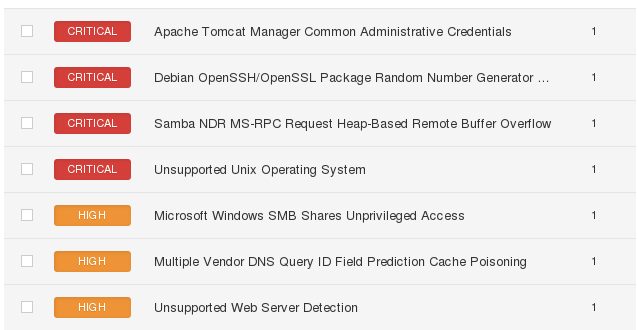
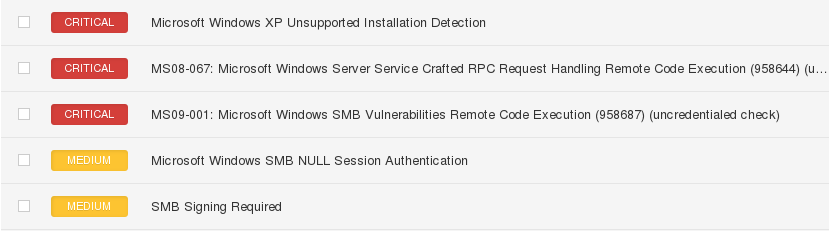
1. 4 Vulnerability from meta os



1. Apache Tomcat Manager Common Administrative Credentials
   1. De gebruikersnaam en wachtwoord zijn ingesteld als standard, dit is makkelijk te patchen door deze te veranderen.
2. Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow
   1. Door een oude versie van Samba, een programma date er voor zorgt dat je met een windows bestanden en printers kunt delen van een unix-systeem, kan je meerdere geheugenoverflows creëren. Deze worden geëxploiteerd door code uit te voeren door de rechten van Samba daemon.
3. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
   1. Het paswoord van de Secure shell is gegenereerd op het system waar een bug in de nummer generator die zicht beving in het openSSL library.
   2. Het probleem is er omdat een debian packager bijna alle bronnen entropie, de informatiedichtheid in en reeks gebeurtenissen, in de afgelegen versie van openSSL.
4. Unsupported Unix Operating System
   1. Het operating system dat op dit moment is geïnstalleerd wordt niet meer ondersteund/geüpdatet. Hiervoor moet je een upgraden naar een nieuwe os.
5. Patchen van de vulnerability

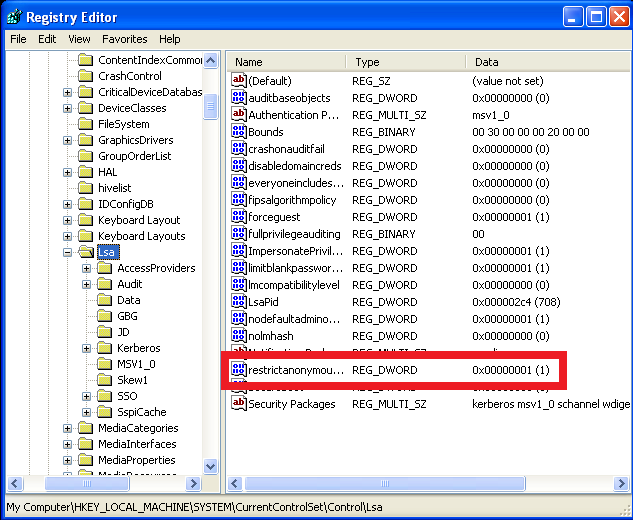
De scan met firewall gaf geen vulnerability.



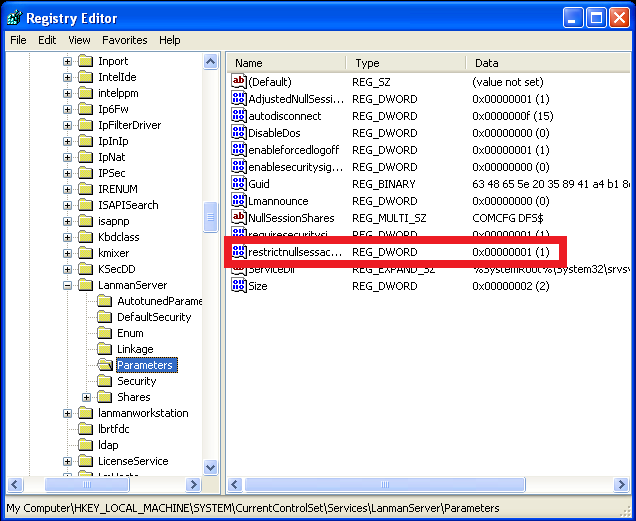
1ste vulnerability is dat het een unsupported os is. Deze kan je enkel oplossen door te upgraden naar een supported os, deze kon ik niet patchen.

2de vulnerability is dat er een buffer overrun is in een van de services, deze kan worden geëxploiteerd door een attacker om code uit te voeren met systeem privileges. Deze heb ik opgelost door alle updates te doen.

3de vulnerability is dat er geheugen corruptie in de SMB zit, dit kan er voor zorgen dat een attacker code of een dos attack kan uitvoeren. Deze heb ik opgelost door alle updates te doen.

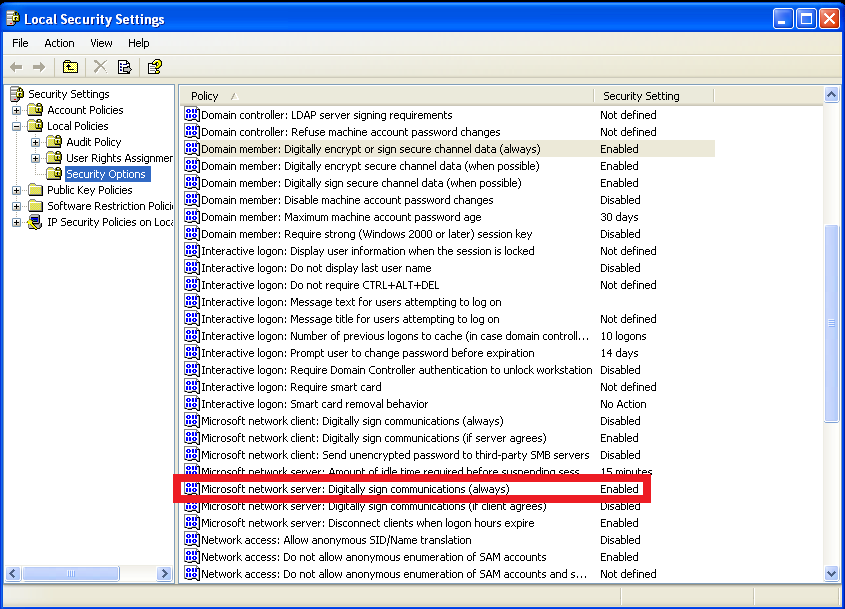
4de vulnerability is dat het mogelijk is om in te loggen op het systeem zonder een login en paswoord te geven. Deze heb ik opgelost door volgende stappen te doen.

De restrictanonymous moest op 1 staan.



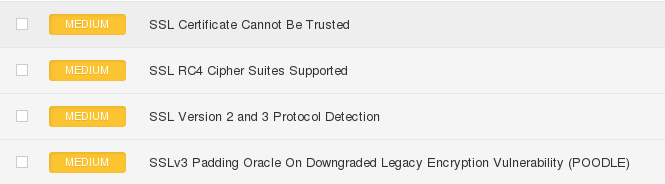
Hier moest de restrictnullsessaccess op 1 staan en moest de NullSessionPipes verwijdert worden.

5de vulnerability is dat het niet nodig is om in te loggen op de SMB server. Deze heb ik opgelost door Microsoft network server: Digitally sign communications(always) op enabled te zetten.



1. 2de scan na patch vulnerability

De scan met firewall gaf geen vulnerability.



1ste vulnerability is dat er voor server x.509 zijn certificaat ongeldig is, dit is op te lossen door een nieuw certificaat te kopen of een nieuwe te genereren.

2de vulnerability is dat er een fout zit in de RC4 cipher, een cryptografische stroomvercijferingsalgoritme op basis van symmetrische cryptografie, dat het iets minder random maakt. Op te lossen door de configuratie aan te passen zodat het geen RC4 cipher gebruikt maar een TLS 1.2.

3de vulnerability is dat de remote service SSL 2.0 en 3.0 accepteert. Deze SSL versies hebben een cryptografie fout. Op te lossen door de SSL versies te disabelen en gebruik te maken van TLS 1.0

4de vulnerability is dat de host een makkelijk doelwit is voor een man in the middle attack. Dit komt door POODLE, Padding Oracle On Downgraded Legacy Encryption. Ze hebben maar 256 requests nodig om 1 byte te onthullen van een geëncrypteerd bericht.

1. Scan van mijn laptop

C:\Users\Stef\Pictures\security\HostLaptopVul.PNG

Inloggen op de SMB server is niet vereist was de enige vulnerability die ik op mijn laptop heb staan.