Stichting NIOC en de NIOC kennisbank

Stichting NIOC (www.nioc.nl) stelt zich conform zijn statuten tot doel: het realiseren van congressen over informatica onderwijs en voorts al hetgeen met een en ander rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin des woords.

De stichting NIOC neemt de archivering van de resultaten van de congressen voor zijn rekening. De website www.nioc.nl ontsluit onder "Eerdere congressen" de gearchiveerde websites van eerdere congressen. De vele afzonderlijke congresbijdragen zijn opgenomen in een kennisbank die via dezelfde website onder "NIOC kennisbank" ontsloten wordt.

Op dit moment bevat de NIOC kennisbank alle bijdragen, incl. die van het laatste congres (NIOC2023, gehouden op donderdag 30 maart 2023 jl. en georganiseerd door NHL Stenden Hogeschool). Bij elkaar bijna 1500 bijdragen!

We roepen je op, na het lezen van het document dat door jou is gedownload, de auteur(s) feedback te geven. Dit kan door je te registreren als gebruiker van de NIOC kennisbank. Na registratie krijg je bericht hoe in te loggen op de NIOC kennisbank.

Het eerstvolgende NIOC vindt plaats op donderdag 27 maart 2025 in Zwolle en wordt dan georganiseerd door Hogeschool Windesheim. Kijk op www.nioc2025.nl voor meer informatie.

Wil je op de hoogte blijven van de ontwikkeling rond Stichting NIOC en de NIOC kennisbank, schrijf je dan in op de nieuwsbrief via

www.nioc.nl/nioc-kennisbank/aanmelden nieuwsbrief

Reacties over de NIOC kennisbank en de inhoud daarvan kun je richten aan de beheerder:

R. Smedinga kennisbank@nioc.nl.

Vermeld bij reacties jouw naam en telefoonnummer voor nader contact.

7

Een virtueel computersecuritylab

Harald Vranken - Open Universiteit Nederland, Faculteit Informatica. harald.vranken@ou.nl, tel. 045 - 576 2373

Herman Koppelman - Open Universiteit Nederland, Faculteit Informatica. Postbus 2960, 6401 DL Heerlen

INTRODUCTIE

Aan de Open Universiteit Nederland is in 2007-2008 een cursus ontwikkeld op gebied van security en IT. Een prominent onderwerp in deze cursus is de veiligheid en de beveiliging van computernetwerken. Hierbij is een virtuele omgeving ontwikkeld (het virtuele computersecuritylab) waarin een student op zijn eigen pc een virtueel computernetwerk kan configureren en simuleren. In dit netwerk kan de student vervolgens experimenten en opdrachten uitvoeren op gebied van security. De student kan in het virtuele lab verschillende rollen aannemen. In de rol van hacker kan hij aanvallen uitvoeren op het netwerk; in de rol van systeembeheerder of beveiliger kan hij het netwerk tegen aanvallen beveiligen; in de rol van gebruiker van computersystemen in het netwerk kan hij de effecten van aanvallen en beveiligingsmaatregelen ervaren. Het virtuele lab beoogt enerzijds om de cursus aantrekkelijk te maken, wat een positief effect heeft op de motivatie van studenten, en anderzijds om de opgedane theoretische kennis met praktische opdrachten te verdiepen en te borgen.

De indeling van dit artikel is als volgt. In sectie 1 beschrijven we de inhoud en de didactische opzet van de cursus Security en IT. In sectie 3 geven we een beknopt overzicht van de verschillende soorten computersecuritylabs zoals die in de afgelopen jaren in de wetenschappelijke literatuur zijn beschreven. Aan de hand daarvan positioneren we ons virtuele computersecuritylab. In sectie 4 gaan we nader in op de architectuur en de implementatie van het virtuele computersecuritylab. In sectie 5 lichten we kort de opdrachten toe die studenten in het virtuele lab uitvoeren. Sectie 6 sluit het artikel af.

DE CURSUS SECURITY EN IT

De cursus Security en IT geeft een breed overzicht van het vakgebied security, waarbij de nadruk ligt op de technische aspecten van beveiliging. De cursus bestrijkt de basisprincipes van cryptografie en de beveiliging van software, besturingssystemen, databases en computernetwerken. Bij elk onderwerp wordt achtereenvolgens bekeken: welke kwetsbaarheden zijn er, welke aanvallen zijn daardoor mogelijk, hoe kunnen we deze aanvallen voorkomen en hoe kunnen we geslaagde aanvallen ontdekken. Daarnaast is er ook aandacht voor beheer, economische aspecten, privacy en actuele ontwikkelingen.
De cursus is gebaseerd op het Engelstalige tekstboek Security in Computing van C.P. Pfleeger en S. Lawrence Pfleeger (4e editie, 2006), en enkele hoofdstukken uit Computer Security van D. Gollmann (2e editie, 2006). Daarnaast heeft de Open Universiteit twee cursusboeken ontwikkeld die de leidraad vormen voor de student. In deze cursusboeken is de leerstof gestructureerd in een aantal leereenheden. Elke leereenheid bevat een afgerond deel van de leerstof dat in 4 tot 8 uur bestudeerd kan worden en bestaat uit een korte inleiding, een overzicht van de leerdoelen, studeeraanwijzingen waarin wordt aangegeven welke delen uit de tekstboeken bestudeerd moeten worden, toelichtingen en aanvullingen bij de tekstboeken, opgaven, praktische opdrachten, een afsluitende zelftoets en een uitgebreide terugkoppeling met antwoorden bij de opgaven, opdrachten en zelftoets. Met behulp van deze cursusboeken kan de student geheel zelfstandig de leerstof bestuderen. De cursus is daarom vooral geschikt voor afstandonderwijs zoals dat door de Open Universiteit wordt verzorgd. Bij de cursus hoort verder een elektronische leeromgeving (ELO) waar de student aanvullende studiematerialen kan vinden, zoals verwijzingen naar achtergrondinformatie, actuele mededelingen, software downloads, oefententamens en een discussieruimte. Het contact tussen studenten en docenten vindt plaats via de ELO en e-mail.
In de cursus voeren de studenten diverse praktische opdrachten uit. Bij het onderwerp cryptografie maken ze gebruik van interactieve webpagina's, bij het onderwerp bufferoverflows voeren ze simulaties uit, en bij het onderwerp netwerken voeren ze diverse opdrachten uit in het virtuele computersecuritylab. De praktische opdrachten in het virtuele lab beslaan circa 10% van de studietijd.

De cursus is sinds 2008 een verplicht onderdeel van de bacheloropleiding Informatica aan de Open Universiteit. Masterstudenten Computer Science

Opname van de Openingssessie

Samen een borrel drinken hoort er ook bij

kunnen deze cursus doen in een schakelprogramma of als keuzevak. De cursus is begin 2008 voor het eerst door 15 studenten gevolgd. De ervaringen van de studenten zijn uitgebreid geëvalueerd en waren doorgaans zeer positief. Aan de hand van deze ervaringen is het cursusmateriaal verder verbeterd. De cursus is ook toegankelijk voor studenten die niet de gehele bachelor- of masteropleiding volgen maar slechts een enkele cursus doen uit interesse of als bijscholing. Om de cursus toegankelijk te maken voor zulke losse cursisten, zijn de ingangseisen voor de cursus beperkt gehouden. Als benodigde voorkennis is globale kennis vereist van de architectuur van het internet en computernetwerken, relationele databases, besturingssystemen en een programmeertaal. Bij het onderwerp cryptografie ligt de nadruk op de werking van algoritmes en toepassingen, waarbij de wiskundige achtergrond bewust is vermeden. (Het tekstboek bevat een hoofdstuk dat dieper op de wiskunde ingaat, maar dat is geen verplichte leerstof. In de bacheloropleiding wordt overigens in een aparte wiskundecursus wel aandacht besteed aan getaltheorie waarop cryptografie is gebaseerd.)

COMPUTERSECURITYLABS

In veel onderwijsinstellingen zijn computersecurity-laboratoria te vinden. Dit zijn veelal ruimtes waarin computernetwerken zijn ondergebracht die volledig zijn geïsoleerd van de rest van de wereld (bijvoorbeeld [1]). Deze volledige isolatie voorkomt dat activiteiten in het lab via het netwerk de buitenwereld kunnen bereiken. Zulke 'fysieke labs' zijn echter ongeschikt voor afstandonderwijs, omdat studenten vanwege tijd- en plaatsbeperkingen het lab niet kunnen bereiken. Een alternatief is een fysiek lab dat door studenten op afstand bereikt kan worden via het internet. Het lab bestaat dan uit een geïsoleerd netwerk met een enkele verbinding naar de buitenwereld. Deze externe verbinding dient zeer goed beveiligd te zijn, bijvoorbeeld door middel van een firewall en toepassing van SSH of VPN. Voorbeelden van zulke labs zijn [2][3] [4][5]. Hoewel zulke labs op afstand bereikbaar zijn, zijn er toch beperkingen voor toepassing in afstand-onderwijs. Bij grote aantallen studenten moet er een reserveringssysteem opgezet worden, waarin studenten van tevoren een tijdslot kunnen reserveren om het lab te gebruiken. Studenten aan de Open Universiteit kunnen op elk moment met de cursus beginnen, waardoor het aantal studenten op een gegeven tijdstip zeer moeilijk in te schatten is. Het bepalen van de benodigde capaciteit in een lab is dan een lastige klus, en zal leiden tot overdimensionering. Naast de administratieve complexiteit rondom een reserveringssysteem, bestaat de kans dat dit studenten ook belemmert in hun vrijheid van studietijd en studietempo.
Het beheer van fysieke labs was in het verleden vaak problematisch. Studenten werken in het lab met root rechten en kunnen naar believen systeemconfiguraties aanpassen. Na afloop van een sessie is het daarom noodzakelijk om de configuraties van systemen weer op orde te brengen, wat soms zelfs complete herinstallaties vereist. In veel labs wordt daarom tegenwoordig gebruik gemaakt van gevirtualiseerde omgevingen, waarmee herconfiguratie en herinstallatie van systemen aanzienlijk vergemakkelijkt en zelfs geautomatiseerd kan worden (bijvoorbeeld [6][7]).

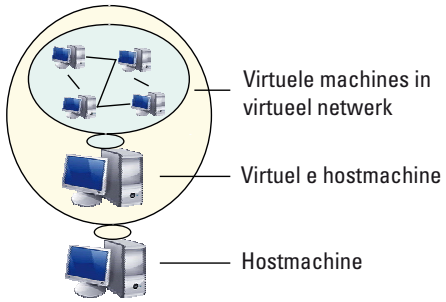
Als alternatief voor een fysiek lab op afstand is voor de cursus Security en IT een stand alone virtueel lab ontwikkeld, dat bestaat uit een virtuele omgeving die elke student op zijn eigen pc kan installeren. De benodigde (open source en gratis) software voor het virtuele lab wordt op een dvd aan de student verstrekt. De student hoeft dus geen verbinding te maken met een lab op afstand. Deze vorm vermijdt exploitatie en beheer van een lab op afstand, en kan voor een ongelimiteerd aantal studenten toegepast worden. Onderhoud en beheer van het lab wordt nu bij de individuele student gelegd, maar door toepassing van virtualisering is dit een minimale taak die beperkt is tot enkele muisklikken en nauwelijks tijd vergt.
Het virtuele lab draait op nagenoeg alle Linux- en Windowsplatforms, en is daarom geschikt voor vrijwel alle studenten-pc's. Deze opzet is uitermate geschikt voor afstandonderwijs, en kan zonder problemen ook bij contactonderwijs ingezet worden. Deze opzet sluit nauw aan bij [8], waar de voordelen van (open source) virtuele omgevingen bij toepassing in (afstand)-onderwijs verder worden toegelicht.

ARCHITECTUUR VAN HET VIRTUELE LAB

Het virtuele computersecuritylab maakt gebruik van virtualisatiesoftware. Deze virtualisatiesoftware introduceert een extra softwarelaag met bijbehorende interface die logische abstractie van de onderliggende hardware en software realiseert [9]. Het principe van virtualisatie dateert al uit de jaren zestig (IBM 370 mainframes), maar heeft sinds eind jaren negentig aanzienlijke, hernieuwde aandacht. Tegenwoordig is er tal van softwareomgevingen beschikbaar waarmee meerdere besturingssystemen in aparte, geïsoleerde omgevingen op een enkel systeem kunnen worden uitgevoerd. Slimme softwarearchitecturen en voorzieningen in de hardware van microprocessoren minimaliseren de afname in performance ten gevolge van virtualisatie.
Het virtuele computersecuritylab bestaat uit een virtuele omgeving op de pc van de student. In deze virtuele omgeving kan de student diverse virtuele machines instantiëren en aan virtuele netwerken koppelen. De student kan op deze virtuele machines met root rechten werken en kan de virtuele netwerken configureren.

De architectuur van het virtuele lab is tot stand gekomen door overweging van de volgende uitgangspunten. Allereerst dient de virtuele omgeving geschikt te zijn voor diverse Windows- en Linuxplatforms, zodat nagenoeg elke student deze thuis op zijn pc

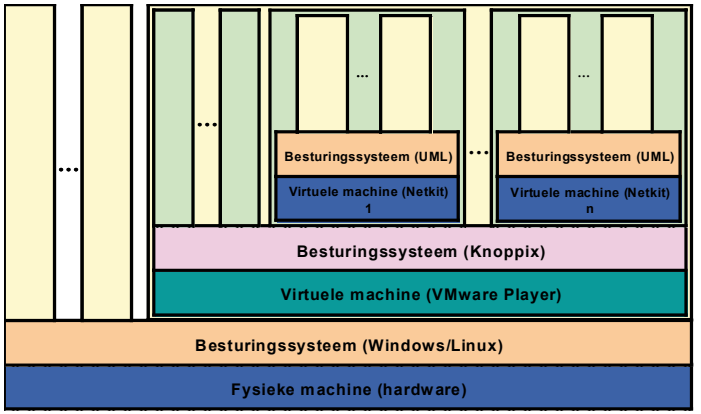
kan installeren. De virtualisatiesoftware dient verder open source of gratis zijn, en tevens betrouwbaar, gebruikersvriendelijk en toekomstbestendig (vooral door ondersteuning van nieuwe versies van Windows en Linux). Verder dient in de virtuele omgeving een natuurgetrouwe simulatie van een computernetwerk mogelijk te zijn. Ten slotte moet de virtuele omgeving volledig van de buitenwereld afgeschermd kunnen worden zodat een student daarin alle mogelijke activiteiten kan uitvoeren op gebied van security, zoals het uitvoeren van aanvallen die strafbaar of op zijn minst ongewenst zijn in een concreet computernetwerk.
Het virtuele computersecuritylab bestaat uit twee virtualisatielagen, zoals conceptueel weergegeven in figuur 1. De pc van de student, met een willekeurig Windows- of Linuxbesturingssysteem, duiden we aan als de hostmachine. Een eerste virtualisatielaag creëert een virtuele omgeving op de host machine. Deze virtualisatielaag wordt gerealiseerd door een softwareapplicatie, die net als elke andere applicatie draait op de hostmachine. Deze eerste virtualisatielaag creëert een virtuele machine waarbinnen het Linux besturingssysteem draait. We duiden dit aan als de virtuele hostmachine. In principe zou in de virtuele host machine ook een ander besturingssysteem gekozen kunnen worden. Het voordeel van Linux is echter dat dit open source software is en onder studenten verspreid mag worden zonder licentiekosten. Op de virtuele hostmachine kunnen Linuxapplicaties worden uitgevoerd. We passen een tweede virtualisatielaag toe, die wordt gerealiseerd door een Linuxapplicatie die draait op de virtuele hostmachine. We kiezen hierbij voor virtualisatie op basis van User Mode Linux (UML), wat het mogelijk maakt om een Linuxkernel als een applicatieproces uit te voeren binnen Linux. Op deze wijze kunnen relatief eenvoudig meerdere virtuele machines worden gecreëerd binnen de virtuele host machine. De virtuele machines beschikken over virtuele netwerkinterfaces en kunnen in virtuele netwerken worden aangesloten.



Figuur 1:
Twee virtualisatielagen

Figuur 2 toont de architectuur van het virtuele lab in meer detail. De eerste virtualisatielaag wordt gerealiseerd door VMware-Player, een softwareapplicatie die draait op de hostmachine. VMware-Player creëert een abstractie van de hardware en het besturingsysteem van de hostmachine. In VMware-Player kunnen we een enkele virtuele machine instantiëren, de virtuele hostmachine die we voorzien van een Linuxbesturingssysteem (Knoppix). In de virtuele host machine passen we de Netkit software toe om meerdere virtuele machines te instantiëren via UML [10]. Op elk van deze virtuele machines kunnen we ten slotte een of meer applicaties uitvoeren.

De software voor het virtuele lab wordt op een dvd aan studenten geleverd. De dvd bevat de installatiesoftware voor VMware-Player op een Windows- en Linux-pc. Verder bevat de dvd een virtualmachine-configurationfile en een ISO-bestand. Bij het opstarten van VMware-Player, selecteert de student de virtualmachineconfigurationfile, waarmee de virtuele hostmachine wordt geconfigureerd en het ISO-bestand wordt geladen. Het ISO-bestand bevat het Linuxbesturingssysteem met daarin alle applicaties (waaronder Netkit) die de student nodig heeft voor het uitvoeren van de opdrachten.



Figuur 2:
Architectuur van het virtuele lab

Voor de installatie van het virtuele lab volstaat het dus om VMware-Player te installeren, wat met behulp van enkele muisklikken in een wizard kan gebeuren. De virtuele hostmachine maakt gebruik van een virtuele disk. Het file system van de virtuele hostmachine wordt opgeslagen op deze virtuele disk, die wordt geïmplementeerd met enkele gecomprimeerde bestanden op de fysieke disk van de hostmachine.
Ook de virtuele machines hebben elk een virtuele disk, waarbij elke virtuele disk wordt geïmplementeerd met enkele gecomprimeerde bestanden op de virtuele disk van de virtuele hostmachine.
Na installatie kan het virtuele lab met een enkele muisklik worden opgestart. Het virtuele lab kan naar keuze worden afgesloten op twee manieren. Bij de eerste manier wordt de toestand van de virtuele host machine niet bewaard en wordt de virtuele host machine gereset. Bij de tweede manier wordt de toestand van het virtuele lab opgeslagen. Als het virtuele lab vervolgens weer wordt opgestart, bevindt het zich in dezelfde toestand als bij het afsluiten. Dit is handig bij het uitvoeren van opdrachten die veel tijd vergen. Als een student onvoldoende tijd heeft om een opdracht volledig te voltooien, kan hij het lab afsluiten en later de draad weer oppakken.
De ervaringen van studenten met het virtuele lab zijn uitgebreid geëvalueerd. Studenten zijn doorgaans zeer positief en hebben nauwelijks problemen ondervonden met de installatie en het gebruik van de software. Een beperking is dat in het virtuele lab alleen met Linux gewerkt wordt. Verder heeft de virtuele hostmachine weliswaar een Windowsomgeving (KDE), maar de virtuele machines kennen slechts tekstgebaseerde in- en uitvoer.

OPDRACHTEN IN HET VIRTUELE LAB

Een student voert een aantal opdrachten uit in het virtuele lab. In elke opdracht instantieert en configureert de student enkele virtuele machines en verbindt deze in virtuele netwerken. Bij de complexere opdrachten

kan de student een script downloaden van de elektronische leeromgeving waarmee de instantiatie en configuratie van virtuele machines en netwerkconnecties wordt geautomatiseerd.
Een eerste reeks opdrachten is gericht op het voorbereiden van een aanval, waarbij met behulp van portscanning en packetsniffing informatie verzameld wordt over een doelwit. In een tweede reeks opdrachten gaat de student een man-in-the-middle-aanval en een denial-of-service-aanval uitvoeren. In een derde reeks opdrachten gaat de student een gedemilitariseerde zone (DMZ) opzetten tussen een virtueel intranet en een virtueel internet met behulp van diverse soorten firewalls. Hierbij wordt ook een intrusiondetectionsysteem toegepast. In een vierde reeks opdrachten oefent de student met toepassing van asymmetrische cryptografie voor het uitwisselen van berichten met behulp van PGP.
In de cursusboeken wordt uitleg gegeven over de opbouw en werking van het virtuele lab. De opdrachten staan eveneens beschreven in de cursusboeken. Hierin wordt stapsgewijs aangegeven welke commando's uitgevoerd moeten worden en wat het resultaat daarvan is. Er worden vragen gesteld, die veelal betrekking hebben op het verklaren van bepaalde waarnemingen. De antwoorden op de vragen zijn in het cursusboek opgenomen.
De opdrachten die de student uitvoert, worden niet expliciet beoordeeld. Voor deze opzet is met name gekozen om de hoeveelheid werk voor de docent te beperken. Omdat studenten de opdrachten zelfstandig uitvoeren zonder bijzijn van de docent, zouden tevens maatregelen nodig zijn om fraude te achterhalen. De kennis die de student geacht wordt op te doen bij de opdrachten in het virtuele lab, wordt op het tentamen getoetst.

Assistentes van de congresorganisatie blij om het verloop van het congres

CONCLUSIE

Ten behoeve van de cursus Security en IT aan de Open Universiteit Nederland is een virtueel computersecuritylab ontwikkeld. In dit lab kunnen studenten in diverse rollen (hacker, gebruiker, beveiliger/systeembeheerder) aan de slag. Het virtuele lab bestaat uit software waarmee twee virtualisatielagen worden gecreëerd. Met deze aanpak kan elke student eenvoudig een stand alone virtueel lab op zijn eigen pc creëren en zelfstandig opdrachten uitvoeren.

DANKWOORD

We danken Marcel Spruit en Pieter Burghouwt van de Haagse Hogeschool, die ons attendeerden op de Netkit software en een aantal praktische opdrachten ontwikkelden. We danken Jörg Keller en Ralf Naues van de FernUniversität in Hagen voor discussies rondom het virtuele lab.

↑

[1]
J. Hill et al., Using an isolated network laboratory to teach advanced networks and security. SIGCSE Bull., 33(1), pp. 36-40, 2001.
[2]
K. Krishna et al., V-NetLab: a cost-effective platform to support course projects in computer security. Proc. Coll. for Information Systems Security Education, 2005.
[3]
J. Hu, D. Cordel en Ch. Meinel, Virtual machine management for Tele-Lab. IEEE Symp. on Computers and Communications, pp. 448-453, 2005.
[4]
J. Keller en R. Naues, Design of a virtual computer security lab. Proc. IASTED Int. Conf. on Communication, Network, and Information Security, pp. 211-215, 2006.
[5]
H. Lahoud en X. Tang, Information security labs in IDS/IPS for distance education. Proc. Conf. on Information Technology Education, pp. 47-52, 2006.
[6]
B. Hay en K. Nance, Evolution of the ASSERT computer security lab. Proc. Coll. for Information Systems Security Education, 2006.
[7]
M. O'Leary, A laboratory based capstone course in computer security for undergraduates. Proc. Techn. Symp. on Computer Science Education, pp. 2-6, 2006.
[8]
A. Gaspar, S. Langevin en W. Armitage, Virtualization technologies in the undergraduate IT curriculum. IEEE IT Pro, pp. 10-17, July-August 2007.
[9]
J. Smith en R. Nair, Virtual machines: versatile platforms for systems and processes (Morgan Kaufmann, 2005).
[10]
M. Pizzonia en M. Rimondini, Easy emulation of complex networks on inexpensive hardware. Proc. Int. Conf. on Testbeds and Research Infrastructures for the Development of Networks & Communities, pp. 1-10, 2008.