Basic Security: Systems & Networks

# Basisopstelling

Voor deze opdracht heb ik gebruik gemaakt van 2 virtuele machines.

Op 1 van de virtuele machines heb ik Kali Linux geïnstalleerd, op de andere heb ik Windows XP SP2 geïnstalleerd, wat de oudste versie van Windows XP was die ik vond.

Op beide virtuele machines heb ik de virtuele netwerkkaart op ‘bridged’ gezet, zodat ze beide een apart IP-adres krijgt.

Op de Kali VM heb ik daarna Nessus geïnstalleerd, en op Windows XP automatische updates afgezet.

Van de Windows XP scans en patches heb ik ook een video gemaakt.

# Werkwijze

## Scannen

Hierna heb ik de Windows machine gescand, zowel met, als zonder firewall.

Bij de scan zonder firewall werden 5 kritieke,1 hoge en 2 medium kwetsbaarheden gevonden.

## Patchen

Om de Windows XP machine te patchen, heb ik gebruikt gemaakt van Service Pack 4.

Dit is een onofficiële Service Pack die alle updates van SP2 en SP3 bevat, alle updates daarna tot de End-Of-Life van Windows XP

Hierna heb ik opnieuw een scan gedaan met Nessus, zonder firewall, waarbij er nog 3 kwetsbaarheden overbleven.

De eerste hiervan was ‘kritiek’, en gaf aan dat Windows XP niet meer ondersteund word.

De tweede en derde waren aangegeven als ‘medium’.

Deze heb ik opgelost door 3 registry keys te wijzigen.  
- HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous  
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess

Deze heb ik beide op 1 gezet   
  
- HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes

Hier heb ik de ‘browser’ waarde uit gewist

Ook heb ik in de Policy Settings ‘Microsoft network server: Digitally sign communications’ op ‘always’ gezet.

## Scannen

Hierna heb ik opnieuw 2 scans gedaan, zowel met als zonder firewalls, bij beide scans werden toen geen kwetsbaarheden meer gevonden

# Gevonden vulnerabilities

* Microsoft Windows XP Unsupported Installation Detection:

Deze kwetsbaarheid spreekt een beetje voor zichzelf, Windows XP word niet meer officieel ondersteund, waardoor er geen updates en patches voor kwetsbaarheden meer uitgebracht worden

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

Deze service word gebruikt voor het delen van bestanden en printers, door een vervormd pakketje te sturen kan men een ‘buffer overrun’ veroorzaken, waardoor een hacker code kan uitvoeren met systeemrechten

* MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution

Deze exploit kan gebruikt worden om een denial of service uit te voeren op de server service, maar theoretisch gezien kan hiermee ook code uitgevoerd worden met systeemrechten

Deze exploit kan misbruikt worden door een speciaal SMB pakketje te sturen naar de Server service

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

Deze bug kan misbruikt worden om code uit te voeren met systeemrechten, deze bug kan worden misbruikt door een vervormd RPC pakketje te sturen naar de server service, het RPC protocol word gebruikt om een service op te vragen van een programma op de computer

* MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution

deze kwetsbaarheid bevind zich in het mailslot protocol, wat een mechanisme is gebruikt door programma’s om data uit te wisselen in 2 richtingen, door een te lang mailslot pakket te sturen naar de computers Server service word een buffer overflow veroorzaakt, waardoor code uitgevoerd kan worden met systeemrechten

* Microsoft Windows SMB NULL Session Authentication

Dit betekent dat je kan inloggen op de File en printer-sharing service zonder in te loggen, waardoor een aanvaller zonder in te loggen verschillende gegevens over de computer kan achterhalen

* SMB Signing Required

Dit betekent dat er geen controle is over de identiteit van een PC bij het verbinden met een SMB-server, hierdoor kan een aanvaller zich voordoen als een andere PC

# Metasploitable

Hierbij heb ik dezelfde Kali VM gebruikt, en de Metasploitable VM image van sourceforge

Dit is een overzicht van een aantal vulnerabilities die ik gevonden heb:

* 32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

De SSH-implementatie bevat een bug in de random number generator, waardoor een aanvaller gemakkelijk de verbinding kan ontcijferen en een man-in-the-middle aanval kan uitvoeren. SSH is een protocol wat gebruikt word bij het inloggen op afstand op een systeem. Een aanvaller kan hiermee dus de ‘remote login’ overnemen.

Deze kwetsbaarheid zou ik oplossen door een andere random number generator te gebruiken en alle keys opnieuw te laten genereren.

* 33447 - Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

De DNS resolver gebruikt geen random poort bij het verbinden met een DNS server.  
Hierdoor kan een aanvaller het antwoord van de server makkelijk vervalsen, waardoor bij aanvraag van een legitieme website, het IP van een valse website kan worden teruggegeven, en de computer dus verbinding maakt met een vervalste website

Deze kwetsbaarheid zou ik oplossen door een andere DNS resolver te gebruiken, en eventueel gebruik te maken van DNSSEC met een DNS server die DNSSEC ondersteunt

* 26928 - SSL Weak Cipher Suites Supported

Het OS ondersteunt het gebruik van zwakke encryptie bij het gebruik van SSL, bij het gebruik van zwakke encryptie kan een hacker makkelijker de encryptie ontcijferen, en zo de gegevens lezen en een man-in-the-middle aanval uitvoeren

Deze kwetsbaarheid kan je oplossen door het gebruik van deze zwakke encrypties uit te schakelen

# Extra

Buiten het scannen van Windows XP en Metasploitable, heb ik nog 2 andere scans gedaan:

een scan op een VM van LXLE, een Linux distributie gebaseerd op ubuntu14.04 en nog een scan op mijn Android GSM ‘moto G’, welke op Android 5.0.2 draait.

Op LXLE werden 2 Vulnerabilities gevonden:

* 26919 - Microsoft Windows SMB Guest Account Local User Access

Dit betekent dat mensen met een guest-account verbinding kunnen maken met de samba-daemon, welke Microsofts SMB-protocol implementeert om bestanden te delen met Windows hosts. Deze kwetsbaarheid is op te lossen door guest-access uit te schakelen in de configuratie van samba

* 57608 - SMB Signing Required

Deze kwetsbaarheid is de zelfde als we zagen bij Windows XP. Er word geen identiteitscontrole gedaan over de gegevens, deze kwetsbaarheid kan je oplossen door ‘server signing’ op ‘mandatory’ te zetten in de configuratie van samba

Op Android werden gelukkig geen vulnerabilities gevonden.