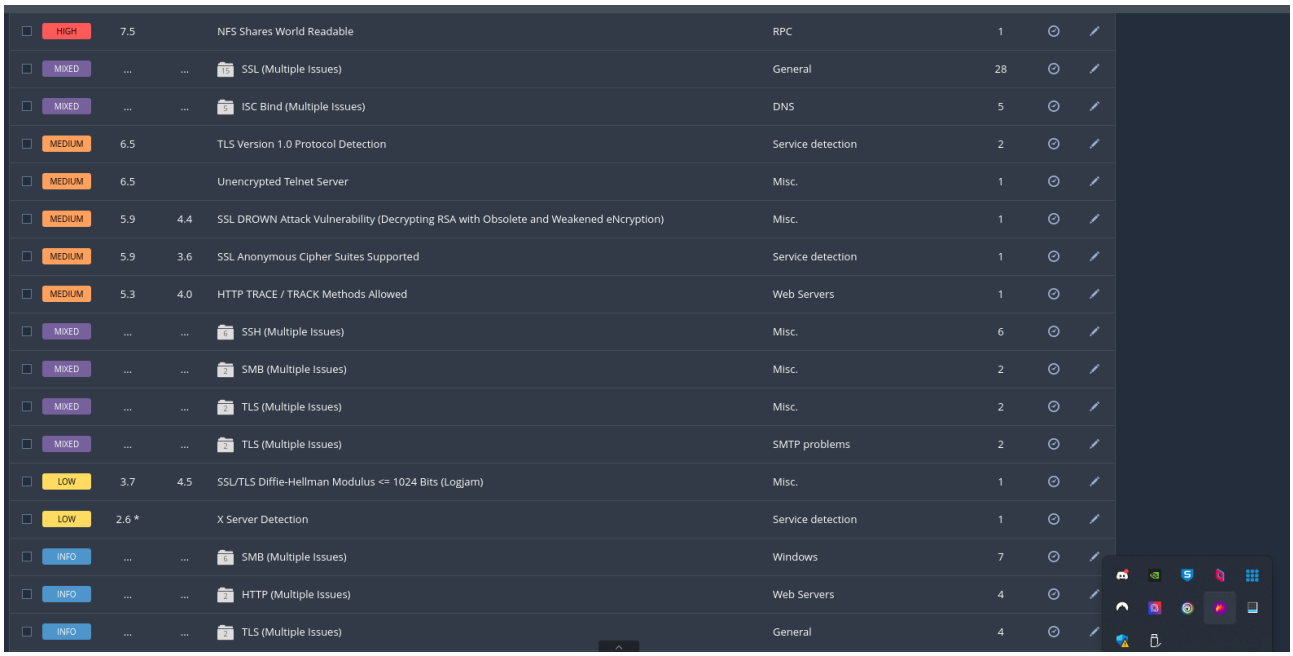
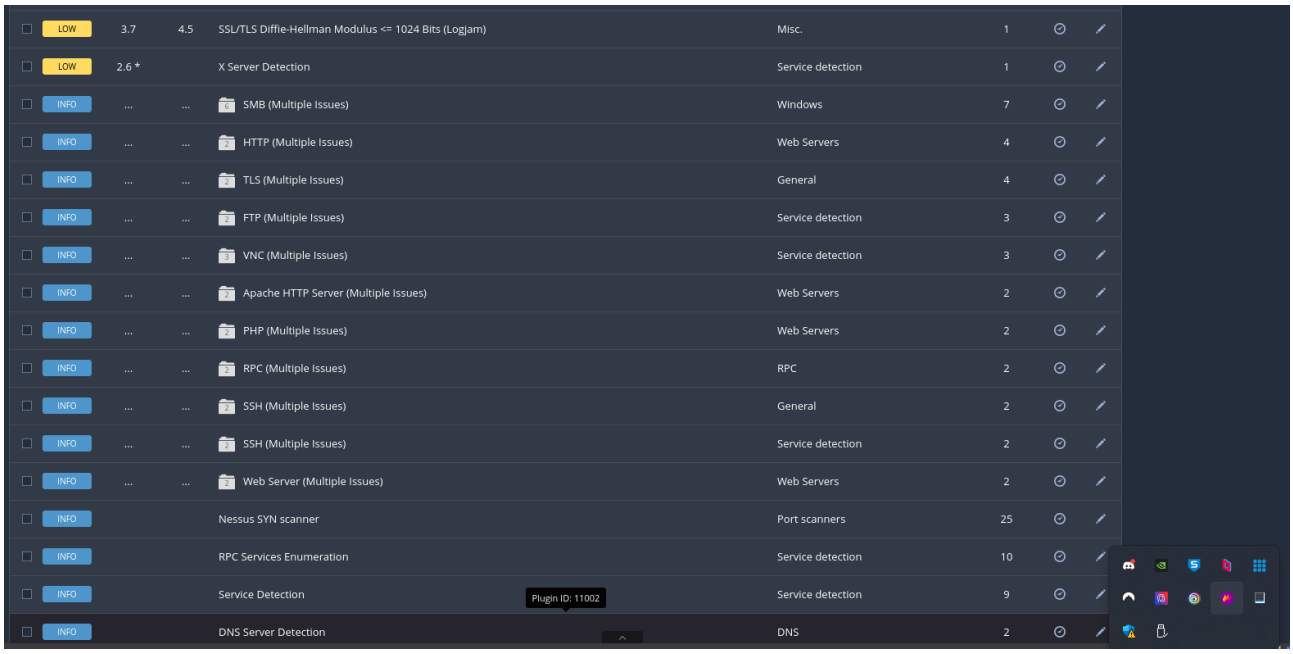
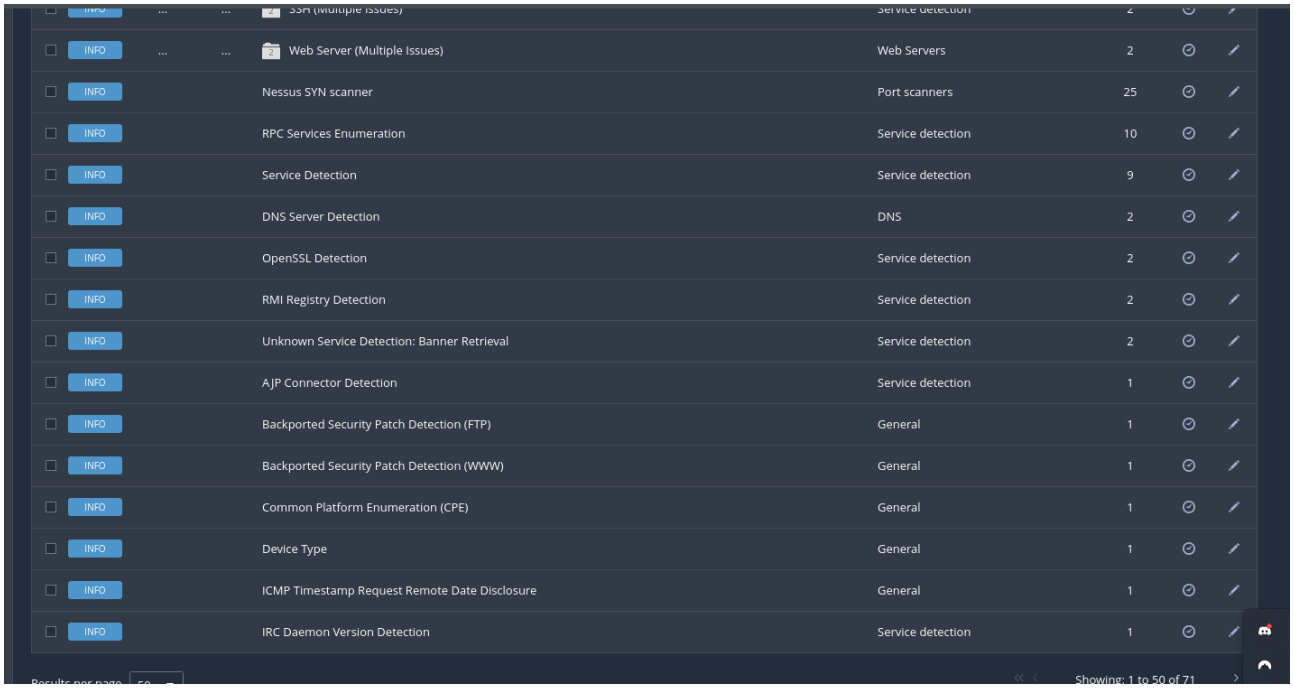

Back to All Scans
Hosts 1
Vulnerabilities 71
Remediations 3
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.49.101
12
7
24
8
133
Scan Details
Policy: Basic Network Sca
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:40 PM
End: Today at 4:59 PM
Elapsed: 19 minutes
Vulnerabilities


Hosts 1
Vulnerabilities 71
Remediations 3
History 1
Filter
Search Vulnerabilities
71 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
CRITICAL 10.0 * 7.4 UnrealIRCd Backdoor Detection Backdoors 1
CRITICAL 10.0 * 5.9 NFS Exported Share Information Disclosure RPC 1
CRITICAL 10.0 Unix Operating System Unsupported Version Detection General 1
CRITICAL 10.0 * VNC Server 'password' Password Gain a shell remotely 1
CRITICAL 9.8 SSL Version 2 and 3 Protocol Detection Service detection 2
CRITICAL 9.8 Bind Shell Backdoor Detection Backdoors 1
MIXED ... ... Apache Tomcat (Multiple Issues) Web Servers 4
CRITICAL ... ... SSL (Multiple Issues) Gain a shell remotely 3
HIGH 7.5 6.7 Samba Badlock Vulnerability General 1
HIGH 7.5 * 5.9 rlogin Service Detection Service detection 1
HIGH 7.5 * 5.9 rsh Service Detection Service detection 1
HIGH 7.5 NFS Shares World Readable RPC 1
MIXED ... ... SSL (Multiple Issues) General 28
MIXED ... ... ISC Bind (Multiple Issues) DNS 5
Scan Details
Policy: Basic Network Sc
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:40 PM
End: Today at 4:59 PM
Elapsed: 19 minutes
Vulnerabilities


HIGH 7.5 NFS Shares World Readable RPC 1
MIXED ... ... SSL (Multiple Issues) General 28
MIXED ... ... ISC Bind (Multiple Issues) DNS 5
MEDIUM 6.5 TLS Version 1.0 Protocol Detection Service detection 2
MEDIUM 6.5 Unencrypted Telnet Server Misc. 1
MEDIUM 5.9 4.4 SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) Misc. 1
MEDIUM 5.9 3.6 SSL Anonymous Cipher Suites Supported Service detection 1
MEDIUM 5.3 4.0 HTTP TRACE / TRACK Methods Allowed Web Servers 1
MIXED ... ... SSH (Multiple Issues) Misc. 6
MIXED ... ... SMB (Multiple Issues) Misc. 2
MIXED ... ... TLS (Multiple Issues) Misc. 2
MIXED ... ... TLS (Multiple Issues) SMTP problems 2
LOW 3.7 4.5 SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) Misc. 1
LOW 2.6 * X Server Detection Service detection 1
INFO ... ... SMB (Multiple Issues) Windows 7
INFO ... ... HTTP (Multiple Issues) Web Servers 4
INFO ... ... TLS (Multiple Issues) General 4





Come si puo vedere Nessus ha evidenziato che la rete scansionata presenta 12 errori critici 7 errori alti 24 errori medi 8 errori bassi e vengono fornite 133 informazioni.

Nfs e un protocollo che permette allà attaccante di scrivere e catturare file .

Si puo inserire un malware allàinterno del server

Quindi mi permette di prender il controllo del server

SSL Version 2 and 3 Protocol Detection

Il servizio remoto accetta connessioni crittografate tramite SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diversi difetti crittografici, tra cui:

- Uno schema di riempimento non sicuro con cifrari CBC.

- Schemi di rinegoziazione e ripresa delle sessioni non sicuri.

Un utente malintenzionato può sfruttare queste falle per condurre attacchi man-in-the-middle o per decrittografare le comunicazioni tra il servizio e i client interessati.

Soluzione

Consultare la documentazione dell'applicazione per disabilitare SSL 2.0 e 3.0.

Usare invece TLS 1.2 (con suite di crittografia approvate) o versioni successive

Samba Badlock Vulnerability

La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, che esiste nei protocolli Security Account Manager (SAM) e Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione impropria del livello di autenticazione sui canali RPC (Remote Procedure Call). Un utente malintenzionato man-in-the-middle in grado di intercettare il traffico tra un client e un server di hosting un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come la visualizzazione o la modifica di dati di sicurezza sensibili nel database Active Directory (AD) o la disabilitazione di servizi critici.

Soluzione

Aggiornamento a Samba versione 4.2.11 / 4.3.8 / 4.4.2 o successiva