Hacken voor dummies

SPIEKBRIEF

Hacken voor Dummies, spiekbrief

Hacken hoeft niet slecht te zijn. De beveiligingstests die in dit boek aan bod komen, leggen beveiligingslekken en zwakke plekken bij computers bloot. Deze spiekbrief biedt een handig overzicht van tools en tips en wijst je op populaire doelwitten van hacks. Al deze informatie maakt het testen van de beveiliging een stuk eenvoudiger.

Onmisbare hacktools

Als expert op het gebied van informatiebeveiliging is je toolkit, oftewel je gereedschapskist, de belangrijkste verdediging tegen hackpogingen, naast je ervaring en gezond verstand. Zorg ervoor dat je de volgende hacktools tot je beschikking hebt (en dat je ze bij elke klus bij je hebt):

- **software om wachtwoorden te kraken,** zoals ophcrack en Proactive Password Auditor;
- **software om netwerken te scannen,** zoals Nmap en NetScanTools Pro;
- **kwetsbaarheidsscanners**, zoals LanGuard en Nexpose;
- **netwerkanalysesoftware,** zoals Cain & Abel en CommView;
- **draadloze netwerkanalysesoftware,** zoals Aircrack-ng en CommView for WiFi;
- **software om bestanden te doorzoeken,** zoals FileLocator Pro;
- **kwetsbaarheidsscanners voor webapps,** zoals Acunetix Web Vulnerability Scanner en AppSpider;
- **beveiligingsscanners voor databases**, zoals SQLPing3;
- **exploitsoftware,** zoals Metasploit.

Zwakke plekken in de beveiliging waar hackers op azen

Beveiligingsprofessionals horen op de hoogte te zijn van bekende beveiligingskwetsbaarheden die criminele hackers en malafide medewerkers het eerst controleren als ze computersystemen hacken. Let op de volgende beveiligingsproblemen tijdens je beveiligingstests:

- goedgelovige of naïeve gebruikers;
- onbeveiligde ingangen bij gebouwen en computerruimten;
- weggegooide documenten die niet door de shredder zijn gegaan en computerschijven die niet zijn vernietigd;
- netwerken met weinig of geen firewallbescherming;
- matige, verkeerde of ontbrekende controle op de toegang tot bestandsdeling en netwerkshares;

SPIEKBRIEF

- webapps met zwakke authenticatiemechanismen;
- draadloze gastennetwerken die mensen in staat stellen om verbinding met het bedrijfsnetwerk te maken;
- laptops zonder volledige schijfencryptie;
- mobiele apparaten met makkelijk te kraken wachtwoorden of zonder wachtwoorden;
- zwakke of ontbrekende wachtwoorden bij apps, databases of besturingssystemen;
- firewalls, routers en switches met makkelijk te raden of standaardwachtwoorden.

Tips voor succesvolle beveiligingsassessments

Je hebt degelijke beveiligingsassessments nodig om je computersystemen tegen hacks te beschermen. Je moet zorgvuldig te werk gaan, maar wel pragmatisch blijven, ongeacht of je de beveiliging van je eigen computers test of dat je systemen van een ander controleert. De volgende tips helpen je bij een succesvolle evaluatie van de informatiebeveiliging:

- Stel doelen op en ontwikkel een plan voordat je aan de slag gaat.
- Zorg dat je toestemming hebt om je tests uit te voeren.
- Zorg dat je de juiste tools hebt voor je werkzaamheden.
- Test op een moment dat geschikt is voor het bedrijf.
- Houd belangrijke mensen tijdens het testen op de hoogte van je vorderingen.
- Besef dat het niet mogelijk is om elke zwakke plek in de beveiliging van elk computersysteem op te sporen.
- Bestudeer het gedrag en de technieken van kwaadwillende hackers en malafide medewerkers. Hoe meer je over de aanpak van slechteriken weet, hoe beter je in staat bent om computersystemen op kwetsbaarheden te testen.
- Sla de niet-technische aspecten van de beveiliging niet over; deze worden vaak als eerste uitgeprobeerd.
- Behandel de geheime gegevens van anderen op zijn minst net zo goed als je eigen geheimen.
- Breng aangetroffen kwetsbaarheden onder de aandacht van het management en neem zo snel mogelijk toepasselijke tegenmaatregelen.
- Behandel niet alle ontdekte kwetsbaarheden op dezelfde manier. Niet alle zwakke plekken vormen een probleem. Evalueer de ontdekte problemen voordat je alarm slaat.
- Laat het management en klanten zien dat beveiligingstests goed voor het bedrijf zijn en dat jij de juiste persoon voor deze taak bent.

Hacken

voor dummies®

Kevin Beaver

BBNC uitgevers

Amersfoort, 2019

Inhoud in vogelvlucht

1 Bouwstenen voor beveiligingstest

IN DIT DEEL . . .

Ontdek je de beginselen van penetratietests.

Kijk je door de ogen van een hacker om zijn beweegredenen te begrijpen.

Plan je beveiligingstests.

Leer je methoden gebruiken voor het opsporen van de meeste (en belangrijkste) kwetsbaarheden.

IN DIT HOOFDSTUK

- **De doelstellingen van hackers en kwaadwillende medewerkers begrijpen**
- **Het ontstaan en de ontwikkeling van beveiligingstests**
- **De gevaren voor computersystemen leren kennen**
- **De beveiliging testen**

Hoofdstuk 1

Inleiding in penetratietests

Dit boek gaat over het testen van zwakke plekken in de beveiliging van je computers en netwerken en het dichten van de gaten die je tegenkomt voordat slechteriken de kans krijgen er misbruik van te maken.

De terminologie leren kennen

Iedereen weet dat er hackers en kwaadwillende gebruikers bestaan. Velen zijn zelfs geconfronteerd met de consequenties van hun criminele activiteiten. Maar wie doen dit eigenlijk en waarom zou je er iets over moeten weten? In de volgende paragrafen lees je meer over deze aanvallers.


BELANGRIJK

In dit boek gebruik ik de volgende termen:

- **Hackers** (ook wel *computerkrakers* of *externe aanvallers genoemd)* proberen voor eigen gewin als ongeautoriseerde gebruiker toegang tot computers of complete netwerken te krijgen, meestal van buitenaf. Hackers vallen bijna elke computer aan waar ze een kans bij denken te maken. Sommige geven de voorkeur aan prestigieuze, goed beveiligde systemen, al verhoogt ook een geslaagde aanval op een bescheiden computer de status van de aanvaller in hackerskringen.

- **Kwaadwillende medewerkers** (*externe* of *interne aanvallers)* proberen van buitenaf toegang tot computers en gevoelige gegevens te krijgen (klanten en zakelijke partners) of van binnenuit als geautoriseerde en vertrouwde gebruikers. Kwaadwillende gebruikers doen dit voor eigen gewin of uit wraak en gebruiken hierbij hun kennis van het systeem.

  Kwaadwillende aanvallers zijn over het algemeen zowel hackers als kwaadwillende gebruikers. Om het boek leesbaar te houden, noem ik beide groepen *hackers* en maak ik alleen onderscheid tussen *hacker* en *kwaadwillende gebruiker* als dit nodig is, bijvoorbeeld als ik het over hun gereedschap, technieken en denkprocessen heb.

- **Ethische hackers** (zogenoemde *good guys)* hacken systemen om kwetsbaarheden op te sporen, zodat die kunnen worden beveiligd tegen ongeautoriseerde toegang en misbruik. Tot deze categorie behoren ICT-onderzoekers, consultants en interne medewerkers.

Hacker

Hacker heeft twee betekenissen:

- Van oorsprong knutselden hackers aan software of elektronische systemen. Hackers vinden het leuk om dingen te onderzoeken en meer over de werking van computersystemen te weten te komen. Ze zijn op zoek naar nieuwe werkmethoden, zowel mechanisch als elektronisch.

- De afgelopen jaren heeft *hacker* een nieuwe betekenis gekregen: iemand die ongeoorloofd bij computers inbreekt voor eigen gewin. Eigenlijk is hier sprake van *crackers* (criminele hackers, oftewel computerkrakers). Crackers breken bij computers in; ze kraken systemen met kwade opzet. Ze zijn uit op roem, intellectuele eigendommen, geld of wraak. Ze veranderen, verwijderen of stelen belangrijke informatie en leggen volledige netwerken plat, waardoor multinationals en overheidsinstanties soms op hun knieën worden gedwongen.


PAS OP

- En dan heb je ook nog eens allerlei hippe toepassingen van het woord *hack*, variërend van *lifehack* tot inmenging bij verkiezingen. Marketeers, politici en mediastrategen weten dat de gemiddelde mens geen idee van de betekenis van het woord *hacken* heeft, dus gebruiken ze het voor alles wat in hun straatje past. Negeer dit gewoon.

Hackers van het type good guy *(white-hat)* houden er niet van tot dezelfde categorie te worden gerekend als hackers van het type bad guy *(black-hat).* De witte en zwarte hoeden stammen trouwens uit de tijd van westerns op tv, waarbij sheriffs en betrouwbare cowboys witte hoeden droegen en slechteriken herkenbaar waren aan hun zwarte hoofddeksels.

Hackers van het type g*ray-hat* zitten hier tussenin. Maar hoe het ook zij, de meeste mensen hebben een negatieve associatie bij de term *hacker.*

Veel kwaadwillende hackers stellen dat ze geen schade aanrichten maar een betere samenleving nastreven. Erg geloofwaardig. Kwaadwillende hackers zijn elektronisch gespuis en horen verantwoording voor hun daden af te leggen.

Verwar criminele hackers niet met beveiligingsonderzoekers. Onderzoekers voeren hacks open en bloot uit en ontwikkelen waardevolle tools die we bij de beveiliging gebruiken. Bovendien publiceren ze (meestal) hun resultaten en is hun broncode vrij toegankelijk.

Kwaadwillende gebruiker

Een kwaadwillende gebruiker is een malafide werknemer, aannemer, stagiair of andere medewerker die zijn of haar bevoegdheden te buiten gaat. Dit is een bekend fenomeen in beveiligingskringen en krantenartikelen over informatiediefstal. Het gaat hierbij meestal niet om inbraak bij interne systemen, maar het misbruiken van toegangsrechten bij computers. Gebruikers neuzen in belangrijke databasesystemen om gevoelige informatie te verzamelen, e-mailen vertrouwelijke klantinformatie naar de concurrentie of een locatie in de cloud, of verwijderen belangrijke bestanden van servers waartoe ze waarschijnlijk geen toegang horen te hebben.

Soms veroorzaakt een onschuldige (of onwetende) medewerker zonder slechte bedoelingen beveiligingsproblemen door gevoelige informatie te verplaatsen, te verwijderen of te corrumperen. Zelfs een onschuldige dikke vinger op het toetsenbord kan in de zakenwereld ernstige gevolgen hebben. Denk maar eens aan alle ransomware-infecties die bedrijven overal ter wereld treffen. Eén muisklik van een onzorgvuldige gebruiker kan voor het volledige netwerk consequenties hebben.

Kwaadwillende gebruikers zijn vaak de gevaarlijkste vijanden van ICT- en beveiligingsafdelingen, want ze weten precies waar ze moeten zoeken en ze hebben geen computerkennis nodig om bij gevoelige informatie te komen. Deze gebruikers hebben toegang tot de informatie die ze zoeken en het management vertrouwt hen, vaak zonder erover na te denken.

Hoe zit het met Edward Snowden, de voormalige medewerker van de NSA die zijn eigen werkgever verraadde? Dat is een lastig onderwerp. (Over de motivatie van hackers lees je meer in hoofdstuk 2.) Snowden misbruikte zijn autoriteit en schond de voorwaarden van zijn geheimhoudingsovereenkomst, ongeacht wat je van zijn daden vindt. Hetzelfde geldt voor

anderen die, om welke reden dan ook, vanwege hun bekendheid op een voetstuk worden geplaatst.

Ethische hackers

Je hebt bescherming nodig tegen de strapatsen van hackers, dus moet je net zo handig worden als de mensen die je systemen aanvallen. Een goede beveiligingsspecialist beschikt over de vaardigheden, denkwijze en hulpmiddelen van een hacker, maar is betrouwbaar. Hij of zij voert hacks als beveiligingstests op computersystemen uit en denkt en werkt hierbij op dezelfde manier als een hacker.


BELANGRIJK

Bij ethisch hacken (dus bij penetratietests door beveiligingsexperts) worden dezelfde tools, trucs en technieken gebruikt die criminele hackers inzetten, met één groot verschil: het hacken wordt met toestemming van het doelwit in een professionele omgeving uitgevoerd. Het doel van zo'n test is kwetsbaarheden te ontdekken vanuit het oogpunt van een kwaadwillende aanvaller om zodoende systemen beter te beveiligen. Penetratietests maken deel uit van een algeheel risicobeheerprogramma dat permanente verbeteringen van de beveiliging mogelijk maakt. Deze beveiligingstests zorgen er ook voor dat de claims van leveranciers over de veiligheid van hun producten geldig zijn.

Penetratietests versus audits

Veel mensen verwarren penetratietests met audits, maar er zijn grote verschillen in de doelstellingen van beide beveiligingsmethoden. Bij een beveiligingsaudit wordt het beveiligingsbeleid van een bedrijf (of het compliancereglement) vergeleken met de dagelijkse praktijk. De bedoeling van een beveiligingsaudit is vast te stellen dat beveiligingscontroles bestaan, meestal met een op risico's gebaseerde aanpak. Bij audits worden bedrijfsprocessen beoordeeld, een aanpak die in sommige gevallen niet erg technisch is. Beveiligingsaudits bestaan soms uit niet meer dan enkele controlelijsten die ertoe dienen om aan een specifiek compliancereglement, oftewel aan nalevingseisen te voldoen.


BELANGRIJK

Niet alle audits zijn van hoog niveau, al zijn sommige die ik heb gezien wel erg simplistisch, zoals de naleving van PCI DSS (Payment Card Industry Data Security Standard) en HIPAA (Health Insurance Portability and Accountability Act). Vaak worden ze uitgevoerd door mensen zonder technische kennis van computers, netwerken of apps of, erger nog, door mensen zonder ICT-achtergrond!

TECHNISCHE INFO

SECURITY TESTING CERTIFICATIONS

Als jij penetratietests uitvoert en een certificaat aan je cv wilt toevoegen, dan kun je Certified Ethical Hacker (C|EH) worden via een certificeringsprogramma van EC-Council. Zie www.eccouncil.org voor meer informatie. C|EH is net als CISSP (Certified Information Systems Security Professional) een bekende en gerespecteerde certificering in de ICT-wereld, geaccrediteerd als ANSI 17024.

Andere mogelijkheden zijn het programma GIAC (Global Information Assurance Certification) van SANS, CPT (Certified Penetration Tester) van IACRB en het programma OSCP (Offensive Security Certified Professional), een praktisch certificeringsprogramma voor beveiligingstests. Deze aanpak bevalt me, want mensen die dit type werk doen, ontberen vaak praktijkervaring met tools en technieken. Zie www.giac.org en www.offensive-security.com voor meer informatie hierover.

Beveiligingsassessments die met ethisch hacken werken, richten zich op kwetsbaarheden die kunnen worden uitgebuit. Deze testbenadering stelt vast dat beveiligingscontroles niet aanwezig of niet effectief zijn. Formele penetratietests zijn soms zeer technisch en soms niet-technisch. Meestal zijn ze minder gestructureerd dan formele audits, al wordt wel een formele methodologie gebruikt. Als audits bij jouw organisatie verplicht zijn (bijvoorbeeld voor SSAE 16 SOC 1/2/3 en ISO 27001), dan integreer je de technieken voor penetratietests die in dit boek worden beschreven in je auditprogramma voor de ICT-beveiliging. Audits en penetratietests vullen elkaar heel goed aan.

Beleidsoverwegingen

Kies je ervoor om penetratietests aan het programma voor informatierisicobeheer van je bedrijf toe te voegen, dan moet je het testbeleid voor de beveiliging ook documenteren. Zo'n beleid bevat informatie over wie de test uitvoert, welk type tests worden uitgevoerd en hoe vaak het testen plaatsvindt. De specifieke procedures voor het uitvoeren van beveiligingstests bestaan dan bijvoorbeeld uit methoden die ik in dit boek behandel. Het kan ook geen kwaad om een document met beveiligingsstandaarden te maken waarin de specifieke beveiligingstools en de medewerkers die de tests uitvoeren worden beschreven. Je legt dan testdatums vast, zoals eenmaal per kwartaal voor externe systemen en halfjaarlijkse tests voor interne systemen, of een ander interval dat voor je bedrijf geschikt is.

Compliance en regelgeving

Het interne beleid bepaalt hoe het management beveiligingsonderzoeken beoordeelt, maar je moet natuurlijk ook rekening houden met de nationale en internationale wetgeving die op je bedrijf van invloed is. Vooral de DMCA (Digital Millennium Copyright Act) zorgt voor veel stress bij onderzoekers. Zie www.eff.org/issues/dmca voor alles wat de DMCA te bieden heeft.

Er zijn veel wetten die degelijke beveiligingscontroles en consistente beveiligingsevaluaties eisen. In Nederland heb je te maken met de AVG (Algemene Verordening Gegevensbescherming) en de GDPR (General Data Protection Regulation) van de Europese Unie. De Verenigde Staten hebben verschillende federale wetten, zoals HIPAA en de bijbehorende HITECH (Health Information Technology for Economic and Clinical Health), GLBA (Gramm-Leach-Bliley Act), NERC (North American Electric Reliability Corporation), CIP (Critical Infrastructure Protection) en PCI DSS. Canada heeft PIPEDA (Personal Information Protection and Electronic Documents) en Japan JPIPA (Personal Information Protection Act). Beveiligingstests die zich aan deze voorschriften houden, bieden een uitstekende manier om de algehele informatiebeveiliging en het privacyprogramma te verbeteren.

De noodzaak om je eigen computers te hacken

Met dieven vang je dieven, oftewel: om een dief te vangen, moet je denken als een dief. Dit inzicht vormt de basis voor penetratietests, want het is essentieel dat je de vijand kent. Met het uitdijend aantal hackers, hun groeiende kennis en de toename van systeemkwetsbaarheden en onbekende factoren worden alle computersystemen en apps uiteindelijk een keer gehackt of gecompromitteerd. Het is van cruciaal belang om je computersystemen tegen slechteriken te beschermen; een algemene beveiliging volstaat niet. Ken je zelf hackerstrucjes, dan ontdek je hoe kwetsbaar je systemen werkelijk zijn.

Hackers zoeken actief naar organisaties met een lakse beveiliging en (nog) niet openbaar gemaakte beveiligingslekken. Er is ook steeds meer bewijs dat allang bestaande, bekende kwetsbaarheden het doelwit zijn, zoals het jaarlijkse rapport Verizon Data Breach Investigations (www.verizonenterprise.com/verizon-insights-lab/dbir) laat zien. Firewalls, encryptie en andere geavanceerde (en dure) beveiligingstechnologieën

geven vaak een misplaatst gevoel van veiligheid. Dit type beveiliging is meestal gericht op kwetsbaarheden van hoog niveau, zoals toegangscontrole en bescherming van informatie tijdens het transport, zonder dat dit invloed heeft op hoe slechteriken werken. Je maakt je eigen computersystemen veiliger door ze zelf aan te vallen, want dan kom je erachter wat de zwakke plekken zijn, vooral makkelijke doelwitten die veel mensen in de problemen brengen. Penetratietests zijn een beproefde methode om systemen goed te beveiligen tegen aanvallen. Als je zwakke punten niet in kaart brengt, is het slechts een kwestie van tijd voordat beveiligingslekken worden misbruikt.

Aangezien hackers hun kennis uitbreiden, moet jij dat ook doen. Je moet net zo denken als zij en op dezelfde manier te werk gaan als je computersystemen tegen ze wilt beschermen. Als ethische hacker moet je weten welke activiteiten onethische hackers ontplooien en hoe je hun inspanningen stopt. Als je weet waar je op moet letten en hoe je die informatie gebruikt, ben je in staat om de inbraakpogingen van hackers te dwarsbomen.


TIP

Het is niet nodig om te proberen je systemen tegen *alles* te beschermen. Dat is niet mogelijk. De enige waterdichte beveiliging tegen alles is de computersystemen los te koppelen en achter slot en grendel te zetten zodat niemand erbij kan, inclusief jijzelf. Maar dit is niet de beste beveiligingsmethode en het komt ook niet ten goede aan de productiviteit. Het gaat erom computersystemen te beschermen tegen bekende beveiligingslekken en veelvoorkomende soorten aanvallen; dit zijn 20 procent van de problemen die 80 procent van de risico's vormen, wat in de meeste organisaties vaak de zwakste punten zijn die over het hoofd worden gezien.

Het is onmogelijk te anticiperen op alle mogelijke kwetsbaarheden in je systemen en bedrijfsprocessen. Je kunt geen rekening houden met alle mogelijke soorten aanvallen, want er zijn ook onbekende. Maar hoe meer combinaties je uitprobeert en hoe vaker je complete systemen test in plaats van individuele computers, hoe groter de kans om kwetsbaarheden te ontdekken die de informatiesystemen in hun geheel beïnvloeden.

Ga niet te ver met je beveiligingstests; het beveiligen van systemen tegen onwaarschijnlijke (of zelfs minder waarschijnlijke) aanvallen heeft weinig zin.


BELANGRIJK

Je streeft het volgende na met je beveiligingstests:

» Leg de nadruk op computersystemen, zodat je je kunt richten op wat belangrijk is.

- Test je systemen op een niet-destructieve manier.
- Noteer alle kwetsbaarheden als bewijs voor het management dat er bedrijfsrisico's zijn.
- Pas resultaten toe om de kwetsbaarheden te verhelpen en je systemen beter te beveiligen.

Bedreigingen voor computersystemen begrijpen

Beseffen dat computersystemen door hackers overal ter wereld en kwaadwillende gebruikers op kantoor worden bedreigd is één, maar het is iets anders om specifieke potentiële aanvallen op je systemen te kennen. In deze paragraaf komen enkele bekende aanvallen aan bod, al zijn er natuurlijk nog veel meer.

Veel zwakke plekken in de beveiliging zijn op zich niet ernstig, maar als tegelijkertijd meerdere kwetsbare plekken worden aangevallen, kan dit zijn tol eisen op een systeem- of netwerkomgeving. Een standaardconfiguratie van het besturingssysteem Windows, een zwak beheerderswachtwoord bij SQL Server en een server die op een draadloos netwerk wordt uitgevoerd, vormen afzonderlijk waarschijnlijk geen groot beveiligingsprobleem. Maar als iemand ze alle drie tegelijkertijd uitbuit, bestaat de kans dat hij ongeautoriseerde externe toegang krijgt en gevoelige informatie (of meer) buitmaakt.


BELANGRIJK

Complexiteit is een vijand van veiligheid.

Kwetsbaarheden en aanvallen zijn de afgelopen jaren enorm gegroeid door virtualisatie, clouddiensten en zelfs social media. Deze drie elementen voegen een enorme complexiteit toe aan de computeromgeving.

Niet-technische aanvallen

Exploits waarbij mensen worden gemanipuleerd (eindgebruikers of zelfs jij), vormen het grootste gevaar voor elke computer- of netwerkinfrastructuur. Mensen zijn van nature goed van vertrouwen, wat kan leiden tot social engineering. Bij *social engineering* wordt misbruik van het vertrouwen gemaakt om informatie in te winnen voor kwaadwillende doeleinden (vaak via phishing). In hoofdstuk 6 lees je meer over social engineering en de manier waarop je je systemen ertegen kunt beschermen.

Andere veelvoorkomende en effectieve aanvallen op informatiesystemen zijn fysiek. Hackers breken in bij gebouwen, computerruimten of kantoren met cruciale informatie en stelen computers, servers en andere waardevolle apparatuur. Tot de fysieke aanvallen wordt ook *dumpsterdiven* gerekend: prullenmanden en afvalbakken doorzoeken op intellectueel eigendom, wachtwoorden, netwerkdiagrammen en andere informatie.

Aanvallen op de infrastructuur van het netwerk

Aanvallen op netwerkinfrastructuren zijn vaak eenvoudig, want veel netwerken zijn overal ter wereld via internet bereikbaar. Voorbeelden van aanvallen op de netwerkinfrastructuur zijn onder andere:

- verbinding met een netwerk maken via een onbeveiligd draadloos toegangspunt dat achter een firewall is bevestigd;
- kwetsbaarheden in netwerkprotocollen uitbuiten, zoals FTP (File Transfer Protocol) en SSL (Secure Sockets Layer);
- een netwerk met te veel verzoeken overspoelen, waardoor geldige verzoeken niet meer doorkomen; dit wordt aangeduid met DoS (Denial of Service);
- een netwerkanalyser op een netwerksegment installeren dat elk passerend pakket vastlegt, waardoor vertrouwelijke informatie in platte tekst zichtbaar wordt.

Aanvallen op het besturingssysteem

Het hacken van een besturingssysteem (OS) is de favoriete aanvalsmethode van slechteriken. Een groot deel van de computeraanvallen bestaat uit OS-aanvallen, eenvoudigweg omdat elke computer een besturingssysteem heeft. Ze zijn vatbaar voor veel bekende exploits, inclusief kwetsbaarheden waar jaren later nog geen patch voor is geïnstalleerd.

Af en toe worden besturingssystemen die standaard veilig zijn, zoals de oude maar nog steeds gebruikte Novell NetWare, OpenBSD en IBM Series i, aangevallen en treden beveiligingslekken op. Maar hackers geven de voorkeur aan aanvallen op Windows, Linux en macOS omdat die veel meer worden gebruikt.

Dit zijn enkele voorbeelden van aanvallen op besturingssystemen:

- zoeken naar ontbrekende patches;

- aanval op ingebouwde authenticatiesystemen;
- beveiliging van het bestandssysteem hacken;
- wachtwoorden en zwakke encryptie-implementaties kraken.

Toepassingen en andere gespecialiseerde aanvallen

Toepassingen en apps zijn regelmatig het doelwit van hackers. Webapps en mobiele apps worden het meeste aangevallen, maar met weinig succes. Hier volgen enkele voorbeelden van aanvallen op apps die vaak deel uitmaken van een bedrijfsnetwerk:

- Webapps worden tegenwoordig algemeen gebruikt. Door zogeheten *schaduw-IT,* waarbij medewerkers van verschillende afdelingen van een bedrijf hun eigen technologie uitvoeren, zijn webapps in alle hoeken en gaten van het interne netwerk en in de cloud terug te vinden. Helaas zijn veel ICT- en beveiligingsprofessionals zich niet bewust van deze schaduw-IT en de risico's die eraan verbonden zijn.
- Mobiele apps worden steeds vaker doelwit van hackers door hun populariteit in een zakelijke omgeving. Er bestaan ook malafide apps in de appwinkels van besturingssystemen die problemen in je computeromgeving geven.
- Onbeveiligde bestanden met gevoelige informatie zijn overal aanwezig op werkstations, server-shares en in de cloud, bijvoorbeeld op plaatsen als OneDrive en Google Drive. Ook databasesystemen bevatten tal van kwetsbaarheden die kwaadwillende medewerkers kunnen misbruiken.

De principes van beveiligingsassessments

Beveiligingsprofessionals horen dezelfde aanvallen als kwaadwillende hackers uit te voeren op computersystemen, fysieke besturingselementen en mensen. In de vorige paragraaf lees je meer over deze aanvallen. Maar de bedoeling van een beveiligingsprofessional is natuurlijk om eventuele zwakke punten bloot te leggen. In delen 2 tot en met 5 vind je gedetailleerde informatie over het uitvoeren van dit soort aanvallen en over specifieke maatregelen tegen aanvallen op je bedrijf.

Om ervoor te zorgen dat beveiligingstests adequaat en professioneel worden uitgevoerd, moet een beveiligingsprofessional enkele basisprincipes volgen. In de volgende paragrafen lees je meer over de belangrijkste hiervan.


PAS OP

Je neemt grote risico's als je deze principes niet volgt. Ik heb gezien dat ICT-afdelingen ze tijdens het plannen en uitvoeren van beveiligingstests negeerden of vergaten. De resultaten waren op zijn zachtst gezegd niet positief.

Ethisch te werk gaan

In deze context betekent het woord *ethisch* dat je werkt volgens hoge professionele standaarden en waarden. Alles wat je doet, moet de bedrijfsdoelstellingen dienen, zonder verborgen agenda en ongeacht of je beveiligingstests uitvoert op je eigen systemen of bij iemand die je heeft ingehuurd. Je moet dus professioneel te werk gaan. Het betekent ook dat je al je bevindingen moet rapporteren, ook als ze mogelijk een politieke weerslag hebben. Dit klinkt misschien logisch, maar ik heb het al verschillende keren meegemaakt dat mensen beveiligingslekken negeerden om problemen uit de weg te gaan of om managers of leveranciers van dienst te zijn.

Betrouwbaarheid is het belangrijkste principe. Het is ook de beste manier om medestanders te krijgen (en te houden) voor je beveiligingsprogramma. Het misbruiken van informatie en macht is uit den boze, want dat is wat slechteriken doen. Zij verdienen de consequenties van hun slechte keuzen. Vergeet niet dat het mogelijk is om ethisch maar niet betrouwbaar te zijn en omgekeerd, een beetje zoals Edward Snowden. Met deze complexiteit moet je beveiligingsprogramma rekening houden. Dit zijn lastige problemen om rekening mee te houden.

Privacy respecteren

Behandel de informatie die je verzamelt met respect. Alle informatie die je tijdens het testen verzamelt, moet privé blijven, zoals fouten in een webapp, e-mailwachtwoorden en persoonlijk identificeerbare informatie (PII). Je schiet er niets mee op om in vertrouwelijke bedrijfsinformatie of het privéleven van medewerkers te neuzen.


TIP

Betrek anderen bij het proces. Organiseer een collegiale toetsing of een vergelijkbaar toezichtsysteem om steun voor de beveiligingsbeoordeling te krijgen.

Het systeem niet laten vastlopen

Een van de grootste fouten die je bij het testen van een eigen computersysteem kunt maken, is het per ongeluk laten crashen. De bedoeling is natuurlijk dat alles operationeel blijft. Computersystemen lopen niet meer zo vaak vast als vroeger, want ze zijn tegenwoordig veel stabieler, maar een slechte planning en timing kan nog steeds negatieve gevolgen hebben.

De kans is misschien niet zo groot, maar het is wel degelijk mogelijk om tijdens het testen een soort DoS-situatie te laten ontstaan. Als je snel na elkaar veel tests uitvoert, loop je de kans dat het systeem vastloopt, er gegevens verloren gaan, computers opnieuw opstarten en andere problemen optreden, vooral als je oude servers en webtoepassingen test. Geloof me, het is mij overkomen. Ga er niet van uit dat een netwerk of specifieke host het pak slaag aankan dat netwerktools en kwetsbaarheidsscanners uitdelen.

Het is zelfs mogelijk om per ongeluk een account of systeem te vergrendelen met een kwetsbaarheidsscan of door via social engineering iemands wachtwoord te laten wijzigen zonder de gevolgen van je acties te overzien. Ga voorzichtig te werk en gebruik je gezond verstand. Maar besef dat deze zwakke plekken bestaan en dat het beter is dat jij erachter komt dan iemand anders!


TIP

Bij veel kwetsbaarheidsscanners is het aantal tests dat tegelijkertijd op elk systeem wordt uitgevoerd in te stellen. Deze instellingen zijn erg handig als je de tests tijdens kantooruren op productiesystemen moet uitvoeren. Wees niet bang om scans langzamer uit te voeren; het proces duurt dan misschien langer, maar je voorkomt veel ellende als je met een onstabiel systeem te maken hebt.

Penetratietests in de praktijk

Net als bij vrijwel elk ander ICT- of beveiligingsproject moet je beveiligingstests goed plannen. Er wordt weleens gesteld dat handelen zonder planning de oorzaak is van elke mislukking. Stel de strategische en tactische aspecten van penetratietests van tevoren vast en maak er afspraken over. Om succesvol te zijn, is het noodzakelijk de tijd te nemen om elke test te plannen, ongeacht of dit een eenvoudige poging is wachtwoorden van het besturingssysteem te kraken of een volledige test van een complexe webomgeving.


PAS OP

Wees erg voorzichtig als je ervoor kiest een 'bekeerde' hacker voor het testen of een onafhankelijk advies in te huren. In hoofdstuk 19 lees je meer over de voor- en nadelen van het inzetten van externe beveiligingsbronnen.

Een plan formuleren

Het is essentieel dat je goedkeuring krijgt voor je beveiligingstests. Zorg ervoor dat wat je doet bekend en zichtbaar is, al is het maar bij leidinggevenden. Steun voor het project is de eerste stap. Op die manier worden je testdoelen gedefinieerd. Steun kan komen van je manager, iemand hoger op de ladder, een klant of van jezelf als je de baas bent. Maar je hebt iemand nodig die achter je staat, want anders kan je test onverwacht worden afgeblazen als iemand beweert dat je nooit toestemming hebt gekregen, waaronder derden zoals cloudservice en hostingproviders. Je loopt dan zelfs het risico op ontslag of een beschuldiging van criminele activiteiten.

De autorisatie mag uit een eenvoudige interne notitie of e-mailbericht van je baas bestaan als je de tests op je eigen systemen uitvoert. Bij testen voor een klant heb je een ondertekend contract met autorisatie van de klant nodig. Regel zo snel mogelijk een geschreven goedkeuring van deze steun om ervoor te zorgen dat geen tijd of moeite wordt verspild. Deze documentatie pleit je vrij als iemand, zoals een internetprovider, clouddienst of verwante leverancier, vraagt wat je aan het doen bent of als de politie op de stoep staat. Lach niet, want het zou niet de eerste keer zijn dat het gebeurde.

Eén foutje kan systemen doen crashen, iets wat je waarschijnlijk niet wilt. Je hebt een gedetailleerd plan nodig, maar geen boekwerk met testprocedures die het plan te ingewikkeld maken. Een goed gedefinieerd plan omvat de volgende informatie:

- **Specifieke systemen die getest worden.** Bij het testen van computersystemen begin je met de belangrijkste systemen en processen of systemen waarvan je vermoedt dat ze het kwetsbaarst zijn. Test bijvoorbeeld eerst de wachtwoorden van serverbesturingssystemen, een webapp op internet of doe een poging tot social engineering via e-mailphishing voordat je systemen diepgaand test.
- **Testrisico's.** Zorg voor een noodplan voor het geval er iets misgaat tijdens het testproces. Stel dat je firewall of webapp er tijdens het testen mee ophoudt. Hierdoor is het systeem misschien niet meer beschikbaar, waardoor de productiviteit van medewerkers afneemt. Dit kan zelfs leiden tot verlies van gegevensintegriteit, gegevensverlies en zelfs slechte

publiciteit. Je krijgt dan zeker met boze mensen te maken en je ziet er niet professioneel uit. Dit zorgt voor bedrijfsrisico's.

Wees erg voorzichtig met social engineering en DoS-aanvallen. Zorg ervoor dat je weet welke invloed ze hebben op de mensen en systemen die je test.

- **Testdatums en algehele tijdsplanning.** Het is belangrijk dat je goed nadenkt over het moment waarop de tests worden uitgevoerd. Bepaal of je tijdens kantooruren gaat testen of dat je het 's nachts of vroeg in de ochtend doet, zodat de productiesystemen niet worden beïnvloed. Zorg ervoor dat anderen je timing goedkeuren.

  Misschien krijg je last van DoS-gerelateerde gevolgen, maar de beste aanpak is een onbeperkte aanval, waarbij elk type test op elk moment van de dag mogelijk is. Slechteriken houden zich niet aan vaste tijdstippen, dus waarom zou jij dit wel doen? Uitzonderingen op deze aanpak zijn het uitvoeren van volledige DoS-aanvallen, social engineering en fysieke beveiligingstests.


TIP

- **Ben je van plan ontdekt te worden?** Misschien is het de bedoeling dat je de tests uitvoert zonder gedetecteerd te worden. Je voert de tests dan bijvoorbeeld op externe systemen of bij een ander filiaal uit zonder dat gebruikers door hebben wat je aan het doen bent. Weten ze dit wel, dan zetten gebruikers of ICT-medewerkers hun beste beentje voor en vertonen ze geen natuurlijk gedrag.
- **Moeten beveiligingsfuncties worden ingeschakeld?** Dit is erg belangrijk, maar wordt vaak over het hoofd gezien. Je moet vooraf beslissen of beveiligingsvoorzieningen zoals firewalls, inbraakpreventiesystemen (IPS'en) en webappfirewalls (WAF's) actief blijven om scans en inbraakpogingen te blokkeren. Laat je deze beveiligingen ingeschakeld, dan test je een realistische situatie. Toch heb je er vaak meer aan om deze beveiliging uit te schakelen (of door whitelisting van je IP-adres), zodat je een blik achter de schermen kunt werpen om de meeste kwetsbaarheden op te sporen.

  Veel mensen willen hun beveiligingsfuncties aan laten staan. Hierdoor ziet het computersysteem er beter uit, want veel beveiligingscontroles worden dan waarschijnlijk geblokkeerd. Zo'n defensieve benadering kan tot een schijnzekerheid leiden, want niet alle delen van de beveiliging van de organisatie komen hierdoor aan bod.
- **Kennis van de systemen voorafgaand aan het testen.** Je hebt geen uitgebreide kennis nodig van de systemen die je test; enige basiskennis is voldoende om zowel jou als de geteste systemen te beschermen. Het is niet moeilijk om de systemen te begrijpen als het je eigen computers betreft. Test je computersystemen van een klant, dan moet je misschien wat dieper graven. Ik ben overigens maar een paar keer door een klant gevraagd een volledig blinde beoordeling uit te voeren.

De meeste ICT-managers en beveiligingsprofessionals zijn nogal huiverig voor blinde assessments, want ze vergen meer tijd, zijn duurder en zijn soms minder effectief. Stem het type test dat je gaat uitvoeren goed af op de behoeften van de organisatie of klant.

- **Maatregelen die genomen worden als een belangrijke zwakte is ontdekt.** Stop niet nadat je een of twee gaten in de beveiliging hebt gevonden; kijk of er nog meer lekken zijn. Het is niet de bedoeling om eindeloos door te gaan of totdat alle systemen zijn gecrasht, maar ga gewoon op de ingeslagen weg verder tot er niets meer te hacken valt. Vind je geen kwetsbaarheden, dan heb je niet goed genoeg gezocht. Er zijn altijd kwetsbaarheden. Ontdek je iets groots, dan moet je deze informatie zo snel mogelijk met belanghebbenden delen (ontwikkelaars, databasebeheerders, ICT-managers), want een lek moet worden gedicht voordat er misbruik van wordt gemaakt.
- **Beschrijving van te leveren resultaten.** Tot de deliverables behoren rapporten van kwetsbaarheidsscanners en je eigen samenvatting over belangrijke kwetsbaarheden en aanbevelingen voor tegenmaatregelen die moeten worden geïmplementeerd.

Tools selecteren

Net als bij elk ander project, is het moeilijk om een taak effectief uit te voeren als je niet over het juiste gereedschap voor de beveiligingstests beschikt. Maar de juiste tools bieden natuurlijk geen garantie dat je alle juiste kwetsbaarheden opspoort. Ervaring is ook erg belangrijk.


TIP

Ken de beperkingen van je gereedschap. Veel kwetsbaarheidsscanners genereren foutpositieven en foutnegatieven (kwetsbaarheden onterecht benoemd). Andere slaan kwetsbaarheden over. In sommige situaties, bijvoorbeeld bij het testen van webapps, heb je meerdere kwetsbaarheidsscanners nodig om alle problemen op te sporen.

Veel tools zijn voor specifieke tests bedoeld en geen enkele tool test alles. Om dezelfde reden dat je een schroevendraaier niet als hamer gebruikt, moet je geen poortscanner inzetten om specifieke netwerkkwetsbaarheden te ontdekken. Je hebt hulpmiddelen nodig die voor de taak zijn ontworpen. Hoe meer (goede) tools je hebt, des te eenvoudiger de beveiligingsonderzoeken zullen zijn.

Zorg ervoor dat je de volgende software voor je taken gebruikt:

- Om wachtwoorden te kraken, heb je tools als Ophcrack en Proactive Password Auditor nodig.

» Voor een diepgaande analyse van een webapp is een kwetsbaarheidsscanner (zoals Netsparker of Acunetix Web Vulnerability Scanner) geschikter dan een netwerkanalyser (zoals Wireshark of Omnipeek).

De mogelijkheden van veel beveiligings- en hacktools worden verkeerd begrepen. Dit onbegrip leidt tot een negatief oordeel over uitstekende en legitieme hulpmiddelen; zelfs verschillende overheidsinstanties overwegen om ze illegaal te maken. Dit misverstand is deels te wijten aan de complexiteit van sommige beveiligingstools. Zorg ervoor dat je de tools die je gebruikt goed leert kennen voordat je ze inzet. Hierdoor ben je in staat ze te gebruiken op de manier waarop ze bedoeld zijn. Ga als volgt te werk:

» Lees de documentatie in de vorm van een readme-bestand, online Help-bestand of FAQ (frequently asked questions).

» Bestudeer de gebruikershandleiding.

» Gebruik de tools in een lab of testomgeving.

» Bekijk uitleg op YouTube (als je tegen de slechte kwaliteit van de meeste video's kunt).

» Volg eventueel indien mogelijk een training van de leverancier of een andere organisatie.

Let op de volgende kenmerken bij tools voor beveiligingstests:

» acceptabele documentatie;

» uitgebreide rapporten over ontdekte kwetsbaarheden, inclusief informatie over misbruik en reparatie ervan;

» algemeen geaccepteerd in de beveiligingswereld;

» beschikbaarheid van updates en technische ondersteuning;

» geavanceerde rapporten die geschikt zijn voor managers en niet-technische medewerkers (tegenwoordig erg belangrijk in een wereld van controle en naleving van regels).

Deze kenmerken besparen veel tijd en moeite bij het uitvoeren van een test en het schrijven van een eindrapportage.

VOORBEELDEN VAN TOOLS VOOR BEVEILIGINGSTESTS

Vraag wat anderen gebruiken voordat je een beveiligingstool selecteert. Win advies in bij collega's en anderen via Google, LinkedIn en YouTube. Er zijn honderden, zo niet duizenden tools voor beveiligingstests beschikbaar. Hierna volgen enkele van mijn favoriete commerciële, freeware en opensourcebeveiligingshulpmiddelen:

- Acunetix Web Vulnerability Scanner
- Cain & Abel
- CommView for WiFi
- Elcomsoft System Recovery
- Metasploit
- Nessus
- NetScanTools Pro
- Netsparker
- Nexpose
- Omnipeek
- SoftPerfect Network Scanner

Deze en veel andere tools worden in delen 2 tot en met 5 besproken bij specifieke tests. In de bijlage vind je een uitgebreide lijst van deze hulpmiddelen als referentie.

Het plan uitvoeren

Een goede beveiligingstest vergt doorzettingsvermogen. Ook tijd en geduld zijn belangrijk. Wees voorzichtig bij het uitvoeren van tests, want een crimineel op het netwerk of een schijnbaar goedaardige werknemer die over je schouder meekijkt, ziet mogelijk wat er gebeurt en kan deze informatie tegen jou of je bedrijf gebruiken.

Het is ondoenlijk om vooraf te controleren of er hackers op je systemen aanwezig zijn. Zorg ervoor dat alles zo rustig en privé mogelijk verloopt, vooral als je testresultaten verzendt en opslaat. Versleutel indien mogelijk e-mails en bestanden die gevoelige testinformatie bevatten, of deel ze via een cloudservice.

Je bent op verkenningstocht. Gebruik zo veel mogelijk informatie over je organisatie en systemen, net als kwaadwillende hackers. Begin met het overzicht en richt je daarna op details. Neem de volgende stappen:

1. **Zoek op internet naar de naam van je organisatie, de namen van de computers en netwerksystemen en de IP-adressen.**

   Google is een goed uitgangspunt.

2. **Concentreer je op de specifieke systemen die je test.**

   Een informele beoordeling kan veel informatie over je systemen opleveren, zowel bij fysieke beveiligingsstructuren als bij webapps.

3. **Voer scans en andere gedetailleerde tests uit om zwakheden op de systemen aan het licht te brengen.**

4. **Voer aanvallen uit en maak gebruik van alle kwetsbaarheden die je aantreft (als je deze aanpak kiest).**

In hoofdstukken 4 en 5 vind je meer informatie en tips over dit proces.

Resultaten evalueren

Beoordeel je resultaten om te zien wat je hebt ontdekt, ervan uitgaande dat de kwetsbaarheden niet eerder aan het licht zijn gekomen. Kennis is belangrijk. Je vaardigheden bij het evalueren van de resultaten en ze aan specifieke kwetsbaarheden koppelen worden beter naarmate je meer ervaring krijgt. Je gaat je systemen veel beter leren kennen dan anderen, waardoor het evaluatieproces veel eenvoudiger wordt in de toekomst.


TIP

Maak een officieel rapport voor het management of de klant, waarin je de resultaten en eventuele aanbevelingen duidelijk omschrijft. Houd deze partijen op de hoogte om te laten zien dat je inspanningen en hun geld goed zijn besteed. Hoofdstuk 17 beschrijft het rapportageproces voor beveiligingsassessments.

Vervolgstappen

Nadat je de beveiligingstests hebt voltooid, moet jij (of de klant) de aanbevelingen ook implementeren om ervoor te zorgen dat de systemen veilig zijn. Doe je dit niet, dan gaat alle tijd, geld en moeite die aan het testen is besteed verloren. Helaas komt dit nog vrij vaak voor.


BELANGRIJK

Er verschijnen voortdurend nieuwe beveiligingslekken. Informatiesystemen veranderen en worden complexer. Nieuwe beveiligingskwetsbaarheden en exploits worden ontdekt. Kwetsbaarheidsscanners worden beter.

Beveiligingstests bieden een momentopname van de beveiliging van computersystemen. Alles kan op elk moment veranderen, vooral nadat je software hebt bijgewerkt, computersystemen hebt toegevoegd of patches hebt toegepast. Dit geeft aan dat je hulpmiddelen vaak moet bijwerken, in feite voor elk gebruik. Test ze regelmatig en consistent (zoals maandelijks, eens per kwartaal of halfjaarlijks). Hoofdstuk 19 behandelt het beheer van beveiligingswijzigingen.