

Cursus Certified Ethical Hacker

Licensed to Hack

Alle door internet verbonden bedrijfsnetwerken zijn één grote jungle. Niets is veilig en ze moeten daarom op een juiste manier beveiligd worden. Voor de beveiliging van je netwerk ben je aangewezen op mensen met kennis. En dan het liefst mensen met kennis hoe je binnen zou kunnen komen, want dan ben je in staat de zwakke plekken te identificeren. Daar dient zich echter een probleem aan. Om een analogie met de niet digitale wereld te maken: zou je je huis laten beveiligen of testen op inbraakgevoeligheid door iemand die zegt deskundig te zijn vanwege een crimineel verleden? Waarschijnlijk niet. En zo is het wellicht ook niet verstandig een hacker in te huren die zegt zich bekeerd te hebben. EC-Council poogt een oplossing te bieden. Zij hebben een cursus ontwikkeld om de IT Professional op te leiden in de werkwijze van de hacker. Op deze manier zou je eenvoudig aan kunnen tonen dat de kennis niet is opgedaan met illegale werkzaamheden.

Frank Korpershoek

Voor LanVision heb ik deze vijfdaagse cursus bij New Horizons gevolgd en het aansluitende examen gedaan. Het was een zware week en een al even zwaar examen. In korte tijd zijn een hoop tools en een nog grotere hoeveelheid switches de revue gepasseerd.

Informatie

Om een systeem binnen te komen moeten er een aantal stappen genomen worden voordat de daadwerkelijke inbraak gepland kan worden. In de eerste stap zal je nog geen echt contact met het slachtoffer hebben.

Informatie vergaren moet namelijk gebeuren zonder dat er alarmbellen gaan rinkelen, want om nu al onnodig de aandacht op je te vestigen zou niet echt handig zijn. De eerste informatie zal je waarschijnlijk halen uit één van de Internet Registries. Om het je makkelijk te maken zijn er een aantal tools zoals Sam Spade of Smart Whois beschikbaar, maar ook online zijn er dergelijke tools te vinden. Zo heb ik Dnsstuff.com bijvoorbeeld al regelmatig in de NGN fora voorbij zien komen. Dit levert ons informatie op over de ip-adressen van het slachtoffer, maar wellicht ook over de beheerder en de lokatie van de site. Een aardige bron om vast te stellen wat voor systemen gebruikt worden zonder contact te maken met het slachtoffer zijn personeelsadvertenties op jobsites of in een ouderwetse krant. Als hierin al niet direct de gebruikte systemen staan vermeld, is dat wel af te leiden uit de gezochte profielen.

Met de verzamelde informatie kan de volgende fase geopend worden. Van het passieve informatie vergaren stappen we over naar het actieve scannen van systemen. Met port- en netwerkscans komen we achter de inrichting van de infrastructuur. En mocht je denken dat firewalls je tegen deze ongein beschermen, dan zou je daar wel eens naast kunnen zitten. Veel beschikbare tools bevatten bijvoorbeeld opties om dit scannen zo rustig mogelijk aan te doen. Hiermee probeert een aanvaller onder de radar te blijven. Overigens kan het met zogenaamd firewalking ook nog eens mogelijk zijn dat een aanvaller achter je firewall regels komt. De methode achter firewalking zit verscholen in de TTL van een netwerk pakketje. Door met deze waarde te spelen kan achterhaald worden of een pakketje gedropt wordt door de firewall of juist doorgelaten. Uiteraard komen ook de wat bekendere tools aan bod: nmap is er zo één. Ik wist alleen niet dat er zoveel opties beschikbaar waren die nog eens nuttig zijn ook! Naast nmap passeren nog een aantal visuele scanning tools de revue. Voordeel van dat soort tools is dat je simpelweg de juiste opties aanvinkt, zonder je te hoeven bekommeren over de juiste switch.

Inmiddels weten we welke poorten van welke systemen open staan. Het wordt tijd voor wat gedetailleerdere informatie. Welke services gaan er achter de open poorten schuil, en nog belangrijker: van welke fabrikant.



Soms kan een simpele telnet naar een poort je de juiste informatie geven. Veel mailservers achter poort 25 zijn bijvoorbeeld zo vriendelijk zich met naam, toenaam en patchlevel te identificeren. Ditzelfde principe geldt uiteraard ook voor een hoop andere services. Maar mocht een systeem gedresseerd zijn om dit soort informatie niet direct prijs te geven, dan kan het OS aan de hand van active stack fingerprinting wellicht achterhaald worden. Het geheim daarvan zit hem in het feit dat elk OS anders reageert op een bepaald soort afgeschoten pakketjes. Elke TCP/IP implementatie bevat kleine eigenaardigheden, die weliswaar binnen de standaarden kunnen vallen, maar wel informatie prijsgeven. Zo zal Windows, in tegenstelling tot andere OSen, bij een niet normaal geopende tcp sessie direct een RST terugsturen. De al eerder genoemde nmap probeert aan de hand van acht verschillende testen een zo accuraat mogelijk beeld te maken over het achterliggende OS.

Bij de volgende stap is het de bedoeling om er achter te komen of er vulnerabilities aanwezig zijn. Ook hiervoor zijn weer genoeg tools beschikbaar, die niet eens altijd hun oorsprong hoeven te hebben in de donkere kant van de internet community. Hoe verder we komen in het proces van inbreken, hoe geavanceerder de tools worden. De tools waarmee we nu werken genereren complete netwerktekeningen (Cheops, Friendly Pinger) of mooie vulnerability rapporten (Retina, GFI Languard). Veel tools werken met een plug-in systeem waardoor het makkelijk

wordt nieuwe onvolkomenheden toe te voegen aan het arsenaal van tests. Op dit punt aangekomen is genoeg informatie vergaard en kan een daadwerkelijke inbraak gepland worden.

Inbraak

Eén methode van inbraak is het achterhalen van user id's en bijbehorende passwords. Een favoriete manier van hackers om achter windows user id's te komen is gebruik te maken van zogenaamde null sessions. In niet goed dichtgetimmerde omgevingen is het mogelijk met simpele tools (dumpsec, enum) complete gebruikerslijsten op te vragen. En voor diegenen die hun administrator account hebben hernoemd; aan de hand van de gevonden sids is het vrij eenvoudig om met de tool sid2user de nieuwe naam te achterhalen.

Een andere methode om achter handige gegevens te komen is het plaatsen van sniffers. Etherreal is een bekende open source sniffer. Daarnaast zijn er sniffers voor specifieke targets. Dsniff is een verzameling tools die het mogelijk maakt om bijvoorbeeld nfs files, mail verkeer of login prompts van de lijn af te plukken. Ook tools die eigenlijk gebruikt worden als verdediging kunnen echter worden ingezet voor snode doeleinden; snort, eigenlijk een IDS, kan je geheel naar eigen wens dresseren en zo op passwords of andere interessante zaken laten triggeren. En mocht je denken dat je veilig bent omdat jouw omgeving geswitched is,

dan heb je het fout. Ook hier zijn tools om de zaak om de tuin te leiden. Met arpspoof zorg je ervoor dat een slachtoffer zijn verkeer niet rechtstreeks naar zijn doel stuurt, maar dat via jouw machine doet. Op deze manier krijg jij dus de mogelijkheid de complete datastroom de bekijken.

Het bezit van user id's is één ding, de passwords een ander! Grofweg zijn de password aanvallen in vier methoden in te delen; passief online (sniffers, man in the middle), actief online (password guessing), offline (de password files aanvallen) en niet-electronisch (shoulder surfing, social engineering). En het kan haast niet anders of ook hier zijn weer handige hulpmiddelen voor te krijgen. L0phtcrack, nat, pwdump3, John the Ripper zijn enkele van de creatieve namen die er aan deze tools zijn gegeven. Sommige van deze tools kan je voeden met een woordenboek, terwijl andere de brute force methode hanteren, al dan niet in combinatie met een woordenboek. In de online varianten proberen ze in te loggen, de offline varianten gaan de password files te lijf die niet altijd even moeilijk te vergaren blijken.

Met een account en password hebben we nu toegang tot een systeem. Mocht dit een gewoon useraccount zijn, dan zijn er weer tooltjes (x.exe, pipeupadmin, getadmin) om de rechten op te schroeven. Met volledige toegang zorg je ervoor dat je de juiste tools op het systeem zet om je optimaal tot dienst te zijn. Zo is niet alleen mogelijk alles te bekijken wat er op het target systeem staat, maar is het ook mogelijk om vanaf afstand de microfoon of webcam aan te zetten. Zorg er dus maar voor dat dat mediacentrum op je slaapkamer goed beveiligd is! Wanneer je als aanvaller tools op een vreemd systeem zet, is het zaak deze goed te verbergen. De meest bekende methode is wellicht een rootkit. Deze zorgt ervoor dat bijvoorbeeld bij het opvragen van een directory bepaalde bestanden niet worden getoond, of bepaalde processen niet meer te vinden zijn. Een voor mij nieuw fenomeen was de mogelijkheid data te verbergen in zogenaamde Alternate Data Streams (ADS). In NTFS is het mogelijk om meerdere data streams in één file te stoppen. Ik nodig je graag uit om de volgende stappen eens te doorlopen:

- maak met 'notepad test.txt' een tekst file aan en controleer de grootte met het 'dir' commando.
- maak nu met 'notepad test.txt:geheim.txt' een tekstfile

aan en controleer opnieuw de inhoud van je directory. Je zult zien dat alleen de test.txt file met de oorspronkelijke grootte aanwezig is.

Met normale tools is niet te achterhalen of er ADS in gebruik zijn. Een eenvoudige maar doeltreffende manier om bestanden te verbergen!

Een andere categorie verborgen functionaliteit is de trojan. Veelal verborgen in leuke spelletjes (tetris) of andere media (rond kerst zullen de rond rennende kerstmannetjes of varianten wel weer rond gemaaild worden!) komen deze tot leven wanneer de argeloze gebruiker er op klikt. Beast, SubSeven, Back Orifice, Deep Throat, Donald Dick, tini, netcat etc zijn in deze categorie bekende namen. Waar de één uitblinkt in eenvoud heeft de ander een onwaarschijnlijke hoeveelheid toeters en bellen. Netcat is zo'n eenvoudige maar effectieve tool. Door deze op te starten op het target systeem met de juiste opties, kan je met een eenvoudige telnet sessie een dosbox op dat target systeem openen.

Web servers

Inmiddels is de cursus beland bij het inbreken via web servers. Wie wel eens door zijn webserver logs heeft gebladerd zal veel methoden wel kennen: directory traversals, unicode aanvallen, of andere vormen waarvan je aan de url al kan zien dat er iets niet mee in de haak is. Maar gelukkig zijn al je systemen up-to-date, toch? En dat is maar goed ook, want veel van dit soort exploits worden volautomatisch gecheckt door meer lieden dan je lief is: op je privé adsl lijn waarschijnlijk om als bot ingelijfd te worden. Soms komt er wat meer handwerk bij kijken, maar dan nog maken tools als metasploit het de script kiddies wel erg makkelijk. Metasploit is een framework waarmee uit een database een exploit gekozen en losgelaten kan worden op een target systeem. Zorg dus dat je volledig gepatcht bent om te voorkomen dat je door bekende vulnerabilities gepakt kan worden. Helaas betekent volledig gepatcht nog niet volledig veilig. Veel bedrijven hebben namelijk al dan niet zelf gebouwde web applicaties. En juist hierin kunnen ongemerkt grote gaten zitten.

SQL injection

Veel web applicaties maken gebruik van achterliggende databases. Wie ooit een database heeft gebruikt of enige kennis van SQL heeft, kan zich voorstellen dat bij



het inloggen in een webapplicatie iets wordt gevraagd als 'SELECT * FROM usertbl WHERE userid=123 AND password=abc'. Zodra de SQL server antwoord geeft, heb je een juiste combinatie ingevoerd. Indien de programmeur niet juist aan inputvalidatie heeft gedaan kan het mogelijk zijn om door middel van het userid invul veld het effectieve SELECT statement om te vormen tot iets als 'SELECT * FROM usertbl WHERE userid=123 or 1=1'. De SQL server geeft nu onafhankelijk van het ingevulde wachtwoord rijen terug waardoor de applicatie denkt ingelogd te zijn. Naast het forceren van een inlog poging, kan met deze manipulatie nog meer uitgehaald worden. Naast SELECT statements kan je INSERT's uitvoeren of stored procedures aanspreken. Zo stond tijdens één van de praktijk oefeningen via een niet al te lastig stappenplan al snel een dosbox van een slachtoffer op je scherm! Waar ik van schrok is de combinatie van een aantal factoren:

- De methode is eenvoudig. Zonder speciale tools (die er overigens wel zijn!) kan je door de URL te manipuleren op plekken komen waar je niet zou mogen komen.
- De methode is slecht te detecteren. Het verzoek aan de webserver blijft valide.
- Wanneer je weet dat de term 'productID=123' in de URL vaak wordt gebruikt om een database te bevragen, is het zeer eenvoudig om met google achter dit soort sites te komen. Met een kleine manipulatie weet je snel of het een potentieel slachtoffer kan zijn.

- SQL injection is niet door één van de grote leveranciers te patchen, slechts door het opleiden van de web programmeur in kwestie kan dit opgelost worden. En aangezien er vele, vele duizenden van dit soort applicaties aan het web hangen is dit een bijna onbegonnen zaak.

In dit artikel heb ik niet de hele cursusweek aan bod kunnen laten komen. Zo hebben we het bijvoorbeeld ook nog gehad over wireless hacking, social engineering, hoe werken buffer overflows, de achtergronden van vulnerabilities, encryptie technieken, virussen, DDos attacks, etc,etc. En niet onbelangrijk; wat kan je tegen de verschillende aanvallen doen. Want ik moet eerlijk zijn, halverwege de week zag ik het niet echt meer zitten. Ik vroeg me af waar we als beheerders nou eigenlijk mee bezig zijn; dweilen met de kraan open! Het interesseert veel gebruikers geen lor dat ze met sticky notes het password op het beeldscherm plakken. En dat van huis meegebrachte wireless access point is ook handig! Nee, echt veilig krijgen we het voorlopig niet, maar dat neemt niet weg dat wij ons in elk geval van de gevaren bewust moeten zijn en zoveel mogelijk mensen in onze omgeving moeten opvoeden. Of we het nou leuk vinden of niet; security moet deel uit maken van ons dagelijks werk. Ik besef me tevens dat de informatie, die in een week tijd mijn hersens in gestampt is, aan veroudering onderhevig is. Bovendien is deze cursus voor een belangrijk deel op windows aanvallen gebaseerd. Toch geeft deze week je een dusdanige dosis kennis in het gedachtegoed van de hacker dat je er wel even mee vooruit kan. Verder krijg je toegang tot het CEH forum alwaar je op de hoogte gehouden wordt van de nieuwe ontwikkelingen. Ondanks het genoemde dipje heb ik mij door de cursusweek heen gewerkt. Zoals ik al eerder aangaf, het was een loodzware week. De hoeveelheid tools zijn werkelijk enorm. Gelukkig krijg je ze, net als de 2000 bladzijden aan cursusmateriaal, ook allemaal mee om ze op het werk in een veilige omgeving nog eens door te lopen. En dat examen? In dik twee en een half uur heb ik de 125 vragen doorgeworsteld en had dus nog een krap half uur over. Het was flink zweten, niet alleen vanwege de zomerse temperaturen, maar ik heb het gehaald en mag mij nu dus Certified Ethical Hacker noemen...

frank.korpershoek@ngn.nl