### Penetrationstestningens betydelse för företagssäkerhet

#### Annika Kråkström

Avhandling för kandidatexamen

Fakulteten för naturvetenskaper och teknik

Åbo Akademi

Åbo, 2018

#### Abstrakt

Den här avhandlingen undersöker penetrationstest och deras betydelse för företag i hopp om att ge en insikt i hur företag kan skydda sig mot hackare. Det kan vara skrämmande för ett företag att bjuda in en person för att hacka sig in i deras system men den här avhandlingen hoppas göra processen mer förståelig och ge företag en känsla av trygghet. Det som diskuteras är: vad ett penetrationstest är, vem som utför testen och varför de behövs, men fokus kommer att vara på processen för penetrationstestet. Avhandlingen går igenom steg för steg vad testaren faktiskt gör och förklarar de aspekter som klienten kan kontrollera och de aspekter som testaren har full kontroll över. Det viktigaste att minnas när det gäller ett penetrationstest är att allting måste diskuteras noggrant innan testet inleds, under den här diskussionen ska klienten förklara exakt varför testet görs, vilka system som ska testas och på vilka sätt. Det är alltså klienten som har full kontroll över processen för att minimera risken för oväntade händelser.

Innehållsförteckning

[1. Introduktion 4](#_Toc510177756)

[2. Definitioner 4](#_Toc510177757)

[3. Vad är penetrationstest? 5](#_Toc510177758)

[4. Varför penetrationstest? 6](#_Toc510177759)

[5. Vem gör penetrationstest? 7](#_Toc510177760)

[6. Vad skyddas? 8](#_Toc510177761)

[7. Vilka är de illvilliga hackarna? 9](#_Toc510177762)

[8. Penetrationstestarens process 10](#_Toc510177763)

[8.1. Överenskommelse 10](#_Toc510177764)

[8.2. Informationssamling och passiv analys 11](#_Toc510177765)

[8.3. Aktiv analys 12](#_Toc510177766)

[8.4. Exploatering 12](#_Toc510177767)

[8.5. Eskalering av privilegier samt insamling av data 13](#_Toc510177768)

[8.6. Rapport 14](#_Toc510177769)

[9. Är det etiskt att lära någon att hacka? 15](#_Toc510177770)

[10. Diskussion och sammanfattning 16](#_Toc510177771)

[Referenser 19](#_Toc510177772)

# Introduktion

I dag finns det en stor risk för att företag blir hackade. Enligt Strand [1] trodde nästan två tredjedelar av alla ledare av IT i Storbritannien att de skulle utsättas för ett hackningsförsök inom de närmaste 12 månaderna och nästan hälften av dem var inte säkra på om de redan hade blivit hackade. Det här visar hur oroligt tillståndet är för företag. De börjar allt oftare undersöka vad de kan göra för att skydda sig mot attacker.

Det finns allt fler lagar som gäller företagssäkerhet och vad ett företag måste göra för att skydda personlig och värdefull information. Enligt finsk lag [2] måste ett företag visa att de tagit relevanta åtgärder för att skydda data, vilka åtgärder som menas specificeras däremot inte. Varje företag måste alltså utföra de åtgärder som de anser vara viktiga utan några fasta riktlinjer.

Så vad är alternativen? Varje företag har förhoppningsvis en brandvägg, antivirus, eventuella övervakningskameror, starka lösenord och anställda som bara har tillgång till den data de verkligen behöver, men det finns mycket man kan göra utöver det för att förstärka säkerheten. En bärbar dator eller telefon blir enkelt stulen eller borttappad så företag borde se till att det aldrig finns värdefull information på dem eller att de är krypterade så att data inte kan läsas utan ett lösenord. Det är dessutom lönsamt att säkerhetskopiera all data med jämna mellanrum, övervaka nätverket och informera anställda om aktivitet som kan utsätta företagets data för risk [3].

Allt det här kan skydda företaget mot små attacker som kanske inte är riktade direkt mot dem, men om en person eller grupp har siktat in sig på ens företag krävs mera. De företag som vill skydda sig så bra som möjligt mot alla eventualiteter gör utöver dessa åtgärder också penetrationstest.

# Definitioner

Innan vi går vidare måste vi reda ut vissa begrepp som är viktiga genom hela avhandlingen. Det är viktigt att veta vad skillnaden är mellan en sårbarhet (eng. *vulnerability*) och en exploit. En sårbarhet är en defekt (en bug) hos ett system eller hos mjukvara som används på ett system som leder till att någon kan interagera med systemet på ett sätt som inte var avsett [4]. En exploit däremot använder en sårbarhet för att kompromettera ett system. Att det finns en sårbarhet i ett system betyder inte automatiskt att det finns en exploit. Det kan finnas ett problem som är välkänt och enkelt kan exploateras men det kan lika gärna vara ett problem som ingen har hittat en exploit för ännu.

I den här avhandlingen talas det om hackare om det syftar på vem som helst som på något sätt försöker bryta sig in i ett system. Termerna etisk hackare, vit-hatt hackare och penetrationstestare är inbördes utbytbara i den här avhandlingen och syftar alla på en person som använder sig av samma tekniker som en hackare för att hitta sårbarheter och utnyttja exploiter men som använder metoderna för att utföra lagliga penetrationstest. När illvilliga hackare eller svart-hatt hackare nämns syftar vi på någon som använder teknikerna för olagliga syften, till exempel för att stjäla eller förstöra data. Se kapitel 6 för en mer detaljerad beskrivning av olika typer av hackare.

# Vad är penetrationstest?

Penetrationstest utförs av en eller flera etiska hackare som anlitats av ett företag för att testa deras säkerhet [4, s. 2]. Det är viktigt att komma ihåg att ett penetrationstest bara kan utföras om ett företag ger sitt samtycke till det, ett test av ett företags säkerhet utan skriftligt tillstånd är inte ett penetrationstest och bryter troligen mot lagen [6]. Målet med penetrationstest är att hitta säkerhetshål innan de kan utnyttjas av illvilliga hackare [7].

Det finns test av företagssäkerhet som inte anses vara penetrations test. En sårbarhetsbedömning (eng. *vulnerability assessment*) använder sig av olika verktyg för att ge en snabb överblick över var det finns risk-områden och i vissa fall hur de kan åtgärdas. Problemet med sårbarhetsbedömningar är att de bara kan hitta välkända problem och verktygen kan inte anpassa sin bedömning till hur nätverket och datastrukturen ser ut vid just det här företaget [7]. Sårbarhetsbedömningar kan ofta ge den etiska hackaren som utför ett penetrationstest en snabb överblick över systemet som testas men det verkliga testet ser inte bara på välkända svagheter. I ett penetrationstest bryter sig den etiska hackaren in i företagets nätverk och visar på ett väldigt konkret sätt var problemområden är och vad som kan hända om företaget inte åtgärdar de problem som finns [7, s. 11]. Det här betyder också att ett penetrationstest faktiskt utnyttjar de säkerhetshål som hittats för att bryta sig in i systemet, medan en sårbarhetsbedömning bara konstaterar att det finns risker [9].

I verkligheten innebär ett penetrationstest att den etiska hackaren använder sig av samma verktyg och trick som illvilliga hackare för att bryta sig in. Många sårbarheter kan hittas med hjälp av ett automatiserat sårbarhetstest, men det krävs bara ett problem som inte hittats för att en kunnig hackare ska kunna bryta sig in. Det är penetrationstestarens uppgift att hitta alla sårbarheter innan de kan utnyttjas, ge förlag på hur de kan åtgärdas och i viss mån förklara hur problemen kan undvikas i framtiden [9]. För det mesta innebär det här att man måste kunna tänka som en hackare för att ha en chans att stoppa illvilliga hackare. Penetrationstestare måste ständigt hålla koll på de nyaste exploiterna och dessutom veta hur hackarna skapar dem eftersom det är enda sättet att testa system som bara används av ett företag. Det är enkelt för vem som helst att köra program som utnyttjar välkända problem, men en etisk hackare som bara vet hur man använder sådana program kan aldrig utföra ett penetrationstest för ett företag som använder sig av programvara som de själv utvecklat. På grund av detta måste de som vill göra penetrationstest ha åtminstone grundläggande kunskaper i programmering, assemblyspråk och minneshantering [7, s. 173]. Det här innebär helt enkelt att de måste förstå hur datorer fungerar på de lägsta nivåerna.

Ett penetrationstest kan inte göra något för att stoppa förlust av data som beror på olyckor, defekter i hårdvara och mänskliga misstag. De här typerna av data förlust kan bara undvikas genom att göra regelbundna säkerhetskopieringar av all data [10, s. 614].

Innan man anlitar en penetrationstestare måste man vara medveten om att penetrationstestet inte åtgärdar svagheter i systemet, den etiska hackarens arbete är att hitta problemen och ge förslag på förbättring men efter det är det upp till företaget att agera på vad testet hittade [8].

# Varför penetrationstest?

Vi hör om och om igen om ett företag som blivit hackat och lovar att fokusera mer på säkerhet. När företaget Equifax som gör kredit kontroller blev hackat rapporterade Wattles och Larson [11] att de inte upptäckte attacken på över två veckor. Att göra ett penetrationstest betyder inte bara att man hittar alla problem i systemet, det betyder också förhoppningsvis att alla företagets anställda blir mer medvetna om säkerhet utan att konsumenterna behöver lida. Equifax var till och med medvetna om sårbarheten i deras system i två månader innan attacken inträffade, under den här tiden borde de ha anlitat säkerhetsexperter för att åtgärda säkerheten. Penetrationstest är inte ett måste, men för företag som ansvarar för känslig information kan det vara ända sättet att undvika katastrof.

Sjukförsäkringsbolaget Anthem blev hackat år 2014. Sienko [12] förklarar att hackarna lyckades få tag på användarinformation för ett antal anställda. Ett penetrationstest kan inte direkt hjälpa mot attacker som utnyttjar svagheter hos människor, men en del av bra säkerhet är att informera alla anställda om risker med att klicka på länkar och öppna email som ser suspekta ut. Ett företag som vill undvika också den här typen av attacken kan inkludera sociala tekniker i sitt penetrationstest för att göra alla anställda mer medvetna om säkerhet.

Hur kan ett penetrationstest hjälpa mer allmänt? Ett penetrationstest kan användas för att ge ett företags säkerhetspersonal en möjlighet att uppleva en attack i en säker omgivning. Det kan alltså träna den personal som redan är anställda hos företaget. Penetrationstestaren kommer att hitta de flesta sätten en hackare kan ta sig in i systemet och förhoppningsvis informera företagets mjukvaruutvecklare om vad de ofta gör fel i sin kod [13].

# Vem gör penetrationstest?

Vem som helst kan skaffa sig en certifikation som etisk hackare genom att studera området och göra ett skriftligt prov, man kan göra det här provet online [14] eller genom att gå på en kurs som avslutas med provet som ger certifikatet [15]. Men för att lyckas som penetrationstestare behöver man dessutom ha kunskaper i programmering, operativsystem, databaser och nätverk och dessutom ha tålamod och uthållighet [5]. Etiska hackare arbetar ofta i grupper, vilket betyder att det ofta kan löna sig att specialisera sig på ett visst område. Enligt Harper *et al.* [7, s. 158] behöver ett penetrationstestningsteam vanligtvis personer som är specialister på fysisk säkerhet, trådlös säkerhet, nätverkssäkerhet, operativsystem och social manipulation. En person kan vara expert på flera områden och någon måste dessutom leda gruppen.

I praktiken behöver man mer än generella kunskaper för att kunna utföra ett penetrationstest, man måste också ha grundliga kunskaper i hur man använder olika verktyg för att utföra testet. Varje penetrationstestare har vissa verktyg som hen föredrar att använda och är expert på, dessutom är det vanligt att hen också har verktyg som hen själv har skapat. Om man vill bli en penetrationstestare måste man ha en process som fungerar och som går att upprepa vid åtminstone de flesta testen [16]. Även om man måste ha verktyg som man känner till bra som en penetrationstestare betyder det inte att man bara kommer att använda de verktygen. Det är alltid viktigt att vara flexibel; ibland måste man använda sig av ovanliga test eller komma på sina egna test för att kunna utgöra sitt arbete grundligt. En person som inte har den här flexibiliteten är troligen inte mycket mer effektiv än en automatisk sårbarhetsbedömning.

Penetrationstestare måste också vara mycket medvetna om vad som är lagligt. Att en person tror sig vara etisk betyder inte att hen inte bryter mot lagen. En penetrationstestare måste alltid vara medveten om vad som är och inte är tillåtet, det är det enda som skiljer en vit hatt från en grå eller svart hatt hackare [9, s. 12].

Det kan vara svårt för en klient att veta om potentiella penetrationstestare har de egenskaper som krävs eftersom det inte bara gäller att ha rätt kunskaper utan också rätt personlighet. Det är därför vanligt att anställa någon som redan gjort test för andra företag som klienten kan diskutera med eller att inkludera en praktisk del av intervjun för att uppskatta kandidaternas lämplighet [18].

# Vad skyddas?

Den etiska hackaren måste också veta hur man skyddar data mot alla typer av attacker. Det som måste skyddas är dess konfidentialitet, autenticitet, integritet och tillgänglighet [5][13, ss. 611-612]. En *Denial-of-service* attack attackerar datans tillgänglighet genom att begära så mycket data från servern att användarna inte kan be om den data de vill ha; stöld av information attackerar datans konfidentialitet; *bit-flipping* attackerar datans integritet eftersom det innebär att den data som når systemet inte kan verifieras; och Mac-adress spoofing är en attack mot autenticitet eftersom det ger en obehörig dator tillgång till data [5].

Ett penetrationstest måste undersöka möjligheten för åtminstone dessa typer av attacker. Penetrationstestaren måste också vara medveten om vilken typ av attack som skulle skada den nuvarande klienten mest.

# Vilka är de illvilliga hackarna?

Barber [19] förklarar skillnaderna mellan hur de flesta ser hackare är och vad de är i verkligheten. Han beskriver hur de som inte vet mycket om ämnet ofta ser på hackare som personer (ofta unga män) som kan bryta sig in i vilket system som helst. Den här bilden av hackare kan leda till att företagsledare tror att det inte finns något de kan göra ifall en hackare riktar in sig på dem. Barber förklarar att de som tror att hackare går att stoppa ofta tror att det är otroligt dyrt, vilket leder till att de väljer att ignorera problemet och hoppas på det bästa. Det hjälper inte att man bara hör talas om attacker som lyckats, inte de som stoppats innan hackaren åstadkommit något.

Oerfarna hackare kallas ofta *script kiddies*, de är ofta unga och vet inte mycket om hackning. Vad de vet är hur man använder sig av verktyg som gör allt arbete för dem [19]. Eftersom de inte förstår sig på vad verktygen gör och varför är det ofta enkelt att stoppa deras attacker. Genom att hålla alla program uppdaterade med de senaste programfixarna och använda en bra brandvägg och anti-virus kan man stoppa de flesta attackerna från den här gruppen. Problemet är när attackerna kommer från personer som förstår sig på alla programmen de använder sig av och som kan anpassa sina attacker för olika system. Enligt Barber [19] är hackare och *crackers* mer erfarna, hackare attackerar system för att visa att de kan medan crackers är de som attackerar system för att förstöra och stjäla data.

Enligt Tanenbaum [13, s. 613] kan man dela in inkräktare i två grupper; aktiva och passiva. En passiv inkräktare vill bara läsa filer som de inte är auktoriserade att läsa, medan aktiva inkräktare vill ändra på systemets data. För att kunna stoppa attacker är det viktigt att man vet vad exakt man försöker stoppa. Det kan vara viktigt för en penetrationstestare att bli informerad om vilka slags attacker ett företag är mest rädd för. Tanenbaum beskriver fyra olika typer av hackare: planlösa personer som bara är nyfikna, personer som vill visa hur duktiga de är och att de kan bryta sig in i systemet, personer som är ute efter pengar och personer som arbetar som spioner för andra företag eller länder.

Det är också viktigt att vara medveten om virus och maskar som skickas ut i världen av en illvillig hackare för att replikera sig själv oändligt. Om det är fråga om en attack av den här typen är en hackare bara indirekt involverad eftersom virus och maskar ofta får ett slags eget liv. Personer som skapar virus bryr sig ofta inte om vem som skadas, de vill bara orsaka kaos [10].

I resten av den här avhandlingen bryr vi oss inte om skillnaden mellan script kiddies, hackare och crackers även om det finns en stor skillnad mellan grupperna, vi bryr oss inte heller om vilken motivation hackarna har. Vad vi bryr oss om är hur ett penetrationstest försöker stoppa alla typer av hackare.

# Penetrationstestarens process

För att förklara hur ett penetrationstest går till används ofta en standard som kallas *penetration testing execution standard*. Det här är en standard som beskriver de olika stegen hos ett penetrationstest. I den officiella versionen [20] indelas testet i sju faser: först har vi *pre-engagement*, som här kallas överenskommelse. Det handlar om vad som borde göras innan själva testet kan börja. Den andra fasen är informationsinsamling, som går ut på att skaffa information om systemet som ska testas. Efter de här två faserna kommer diskussionen här avvika från standarden. I standarden talas det om identifiering av hot, sårbarhetsanalys, exploatering, post-exploatering och rapportering. Eftersom den här avhandlingen inte kräver en så djupgående analys av processen används här ett lite annorlunda upplägg som bara tar upp det mest relevanta. Den här översikten är inte avsedd för blivande penetrationstestare, utan snarare som en överblick för de som överväger att anlita en penetrationstestare.

## Överenskommelse

Företaget som vill göra ett penetrationstest måste tänka på vad exakt de vill testa. Det kan leda till stora problem om ett företag bara förväntar sig ett enkelt test men penetrationstestaren gör ett väldigt ingående test [8, ss. 1-2]. Man måste också vara medveten om vilka typer av test som finns, det är ganska stora skillnader mellan ett test som utförs utan någon information alls om företaget (ett så kallat *black box* test) och ett test där man antar att angriparen är en arbetstagare eller någon annan som redan har tillgång till nätverket (vilket kallas ett *white box* test) [8], [9].

Weidman [8, s. 2] förklarar att det är i det här skedet som klienterna förklarar varför de vill göra penetrationstestet, vad de vill testa, vilka slags attacker de oroar sig för och ifall det finns ömtåliga eller viktiga system som testaren måste vara försiktig med. Vidare beskriver hon hur penetrationstestaren måste få noggranna instruktioner om vilka system som ska testas, bli informerad om hur viktigt det är att testen inte kraschar systemen och få information om ifall företaget också vill testa personalen genom sociala tekniker och testa den fysiska säkerheten. Andra saker Weidman nämner som borde diskuteras är vilka tider under dagen testen ska utföras och skapandet av dokument som ger testaren skriftligt tillstånd att utföra testet så väl som ett sekretessavtal.

Det kan också leda till problem för penetrationstestare om ett system blir hackat av någon annan under eller efter ett penetrationstest. Penetrationstestaren kan inte garantera att alla problem hittas, ofta har de en strikt deadline och hinner kanske inte göra testen så noggrant som de borde. Jamil och Khan [21] skriver hur penetrationstest är till för att drastiskt minska risken att ett företag blir hackat i framtiden, det är inte en garanti att det aldrig inträffar. Det är enkelt för ett företag att skylla på penetrationstestaren om något går fel. Det är därför viktigt att dokumenteringen som görs upp tar detta i beaktande.

## Informationssamling och passiv analys

Informationssamling borde vara en viktig del av alla penetrationstest. Även om testet är ett white box test, och testaren redan har tillgång till nätverket behöver all data analyseras för att se var det kan finnas svagheter och vad det kan vara lönsamt att fokusera på. Graves [4, s. 33] förklarar det här och beskriver också hur sociala tekniker kan accelerera informationssamlingen. Det första en penetrationstestare försöker lista ut är, enligt Graves, var, hur och när de anställda arbetar för att hitta mönster som kan leda till en exploit. Det här är värdefull information för den fysiska delen av ett penetrationstest som undersöker hur enkelt det skulle vara för en angripare att fysiskt få tillgång till företagets system.

Den information som hackare vill hitta är till exempel: domän namn, nätverksstruktur, nätverkstjänster och program, anti-virus och IP-adresser [4, s. 39]. I det första steget av informationssamlingen utförs en passiv analys av företaget som ofta kallas *footprinting*. Allt som krävs för den här delen av processen är websidor där man kan slå upp domännamn, och personnamn samt vanliga söktjänster som Google [9]. Det är också enkelt att använda *traceroute* kommandot för att se hur ett paket rör sig genom nätverket och upptäcka brandväggar som stoppar paketet [4].

## Aktiv analys

Efter den passiva informationsinsamlingen är det dags att använda mer påträngande metoder som port-, nätverks- och sårbarhetsanalyser. Dessa metoder används för att begränsa den data som samlats till det som faktiskt kan leda till en exploit [9]. Till skillnad från passiva analysmetoder kan de aktiva metoderna upptäckas så under det här skedet måste hackare vara extra försiktiga. De metoder som används i den här fasen är till exempel portanalyser, nätverksanalyser och sårbarhetsanalyser. Portanalyser används för att avslöja vilka portar som är öppna och kan användas för att se vilka system som används och vilka program det går att kommunicera med [8, ss. 123-124]. En ingående portanalys kan ge hackare informationer om vilka program som används på systemet om de använder välkända portar. Om det redan finns en exploit för något av programmen är deras arbete mycket enklare, allt de behöver göra är att ladda ner och köra exploiten. En nätverksanalys hittar alla värdar som är aktiva och en sårbarhetsanalys hittar operativsystem och deras svagheter [4, s. 66].

Med hjälp av all den information som samlats in hittills kan hackaren nu använda sig av en process som kallas *enumeration* för att skaffa ännu mer värdefull information [12, s. 70]. Det vanligaste sättet är att göra en förfrågan på en port som hackaren redan vet är öppen, den data som hackaren får tillbaka innehåller vanligtvis information om applikationen som skickade den [12, s. 71]. Hackaren kan identifiera applikationen och dess version med hjälp av dem data som skickas vilket gör det enkelt att hitta applikationer som har välkända exploiter.

## Exploatering

I det här skedet gäller det att bevisa att de sårbarheter som hittats faktiskt kan exploateras. Det kan ofta verka som att det här steget är onödigt, ifall testaren redan har hittat problemen varför behövs det här steget? Allen [17, ss. 141-142] nämner tre orsaker att utföra exploateringen, inte bara analyser. Exploateringen visar att risken är verklig och ger information om vilka data som äventyras, den gör att det blir mycket enklare att undersöka om de åtgärder som utvecklas för att eliminera problemen faktiskt fungerar och dessutom blir sannolikheten att alla säkerhetshål hittas mycket större.

Så vad innebär det att exploatera sårbarheter? Det penetrationstestare vill göra är ett så kallat *proof of concept*, det här betyder helt enkelt att de vill visa att systemet faktiskt kan komprometteras ifall sårbarheten inte åtgärdas. Penetrationstestare kan använda exploiter som skrivits av andra personer eller utveckla sina egna exploiter för att testa sårbarheten. Wilhelm [12, s. 212] förklarar att det är svårt att verifiera en exploit utan att faktiskt genomföra exploateringen, vilket innebär att penetrationstestaren alltid kommer vara tvungen att utsätta systemet för en viss risk. Enligt Wilhelm är det viktigt att penetrationstestare testar sina exploiter på en testserver innan den används mot klientens system. Penetrationstestarnas mål är att se till att klientens system är säkert och om deras exploit visar sig vara farlig för systemet kommer de inte att utföra den. Wilhelm nämner också att det ibland kan visa sig att en exploit som inte verkade farlig när den användes mot en testserver kan skada klientens system, det är därför viktigt att klienten är medveten om riskerna.

Vanliga typer av exploiter som kan nämnas är SQL injektion, *cross-site scripting* (XSS) och operativsystem eller program som är konfigurerade fel. För mer information om vanliga attacker, konsultera Owasp [24], det är en online bok som ger en översikt över de tio vanligaste attacktyperna år 2017. En SQL injektion lurar en server genom att ge input som verkar korrekt men som ger hackaren tillgång till konfidentiella data. Ett konkret exempel och mer information finns tillgängligt på nätet [25]. En XSS attack utnyttjar webbservrar som inte validerar data noga. Den vanligaste typen fungerar enligt Owasp genom att en websida använder input från en användare som output för nästa, till exempel kan det handla om en websida som visar senaste kommentarer utan att validera de kommentarer som den fått. Hackare kan skriva programmeringskod (vanligen JavaScript) in i sina kommentarer och den här koden körs på de nästa användarnas datorer.

## Eskalering av privilegier samt insamling av data

När penetrationstestaren har hackat sig in i systemet verkar det kanske som att testet borde vara färdigt, men det här visar bara att det är möjligt för en hackare att bryta sig in. För att få mer ut av penetrationstestet är det viktigt att också se vilken data som är i fara. I exploaterings-steget kan penetrationstestaren få tag på information i förbifarten, men i det här skedet är målet att hitta all information som en hackare skulle få tillgång till. Det här steget följer principen att den säkraste systemen har många lager av skydd [10, ss. 690-691].

Ibland kan en hackare kanske ta sig in i systemet utan att faktiskt lyckas åstadkomma något, det här beror på att det finns olika typer av användare på en dator. Vissa användare har bara tillgång till et litet antal filer som de kanske bara får läsa och inte ändra på. Andra användare har tillgång till alla filer och kan ändra på allting. Det här kallas i Windows system *Windows Access Control* [8, ss. 526-527]. Om en hackare lyckas exploatera ett program som startades av en användare med väldigt lite kontroll över systemet måste hackare eskalera sina privilegier innan hen kan åstadkomma något. Strategierna för att göra det här är komplicerade och inte viktiga för den här diskussionen. Det viktiga är att förstå att man kan skydda sitt system från hackare på flera nivåer och penetrationstestaren måste testa säkerheten på alla nivåerna.

Det är på grund av det här steget av penetrationstestet som det är viktigt att penetrationstestaren skrivit under ett sekretessavtal eftersom det är troligt att hen kommer att få tag på konfidentiell information [17, ss. 266-267].

## Rapport

Enligt Kim [16] är rapporten det enda som företaget bryr sig om. Att ha gjort alla testen perfekt betyder ingenting om penetrationstestaren inte kan förmedla sina fynd till klienten. Han nämner vissa saker som är viktiga för att skriva en bra rapport. Det är viktigt att vara tydlig med hur allvarliga olika säkerhetshål är. Om ett företag får in en lista på hundratals saker som måste åtgärdas blir de flesta antagligen ogjorda och det kanske är de som kan skada företaget mest som aldrig åtgärdas [7, s. 169]. Kim beskriver också hur en bra rapport inte bara borde ha ett konsistent och enkelt sätt att värdera säkerhetshålen, den borde också innehålla information om ifall det just nu finns en välkänd exploit som utnyttjar hålet. Ifall en exploit finns borde företaget meddelas att hålet borde åtgärdas så snabbt som möjligt. Säkerhetshål kan också dyka upp i informationssamlingsskedet som visar sig vara felaktigt positiva, de borde inte inkluderas i rapporten [12, s. 360].

Rapporten är till för att hjälpa företaget så mycket som möjligt, därför borde den alltid inkludera lösningar eller förslag på hur risken kan minskas för alla säkerhetshål [16], [17]. Kim kommenterar också hur viktigt det är att inkludera rådata och information till IT-teamet som beskriver hur de kan reproducera exploiten för att hjälpa dem att åtgärda problemet.

Om det är fråga om ett test för ett stort företag kan det vara nödvändigt att dela in rapporten i delar och bara förmedla det som är relevant till olika grupper [7, s. 169], det som är viktigt för en ingenjör att veta är troligen förvirrande och onödigt för företagsledare [12, ss. 358-359]. Ibland kan det också vara nödvändigt att hålla viss information hemlig från de anställda som inte måste veta om det, speciellt när det gäller säkerhetshål. Penetrationstestaren borde vara medveten om hur situationen ser ut vid företaget och om olika grupper kommer ansvara för olika slags säkerhetshål. Det här gäller också eventuella möten för att diskutera rapporten [7, s. 169].

# Är det etiskt att lära någon att hacka?

Jamil och Khan [26] skriver om hur svårt det är att veta vilken motivation någon har för att lära sig hackning. Det som lärs ut i penetrationstestningskurser kan användas för att hjälpa företag eller för att stjäla information. Jamil och Khan förklarar också hur en del av skulden alltid kan placeras på personen som gav undervisning åt en illvillig hackare. Som en jämförelse borde vi också tänka på hur många personer som blivit utbildade i en armé och sedan använt sina kunskaper för att skada andra. Det är alltid en svår etisk fråga när man överväger risker och fördelar med att lära ut färdigheter som kan leda till stora skador.

En person som tycker om att bryta sig in i andra personers system skulle antagligen lista ut hur de kan göra det även utan undervisning, speciellt med hur mycket information som finns tillgänglig på nätet [10, s. 670]. Att lära dem använda sina färdigheter för att göra penetrationstest istället för att hacka olagligt kan till och med leda till att de får arbeta med något som de tycker om att göra och inte längre har tid eller vilja att hacka olagligt. Det här är förstås bara spekulation, men det är alltid viktigt att betrakta situationer ur alla synvinklar.

Om en penetrationstestare förlorar sitt arbete måste man också vara medveten om risken att hen tar ut sin upprördhet på företaget genom att hacka dem [21]. Om en penetrationstestare redan känner till systemet är det enkelt att bryta sig in och förstöra något värdefullt. Jamil och Khan förklarar också hur enkelt det är för människor att bli lockade, de kanske en dag börjar fundera på hur enkelt det skulle vara att bara sätta in lite pengar på ett konto medan de gör ett penetrationstest. Om man redan vet exakt hur man kan göra för att bli rik på bara några sekunder kan det vara svårt att motstå frestelsen.

En sak är säker, om etiska personer inte studerar hackning kommer det leda till att illvilliga hackare får göra vad de vill. Kanske de attacker som de illvilliga hackarna utförde skulle vara enklare att stoppa eftersom de aldrig tävlat mot etiska hackare och blivit tvungna att utveckla sina tekniker, men möjligheten för etiska personer att skydda system innan de blev attackerade skulle försvinna. De som utvecklar antivirusprogram måste veta allt om hackning för att kunna stoppa attacker innan de inträffar. Man måste veta hur ett system blir infekterat innan man kan komma på hur man kan desinfektera det [10, s. 673].

Varje programmerare borde också ha en viss förståelse för hur ett program blir sårbart. Alla sårbarheter skapas på någon nivå av programmerare, vilket betyder att ju fler programmerare som är insatta i hackning desto säkrare kommer programmen de skriver bli.

# Diskussion och sammanfattning

Lagar som gäller internet och datorer utvecklas hela tiden och varje gång en ny lag skapas krävs det mera av företag. En ny EU lag hotar företag med böter ifall de är oförsiktiga med personuppgifter [27]. Nya lagar tvingar allt oftare företag att vara mer omsorgsfulla och mer medvetna om de risker som alltid associeras med att ha data tillgängligt på ett nätverk. Risken att bli hackar kommer alltid att finnas kvar, men företag som har stark säkerhet och gör regelbundna penetrationstest kan inte anklagas för att vara oansvariga. De som gjort allting i sin kraft för att undvika en katastrof behöver aldrig oroa sig lika mycket för hackare. Många lager av stark säkerhet kring sitt nätverk och krypterade filer gör det troligtvis omöjligt för en hackare att få tag på viktig information.

Den här avhandlingen har gett en grundläggande insikt i hur ett penetrationstest går till; hur de struktureras, hur de planeras och hur de utförs. Det som skiljer ett penetrationstest från alla andra typer av hackning är att företaget och penetrationstestaren kommer överens om alla testets detaljer innan någon hackning utförs. Det är företaget som bestämmer exakt vad som ska ingå i testet, vad, hur och när testet ska utföras. Här har också förklarats att penetrationstest bara innebär att hitta problemen, inget kommer att åtgärdas bara för att testet utförs. Företaget måste alltid se till att agera på vad testet hittade för att det ska kunna åstadkomma någonting.

När ett penetrationstest övervägs är det viktigt att vara medveten om vilka slags personer som man funderar på att ge tillgång till alla företagets hemligheter, därför diskuterades kvalifikationer för penetrationstestare. En framgångsrik penetrationstestare måste ha rätt personlighet, inte bara rätt kunskaper. De egenskaper som en penetrationstestare har mest nytta av är kreativitet och tålamod så väl som integritet.

Alla attacker är inte inriktade på samma saker, vissa attacker vill skada ett företags möjlighet att distribuera den data de lovat sina kunder, andra attacker vill se till att företaget inte kan lita på sin egna data, eller kanske inte ens läsa den. De attacker som de flesta tänker på när de hör ordet hackning är attacker som går ut på att stjäla konfidentiell information och det är ofta den här typen av attacker som kan leda till de största konsekvenserna. Ett penetrationstest kan fokusera på ett område eller försöka få en överblick över alla typer av attacker som är möjliga. Det är igen något som måste diskuteras innan testet kan börja.

Ett penetrationstest motiveras vanligen av att ett företag oroar sig för en viss typ av attack. Troligtvis är de attacker som oroar de flesta också de attacker som rapporteras i nyheterna. Den här avhandlingen nämnde några fall där företag som hackades kunde ha gjort mera för att se till att det aldrig hände. Det är viktigt att lära sig av andras misstag och ta de åtgärder som behövs innan det är för sent.

Hur ett penetrationstest struktureras förklarar på ett mer genomgående sätt exakt vad ett penetrationstest är, därför gick den här avhandlingen igenom de viktigaste stegen som ingår i testen. Överenskommelsen och rapporten kommer alltid att vara de viktigaste delarna av testet för ett företag. Hur penetrationstestaren åstadkommer allt hen gör är intressant, men oftast inte relevant för företagsledare. Det kan därför argumenteras att en penetrationstestare också behöver goda kunskaper i kommunikation och skrivkonst. Ett penetrationstest kan bara vara effektivt om penetrationstestaren vet exakt vad som ska testas och kan förmedla sina fynd grundligt och precist.

Det kommer alltid att finnas alternativ för de som inte känner sig bekväma med att göra ett penetrationstest. Man kan alltid utföra en enkel sårbarhetsanalys med hjälp av mjukvara istället och anlita kunnig säkerhetspersonal. Poängen med den här avhandlingen är inte bara att förklara penetrationstest utan också att göra företag mer medvetna om riskerna och ge dem enkla tips om hur de kan lappa hålen i sin säkerhet. Saker som ännu kan nämnas är tillämpning av regler för hur anställda skapar sina lösenord och hur ofta de byts ut, kryptering av data samt undervisning för anställda som förklarar hur man undviker misstänksamma websidor och email. Det finns så mycket mera ett ansvarsfullt företag kan göra, men de här sakerna borde alla företag åtminstone hålla i bakhuvudet.

Det är ett nytt sätt att tänka att alltid fundera på säkerhet, ett företag som inte tidigare har haft hand om känslig information kan helt plötsligt tvingas se världen på ett helt nytt sätt. Det kommer alltid att finnas personer som vill hitta genvägar för att bli rika eller skada ett företag som skadat dem, och ju mer välkänt ens företag blir desto större är riskerna. I dagens samhälle måste vi vara mer och mer medvetna om riskerna för identitetsstöld och utpressning som blir enklare hela tiden med hjälp av nätet.

# Referenser

[1] C. Strand, “Challenging Confidence in Cyber-Security,” *Comput. Fraud Secur.*, vol. 2014, no. 12, pp. 12–15, 2014.

[2] “Personuppgiftslag,” 1999. [Online]. Available: http://www.finlex.fi/sv/laki/ajantasa/1999/19990523#L7. [Accessed: 24-Jan-2018].

[3] R. Davis, “10 Cyber Security Measures That Every Small Business Must Take,” *Tech.co*, 2014. [Online]. Available: https://tech.co/10-cyber-security-measures-every-small-business-must-take-2014-11. [Accessed: 25-Jan-2018].

[4] “Vulnerabilities, Exploits, and Threats : Defining Three Key Terms in Cybersecurity.” [Online]. Available: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/. [Accessed: 13-Mar-2018].

[5] K. Graves, “CEH Certified Ethical Hacker Study Guide.” Wiley Publishing, Inc., Indiana, 2010.

[6] Uladzislau Murashka, “Penetration Testing by Letter of the Law,” 2017. [Online]. Available: https://www.securitymagazine.com/articles/88489-penetration-testing-by-letter-of-the-law. [Accessed: 31-Jan-2018].

[7] A. Tang, “A guide to penetration testing,” *Netw. Secur.*, vol. 2014, no. 8, pp. 8–11, 2014.

[8] A. Harper, J. Ness, G. Lenkey, S. Harris, C. Eagle, and T. Williams, “Gray Hat Hacking - The Ethical Hacker’s Handbook.” McGraw-Hill Companies, United States of America, 2011.

[9] G. Weidman, *Penetration Testing : A Hands-On Introduction to Hacking*. United States of America: William Pollock, 2014.

[10] A. Tanenbaum, *Modern Operating Systems*, Third edit. United States of America: Pearson Education International, 2009.

[11] J. Wattles and S. Larson, “How the Equifax data breach happened: What we know now,” *CNN Tech*, 2017. [Online]. Available: http://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html. [Accessed: 30-Mar-2018].

[12] Chris Sienko, “The Breach Of Anthem Health - The Largest Healthcare Breach In History,” *Infosec Institute*. [Online]. Available: http://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-attack-statistics-and-case-studies/case-study-health-insurer-anthem/#gref. [Accessed: 30-Mar-2018].

[13] Security Innovation Europe, “What is Penetration Testing and Why is it Important?,” 2016. [Online]. Available: https://www.securityinnovationeurope.com/blog/page/what-is-penetration-testing-and-why-it-important. [Accessed: 30-Mar-2018].

[14] EC-Council, “Certified Ethical Hacker (Practical),” 2018. .

[15] Net Com Learning, “CEH: Certified Ethical Hacker Certification Classes in Helsinki, Finland,” 2018. .

[16] P. Kim, *The Hacker Playbook, Practical Guide to Penetration testing*. North Charleston: Secure Planet LLC, 2014.

[17] T. Wilhelm, *Professional Penetration Testing : Creating and Learning in a Hacking Lab*, 2nd ed. United States of America: Elsevier Science, 2013.

[18] J. Yeo, “Using Penetration Testing to Enhance Your Company’s Security,” *Comput. Fraud Secur.*, vol. 2013, no. 4, pp. 17–20, 2013.

[19] R. Barber, “Hackers Profiled : Who Are They and What Are Their Motivations?,” *Comput. Fraud Secur.*, vol. 2001, no. 2, pp. 14–17, 2001.

[20] The PTES Team, “The Penetration Testing Execution Standard Documentation,” *Online*, 2017. [Online]. Available: https://media.readthedocs.org/pdf/pentest-standard/latest/pentest-standard.pdf. [Accessed: 13-Mar-2018].

[21] D. Jamil and M. N. A. Khan, “Is Ethical Hacking Ethical?,” *Int. J. Eng. Sci. Technol.*, vol. 3, no. 5, pp. 3758–3763, 2011.

[22] S. McClure, J. Scambray, and G. Kurtz, *Hacking Exposed : Network Security Secrets and Solutions*, 4th ed. United States of America: The McGraw-Hill Companies, 2003.

[23] L. Allen, *Advanced Penetration Testing for Highly-Secured Environments The Ultimate Security Guide : The Ultimate Security Guide*. Birmingham: Packt Publishing, 2012.

[24] Owasp, *OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks*. Creative Commons, 2017.

[25] w3schools, “SQL Injection.” [Online]. Available: https://www.w3schools.com/sql/sql\_injection.asp. [Accessed: 29-Mar-2018].

[26] D. Jamil and M. N. A. Khan, “Is Ethical Hacking Ethical?,” *Int. J. Eng. Sci. Technol.*, vol. 3, no. 5, pp. 3758–3763, 2011.

[27] N. Fagerström, “Tusentals föreningar oförberedda på nya dataskyddsregler - riskerar böter,” *Yle Nyheter*, 2018. [Online]. Available: https://svenska.yle.fi/artikel/2018/03/09/tusentals-foreningar-oforberedda-pa-nya-dataskyddsregler-riskerar-boter. [Accessed: 02-Apr-2018].