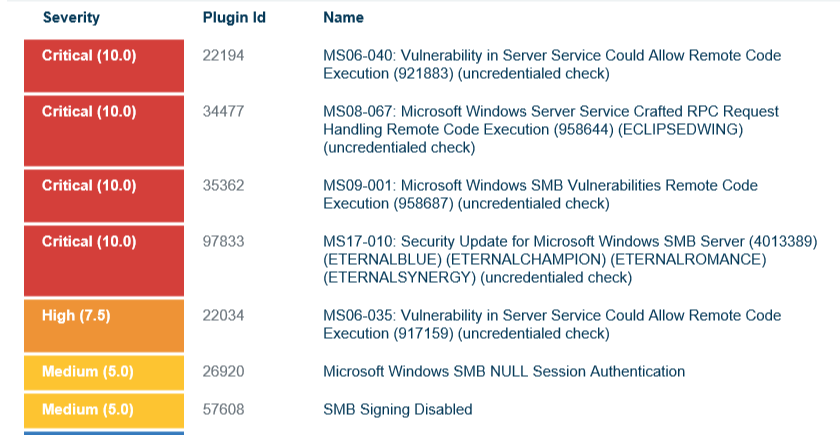
**Nessus scan (https://www.youtube.com/watch?v=5jvNYzkPkRo)**

**Omschrijving van de vulnerabilities WINDOWS XP zonder FIREWALL**



Critical:

* MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution

Omschrijving:

* Een aanvaller kan willekeurige code kan uitvoeren op de host op afstand met 'SYSTEM' privileges.

Oplossing:

* Windows besturingssysteem updaten/Firewall aanzetten

Critical:

* MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution

Omschrijving:

* Deze beveiligingslek kan externe code uitgevoerd worden als een systeem dit probleem optreedt en een speciaal ontworpen RPC-verzoek ontvangt. De aanvaller kan dit beveiligingslek zonder verificatie willekeurige code uitvoeren.

RPC-request = Een remote procedure call, kortweg RPC, is een technologie die een computerprogramma op één bepaalde computer toestaat om code uit te voeren op een andere machine zonder dat de programmeur de code expliciet hiervoor geschreven heeft.

Oplossing:

* Windows besturingssysteem updaten/Firewall aanzetten

Critical:

* MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)

Omschrijving:

* De aanvaller die misbruik weet te maken van deze beveiligingslek kan programma’s installeren, bekijken, wijzigen, verwijderen van gegevens of een nieuwe account maken met volledige gebruikersrechten.

Oplossing:

* Windows besturingssysteem updaten/Firewall aanzetten

Critical:

* MS17-010: Security Update for Microsoft Windows SMB Server

Omschrijving:

* Deze beveiligingslek kan leiden tot uitvoering van externe code als een aanvaller RPC-berichten stuurt naar de target host.

Oplossing:

* Windows besturingssysteem updaten/Firewall openen

High:

* MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)

Omschrijving:

* De aanvaller die dit beveiligingslek misbruikt kan op afstand volledige controle krijgen over een systeem waarin dit probleem optreedt. De aanvaller kan vervolgens programma’s installeren, bekijken, wijzigen, verwijderen van gegevens of een nieuwe account maken met volledige gebruikersrechten.

Oplossing:

* Windows besturingssysteem updaten/Firewall openen

Medium:

* Microsoft Windows SMB NULL Session Authentication

Omschrijving:

* Wanneer een programma of een service wordt gestart met ‘System’ user. Dit kan een potentieel beveiligingsrisico zijn omdat het zorgt voor een niet-geverifieerde aanmeldingen bij het systeem. Een hacker kan dit beveiligingslek misbruiken en toegang krijgen tot gevoelige gegevens op het systeem.

Oplossing:

* Windows besturingssysteem updaten/Firewall openen

Medium:

* SMB Signing Disabled

Omschrijving

* Zonder SMB-ondertekeningen kan de ontvanger van SMB-pakketten hun authenticiteit niet bevestigen en hierdoor kunnen er ‘man in the middle’ aanvallen gebeuren.

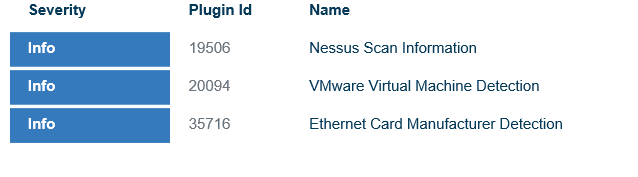
Een man-in-the-middle-aanval is een aanval waarbij informatie tussen twee communicerende partijen onderschept wordt zonder dat beide partijen daar weet van hebben. Hierbij bevindt de computer van de aanvaller zich tussen de twee communicerende partijen.

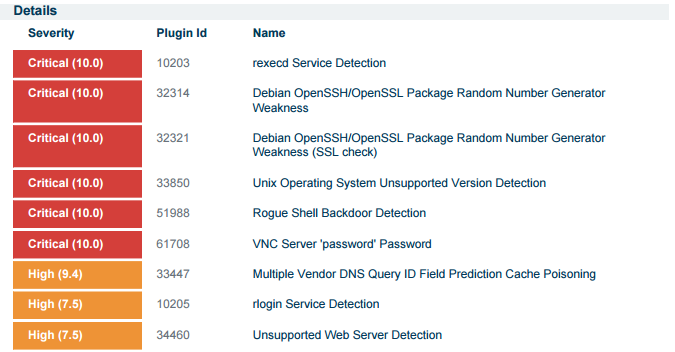
Oplossing:

* Windows besturingssysteem updaten/Firewall openen

**Patchen van bovenstaande vulnerabilities**

Firewall aanzetten

**Omschrijving/oplossingen van 4 vulnerabilities van METASPLOITIBLE OS**



**Critical**:

* rexecd Service Detection

Omschrijving:

* De rexecd-service loopt op de externe host. Deze service is

Ontwerp om gebruikers van een netwerk in staat te stellen externe opdrachten uit te voeren.

Rexecd geeft echter geen goede verificatiemiddelen, dus

Het kan worden misbruikt door een aanvaller om een ​​host van een derde te scannen.

Oplossing:

* Comment out the 'exec' line in /etc/inetd.conf and restart the inetd  
  process.

**Critical**:

* Rogue Shell Backdoor Detection

Omschrijving:

* Een shell luistert op de externe poort zonder enige authenticatie

Nodig zijn. Een aanvaller kan het gebruiken door op de afstand te verbinden

en direct commando’s te verzenden.

Oplossing:

* Het systeem opnieuw installeren

**Critical**:

* VNC Server 'password' Password

Omschrijving:

* De VNC-server die op de externe host wordt uitgevoerd, is beveiligd met een zwak

wachtwoord. Nessus was in staat om in te loggen met behulp van VNC authentication en als

Wachtwoord 'wachtwoord' te gebruiken. Een externe, niet-geverifieerde aanvaller kan

Gebruik maken van dit om de controle van het systeem te nemen.

Oplossing:

* Beveilig de VNC-service met een sterk wachtwoord.

**High**:

* rlogin Service Detection

Omschrijving:

* De rlogin-service loopt op de externe host. Deze service is

Kwetsbaar omdat gegevens tussen de rlogin-client en de server worden overgedragen

In cleartext kan Een man-in-the-middle aanvaller dit gebruiken om

gebruikersnamen en wachtwoorden te vinden. Ook kan het slecht geverifieerde aanmeldingen toestaan zonder wachtwoorden

Oplossing:

* Verwijder de 'login'-regel in /etc/inetd.conf en start de inetd opnieuw

op. Als alternatief kunt u deze service uitschakelen en in plaats daarvan SSH gebruiken.