Basic Security Project: System & Networking verslag

# Vulnerabilities in Windows 8 Desktop

**Systeemomschrijving**: We hebben een VM gemaakt met een clean install van Windows 8. We hebben de firewall uitgeschakeld en XAMP geinstalleerd met de standaardconfiguratie. Nesus Basic Host Scan heeft de volgende vulnerabilities gevonden. Het rapport van deze scan kan teruggevonden worden in Basic\_scan\_windows.pdf.

**Vulnerabilities:**

Een gedeelte van deze vulnerabilities worden veroorzaakt door security flaws in de geinstalleerde serverplugins. Deze flaws zijn echter reeds door de developers zelf verholpen en kunnen dus simpelweg worden opgelost door te updaten naar de laatste versies van de programmas. Het gaat om de volgende serverplugins:  
  
PHP

OpenSSL

Tomcat

De laatste versie van XAMP afhalen is vanzelf sprekend genoeg, maar voor OpenSSL moeten we iets meer doen. Het makkelijkst is om hier (<http://slproweb.com/products/Win32OpenSSL.html>) een OpenSSL 1.02h installer af te halen

De Tomcat server bevat ook voorgeïnstalleerde voorbeeld JSPs en servlets. Dit geldt ook als een vulnerability aangezien een aanvaller deze een aanvaller kunnen helpen informatie over de Tomcat installatie of de host kunnen achterhalen. De oplossing is om deze voorbeeld JSPs en servlets te verwijderen.  
  
Het is ook mogelijk om informatie over de Apache webserver configuratie te achterhalen door de URL ‘/server-info’ te gebruiken. Dit is natuurlijk zeer interessant voor een potentiële aanvaller. De oplossing is om in de Apache configuratie ‘mod-info’ uit te schakelen of ervoor te zorgen dat de toegang gelimiteerd is tot geldige gebruikers of hosts.

Analoog aan het voorgaande kan de Apache server activiteit en prestaties opgevraagd worden via de URL ‘/server-status’. Ook hier kan dan ook best ‘mod\_status’ uitgeschakeld worden of gelimiteerde toegang worden ingesteld.  
  
Verder is het nog mogelijk om de HTTP debug methodes TRACE en TRACK op de webserver te gebruiken. Ook deze kunnen door aanvallers misbruikt worden aangezien ze informatie verschaffen over de connecties die de server legt. Ze worden dus best uitgeschakeld eens de server geïnstalleerd is en publiek wordt gemaakt. Ook dit gebeurt in de configuratie file.  
  
Onderteken van boodschappen is niet vereist op de SMB server. Een aanvaller heeft dus geen authenticatie nodig en zou een ‘man-in-the-middle’ attack kunnen uitvoeren op de SMB server. De oplossing is ‘message signing’ te verplichten via de configuratie. In Windows gebeurt dit via een policy setting.  
  
De server is ook nog niet voorzien van een geldig SSL certificaat. Een gebruiker kan dus niet verifiëren of hij met de echte server verbonden is of met een aanvaller die een ‘man-in-the-middle’ attack uitvoert. De server genereert momenteel zelf een SSL certificaat, maar hier heeft een gebruiker die voor de eerste keer verbindt uiteraard niets aan, hij kan enkel kijken of het certificaat hetzelfde is als de vorige keer dat hij verbinding maakte. Bovendien meldt de Nessus scan dat het certificaat getekent is met een cryptografisch zwak algoritme met een Diffie-Hellman Modulus van 1024 bits of kleiner. Dit betekent dat een aanvaller mogelijks het certificaat kan decrypteren en daarna vervalsen. Om dit te verhelpen moet een geldig SSL certificaat aangekocht worden. Out

# Vulnerabilities in Metasploitable OS

**Systeemomschrijving:** Metasploitable is een OS die bedoeld geconfigureerd is om vulnerabilities te hebben. We hebben deze OS gerund in een VM en deze gescand met Nessus. Het rapport van deze scan vind u in Basic\_scan\_metasploitable.pdf.  
  
**Vulnerabilities:**

vsftpd, een FTP server die geïnstalleerd is op de Metasploitable, is een illegitieme versie die gecompileerd is met een backdoor. Als er bij het inloggen op de server een smiley :) in de username wordt ingegeven activeert de backdoor en wordt er een shell gecreëerd die luistert op TCP poort 6200. Deze shell kan dan door een aanvaller gebruikt worden om eender welke code uit te voeren. Om de vulnerability op te lossen moet vsftpd opnieuw geïnstalleerd worden van een geverifieerde bron.  
  
  
De SSH host key van de server voor remote verbindingen is kwetsbaar. Dit komt door een bug in Debian packager die bijna alle bronnen van entropie verwijdert in de remote versie van OpenSSL. Entropie wordt gebruikt door random number generators om zo willekeurig mogelijke getallen te genereren. Deze entropie wordt genereerd door hardware bronnen zoals muisbewegingen of ingebouwde entropiegenerators. De informatie gegenereerd door deze entropie wordt dan in een wiskundig algoritme gevoed om willekeurige getallen te genereren. Als de gebruikte entropie zeer beperkt is, worden de “willekeurige” getallen die genereerd worden voorspelbaar. Een aanvaller die hier weet van heeft kan hierdoor proberen de key te gokken met een veel beperkter aantal mogelijkheden. (https://en.wikipedia.org/wiki/Entropy\_%28computing%29)  
Om dit te verhelpen moeten alle met Debian gegeneerde keys opnieuw gegenereerd worden met een RNG die deze vulnerability niet heeft.  
  
De Unix versie die geïnstalleerd is op de server wordt niet langer ondersteund. Dit betekent dat er geen security patches meer voor uit komen die eventuele vulnerabilities oplossen. Het is ten zeerste aan te raden te upgraden naar een meer recente versie die nog ondersteund wordt.  
  
De rlogin service is enabled op de server. Dit is een zeer onveilige manier van inloggen aanezien de login en paswoord gegevens tuseen client en host worden doorgegeven in plain tekst. Dit laat een aanvaller toe de gegeven makkelijk te onderscheppen via sniffing. Het kan ook ongeauthoriseerde logins zonder paswoord toelaten als de server kwetsbaar is voor TCP sequence number guessing (https://en.wikipedia.org/wiki/TCP\_sequence\_prediction\_attack) of IP spoofing. Ook kan men rlogin gebruiken om file-write access in volledige controle om te zetten door de .rhosts en rhosts.equiv files te wijzigen. Best kan men deze service uitschakelen en in de plaats SSH gebruiken.