COMPUTERWORLD

IT sikkerhedsuddannelse

Artiklen er lang (næsten 8 A4 sider, så er du advaret) den indeholder mit bud på hvordan du kan gribe en it sikkerhedsuddannelse an, der er selvfølgelig andre måder

Skrevet den **03. Feb 2009** af **bufferzone** I kategorien **Sikkerhed / Generelt** | ★★★☆☆

IT sikkerhedsuddannelse, sådan kommer du til at arbejde med IT sikkerhed.

Jeg bliver ofte spurgt om hvilken uddannelse man skal gå efter hvis man vil arbejde med IT sikkerhed. Dette spørgsmål er vanskeligt at svare enkelt på, da der er mange forskellige veje og da uddannelsen kræver viden og erfaring man faktisk ikke kan få ved en formel uddannelse. Denne artikel indeholder derfor ikke VEJEN, men en beskrivelse at, hvilken viden og erfaring der er nødvendig samt nogle bud på hvordan denne vil kunne fås. Endelig vil jeg give nogle bud på hvordan man kan dokumentere sin viden så man også har en chance for at få et job i branchen.

Viden.
Lad os starte med den nødvendige viden. Denne skal være både bred og dyb.

Du skal have et indgående kendskab til operativsystemer, både workstation- og server operativsystemer. Det er ikke nok at du kan konfigurere og administrere dem, du er faktisk nødt til at have kendskab til hvordan de er skruet sammen, hvordan den interne arkitektur ser ud, hvilke protokoller de benytter sig af, hvordan de kommunikerer og replikerer, hvor de forskellige filer er placeret, hvilke services der køres/kan køres, hvordan rettigheder er sat/kan sættes.

Du skal have et indgående kendskab til applikationer, både almindelige- og server applikationer. Du skal vide hvordan de installeres, hvilke delservices der findes, hvad den enkelte delservices gør og hvordan de virker sammen. Du skal kende de vigtigste applikationers arkitektur, hvilke protokoller de anvender og hvordan de arbejder sammen.

Du skal have et indgående kendskab til alle former for netværk. Du skal kunne opsætte forskellige netværk i praksis, du skal kende til forskellige topologier, du skal kende alle de protokoller der hører til og du skal kunne både administrere og fejlfinde.

Du skal have et indgående kendskab til computer hardware. Du skal vide hvordan en PC er sat sammen, hvordan de enkelte enheder konfigureres, hvordan arkitektur og dataflow sker. Du skal vide hvordan en server er sat sammen. Og hvordan den adskiller sig fra en PC, du skal have et indgående og dybt kendskab om netkort af forskellige typer og du skal kunne konfigurere dem i søvne.

Du skal have et indgående kendskab til netværks enheder. Du skal kunne konfigurere routere, switche og firewalls. Du skal vide hvordan de enkelte enheder funger i detaljer, hvordan deres funktionalitet udnyttes i praksis og hvordan de arbejder sammen. Herunder også trådløst udstyr

Du skal have et indgående kendskab til forskellige gadgets, f.eks. PDA'er og andre håndholdte devices som du vil møde i dit net.

Du skal have viden om programmering og hvad der hører til af afledte ting. Dels er web baserede systemer et yndet mål og sikring af disse er særligt vigtigt da de jo oftest har direkte adgang til Internettet, og dels er det nødvendigt at du som IT sikkerheds mand kan gennemskue exploits og plugins

til diverse sikkerhedsscannere herunder særligt nessus. Du vil have brug for at kunne programmere i f.eks. HTML, Javascript, VB script, ASP, PHP og andre normale web programmerings og script sprog. Jeg vil især anbefale at du gør noget ud af Perl. Dette sprog er rigtigt stærkt til administration og automatisering af opgaver, der er mange exploits der er skrevet i Perl og Nessus plugins er skrevet i en forenkling af perl der hedder nessus Attack scripting language. Kendskab til et kompileret programmeringssprog er en nødvendighed hvis du vil være specialist i den tunge ende. Viden og kunden inden for C, assembler og Shellcode er nødvendig for at kune skrive og gennemskue exploits og har du også kendskab til højere niveauer som C++ eller/og C# er det kun en fordel.

Databaser er et andet område du er nødt til at kunne håndtere. Alle dynamiske sites er bygget oven på en eller anden form for database, og denne er et yndet mål som springbræt når hackere vil videre ind i dine systemer. Du skal altså både kunne håndtere den fysiske administration af f.eks en MYSQL eller ORACLE server, du skal kunne programmere databaserne og du skal kunne håndtere tilgangen til disse via SQL Statements.

Du skal have et indgående kendskab til Internettet. Hvordan er arkitekturen, hvordan virker teknologien, hvilke protokoller benyttes, hvor findes informationerne, hvordan udvikles de forskellige teknologier, hvor er markedsførende og hvem driver hvilke teknologier. Du skal kende Internettet bedre end du kender dit eget værelse.

Du skal have mere end indgående kendskab til TCP/IP protokol suiten. Jeg har nævnt protokoller flere gange, men da det er protokollerne der definere kommunikationen kan dette emne ikke fremhæves nok. Du skal kende TCP/IP på bit niveau, du skal kunne aflæse bit-strømme og vide præcist hvad det betyder når en navngiven bit har værdien 1 eller 0, du skal faktisk kunne tale både binært og hexadecimalt samt kunne oversætte flydende mellem de to

Du skal have indgående kendskab til hvordan en hacker arbejder, hvilke metoder og værktøjer findes, hvordan virker de, hvordan ser deres signaturer ud og hvordan beskytter man sig mod disse. Du skal vide hvor hacker ressourcer findes på nettet og hvad der rør sig i miljøet.

Erfaring.
Erfaring er en svær ting at beskrive og også at kvantificerer, men hvis du vil arbejde med IT sikkerhed er erfaring altafgørende. Du kan ikke identificere unormal og mistænkelig opførsel hvis du ikke har god føling med hvad der er normalt.

Du skal have erfaring med hvordan PC'er normalt opfører sig, både som stand alone maskiner og i netværk. Hvad er normale problemer, hvad går normalt i stykker, hvor meget plads bruges normalt på harddiskene, hvor stor processor belastningen normalt er, hvilke processer der normalt kører på en pc, hvilke services er normalt startet op, hvad der normalt skal konfigureres, hvordan registreringsdatabasen tweekes, hvor de vigtige filer befinder sig, hvad de gør, hvor store de er, hvad deres versions numre osv, osv

Du skal have erfaring med servere. Udover det der gælder for en pc, skal du have erfaring med hvad der normalt skal vedligeholdes og hvor ofte, hvordan belastningen normalt fordeler sig på en server i drift i et netværk, Hvilke nedbrud og hændelser der er normale at opleve. I det hele taget skal du have erfraing med hvad der er normal drift for både servere og arbejdsstationer i et netværk.

Du skal have erfaring med netværks administration og kommunikation helt ned på bit niveau. Hvad er normal netværkskommunikation, både mængden og arten, hvilke IP pakker forekommer normalt på dit net, i hvilke mængder og hvor ofte. Hvilke protokoller bruges og hvordan påvirker de dit net, Hvilke administrative tiltag foretages normalt og hvilke fejl ses og hvad er de enkelte fejls normale hændelsesfrekvens.

Du skal have erfaring med perimetermiljøet. Med dette mener jeg, at du skal vide hvad der røre sig ude på nettet. Hvilke orme og vira kører på nettet i øjeblikket, hvad er deres signatur og hvor ofte forekommer disse signaturer i din firewall log. Hvilke exploits, hackerværktøjer og scripts er populære i øjeblikket, hvordan er deres signatur og hvor ofte ses de i dine logfiler,

Du skal have erfaring med brugere. Hvad kan du forvente af dine brugere, hvilke dumme ting gør de, hvad kan de finde på at gøre for at omgå sikkerheden, husk at 80 % af alle sikkerhedsbrud kommer inde fra. Du er også nødt til at vide hvor dine brugere normalt mangler forståelse og viden, hvordan de håndtere passwords, det vil sikkert overraske dig hvor mange brugere der skriver deres password ned på små gule sedler, og så placere disse sedler nøjagtigt de samme steder som alle andre.

Du skal have erfaring med business kultur. Hvilke kommunikations behov har en normal forretning, hvilke procedurer, regler og krav eksistere, hvad siger lovgivningen, hvad koster det forskellige og hvor har en normal virksomhedsledelse fokus. Hvilke områder har en normal virksomhedsledelse problemer med at forstå, hvad vil de acceptere og hvordan skal de takles når problemer, hændelser, budgetter og andet skal præsenteres.

Uddannelserne.
Du kan finde masser af eksempler i IT branchen på folk der har meget lidt formel uddannelse og klaret sig rimeligt alligevel. Du finder dog flere eksempler på at folk med god solid uddannelsesmæssig baggrund klare sig til tops og eftersom der nu også i IT branchen findes forskellige formelle uddannelsesmuligheder vil de selvlærtes muligheder være mere begrænsede.
Jeg vil anbefale at du starter med en af de tungere teknologiske uddannelser af længere varighed, f.eks. ingeniør eller datalog. Anden naturvidenskabelig akademisk uddannelse f.eks. fra IT universitetet kan også gøre det, især hvis de kombineres med forskellige certificeringer, mere her om senere.
Nu sidder du måske og tænker, "er en datafagtekniker, IT supporter, datamatikker ikke nok?" Mit svar på det spørgsmål er "nok til hvad?". Det er klart at du med disse uddannelser kan komme til at arbejde med f.eks. routere, servere eller firewalls som specialist på et af disse områder, og hvis du er dygtig, heldig og har egenskaberne kan du også opnå en ledelsesmæssig stilling inden for IT sikkerhed eller en stilling hvor du arbejder med IT sikkerhed i bredere forstand. Det der er afgørende er vidensdybden, erfaringen samt selvfølgelig indstilling, holdning og kemi.

Certificeringer.
Af en eller anden grund er certificeringer ikke så almindelige i Danmark som i f.eks. USA. Der er masser af folk der tager kortere kurser, der egentlig er beregnet til certificering, men af forskellige grunde undlader de at gå op til prøverne og tage certificeringen.
Certificeringer er en udmærket måde at dokumentere viden på. Det er klart at certifikater ikke kan stå alene, men kan du dokumentere erfaring vil du have stor gavn af at kunne dokumentere din IT og IT sikkerhedsmæssige viden med certificeringer, især hvis du f.eks. ikke har en formel højre uddannelse. Her er hvad du med fordel kan tage af certificeringer:

MCP, MCSA og MCSE.
Microsoft har lavet en hel serie af certificeringer, der er internationalt anerkendte og som kan tages på forskellige måder i Danmark også.

Microsoft Certified Processional (MCP) er den titel du får når du tager den første enkelt certificering, du kan f.eks. være MCP på Windows XP eller på Windows 2003 server.

Microsoft Certified System Administrator kræver 6 MCP certificeringer og der er selvfølgelig krav til hvilke certificeringer du skal have, men der er nogen valgfrihed

Microsoft Certified System Engineer kræver 7 MCP certificeringer, der er nogen sammenfald med MCSA, men skal du have dem begge er du nødt til at tage i alt 8 certificeringer

Du opdager hurtigt at f.eks. en MCSE er dyr hvis du skal betale dig fra det hele, men det kan selvfølgelig

gøres billigere hvis du tænker dig om. Der findes meget godt bogmateriale, der indeholder øvelser og alt nødvendigt til at tage disse certificeringer, men du er nødt til at lave øvelserne i praksis for at bestå. Køb dette materiale, læs det til du kan det i søvne, lav alle øvelserne til du kan det i søvne, og køb så en prøve hos en autoriseret udbyder. Der findes også test prep materiale, hvor du kan øve dig på selve eksamensformen før du går til prøve. Jeg vil tro at du kan tage den første MCP for omkring 3.000,- kr. samt en masse hård arbejde.
Fidusen er at de fleste godkendte udbyderne jævnligt kører kampagner med tilbud til dem der allerede er MCP. Dette betyder at der er mulighed for at tage de efterfølgende certificeringer med 50 % på selve prøven. Dette skulle give dig mulighed for at tage de resterende 6 certificeringer for omkring 2.000,- kr. stykket, hvilket så giver en samlet pris for hele MCSE'en på 15.000,- kr. Dyrt måske, men det er din egen fremtid du investere i.

LPI
Også Linux er kommet med på certificerings kortet med Linux Professional Institute (LPI) certificeringen. Denne certificering er relativt ny, og der er ikke hel serien der udbyder i Danmark endnu. Certificeringen består af to niveauer med to eksamener på hvert niveau. Første niveau er Basic Level Administration med prøverne Linux Install and Use og Linux Install and Use. Andet niveau er Advanced Level Administration med prøverne Linux Administration Advanced og Linux Networking Advanced. Ligesom med Microsoft certificeringerne koster disse en del, dog ikke så dyrt og ligesom med Microsoft certificeringerne kan det gøres billigere. Prøvernes indhold er tilgængeligt og Linux er jo open source, så der er også masser af godt materiale til rådighed på nettet. Læs og øv dig til hoved falder af og tag så prøverne.

CCNA
Cisco har også en certificerings serie hvor Cisco Certified Network Associate CCNA er en af dem. Disse certificeringer har megen anseelse og hvis du skal arbejde men netværksinfrastruktur er disse absolut en fordel. Jeg har selv ingen af disse certificeringer hvorfor jeg her vil nøjes med at henvise til Cisco's hjemmeside hvor de er beskrevet i detaljer.

CPSA, (CPSM er udgået) CPSP, CISSP og GCFW
Når du er færdig med de fundameltale certificeringer, kan du gå i gang med de dciderede sikkerheds certificeringer. Her har firmaet Protego A/S været markedsledende og iværksat et par egne certificeringer, der efterhånden er anerkendt i hele landet.

CPSA er Certified Protego Security Analyst og handler om sårbarhedsanalyse, uddannelsen tager 3 gange 2 dage samt en hel dags certificeringsprøve. Uddannelsen er meget comprimeret, og det er absolut en nødvendighed at du arbejder med tingene før du tager prøven.

Selve prøven er tre delt.

I del 1 skal du på 3 timer lave en sårbarhedsanalyse af en web server og aflevere en rapport der beskriver dine fund, Med kun 3 timer til rådighed skal du vide hvad du gør, ellers når du det ikke.

Næste del drejer sig om at hardene den server du har analyseret for at fjerne de fundne sårbarheder og stramme op på sikkerheden. Dette har du 2 timer til. Da du kan risikere at stå over for en server der slet ikke er opdateret, er det også nødvendigt at du har helt styr på hvad du skal gøre, ellers kommer dine 2 timer hurtigt til at gå med genstarter.

I sidste del, bytter du server med en af de andre prøvedeltagere der har hardenet sin server og du skal nu på 2 timer lave en sårbarhedsanalyse samt en rapport. Igen tiden er knap og du skal vide hvad du gør.

CPSP er Certified Protego Security practicioner og lige som de andreprotego certificeringer et tre delt kursus. Kurset indeholder bl.a. opsætning og sikring af trådløse netværk, VPN, Intrution detection, Intrution prevention, Computer Forensic, Sikring af mail systemer og meget andet

CPSM er Certified Protego Security Manager er i dag erstattet helt af uddannelse til CISSP. Danske forhold,

herunder lovgivning gennemgås dog stadigt, hvor CISSP er meget international.

CISSP er Certified Information system Security Professionals og er nok en af de mest kende grundlæggende sikkerheds certificering på det internationale marked. CISSP arbejder med begrebet Common body of knowledge og de beskriver selv deres certificering som værende "a mile wide but an inch deep". CISSP er en grundlæggende certificering der i mange sikkerhedsvirksomheder er et krav til alle ansatte. Du kan tage CISSP'en ved selvstudie, (eksamen koster selvfølgelig) og mange anvender CPSM som forberedelse til CISSP.

GCFW er GIAC Certified Firewall Analyst og en af de hårdeste men også mest anerkendte sikkerhedscertificeringer på markedet. GIAC er Global Information Assurance Certification og som sådan organisationen SANS uddannelses og certificerings del. SANS er en forkortelse for SysAdmin, Audit, Network, Security og en af de mest anerkendt IT sikkerheds organisationer i verden (Sammen med CERT). Selve GCFW certificeringen kan gennemføres som selvstudie eller gennem Protego A/S som mentor uddannelse. (se www.protego.dk) Certificeringen er tredelt. Først skal du bestå 2 adskildte online multiple choice prøver i grundlæggende TCP/IP og firewall teknologi. 75 spørgsmål på 2 timer pr. prøve og sværhedsgraden er høj og selvom du må bruge materialet, har du ikke tid til at slå ret meget op. Herefter skal du lave et speciale (kaldet en practical) på engelsk på max 100 sider. Opgaven er bundet og drejer sig om at designe sikkerheden for en fiktiv virksomhed. Detaljeringsgraden er stor, du skal lave et færdigt firewall setup med konfiguration og det hele, et router setup med konfiguration og det hele og et VPN setup, ligeledes med konfigurations filer og alt andet. Du kan her se et eksempel på et speciale lavet af Protegos tekniske direktør, specialet fik Honers, hvilket betyder at det er usædvanligt godt.
http://www.giac.org/practical/Peter_Vestergaard_GCFW.zip

Start som Hacker???
Man hører ofte at dem der bliver taget for hacking eller for at lave virus ender med at få et godt job i IT sikkerhedsbranchen og så kunne man måske få den ide at det var en metode til at få job. Det vil jeg advare kraftigt imod. Selvom nogle at de meget kendte hackere har fået arbejde inden for branchen er der endnu flere der har fået meget store problemer ud af at forsøge sig med hacking. Problemer som fængselsstraffe og meget store erstatningskrav, da IT sikkerhed har mere fokus nu end før, er det min opfattelse at man vil gå endnu hårde til værks i fremtiden. Hvis du spørger de kendteste af de IT sikkerhedsfirmaer der findes i Danmark siger de alle samstemmende at de ikke ansætter folk med plettede straffe attester og især ikke når pletterne stammer fra IT relateret kriminalitet. Dette er egentligt ganske logisk. Disse firmaer skal have adgang til deres kunders inderste hemmeligheder og ressourcer, hvilke kræver tillid og integritet, derfor kan man selvfølgelig ikke sende folk ud der har en plettet fortid. Hacking er den sikre måde at sørge for at du aldrig kommer til at arbejde med IT sikkerhed, så lad være med at forsøge dig her.

Mig selv sagde hunden
Jeg er selv en af den der har en lidt speciel tilgang til arbejdet med IT og IT sikkerhed. Af uddannelse er jeg Officer i Hæren. Min nuværende grad er kaptajn og jeg arbejder med IT infrastruktur og drift ved Forsvarets Koncernfælles Informatik tjeneste. Min soldatermæssige tid startede ved Marineregimentet Bornholms Værn og da det blev nedlagt blev jeg Husar.
Officersuddannelsen er faktisk skruet sammen nogenlunde som en læges. Man starter med 3 års grundlæggende officersuddannelse, er så ude og virke som leder på forskellige niveauer i 3 til 8 år, hvorefter man (da jeg gennemførte det, i dag er det anderledes) gennemgik videregående officersuddannelse der var delt i to. En generel del og så en del hvor man kunne vælge mellem teknisk og operativ uddannelse. Jeg tog den tekniske.
Umiddelbart efter endt videreuddannelse blev jeg lærer i Informatik ved Hærens Officersskole og ikke ret længe efter chef for sektionen.
I den tid jeg har haft stillingen som IT chef, har jeg gennemgået forsvarets IT uddannelse (der svare nogenlunde til MCSE), uddannelse som IT sikkerhedsofficer, samt en masse kortere IT kurser ved forskellige civile IT kursusudbydere.
Jeg er pt. CPSA og GCFW certificeret, og håber at være CPSM og CISSP certificeret inden årets udgang.

Næste år er det planen at kikke på en formel MCSE/MCSA og hvis jeg får tid også LPI. Jeg overvejer også en masters fra ITU. se http://www.itu.dk

Denne lidt (meget) lange artikel er tænkt som nogle bud og inspiration på/til hvordan man kan gribe sin uddannelse an, hvis man er interesseret i at arbejde med IT sikkerhed. Den skal ikke betragtes som en facitliste. Skulle du have spørgsmål eller kommentarer til indholdet, så beder jeg dig maile mig på kim@bufferzone.dk i stedet for at ligge dem i artiklens kommentarer, dem kan jeg jo ikke svare på

Kommentar af immergut d. 07. Feb 2005 | 1

Kommentar af fastwrite d. 21. Dec 2004 | 2

Superflot artikel, Bufferzone! Du brillerer virkelig med dine artikler! Hvornår skriver du din næste? ;o)

Jeg fik lært meget, og jeg læste ALT hvad du skrev her kl. 01:30 om morgenen. Jeg er selv systemkonsulent med sikkerhed i høj fokus, men har ikke så mange uddannelser eller fine titler bag mig.. endnu. Men det kommer!

Kommentar af brixz d. 16. Apr 2007 | 3

Det var rigtig spændende læsning

Kommentar af basementjack d. 30. Oct 2004 | 4

Lang og informativ artikel, hvis man tænker på den type uddannelse uden at vide noget, er den nok 5 point værd. :)

Kommentar af blackadder d. 30. Jan 2005 | 5

Fint overblik, god artikel.

Jeg kunne dog ikke umiddelbart finde information om en master uddannelse på www.itu.dk

Der er vistnok en masteruddannelse på Århus Universitet:
http://www.aicis.alexandra.dk/projekter/master.htm

Derudover er der en kort oversigt over de offentlige uddanelser i IT-sikkerhed her:
http://www.rfits.dk/Uddannelser.3294.0.html

Kommentar af xyborx d. 23. Dec 2004 | 6

Der kan man bare se. Interessant :)

Kommentar af googolplex d. 21. Nov 2004 | 7

Kommentar af kmunk1975 d. 12. Mar 2005 | 8

Jamen hvad med os it nørder som render rundt og sætter computer og sikkerhed op. Hvad gør vi får at nå videre.. inden for området lokalnet og xp og hjemme sikkerhed. km
Men flot præsenteret!
Det andet

Kommentar af htmlkongen d. 23. May 2006 | 9

Avanceret artikel. Den er ikke til "Den almindelige bruger". Det er på noget højere plan. Ellers ganske fremragende, dog lidt "overdrevet" på NOGLE punkter til "normalt behov". Fx. "Lad os starte med den nødvendige viden. Denne skal være både bred og dyb."
---------->
"Jeg vil især anbefale at du gør noget ud af Perl. Dette sprog er rigtigt stærkt til administration og automatisering af opgaver, der er mange exploits der er skrevet i Perl og Nessus plugins er skrevet i en forenkling af perl der hedder nessus Attack scripting language" ------> Det er på noget højt niveau (ellers så er det bare mig der er på lavt)

Alt i alt en fremragende artikel. Der er INGEN tvivl om at hvis man forstår og kan disse ting i praksis er man en MEGET dygtig person med et stort indblik i hvordan tingene hænger sammen.....!!

Meget flot stykke arbejde...!

/Htmlkongen

Kommentar af dustie d. 19. Dec 2008 | 10

Super som altid.

Kommentar af bernie d. 30. Oct 2004 | 11

bufferzone har gjort det igen :D

Kommentar af bigshow d. 14. Feb 2005 | 12

Hvad skal jeg sige, det kunne jeg ikke engang, gøre lige så godt.

Kommentar af sorenbs d. 01. Nov 2004 | 13

TAK!!!

Kommentar af jeanette18 d. 17. Aug 2005 | 14

Ganske stort må jeg sige :)

Kommentar af freehelp d. 01. Jan 2005 | 15

Flot artikel!

Kommentar af optical d. 07. May 2005 | 16

brøl

Kommentar af alaflam d. 01. Nov 2004 | 17

Fanatastik

Kommentar af areon d. 25. Nov 2004 | 18

Jamen kan ikke få sluttet med det læsning da DINE artikler simpelhen bare er SUPER!!

Kommentar af brian-johansen d. 26. Mar 2007 | 19

Kanon artikel
/Brian
http://relay.thingholm.dk/fidibus

Kommentar af cybergeek d. 23. Dec 2004 | 20

Det må jeg nok sige, den er sgu kanon flot denne artikel :D tror jeg har fået mere blod på tanden til at finde arbejde inden for it sikkerhed, og prøve at tage nødvendige kursuer og sådan

Kommentar af cookie_ll d. 15. Jan 2005 | 21

Fantastisk inspirerende artikel! (Sorry, men lidt internt: Guldbar med Knas, igen krydses vores veje ;o)! Knuz Cookie_ll)