Jack-Benny Persson
LX13
Säkerhet
2014-05-10

Fördjupningsarbete i säkerhetskurs
Ämne: Penetrationstestning

Jack-Benny Persson
LX13 - EC-Utbildning Helsingborg
Maj 2014

Jack-Benny Persson
LX13
Säkerhet
2014-05-10

Innehåll

Jack-Benny Persson
LX13
Säkerhet
2014-05-10

Syfte

Att göra en fördjupning inom området penetrationstestning med utgångspunkt från de metoder och begrepp som beskrivs i OSSTMM 3[1]. Jag tänker också gå igenom hela processen så noggrant som möjligt, d.v.s. de olika faserna, d.v.s. vilka godkännande som krävs av företaget, insamlingsfasen, hacking-fasen och dokumentationsfasen. När man börjar titta på penetrationstestning så inser man snart att området omfattar alla dessa faser. Själv hackingen eller penetreringen är bara en av delarna inom penetrationstestning. Detta arbete kommer att fokusera på svenska förhållanden, d.v.s. svensk lagstiftning, svenska system, svenska standarder som gäller etc. Detta arbete kommer också att fokusera på den formen av penetrationstest som kallas för *Double Blind* enligt OSSTMM 3. Jag kommer även att försöka att kort gå igenom de övriga testerna (*Blind, Tandem* etc) för intressets skull. Fokus kommer att läggas på *Double Blind.*

Frågeställningar

De frågeställningar som jag kommer att försöka få svar på i detta fördjupningsarbete är

- ***vad är penetrationstestning?***
- ***hur utförs det?***
  - *hur läggs arbetet upp?*
  - *juridiska hinder, skadestånd, avtal?*
  - *etik och moral?*
  - *hur rapporteras allt?*
  - *hur arbetar pen-testaren eller angriparen?*
- ***hur ser det ut i Sverige med penetrationstestning?***

Avgränsningar

Då jag ganska snabbt inser att ämnet är väldigt stort kommer jag inte gå in så detaljerat på rena tekniska detaljer då det finns tusentals olika sätt att penetrera en server, helt beroende av vad för system som målet använder, vilka tjänster det gäller, hur gamla systemen är osv. Dessutom uppdateras program och tjänster dagligen så det är svårt att göra en djupdykning i detta då det som är en stor nyhet idag om det senaste säkerhetshålet i en viss programvara är patchat och bortglömt imorgon. Fokus kommer istället att läggas på t.ex. administration, rekognosering, insamling, skanning, social manipulation samt då ett försök att skrapa på ytan när det gäller själva hackingen.

1 OSSTMM 3

Jack-Benny Persson
LX13
Säkerhet
2014-05-10

Avhandling & fördjupning

Vad är penetrationstestning?

Penetrationstestning är en metod för att testa ett måls säkerhet genom att helt enkelt försöka bryta sig in i det. Ofta är det målföretaget själv som köper detta som en tjänst av ett extern konsultföretag. Det verkar inte vara så många företag som faktiskt pysslar med denna form av tjänst i Sverige. Vad jag kan hitta så är det bara ett fåtal företag som erbjuder denna form av tjänst och då är det ofta mindre företag med 1-5 anställda. Sen kanske det bara är jag som inte lyckats hitta alla företagen, det vet man ju faktiskt inte. Anledning för ett mål att att köpa denna form av tjänst är för att hitta svagheter i deras säkerhet. Dessa svagheter kan vara alltifrån den mänskliga faktorn, datorsystem, skalskydd m.m. Ofta är det dock just IT-systemen man testar i penetrationstester, åtminstone i Sverige. Och för många företag är det just också detta som är det intressanta.

Det finns också olika former av penetrationstester som alla testar utifrån olika kunskaper som angriparen respektive målet besitter. Se *Olika typer av penetrationstester.*

Försiktighet, tillstånd och juridiska konsekvenser

Innan ett penetrationstest genomförs är det viktigt att se till att man har godkännande från företagsledningen på det företag där man ska genomföra testet hos. Detta gäller all form av penetrationstestning, oavsett om det gäller COMSEC (Communication Security), PHYSSEC (Physical Security) eller SIGSEC (Signal Security). Straffet för att genomföra intrång i datorsystem utan tillåtelse från ägaren av systemet kan ge upp till två års fängelse[2]. Den som testar säkerheten i telefonsystem eller använder avlyssning av telefonsystem som ett sätt att samla information inför ett annat penetrationstest kan också råka riktigt ill ut om han inte har godkännande. Den som avlyssnar ett telefonsamtal där han ej själv medverkar döms för *olovlig avlyssning* till böter eller fängelse i upp till två år[3]. Man skall också vara extra försiktig om man i sitt test försöker ge sig på att avlyssna, penetrera eller modifiera målets telefonsystem via det allmänna telenätet. Skulle olyckan vara framme och man råkar förstöra något som har med det allmänna telesystemet att göra så är det ännu högre straff på detta. I lagen står att den som *allvarligt stör eller hindrar den allmänna samfärdseln eller användningen av telegraf, telefon, radio eller dylikt allmänt hjälpmedel* kan dömas för saborage i upp till 4 års fängelse[4]. Om det skulle vilja sig riktigt illa och en domstol dömer brottet som grovt är det straffet uppe i hela 18 år eller livstid[5]. Att hävda okunnighet är ingen ursäkt i lagens mening. Däremot tittar en domstol på om man haft uppsåt eller om brottet har begåtts av en ren olyckshändelse. Men att hävda olyckshändelse är inte mycket till försvar om man arbetar med penetrationstester då man anses ha de rätta kunskaperna att utföra arbetet på ett säkert sätt. När vi nu ändå talar om brott & straff kan det nämnas att det är faktiskt en mindre risk, rent juridiskt att syssla med fysisk penetrationstestning mot målet. Jämför de höga straffen på upptill två års fängelse för dataintrång och olovlig avlyssning mot straffet för *olaga intrång* som endast ger böter såvida det inte är grovt då straffet istället hamnar på två års fängelse[6]. Om brottet är grovt eller inte beror oftast på om man forcerat en låst dörr eller dylikt. Notera att detta bestäms utifrån vissa praxis och inget man själv kan fundera ut i förväg.

Så länge man har tillåtelse från målet (företag man utför penetrationstestet hos) är man ofta på det fria. Har jag en tillåtelse att bryta mig in hos någon har jag ju inte *olovligen* brutit mig in. Likaså får jag ju bryta mig in hos mig själv hur mycket jag vill.

2 Brottsbalken 4 kap. 9 c §
3 Brottsbalken 4 kap. 9 a §
4 Brottskalken 13 kap. 4 §
5 Brottsbalken 13 kap. 5 §
6 Brottsbalken 4 kap. 6 §

Jack-Benny Persson
LX13
Säkerhet
2014-05-10

Ett giltigt kontrakt och försäkringar

Innan någon som helst av penetrationstestning eller informationsinsamling påbörjas är det av högsta vikt att man har ett påskrivet giltigt kontrakt mellan sig själv som testare och målet, det företag som penetrationstestningen ska utföras mot. Kontraktet ska vara detaljerat som möjligt där det uttryckligen står att penetrationstestning får lov att utföras mot företaget. Det är också viktigt med någon typ av ansvarsförsäkring om något skulle gå fel. Det är dock något som man själv måste stå för som konsult. En ansvarsförsäkring är något man alltid bör ha som konsult, oavsett yrke eller område. Vad man också måste tänka på när man tecknar en ansvarsförsäkring är att också lägga till något som heter proffesionsförsärking som gäller för rena förmögenhetsskador som uppstår genom t.ex. dåliga råd eller om man orsakat ett driftstopp hos kunden man arbetar för[7][8].

Avtalet / kontraktet

Det finns en rad olika saker som är extra viktiga som skall finnas med i avtalet mellan angriparen och målet[9]. Dessa listas här nedan med en kort förklaring och fundering över vad det innebär.

- **Omfång & begränsningar**
  Dettta är nog en av de viktigaste sakerna att reda ut innan testerna påbörjas. Om inte angriparen vet omfånget av testet kanske han av antingen misstag eller av ”iver” testar målets alla dotterbolag, personalen m.m. när detta kanske inte alls var syftet med testet från början. Häri bör också **syftet** med testas finnas.
- **Tidsåtgång**
  Här reglerar man tiden för testet. Som nämns i både Carl-Johans examensarbete (se sidfoten) och OSSTMM är det viktigt att man skiljer på mantimmar och tidsåtgång då målet ju inte på förväg ska veta om exakt när angreppen kommer att ske. Detta är för att inte målet ska sättas i höjd beredskap under testets gång. **Mantimmarna** är å sin sida den tid som går åt till själva testet och som målet/kunden betalar för.
- **Tidsfönster**
  Detta anger om det finns några begränsningar när testerna får utföras, t.ex. om testerna inte får utföras när servrarna har som högst trafik för att inte störa den dagliga produktionen.
- **Destruktiva tester**
  Hur ställer sig målet till att genomföra destruktiva tester, t.ex. att krasha servrar eller överbelasta nätet med DDoS-attack. Detta är en av de viktigaste punkterna i avtalet mellan angripare och mål så att inte angriparen blir skadeståndsskyldig.
- **Inga stabilitetsgarantier**
  Denna är lika viktig som ovanstående och kan ses som en friskrivning för angriparen om något trots allt skulle gå snett och en server eller tjänst går ner trots försiktighet från angriparen. Detta gör ju också att angriparen kan arbeta mer fritt, annars kanske han inte hade vågat testa allting om han hela tiden oroar sig för följderna.
- **Utnyttjande av sårbarheter**
  Detta punkt är till för att klaragöra om sårbarheter i systemet får utnyttjas, och om så sker,

7 Foretagande.se → http://www.foretagande.se/sa-kan-it-konsulter-minska-forlusterna-vid-ansvarsskada/
8 IF.se → http://www.if.se/web/se/foretag/varaforsakringar/itdataforetag/pages/itdataforetag.aspx
9 Penetrationstester: Offensiv säkerhetstestning, av Carl-Johan Bostorp vid Linköpings Universitet → http://www.diva-portal.org/smash/get/diva2:22798/FULLTEXT01.pdf

hur långt in i systemet får angriparen då gå. Det bästa vore om det finns en viss tillgång som angriparen är ute efter så att testerna blir mer målmedvetna. Det är iaf vad jag anser vore lämpligt. Det vore också bra om angriparen fick fria händer att penetrera alla system så att det blir så ”verklighetsförankrat” som möjligt utan begränsningar.

- **Sekretessavtal**
  En oerhört viktig punkt för att målet ska känna sig trygg med testerna. Ett sekretessavtal som tydligt talar om att inga resultat av testerna får nå någon annan än målet självt (och angriparen som utför testerna). Det är också viktigt så att målet får ett högre förtroende gentemot angriparen/pen-testaren, som ju trots allt lägger mycket i händerna i angriparen/testaren.
- **Åtkomstpunkter**
  Varifrån testerna får lov att ske eller om det upprättats särskilda åtkomstpunkter för angriparen. Kanske vill man inte att angriparen ska testa från internet av olika anledningar.
- **Kontaktuppgifter**
  Kontaktuppgifter till både angriparen och målet så att de båda kan nå varandra om det skulle uppstå problem eller frågor. En tanke som väcks här är t.ex. om målet upptäcker andra angrepp på sin verksamhet och snabbt vill fråga testaren om det är han som attackerar systemet eller om det är ett riktigt, live-angrepp mot målet. Det finns verkliga exempel på detta när militären har utfört övningar och en fiende har utnyttjat övningarna/testerna för att maskera sin egen attack.
- **Ändringar av avtalet**
  Hur skall ändringar hanteras som sker under testets gång? Detta måste också regleras i förväg.

Etik & moral

Nu när vi gått igenom allt det juridiska och vi har alla avtal på vår sida är det dags för ett lite svårare kapitel, nämligen etik & moral. Med det menar jag de etiska dilemman man måste ta ställning till, helst innan testerna påbörjas. Det gäller främst *social engineering*, eller på svenska social manipulation, där man lurar och bedrar personalen hos målet att ge ut information eller att utföra vissa handlingar. Ur ett rent pen-testing och säkerhetssynfält är det viktigt att även testa just detta. Men om man kör ett *Double Blind*-test där målet inte har en aning om en attack är på gång och därmed inte har tid att förbereda sig så kan ju den utsatte känna stor skam efter att ha blivit lurad. Dessutom riskerar ledningen att få fiender då de är dessa som beställt uppdraget. Om man nu ändå bestämmer för att gå hela vägen, med social manipulation och allt för att det ska bli så verklighetsförankrat som möjligt så är det viktigt att efteråt samla alla inblandade och poängtera att det var ett test och att ingenting skall ligga någon i fatet. Dessutom tycker jag inte att angriparen ska avslöja några namn på inblandade i den sociala manipulationen för ledningen då detta med största sannolikhet då kommer att slå tillbaks på offret. Den rapport som ledningen ska få bör innehålla alla viktiga detaljer, så som att attacken var lyckat p.g.a. det gick att lura av personalen viss information, men inga namn ska nämnas. Jag anser det är viktigt att skydda det personliga integriteten här. Testet kan ändå vara till nytta för framtida utbildningar för personalen, utan att någon enskild person behöver hängas ut.

Jack-Benny Persson
LX13
Säkerhet
2014-05-10

Olika typer av penetrationstester

Double Blind (Penetrationstest)

Det finns en rad olika former av penetrationstester som alla beskrivs i OSSTMM 3, det är dock bara en av dessa som verkligen kallas för *penetrationstest* och det är den som också heter *Double Blind Test.* De olika formerna av tester som beskrivs i manulen syftar alla på att förklara testet utifrån den kunskap som målet respektive angriparen har. I fallet med *Double Blind* som syftar detta till att både målet och angriparen saknar kunskaper, d.v.s. målet vet inget om attacken (bortsett från ledningen som godkänt testet) och angriparen har ingen kunskap om målet i sig. Därav namnet *Double Blind*, båda parter är blinda. Detta test syftar till att vara så realistiskt som möjligt då målet inte i förväg vet om attacken och därmed testar beredskapen på en oväntad attack. Angriparen kommer från utsidan utan någon tidigare kunskap om målet och det är således helt upp till angriparens skicklighet att skaffa sig tillräckliga underrättelser för att kunna genomföra ett lyckat intrång. Allt detta gör då att testet blir så verklighetstroget som möjligt. Det är framförallt denna form av test som detta fördjupningsarbete kommer att handla om.

Blind (Wargaming)

Detta test syftar till att testa försvaret hos målet när målet vet om attacken och är beredd på den. Angriparen däremot vet inget om målet, han är alltså helt *blind* och det är upp till angriparen att försöka skaffa så mycket underrättelser han kan om målet för att försöka penetrera det. Man brukar även kalla detta test för Wargaming.

Gray Box (Vulnerability test)

Här har angriparen viss information om målet medan målet självt vet allt om angreppet i förväg. Detta testa testar alltså säkerheten när en angripare har fått viss information om målet sedan tidigare, kanske från en källa hos målet. Då målet i förväg vet om att angreppet kommer att komma så är målet försatt i viss höjd beredskap. Detta kallas även för ett sårbarhetstest eller vulnerability test.

Double Gray Box (White box)

I ett *Double Gray Box* test så känner angriparen till allt om målets kanaler (*Human, Physical, Signal, Communication, Wireless)* medan målet självt inte vet något om vilka kanaler som kommer att testas men däremot vet allt annat om testet så som tidsspann, tillgångar m.m.

Tandem (Crystal Box)

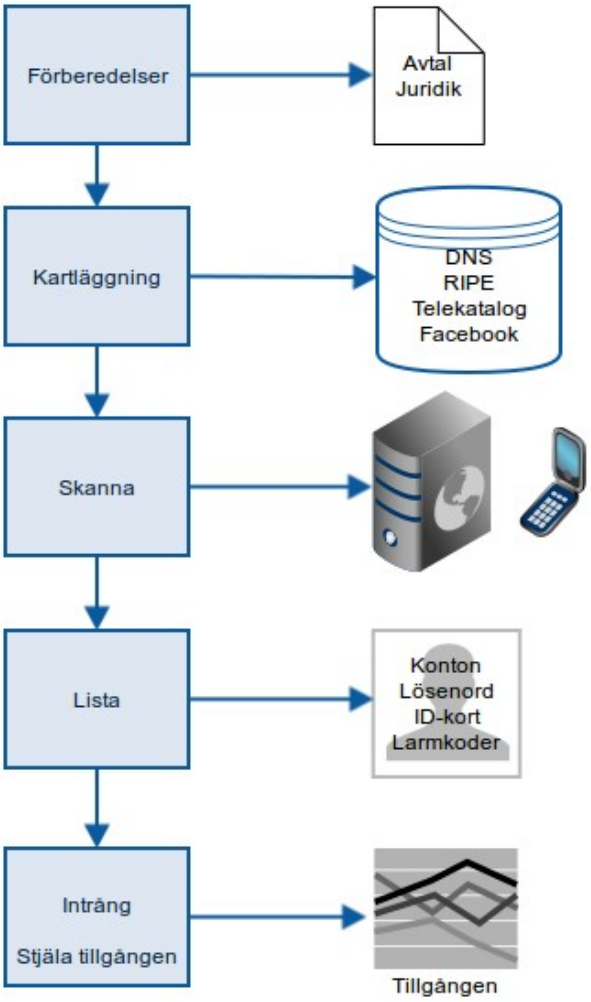
I ett *Tandem Test* så har båda parterna full kunskap om allt. Ett *Tandem Test* är således mer en säkerhetsgenomgång än ett penetrationstest. Här går man istället igenom säkerheten och alla vet allting om testet.

Reversal (Red Team Exercice)

Detta verkar vara ett väldigt roligt och intressant test där angriparen har all kunskap om målet och testet medan målet inte vet något om testet alls. Detta syftar således till att testa ett angrepp från insidan. Detta kan ju t.ex. då vara någon i personalen som angriper målet, d.v.s. en insider som genomför själva angreppet. Detta kan vara ett väldigt användbart test att genomföra på företag, särskilt de företag som arbetar med mycket känslig information eller på annat sätt löper en stor risk för insiders. Ett företag som t.ex. har stora världen i form av företagshemligheter, t.ex. en industri som tillverkar väldigt speciella produkter när en kopieringen av deras tillverkningsprocess kan få stora konsekvenser.

Penetrationstestets olika faser[1011]

När man utför ett professionellt penetrationstest består detta av flera olika faser eller delar. Den stora anledningen till att man delar in det i olika faser är för att det ska bli lättare att överskåda och främst för att man inte ska missa någonting. Det är mycket lättare att göra något noggrant när man har vissa delar man ska genomföra och följa. Här kommer jag gå igenom dessa olika faserna i den ordning det utföres i. Då detta fördjupningsarbete till största delen handlar om *Double Blind* och *Blind* tester så kommer stor vikt läggas vid fördjupning i just kartläggning och insamling av underrättelser om målet då angriparen inte vet något om målet till att börja med. Alla information om målet som han behöver måste han införskaffa själv på egen hand. Det är detta som gör det så spännande med *Blind*- och *Double Blind*-tester då mycket av penetrationstestet handlar om att skaffa sig underrättelser på olika vis om målet. Den allra första delen förutom dessa faser som gås igenom här nedan är självklart att fastställa vad tillgången är. D.v.s. vad är det vi ska försöka stjäla eller komma över. Att bara bevisa att man lyckats hitta en bugg i målets DNS-server som tillåter en komplett listning av allt innehåll är inte att anse som ett lyckat angrepp. För att angreppet ska anses vara lyckat måste angriparen ha kommit över tillgången eller ”asset” som det benämns i OSSTMM. Bilden här nedan visar ett enkelt flödesschema över hur de olika faserna.



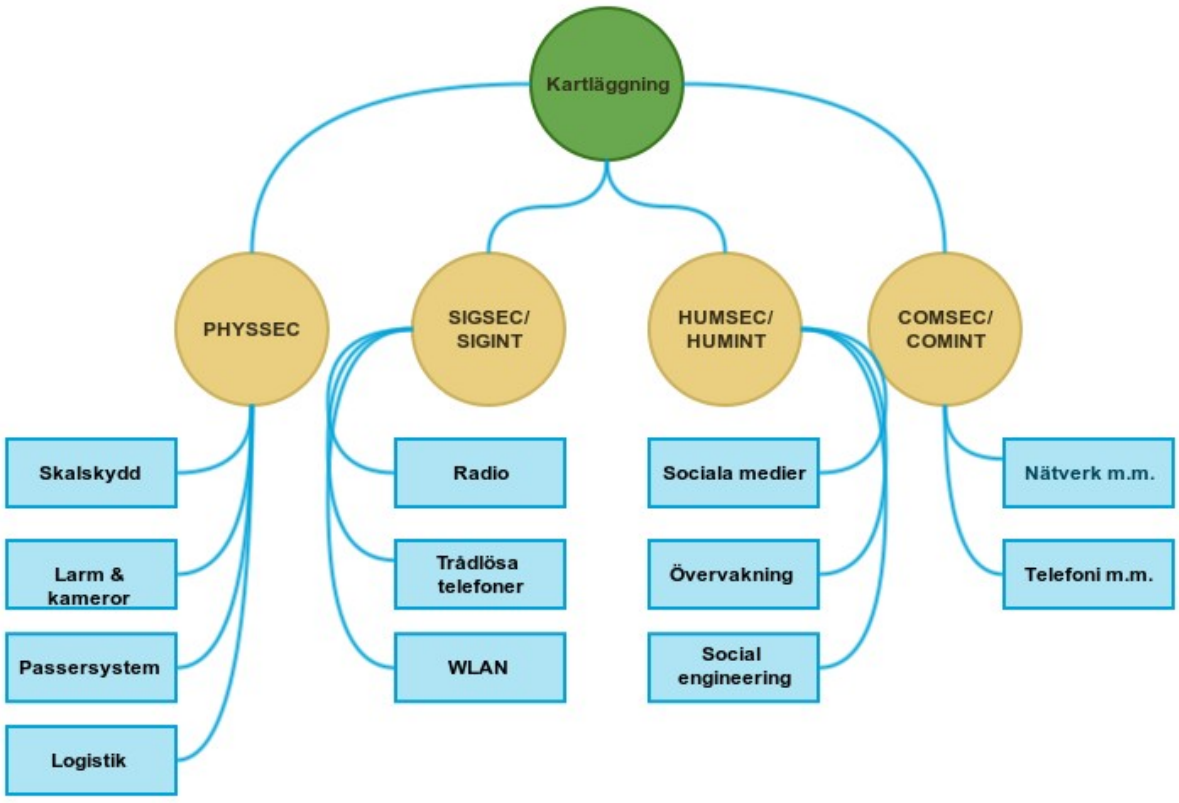
10 Hacking i Fokus (2002)
11 OSSTMM 3

Jack-Benny Persson
LX13
Säkerhet
2014-05-10

Kartläggning / Informationsinsamling

I den här fasen kartlägger man så mycket som möjligt om målet via olika kanaler. Det kanaler som främst används är kanske COMSEC, SIGSEC, PHYSSEC och HUMSEC där COMSEC avser både telekommunikation och datorkommunikation, SIGSEC avser signalspaning, PHYSSEC avser fysisk rekognosering och HUMSEC avser människor, d.v.s anställda och andra personer som har kännedom om målet. För att göra det mer lätthanterligt så brukar man dela upp kartläggningsfasen i dessa kanaler och testa varje kanal för sig. Det kan dock hända att kanaler går in i varandra men detta gör ju ingenting så länge man får den information om man är ute efter. Ett exempel på när kanalerna skulle kunna gå in i varandra är när man via t.ex. Facebook söker efter anställda på företaget/målet och sedan via öppna sökningar skapar en dossier om personen. Sedan kan man testa att muta personen eller försöka komma över personens ID-kort, koder m.m. Man har då gått från COMSEC till HUMSEC kanalen.

Karläggningsfasen syftar till att kartlägga målet för att angriparen ska kunna skaffa sig en överblick över målet, t.ex. hur stort målet är, hur många anställda de har, hur många externa IP-adresser de har, hur många inkommande telefonnummer det finns, hur många dotterbolag det kan finnas, hur stort deras fysiska komplex är, namn på nyckelpersoner på företaget, underleverantörer m.m. Har man inte denna information och direkt börjar hacka eller bryta sig in på företaget så famlar man i mörkret utan att veta vad man håller på med eller är ute efter. Det är viktigt för angriparen att spara allting som hittas under de olika faserna, speciellt då kartläggningen. Denna kartläggningen ligger sedan till grund för skanningsfasen, där angriparen skannar de nät, IP-nummer, telefonnummer m.m. som han hittade under kartläggningen.



COMSEC / COMINT (Internet, nätverk)

Den enklaste delen att börja med är COMSEC (nätverk & telefoni). Målets DNS-servrar och det IP-spann de har fått tilldelat sig kan säga mycket om målet storlek och dess nätverk och IT-miljö. Jag börjar med att titta på de vanligaste formerna nedan, så som just DNS-servrar m.m. Mycket av denna information har hittats i Hacking i Fokus från 2002, se [10] på föregående sida.

DNS

En felkonfigurerad DNS-server som tillåter zonöverföringar till vem som helst är en guldgruva för angriparen. Lyckas en sådan zonöverföring så har helt plötsligt angriparen en väldigt stor karta över alla publika maskiner och tjänster. För ett testa att göra en komplett zonöverföring så kan man använda komandot *dig* till detta, som i exemplet neden.

```
dig @ns1.example.com example.com -t AXFR
```

-t AXFR betyder att typen ska vara AXFR, d.v.s. en zonöverföring. Även om det inte går att göra en zonöverföring kan man ändå hämta mycket information från DNS-servern, så som en lista på alla mailservrar, alla TXT-records m.m. med nedanstående kommando.

```
dig @ns1.example.com example.com -t MX
dig @ns1.example.com example.com -t TXT
```

Här kan man då också se om målet har mailservrarna in-house, d.v.s. om det sköter sin egna mailservrar eller om dessa sköts av en extern firma, t.ex. ett hosting-bolag.

IP-spann / RIPE-databasen

Genom att göra en WHOIS-fråga på de IP-nummer man får fram genom antingen DNS-frågor eller genom att direkt uppslag på t.ex. www.example.com, example.com osv kan man se vilket IP-spann dessa befinner sig i och om företaget är så stort så att de har egna IP-nummer eller om dessa tillhandahålls av en ISP. Här får man då också reda på vilken ISP målet använder sig av.
RIPE-frågor kan göras på https://apps.db.ripe.net/search/query.html.
Även IANA-databaserna kan vara intressanta att titta igenom här.

Målets webbsida och dess källkod

Man får inte att glömma att även gå igenom målets egna webbsida, här finns också mycket information om företaget. Även detta är helt offentlig information är det ändå ej att underskatta. Sen kan man även ta sig en titt på källkoden till hemsidan efter gamla utkommenterade kodstycken, kommentarer till koden m.m. Ofta när ändringar görs så kommenteras bara den gamla kod ut för att sedan testa den nya koden. Fungerar den nya koden bra så händer det att den gamla koden ligger kvar som kommentarer en tid efter, eller helt enkelt glöms bort.

En av de kanske viktigast sakerna att leta upp på webbsidan är e-postadresser och telefonnummer till systemansvariga på målföretaget. Men hjälp av e-postadresser till systemansvariga kan vi sen i nästa steg här nedan med hjälp av Google-sökningar hitta foruminlägg m.m. som gjorts av dessa personer. Ibland är det så att dessa systemansvariga helt öppet använder sin vanliga e-postadress när det postar frågor som ”Vi har precis införskaffat nya Cisco PIX-brandväggar på jobbet och jag undrar hur man ändrar standard-lösenordet då jag inte kan hitta detta i manualen”. Dessa sortens frågor kan vara förödande, men händer väldigt ofta[12].

12 Föreläsning av Rikard Bjurenbäck i Routing & Switching på EC-Utbildning

Google-sökningar

Genom att söka på Google kan man hitta mycket information. En del av det som tas upp här gränsar in på skanningsfasen en del. Här tas ett axplock upp av olika saker man kan hitta om målet via Google[13]. Som jag nämnde ovan i förra stycket så är det enkelt att leta upp alla forumposter och diskussioner i mailinglistor som systemansvariga har deltagit i. Informationen från dessa forum kan vara alltifrån vilka system, brandväggar, routrar m.m. företaget använder till att de inte har lyckats ändra standard-lösenord m.m. Man kan också få upp en uppfattning om hur kunnig en systemansvarig är och hur engaerad han verkar vara. Jag testar lite sökningar på mig själv för att se vad för information som dyker upp.

```
”Jack-Benny Persson”
```

En sökning på mitt namn med citattecken som nedan ger ca 35 500 träffar. Här är det viktigt att ange citattecken för att minska antalet träffar lite. 35 500 träffar är ändå på tok för mycket att gå igenom då långt ifrån allt verkligen gäller mig. Jag ser snabbt att det finns en skådespelare och komiker som heter Jack Benny. För att få bort dessa resultaten gör jag istället en ny sökning som ut så här:

```
”Jack-Benny Persson” -actor -jokes -humor -chicago
```

Detta ger nästan 10 000 färre resultat och när man väl börjar bläddra bland resultaten är faktiskt alla relevanta. De som inte är relevanta tas bort av Google själv efterhand som man bläddrar bland sidorna. Jag testar nu istället att göra sökningar på mina två e-postadresser. Dessa förfrågningar görs som visas nedan, d.v.s med nyckelordet *intext* som talar om att söksträngen måste finnas i dokumenten. Detta ger något bättre resultat.

```
intext:jack-benny@cyberinfo.se
intext:jake@cyberinfo.se
```

Den övre sökningen ger 85 träffar och den nedre sökningen ger 137 träffar. När man bläddrar igenom den nedre sökningen hittar jag forum och diskussionsgruppsinlägg som är daterade ända tillbaks till 2006. Internet glömmer aldrig som det heter...

Många siter idag försöker dölja e-postadresser från robotar på internet och det med alla rätt. Dessa robotar söker igenom internet efter e-postadresser att spamma. Det finns en rad olika använda tekniker och omskrivningar för att dölja e-postadresser på nätet, så som att skriva ”jack-benny at cyberinfo dot se” istället för jack-benny@cyberinfo.se. Detta kan vi använda oss av när vi söker på Google också. Mycket riktigt så ger en sökning på ”jack-benny at cyberinfo” 9 st nya träffar.

Andra väldigt bra sökningar på Google kan vara att söka efter en viss typ av dokument och därefter utläsa metadatan från dessa dokument om inte dokumenten i sig är av intresse. Sådana sökningar kan se ut enligt nedan

```
site:cyberinfo.se filetype:pdf
”Jack-Benny Persson” filetype:pdf
site:cyberinfo.se filetype:pdf ”Firewalker”
```

Osv osv, det finns mängder av olika Google-sökningar man kan göra för att hitta och filtrera information. Det finns ett väldigt bra verktyg som heter *Metagoofil* som använder just Google för att söka efter dokument och sedan automatiskt extrahera metadata från dessa dokument. Det är här all kartläggning bör börja[14].

13 Google Hacking for Penetration Testers, Volume 2. ISBN: 978-1-59749-176-1
14 Föreläsning av Martin Sörensson, Säkerhetskurs på EC-Utbildning

Bekräfta e-postadresser

Nu när vi har hittat en mängd forumposter m.m. och systemansvariges e-postadress kan vi gå vidare att bekräfta dessa e-postadresser. Det kan vi helt enkelt göra genom att logga in på en av de e-post servrar som vi hittade ovan under **DNS**-avsnittet. Detta görs enklast med telnet till port 25 till servern. En enkel session visas här nedan, med både en falsk e-postadress som inte finns, d.v.s. lisavonanka och en som finns, d.v.s. jack-benny.

```
Connected to mail.mynet.test.
Escape character is '^]'.
220 mail.mynet.test ESMTP Postfix (Ubuntu)
mail from: jake@test.com
250 2.1.0 Ok
rcpt to: lisavonanka@cyberinfo.se
550 5.1.1 <lisavonanka@cyberinfo.se>: Recipient address rejected: User unknown in virtual alias
table
rcpt to: jack-benny@cyberinfo.se
250 2.1.5 Ok
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Här bekräftade vi att jack-benny@cyberinfo.se är en aktiv och fungerade e-postadress.

Andra verktyg

Det finns en rad andra användbara verktyg så som domaintools.com, whois, ip-lookip.net, theharvester, metagoofil m.m.

HUMSEC / HUMINT (Människor)

HUMSEC eller dess motsvarighet, HUMINT[15] (Human Intelligence) handlar om den mänskliga faktorn. HUMINT är just benämningen som underrättelsetjänster använder för att benämna en viss typ av insamling av underrättelser, den via mänskliga kanaler. I och med internet, Google och Facebook är det nu lättare än någonsin för en angripare att skapa sig kompletta dossiers över personalen. Dessa dossiers kan sedan ligga till grund för diverse angrepp mot personalen för att komma vidare in i företaget. Sådana angrepp kan vara mutor, påtryckningar, utpressning eller helt enkelt bara hitta anställda för att sedan försöka komma över deras ID-kort, PAC-brickor m.m. Huruvida det är etiskt och morals rätt eller fel att göra så i ett penetrationstest kan diskuteras. Att försöka stjäla en anställds nyckelkort kan jag tycka är helt ok i ett penetrationstest, men däremot att muta en anställd i ett penetrationstest tycker jag verkligen inte är ok. Det skulle kunna vara ok om målet är militärt möjligtvis, men knappast på ett civilt mål. Det finns faktiskt exempel i historien när kvinnliga hackare har använt sex för att komma över militärpersonals ID-handlingar[16]. Detta var dock regelrätta hack och intrång, och inte något penetrationstest. Oavsett vad informationen i framtiden kommer att användas som i penetrationstestet så är det ofta väldigt användbar information som kan hittas via t.ex. Facebook. Ofta har företagen egna Facebook-grupper som de anställda kan bli medlem i. Dessa gruppar är dessutom ofta offentliga så att alla kan se medlemmarna i gruppen. Och skulle det vara så att gruppen är privat är det inte svårt att skapa en fejk-profil på Facebook i ett namn på en anställd på företaget och försöka bli medlem i gruppen och då få en förteckning över alla anställda och vad de pysslar med m.m.

PHYSSEC (Fysisk säkerhet)

Att skaffa sig underrättelser om den fysiska säkerheten inför ett penetrationstest behöver inte vara svårare att faktiskt ta sig företagets lokaler och kolla av läget. Har de en väktare på dagtid, t.ex. en portvakt? Hur ser skalskyddet ut? Använder de kortläsare/PAC-brickor etc? När det anställda går in, drar de enbart sitt kort eller behöver de även slå en kod? Används bara kortet utan kod är det enkelt att ta sig in. Det enda angriparen behöver göra är att ”råka” stöta ihop med en anställd och ta passerkortet som vilken ficktjuv som helst. Innan personen hinner förlustanmäla sitt kort har angriparen kunnat ta sig långt in i byggnaderna, kanske under flera dagar.

När testaren eller angriparen tar sin tur runt området kan han fotografera och filma för att senare i lugn och ro gå igenom bilderna och filmerna för att hitta ytterligare svagheter som han inte fann när man var på plats. Det är också viktigt att angriparen inte upptäcks av personalen eller väcker misstankar då personalen och kanske framförallt eventuella väktare då automatiskt blir extra uppmärksamma i och med en höjd paranoia[17].

Vad som också är viktigt för angriparen att lägga märke till vid rekognoseringen är vägar till och från målet, omgivande terräng m.m. Allt detta behövs senare vid själva intrånget för att organisera logistiken m.m. för angriparen. Likaså bör stor vikt läggas vid att försöka lokalisera yttre kameror och larmanordningar så att dessa senare kan undvikas. Något som penetrationstestaren/angriparen också bör titta efter är om det finns alternativa angreppsvägar, d.v.s. angreppsvägar som inte målet förväntar sig. Detta kan t.ex. vara om företaget ligger vid vattnet och har något sämre skalskydd på denna sida så kan angriparen istället ta sig från detta håll via t.ex. en båt. Andra bra sätt att angripa företaget på är via taket då många företag saknar skalskydd just här. En annan sak som angriparen

15 HUMINT på Wikipedia → http://en.wikipedia.org/wiki/Humint
16 Copyright Finns Inte, kapitlet om Kvinnliga Hackare → http://www.df.lth.se/~triad/book/
17 OSSTMM 3

kan göra är att utlösa ett larm från utsidan, t.ex. genom att ”smacka” en femkrona mot en glasruta så att larmet utlöses[18] och sedan gömma sig en bit bort och klocka hur lång tid det tar för väktaren att komma till platsen. Likaså kan man då kontrollera hur många väktare som rycker på larmet, vilket företag det är som utför bevakningen, om väktaren är ung och ny på jobbet eller erfaren m.m. Detta kan vara värdefull information vid ett eventuellt senare fysiskt intrång på företaget.

SIGSEC / SIGINT

Detta kallas även signalspaning i underrättelsetjänster och militärbruk. Detta syftar helt enkelt på att leta efter och avlyssna radiosignaler. Detta kan vara alltifrån trådlösa telefoner och komradio till personsökare/Minicall. Exempelvis Minicall är väldigt enkelt att lyssna av då en personsökning i Minicall-systemet skickas ut över alla master i hela landet. D.v.s en angripare kan sitta i Skåne och snappa upp personsökningar i Stockholm[19][20][21]. Personsökarmeddelanden är dessutom väldigt enkla att avlyssna. Det enda som krävs är ett program för att koda av POCSAG-signaler och en helt vanlig radioskanner som kan införskaffas i vilken elektronikaffär som helst. Sedan är det bara att koppla ihop radioskannern med datorns ljudkort och starta upp POCSAG-programmet och ställa in skannern på rätt frekvens (169,800 Mhz & 161,4375 Mhz). Lyssnar man här i några dagar eller veckor får man gigantiska mängder med larmmeddelanden från larmsystem, personsökningar, meddelanden från automatiskta processer och industrier, displaymeddelanden m.m. Börjar man sedan filtrera all datan kan man lätt hitta relevant information om målet. Ofta kan man här utläsa information om larmtyper, beskrivningar av larm (t.ex. Företaget AB - magnetkontakt, huvudentré, norra sidan). Nu vet man t.ex. att deras dörrar och fönster i huvudentrén är försedda med magnetkontakter och att larmen går iväg direkt via Minicall-nätet, troligtvis till någon väktare.

Likaså finns det kanske komradio som företaget använder för att kommunicera internt. Här kan man då snappa upp mycket matnyttig information. Frekvenslistor finns tillgängligt via internet på diverse skanningssidor så som http://www.frekvenslista.com/, http://www.scanner.nu/frek.asp m.fl.

Nästa steg blir då att avlyssna dessa frekvenser vilket kommer under skanningsfasen.

18 Svensk Säkerhet 2001, s. A50-A51
19 Scanner.nu, *Digitala Radiosystem i Sverige - 120Bd* → http://www.scanner.nu/faq_digital.htm
20 Wikipedia, *Personsökare* → http://sv.wikipedia.org/wiki/Persons%C3%B6kare
21 Generic Mobile, *Minicall tjänster* → http://genericmobile.se/minicall-tjanster

Skanning

I OSSTMM 3 finns mycket matnyttigt när det gäller just skanningen (och även penetrationstestet i sig). Olika böcker och manualer benämner denna fasen olika. I boken Hacking i Fokus benämns det skanning i listning (dessa två går in i varandra lite) och i OSSTMM som insamling. Syftet verkar ändå vara detsamma, d.v.s. att skanna av och samla in information om målet. Detta kan vara portscanning, radioscanning m.m.

Detta är alltså en mer aktiv form av informationsinsamling även om en del tekniker ändå är passiv, så som t.ex. radioavlyssning är en passiv aktivitet. Däremot portskanning är en aktiv skanning. I denna fas använder angriparen verktyg som Nmap, Nessus, Wireshark m.fl. för COMSEC/COMINT kanalen och radioskanners, stora antenner, avkodare m.m. för SIGSEC/SIGINT. När det gäller HUMSEC/HUMINT och PHYSSEC finns det inte mycket kvar att att göra i skanningsfasen då det mesta täcktes in under kartläggningen. De steg som eventuellt skulle kunna falla in under skanningsfasen för HUMSEC/HUMINT är i så fall att närma sig målets personal/vänner för att bli vän med dessa och sedan försöka få ut så mycket information som möjligt. Detta komma att kort tas upp här. När det gäller PHYSSEC så kan skanning vara att aktivt stjäla passerkort, testa koder på yttre passersystem, aktivt lösa ut larm för att klocka respsonstid m.m. Fokus i detta fördjupningsarbete när det gäller skanning är dock på COMSEC, både nätverk/IT och telekom.

Skanningsfasen går kort ut på att skanna de IP-adresser, telefonnummer och eventuellt de människor som hittats och kartlagts i kartläggningsfasen / informationsinsamlingsfasen.

COMSEC/COMINT (Nätverk, IT)

Här går jag kort igenom de olika tekniker en angripare skulle kunna använda för att skanna nätverk efter tjänster. Detta involverar saker som portskanning (hitta öppna portar), OS-fingerprinting (ta reda på vilket OS servern kör) och lista banners (tjänsters välkomstbanners med versionsnummer m.m.)

Portskanning & OS-fingerprinting

Verktyget *Nmap* är det som är mest använt för portskanningar. Med Nmap kan man skanna enskilda IP-adresser eller hela spann. Men kan dessutom välja hur aggressiv skanningen ska vara och om det skanningen ska omfatta både TCP & UDP osv. Nedan visas några exempel på Nmap's användning.

```
jake@olivia:~$ nmap 192.168.0.101

Starting Nmap 6.40 ( http://nmap.org ) at 2014-05-08 13:02 CEST
Nmap scan report for test.mynet.test (192.168.0.101)
Host is up (0.00024s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http

Nmap done: 1 IP address (1 host up) scanned in 5.96 seconds
```

Här hittade Nmap fyra öppna portar på IP-adress 192.168.0.101. Nmap kan som sagt även användas för OS-fingerprinting vilket visas här nedan.

```
root@olivia:~# nmap -O -sV 192.168.0.101

Starting Nmap 6.40 ( http://nmap.org ) at 2014-05-08 13:06 CEST
Nmap scan report for test.mynet.test (192.168.0.101)
Host is up (0.00013s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.4p1_hpn13v11 (FreeBSD 20100308; protocol 2.0)
25/tcp   open  smtp    Sendmail 8.14.5/8.14.5
53/tcp   open  domain  dnsmasq 2.55
80/tcp   open  http    lighttpd 1.4.29
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Device type: specialized|general purpose
Running (JUST GUESSING): Comau embedded (92%), OpenBSD 4.X (86%), FreeBSD 8.X (85%)
OS CPE: cpe:/o:openbsd:openbsd:4.0 cpe:/o:freebsd:freebsd:8
Aggressive OS guesses: Comau C4G robot control unit (92%), OpenBSD 4.0 (86%), FreeBSD 8.1 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: test.mynet.test; OSs: FreeBSD, Unix; CPE: cpe:/o:freebsd:freebsd

OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.10 seconds
```

Här fick vi fram typ av tjänst på alla portarna tillsammans med versionsnummer för dessa tjänster. Operativsystemet gissade Nmap var Comau embedded vilket desvärre var fel. Nmaps nästa gissning var dock korrekt, FreeBSD (vilket även kan ses i versionsnumret till OpenSSH). Nmap är alltså ett väldigt användbart verktyg som ej ska underskattas. Mycket mer om hur Nmap används finns att läsa på www.nmap.org och i dess manualsida på systemet med *man nmap.*

Nmap kan också användas för att finna datorer som är uppe. Detta kan enkelt göras enligt nedan exempel.

```
jake@olivia:~$ nmap 192.168.0.0/24 -sn

Starting Nmap 6.40 ( http://nmap.org ) at 2014-05-08 13:41 CEST
Nmap scan report for firewall.mynet.test (192.168.0.1)
Host is up (0.00045s latency).
Nmap scan report for emma.mynet.test (192.168.0.8)
Host is up (0.00083s latency).
Nmap scan report for laura.mynet.test (192.168.0.11)
Host is up (0.0014s latency).
Nmap scan report for labrat.mynet.test (192.168.0.27)
Host is up (0.00048s latency).
Nmap scan report for ella.mynet.test (192.168.0.35)
Host is up (0.00057s latency).
Nmap scan report for olivia.mynet.test (192.168.0.55)
Host is up (0.0010s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.12 seconds
```

COMSEC/COMINT (Telefoni)

När det gäller att skanna telefonsystem så handlar detta ofta om en väldigt gammal och beprövad teknik så kallad Wardialing. Steg ett blir att leta reda på alla offentliga telefonnummer via t.ex. målets webbsida, Eniro m.m. Här brukar man se mönster, ofta brukar ett företag köpa ett visst spann med telefonnummer som de kan använda. Dessa nummer går sedan genom företagets växel. Det man kanske vill hitta här främst är alla de nummer som inte finns listade någonstans. När man väl har hittat spannet t.ex. 999001 till 999500 och har lokaliserat alla telefonnummer som går till olika personer på företaget så tar man bort dessa nummer från spannet. Resterande nummer programmerar man sedan en dator med ett modem kopplat till sig att ringa upp alla dessa nummer[22]. Det man då letar efter är modem, kopplingstoner m.m. Än idag existerar det uppringda förbindelser in till företaget via olika former och tjänster, så kallade dial-in. Detta kan vara alltifrån att fjärradministrera servrar ifall nätet skulle ligga nere till access till telefonväxlar för att kunna underhålla dessa via fjärruppkoppling. Problemet idag är att företag lägger ner massvis med pengar och resurser för att säkra upp sina brandväggar och alla servrar som vetter mot internet, men glömmer helt och hållet bort alla inkommande modemlinjer[23].

Det är dock inte bara inkommande modemlinjer som utgör ett mål för angriparen. Även telefonväxlar, faxar, maskinstyrning m.m. är av intresse för angriparen[24]. Telefonväxlar är väldigt användbara om angriparen kan få administratörsaccess till dessa. T.ex. skulle en angripare då kunna ringa från lednings telefonnummer och begära uppgifter, eller bara helt enkelt koppla sina egna samtal via växeln för att ringa gratis eller till lokalsamtalstaxa.

Värt att notera här också är att det ofta är väldigt simpla lösenord på inkommande modemlinjer, telefonväxlar m.m. av den anledningen att man helt enkelt inte tror att någon kommer att hitta telefonnumret till resursen.

Ett av de mest använda programmen för Wardialing sedan 90-talet fram tills idag är THC Scan, se https://freeworld.thc.org/thc-scan/

HUMSEC/HUMINT

När det gäller själva skanningsfasen i HUMINT är det främst social manipulation eller *social engineering* som kommer att gås igenom här. Det mesta har redan täckts in under Kartläggningsfasen / Informationsinsamlingsfasen.Fast just i denna fas går angriparen ett steg längre och använder de kunskaper och personmappar/dossiers som han samlade ihop i informationsinsamlingen för att manipulera, utpressa och muta sitt offer. Det är förvånande att man kan åstadkomma så pass mycket genom att bara fråga efter information om man uppträder och låter som om man hörde hemma på företaget eller i den miljö man befinner sig. Med lite jargong kan man komma väldigt långt. Ett exempel på detta är hur Stanley Mark Rifkin lurade Security Pacific National Bank på runt 10 miljoner dollar utan att någonsin använda en dator[25]. Det enda han använde var en telefonautomat och de kunskaper han sett när han vandrat runt på banken som konsult.

Om det sen är rätt eller fel att försöka muta och bedra människor i ett penetrationstest kan diskuteras länge. Dess syfte är i alla fall att skaffa sig information om målet och/eller tillträde dit.

22 Wikipedia, Wardialing → http://sv.wikipedia.org/wiki/Wardialing
23 Hacklabs, *Wardialing Penetration Test* → http://www.hacklabs.com/war-dialing-penetration-test/
24 SecureState, *Wardialing* → http://www.securestate.com/Services/Risk%20Management/Pages/War-Dialing.aspx
25 Bedrägerihandboken (2002), s. 22-25

SIGSEC/SIGINT

Även här har det mesta redan täckts in i karläggnings- och informationsinsamlingsfasen. Skillnaden här skulle i så fall vara att här avlyssnar man aktivt de frekvenser, kanaler och RIC-nummer man hittade insamlingsfasen (RIC-nummer är en form av ID-nummer för personsökare). I SIGSEC/SIGINT kan man även räkna in WLAN-skanning och WLAN-sniffing. WLAN är alltid en stor risk att sätta upp för målet. WEP är t.ex. väldigt osäkert och kan knäckas på under tre minuter[26]. Även WPA är numera att anse som osäkert, framförallt då WPA med TKIP[27][28]. WPA2 med AES är det enda som kan anses vara säkert, men är mycket beroende på hur långt lösenord man använder sig av då det är möjligt att samla in paket från ett WPA2-nätverk för att sedan utföra en offline-attack mot lösenordet[29]. Den största risken för WPA & WPA2 är WPS, WiFi Protected Setup. Här utnyttjar man den korta PIN-kod som används för att koppla ihop enheterna. Använder målet WPS är det således relativt enkelt för angriparen att ta sig in i det trådlöst nätverket. Se sidfötterna [27, 28, 29] för mer information om detta.

Även om det inte finns några officiella trådlösa accesspunkter är det inte alltför ovanligt med så kallade rouge accesspoints på företag. D.v.s accesspunkter som någon anställd sätter upp på eget bevåg för att kunna surfa trådlöst på företaget. Det sker ofta i tron att det är helt ok, även om det inte är så. Personen sätter alltså oftast inte upp rouge accesspoints med illvilja, utan med ren okunskap. Det är också något som angriparen/pen-testaren får leta efter. D.v.s. även om inte Access Punkten heter ”Företaget AB” kan den likaväl vara kopplad till nätverket. Här bör man dock se upp som pen-testare! Att ta sig in på ett trådlöst nätverk man inte har tillstånd till är en olaglig handling som kan medföra böter eller fängelsestraff. Pen-testaren bör därför vara ytterst försiktig när han testar access punkter som han bara tror går till målet. Det är trots allt bara målet som pen-testaren har fått tillstånd att bryta sig in i, ingenting annat!

En lista på de mest använda verktygen för att ta sig in på trådlösa nätverk finns på http://sectools.org/tag/wireless/

Trådlösa telefoner kan också vara mycket enkla att avlyssna, särskilt de som inte använder DECT-teknik. Dessa använder vanlig analog signal mellan telefonen och basenheten och går att avlyssna som vilken komradio som helst. Även vanliga DECT-telefoner går att avlyssna, även om det dock kräver mer arbete så är det möjligt[30].

PHYSSEC

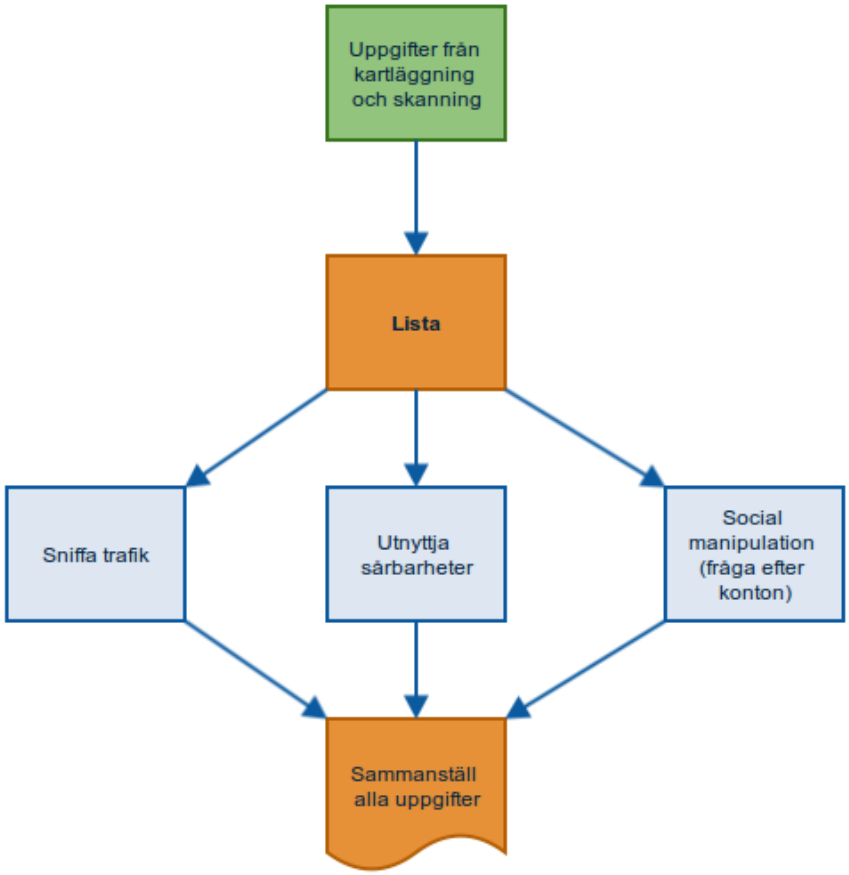
Att ”skanna” den fysiska säkerheten kan innefatta att testa att lösa ut larm m.m. och klocka responstiden, men detta har jag redan gått igenom i kartläggning- och informationsinsamlingsfasen. Vad pen-testaren också kan göra för att skanna den fysiska är att säkerheten testa olika koder på eventuella yttre larmpaneler, testa de kort han stulit eller på annat sätt kommit över. Annars finns det inte så mycket kvar att göra här förens det är dags för det riktiga inbrottet.

---

26 Wikipeda.org, *Wired Equivalent Privacy* → http://sv.wikipedia.org/wiki/Wired_Equivalent_Privacy
27 Wikiepdia.org, *WPA* → http://sv.wikipedia.org/wiki/WPA
28 HowToGeek, HTG *explains the difference between wep wpa and wpa2 wireless encryption and why it matters* → http://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/
29 PaloAltoNetworks, *Attacks on WPA/WPA2* → http://researchcenter.paloaltonetworks.com/2013/09/risks-to-wireless-networks-attacks-on-wpawpa2/
30 NyTeknik, *Lätt avlyssna trådlös telefon* → http://www.nyteknik.se/nyheter/it_telekom/allmant/article258109.ece

Lista

Detta är den sista fasen innan själva intrånget och stölden kommer att ske och går i princip ut på att försöka komma över och ”lista” alla konton, lösenord, ID-brickor, larmkoder, kryptonycklar, valvkoder, fysiska nycklar m.m. Kort och gott att inventera de nyckelkort, lösenord och konton som pen-testaren redan kommit över och göra nya försök att komma över fler där detta krävs. I listningsfasen går man då ett steg längre jämfört med de andra faserna kartläggning och skanning. I listningsfasen gör man ofta aktiva intrång för att komma över kontoinformation, användarnamn, resursnamn m.m[31]. I denna fas använder man t.ex. de sårbarheter man hittat för de olika tjänsterna i skanningsfasen för att ta sig in i systemet och där försöka komma över kontonamn och lösenord. Detta kan t.ex. innefatta en bugg i ett PHP-skript som tillåter en angripare att dumpa hela /etc/passwd filen. Lyckas detta har angriparen nu alla användarnamn för hela den servern. Det kan också innefatta någon form av bugg där användaren kan öppna upp ett skal till servern, men med begränsade rättigheter. Det första målet då för angriparen är då återigen att dumpa /etc/passwd eller andra filer med kontonamn, t.ex. en fil med virtuella användarkonton för Postfix, FTPd eller liknande. Ett annat mål kan vara att lista alla NFS-resurser med *showmount -e <IP>* för att hitta utdelningar. Andra intressanta listningar kan vara att avlyssna nätverkstrafiken med t.ex. Wireshark för att hitta och identifiera VLAN, routingprotokoll (och dess rutter), CDP (Cisco Discovery Protocol) m.m. Genom att sniffa upp CDP-paket på nätverket kan angriparen få information om exakt vilken slags Cisco-utrustning som används, versionsnummer av IOS m.m. CDP är ett väldigt informativt protokoll att sniffa för en angripare eller pen-testare.



31 Hacking i Fokus (2002), s. 69-125.

Intrånget / stjäla tillgången

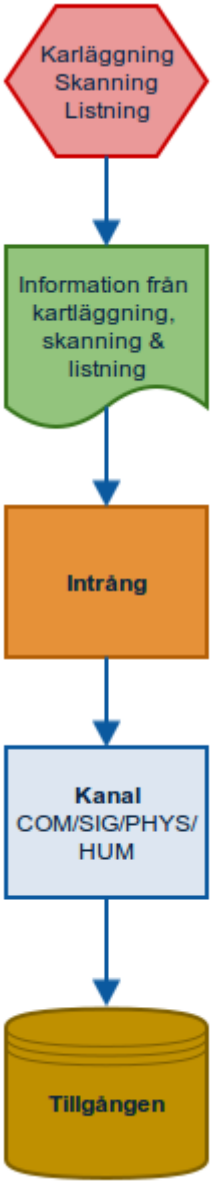
Nu bör angriparen ha all den information som behövs i form av underrättelser, konton, lösenord, sårbarheter, passerkort, nycklar, larmkoder m.m. för att kunna utföra det egentliga intrånget för att komma över resursen som målet försöker skydda. Här bör angriparen överväga vilken av kanaler som är enklast att penetrera för kunna stjäla tillgången utifrån de uppgifter han samlat in i de andra faserna. Kanske är det till och med så att samtliga kanaler behöver användas för att komma över resursen. HUMSEC/HUMINT för att lura bort väktaren, COMSEC/COMINT för att blockera eller koppla ur larmet, SIGSEC/SIGINT för att blockera radiotrafik och till sist PHYSSEC för att göra det faktiskt inbrottet. Eller kanske är det så att det enda som behövs är COMSEC/COMINT (datornätverk) för att ta sig i i nätverket och stjäla den information som målet försöker skydda. När väl så har skett är målet med penetrationstestet uppfyllt. Observera dock att även en misslyckad stöld är att anse som ett lyckat pentest. Penetrationstestet går ju ut på att testa att penetrera säkerheten och visar det sig då att målet har tillräcklig säkerhet så att det inte går att penetrera måste ju även detta rapporteras (tillsammans med de sårbarheter som faktiskt hittades).

Hur angriparen går vidare i själva intrångsfasen beror alltså helt och hållet på de uppgifter han samlat in i alla de andra faserna och hur målet ser ut m.m. Det kanske till och med visar sig vara så enkelt att målet använder sig av WEP-skyddat WLAN och angriparen har lyckats knäcka detta och har full access till hela nätverket och har hittat en resurs som delar ut den skyddade informationen. I så fall är denna fasen över på fem minuter. Om det å andra sidan inte finns några vägar in via varken internet, modem, telefonlinjer, WLAN m.m. så kanske ett fysisk intrång måste ske. Detta involverar då en hel del planering och logistik som inte behövs i lika stor utbredning inom kanske COMSEC och SIGSEC. Det finns en hel del vettiga rekommendationer och saker att tänka på i OSSTMM 3 [1] angående just att PHYSSEC. Här nämns bland annat att pen-testaren bör vara vid god fysik, smidighet och uthållighet. Ytterligare utrustning kan krävas så som mörkerkikare, dyrkset, skruvdragare/borrmaskiner, bräckjärn m.m. Här kan man också läsa om vad pen-testaren bör tänka på när det gäller själva resultatet, så som att inte överskatta sin egen fysiska förmåga och/eller intelligens genom att tänka tanker som ”det är nog bara jag som klarar detta eftersom jag har kunskaper om just detta larmsystemet” eller ”klarar inte jag att klättra upp taket så klarar ingen annan det heller”. Pen-testaren behöver också planera sin flyktväg, hur han ska hålla sig gömd, hur han ska undvika larm/kameror/väktare m.m. Likaså behöver han i förväg veta om tillgången går att flytta från platsen eller om det bara går att fotografera tillgången eller liknande, eller om det behövs bärhjälp etc. OSSTMM 3 [1] tar också upp ett väldigt bra exempel på hur en stöld genom PHYSSEC-kanalen kan gå till, nämligen att kombinera den med HUMSEC/HUMINT genom att t.ex. utge sig för att t.ex. köra en budbil och helt sonika köra in på målets annars skyddade område, lasta ombord tillgången och köra ut igen som vilket bud som helst. OSSTMM 3 tar upp möjligheten att använda kaos och panik för att kunna utföra stölden. Detta skulle t.ex. kunna vara att utlösa brandlarmet hos målet och under utrymningen och den kaos som följer ta sig in och stjäla tillgången när området är tomt. Detta skulle ju faktiskt kunna göras än mer kaosartat genom att faktiskt använda någon form av rökkanon för att rökfylla ett eller flera rum, förslagsvis då rum som är en bit bort från där tillgången förvaras för att inte riskera att stöta ihop med räddningstjänsten eller liknande.

Vid ett nätverksintrång använder angriparen/pen-testaren istället alla de sårbarheter, lösenord, resursnamn m.m. som han tidigare har kommit över i de andra faserna för att utföra själva attacken/stölden. Ett exempel på detta kan vara att han först tar sig in i en server via en äldre bugg i SSH för att sedan ladda ner resursen från en NFS-utdelning som hade hittade i listningsfasen. Till sist för angriparen bara över resursen till sin egna maskin.

Om intrånget eller stölden istället kommer att ske via HUMSEC/HUMINT kan detta gå ut på att nu använda de ID-kort, den jargong, klädkod, koder m.m. som han skaffat sig genom de tidigare faserna. Angriparen kan då bygga upp ett helt scenario där han på förväg använder t.ex. SIGINT-kanalen för att blockera och störa ut alla WLAN-stationer hos målet, väntra några timmar eller dagar för att sedan dyka upp som konsult från rätt företag (uppgifter som tidigare har samlats in) för att lösa problemet. Ett annat enklare exempel kan helt enkelt vara att be en receptionist om tillgången och visa upp korrekta papper och behörigheter för denna (papper och behörigheter som samlats in i de tidigare faserna).

Det är alltså i denna fas som allt de material som vi tidigare har samlat in kommer till användning. Det är också här man faktiskt ser vikten av informationen som angriparen har samlat in. Utan den informationen som angriparen fått från kartläggningen, skanningen och listningen hade han eller hon aldrig lyckats med ett intrång. Hade angriparen lyckats hade han eller hon troligen blivit tagen på bar gärning. Informationsinsamlingen innan själva angreppet sker är alltså väldigt viktigt och det gäller att vara så metodisk som möjligt i dessa faser för att inte missa någon viktig information.



Rapport

När penetrationstestet är genomfört är det dags för pen-testaren att rapportera alla sina fynd, d.v.s hur han kom in, vilka sårbarheter han hittade på vägen, vad han lyckades stjäla m.m. Det är viktigt att pen-testaren sparat information om alla de steg han tagit för att nå målet och även allt annat runt omkring som kan vara intressant för målet/kunden. Kanske upptäckte pen-testaren t.ex. att det är enkelt att göra en deface på målets webbsida, men eftersom detta inte var en del av pentestet så är det kanske lätt att glömma bort att rapportera denna brist. Allt sådant skall finnas med i professionell rapport.

All försvagning av säkerheten som pen-testaren kan ha åstadkommit ska också rapporteras, likaså eventuella skador han kan ha orsakat. Det är t.ex. om han brutit upp lås och skadat dessa, förbikopplat larm som ej återställts, installerat bakdörrar på servrar och datorer, ändrat lösenord på telefonväxlar etc. Allt detta för att målet ska kunna återställa säkerheten efter penetrationstestet. Dess syfte är ju trots allt att förbättra säkerheten, inte försvaga den.

Däremot är det alltid en moralisk fråga om rapporten ska innehålla namn på personer som pen-testaren lyckades utföra social engineering på. Detta brukar dock regleras på förväg genom avtal m.m.

Sekretess

När det gäller avrapporteringen av ett pentest är det av yttersta vikt att enbart rätt personer tar del av rapporten. Detta är pen-testarens ansvar att se till! Det allra bästa är om rapporten kan levereras personligen mellan fyra ögon till den i ledningen som begärt testet. Det näst bästa är via ett krypterat mail, med t.ex. GnuPG eller PGP. Aldrig får en rapport från ett pentest skickas med vanligt mail utan kryptering! Detsamma gäller att rapporten aldrig får skickas med vanlig snigelpost. När väl rapporten är överlämnad till rätt person är det målföretaget som tar ansvar för rapporten. Här uppstår dock en fråga som målföretaget bör ta ställning till, skall pen-testaren spara en kopia på rapporten (självklart i krypterad form) under en tid framöver eller direkt radera alla kopior av den efter leverans till kunden.

Om en pentesting-rapport skulle komma på villovägar är det riktigt illa för målet då den som får tag i rapporten då har all kunskap som krävs för att enkelt ta sig in. Och inte nog med det, troligen har upphittaren då också koder, personuppgifter m.m. till anställda på företaget. Detta är något som alltså inte får hände under några omständigheter och kan leda till både skadestånd och väldigt dålig PR för pen-testaren.

Kritik mot penetrationstester

Även om penetrationstester är ett bra verktyg för att testa säkerheten hos ett mål då det blir ett verklighetsförankrat angrepp utifrån så finns det ändå vissa saker att ta i beaktande. Viss kritik har riktats mot just penetrationstestning och denna bör tas på allvar.

Den mest nyliga kritiken är nog Åsa Schwarz artikel *Penetrationstester - Varför blir det så fel?*[32]. I artikeln kritiserar Åsa de så kallade black-box-testerna för att pen-testarna då gör allt för att komma in i systemet, utan något egentligt mål eller tillgång att komma åt. Syftet blir således bara att ”komma in” i något av kundens system, oavsett vad, och då kanske missar det som kunden vill skydda mest. Kunden blir imponerad av pen-testarnas kunnande även om de aldrig har testat säkerheten runt företagets känsligaste delar. Så länge de kom in var alla nöjda och glada. Detta bottnar dock i att kunden inte specificerar tillräcklig vad som ska testas och ger inte pen-testarna något egentligt mål att att gå efter. Här är det viktigt för pen-testarna att förklara syftet för kunden innan man börjar med själva testerna. OSSTMM 3 guidar ganska bra i just dessa avseenden och förklarar just att en noggrann metodik är A och O för ett lyckat test.

En annan form av kritik som framförs är den av Craig S. Wright i *A Taxonomy of Information Systems Audits, Assessments and Reviews*[33]. Kritiken han framför är den att ett penetrationstest ger väldigt lite information om den faktiska säkerhet jämfört med en riktig säkerhetsanalys som genomförs inifrån företaget. Vad han avser här med riktig säkerhetsanalys är en sådan analys som t.ex. beskrivs i OSSTMM 3 där man noga går igenom alla attackytor, områden, interaktiva punkter, kontroller m.m. En sådan analys blir mycket mer genomgående än ett penetrationstest. Ofta går det dessutom fortare menar Craig på att genomföra en komplett säkerhetsanalys än att låta en pen-testare ta sig igenom alla stegen för ett lyckat penetrationstest. En säkerhetsanalys blir alltså både mycket mer noggrann och informativ och går dessutom fortare att genomföra än ett penetrationstest. Dessutom är det lätt hänt att det blir både falska positiva och falska negativa resultat i ett penetrationstest. Detta slipper man till stor del i en säkerhetsanalys då man där istället tittar på de faktiska kontrollerna och hur de faktiskt fungerar. Likaså är det lättare att få med de viktiga delarna i säkerhetsanalys.

32 Computer Sweden, *Penetrationstester - Varför blir det så fel?* → http://computersweden.idg.se/2.29373/1.526204/penetrationstester--varfor-blir-det-sa-fel

33 SANS, *A Taxonomy of Information Systems Audits, Assessments and Reviews,* s. 43-49 → *http://www.sans.org/reading-room/whitepapers/auditing/a-taxonomy-of-information-systems-audits-assessments-and-reviews-1801?show=1801.php&cat=auditing*

Företag som är arbetar med penetrationstester

Som jag nämnde i inledningen verkade det inte finnas många företag i Sverige som arbetar med penetrationstester i Sverige, men efter lite ytterligare letande så hittar jag faktiskt en hel del företag som sysslar med detta. De flesta företag är någon form av säkerhetskonsultföretag som då också arbetar med just penetrationstestning. En del av dessa företag listas här nedan. Värt att nämna att många av dessa företaget har utvecklat egna metodiker och arbetar inte efter den metodik jag har skrivit om i detta fördjupningsarbete. De flesta företaget förklarar sin metodik på deras webbsida.

Observera att företagen som listas här nedan inte på något sätt har med detta fördjupningsarbete att göra! Detta är bara en kort lista av de företag som arbetar med penetrationstestning som jag lyckades hitta via Google-sökningar. Denna listan är dessutom på inget sätt komplett.

- **Sentor**
  http://www.sentor.se/konsulttjanster/penetrationstest/
- **Deloitte**
  http://www2.deloitte.com/se/sv/pages/technology/solutions/informationssakerhet-security-privacy-resiliency/sarbarhetsanalys-och-penetrationstestning.html
- **Sedab**
  http://www.sedab.se/tjaenster/it-saekerhet/66-penetrationstester.html
- **Nowsec**
  http://nowsec.se/penetrationstestning.html
- **Bitsec**
  http://www.bitsec.se/it-sakerhet/
- **WarpNine**
  http://www.warpnine.se/?q=node/4
- **KnowIT**
  http://www.knowit.se/Vara-tjanster/IT/Forsvarssystem/
- **NSEC**
  http://www.nsec.se/penetrationstest.htm
- **TrustSec**
  https://www.truesec.se/sakerhet/tjaanster/analystjaanster/penetrationstest
- **Certezza**
  https://www.certezza.net/sv/tjaenster/penetrationstest/
- **Basefarm**
  https://www.basefarm.com/se/wikitech/sakerhetsarbete
- **Seccredo**
  http://www.seccredo.se/risk/informationssakerhet/

Jack-Benny Persson
LX13
Säkerhet
2014-05-10

Reflektioner

Det var intressant att se hur man arbetar med penetrationstestning i Sverige. Till detta hade jag ganska stor nytta av Carl-Johan's examensarbete som han skrivit i detta ämnet. Det finns ganska mycket litteratur i ämnet när man väl börjar gräva lite i det, dock är mycket amerikansk litteratur och inriktar sig på amerikansk lagstiftning och deras etik & moral, vilket inte alltid stämmer överens med Sverige.

Det jag tycker var absolut roligast att fördjupa mig i var kartläggningen och informationsinsamlingen om målet. Man kan hitta väldigt mycket information om ett mål genom Google, Facebook, Twitter, LinkedIn m.m. Slår man sedan samman detta med information man kan hitta på Eniro, AllaBolag, SolidInfo m.m. tillsammans med metadata man kan få fram från MS Word-dokument, PDF-filer m.m. så kan man kan skapa kompletta dossiers om ett företags personal eller målpersonen. När jag gjorde detta mot mig själv hittade jag väldigt gamla dokument som jag helt hade glömt bort att jag en gång i tiden hade lagt upp på nätet för 12 år sedan. Jag tror mycket väl det kan vara så för företag och nyckelpersoner också, att de publicerar saker som de sedan glömmer i bort i kanske 10-12 års tid. Dessutom kan man via metadatan i dessa dokument ta reda på vad företag använder för system på klientnivå. Är det TeX-dokument använder de troligen något UNIX-system. Är det ett MS Office 2010 eller nyare använder de troligen Windows 7 eller nyare. Är det ett MS Office XP eller äldre använder de troligen ett gammalt OS så som Windows XP. Med denna informationen blir det sen så mycket enklare att göra det riktiga hacket eller intrånget. Denna kartläggningsfas och insamlingsfas är nog den viktigaste i hela arbetet skulle jag tro. Utan denna information famlar man nog mest runt på måfå bara.

Att samla in information om personer och skapa hela dossiers är också något jag finner väldigt intressant. Särskilt med tanke på hur enkelt det faktiskt är med Facebook, Google, Twitter, LinkedIn. Tänk att med några sökningar kunna sammanställa en hel persons liv, alltifrån arbete, utbildningar, politiska åsikter, vänner, fiender, föreningsliv m.m. För 10-15 år sedan var detta infomation som tog väldigt lång tid för en underrättelsetjänst att leta fram och sammanställa. Och då var informationen kanske inte ens så exakt som den information man själv kan få fram idag genom att bara sitta framför datorn. Om man sen tar det ett steg längre kan man begära ut ytterligare uppgifter från myndigheter så som Skatteverket för att bara nämna ett exempel. Ytterligare ett steg vore att ha någon form av övervakning av personen, prata med hans eller hennes vänner, före detta arbetsgivare etc. Man kanske till och med skulle försöka sig på att bli vän med någon av målets vänner. Detta vore ju inte alltför svårt egentligen. Man skulle kunna kolla igenom personen vänlista på Facebook och sedan kolla upp en av dessa närmre. Steget därefter hade blivit att börja handla i samma affärer som denna vännen gör och kanske börja lite försiktigt att prata med han eller hon i kön till kassan etc.

Men för att återgå till penetrationstester så tycker jag också att den fysiska säkerheten är viktig, och ack så intressant. Dels för att jag själv arbetat med denna formen av säkerhet och dels för att det ibland är enklare att faktiskt ta sig in på företaget rent fysiskt än att försöka hacka datorer och servrar från ”utsidan”. En sådan enkel sak som att stjäla en anställds passerkort kan ta en angripare långt i företaget. Särskilt om det är ett lite större företag då alla anställda inte känner varandra. Mindre företag kommer det dock bli svårt så de flesta känner varandra och hade reagerat ifall det gick en okänd människa i korridorerna.

När det kommer till portskanningen så är informationen man får fram här ovärderlig. Kör man Nmap med portskanning med OS-fingerprinting och versionsnummer och banners på tjänster får man fram väldigt mycket information. Versionsnumren för alla tjänster på systemet behövs för att

kunna gå vidare och leta upp sårbarheter till just de tjänster och de versioner som angriparen kör. Det är att hitta sårbarheter som sedan blir det dryga arbetat. Att skanna alla datorerna och servrarna kanske går på 10 minuter. Men att sedan hitta sårbarheter för de tjänsterna kanske tar flera dagar. Men när angriparen väl har hittat sårbarheterna kan han med enkelhet ta sig in på servrarna. Väl inne på en server är det sen oftast fritt fram till det interna nätverket och alla servrar som sitter bakom brandväggarna. Ofta skydda man ju just från utsidan, men väl på insidan är skyddet sämre. Det är egentligen det här som allting bottnar i när det gäller penetrationstestning och dataintrång i stort; att hitta sårbarheter för just de tjänster som målet använder sig av. Ett annat bra mål att rikta in sig på som pen-testare är inkommande modemlinjer då dessa ofta tycks glömmas bort av företaget och säkerhetsavdelningen. Det kanske inte är så konstigt egentligen, jag tror många tänker som så att ”vem skulle komma på att ringa till modemet när alla angripare kommer från internet?” Och likaså tror nog många företag att phreaking & wardialing m.m. hör till det förflutna

När det gäller själva intrånget var det ganska svårt att skriva om just detta då finns så otrolig många sätt att genomföra detta på, helt beroende på vad för slags information som angriparen har skaffat sig i de tidigare stegen. Detta var lite synd då själva intrånget ändå är essensen av allt arbete som angriparen har lagt ner.

När jag började detta arbetet hade jag ganska svårt att hitta företag som faktiskt arbetade med penetrationstestning, men efter lite sökande på Google så hittade jag trots allt en hel del företag som arbetar med detta. Det verkar dock vara väldigt få företag som uteslutande arbetar med penetrationstester, utan detta är bara en utav alla tjänster som de sysslar med. Däremot finns det de företag som mestadels verkar arbeta med just penetrationstester.

Den kritik jag hittade mot att använda penetrationstester verkar vara välgrundad. Särskilt de argument som lades fram att man missar mycket viktigt i ett penetrationstest som annars inte hade missats i en mer djupgående säkerhetsanalys inifrån själva företaget. Penetrationstester tror jag dock ändå är ett bra redskap att arbeta med, man ska dock vara medveten om dess begränsningar och bara använda penetrationstester där detta faktiskt fyller en funktion, ett syfte. Och likaså när man väl genomför ett penetrationstest bör man vara tydlig med att ange ett mål, alltså en tillgång som är viktig för företaget att skydda. Det är denna tillgång som då angriparna/pen-testarna ska inrikta sig på. Annars blir det lätt så som Åsa Schwarz skrev att angriparna gör allt för att ”ta sig in” på systemet utan något egentligt mål. Angriparna kommer att famla i blindo efter en väg in i något av företagets system, bara för att ta sig in. Kvalitén på testet kommer alltså att höjas avsevärt om syftet med testet styrs upp på förväg med bestämda tillgångar som angriparna skall komma över. Det hela blir alltså mer riktat då.

Det hade varit väldigt intressant att arbeta med penetrationstestning även om jag tror det hade varit minst lika intressant att få arbeta med säkerhetsanalyser. Säkerhetsanalyser kräver nog mer en analytisk förmåga medan penetrationstestning kräver en mer kreativ förmåga.

Det har i varje fall varit väldigt intressant att få tillfälle att fördjupa sig i detta stora och breda ämne under dessa timmar det har tagit mig att läsa, skriva och fundera om ämnet.

Källhänvisningar

[1,11,17] Pete Herzog (2010), *OSSTMM 3*, http://www.osstmm3.org

[2,3,4,5,6] Torkel Gregow (2007), *Sveriges Rikes Lag,* Nordstedts Juridik AB, Stockholm

[7] Företagande.se, *Så kan IT-konsulterna minska förlusterna vid ansvarsskada.* http://www.foretagande.se/sa-kan-it-konsulter-minska-forlusterna-vid-ansvarsskada/
Läst 2014-05-02

[8] If.se, *IT-konsult och datakonsult.* http://www.if.se/web/se/foretag/varaforsakringar/itdataforetag/pages/itdataforetag.aspx
Läst 2014-05-02

[9] Carl-Johan Bostorp (2006), *Penetrationstester: Offensiv säkerhetstestning*, Linköpings Universitet.
http://www.diva-portal.org/smash/get/diva2:22798/FULLTEXT01.pdf

[10, 31] Stuart McClure, Joel Scambray, George Kurtz (2002), *Hacking i Fokus*, Pagina Förslags AB, Sundbyberg, ISBN: 91-636-0707-7

[12] Anteckningar från föreläsning av Rikard Bjurenbäck i ämnet Routing & Switching på EC-Utbildning i Helsingborg, 2014.

[13] Johnny Long (2008), *Google Hacking for Penetration Testers, Volume 2*, Syngress Publishing Inc. ISBN: 978-1-59749-176-1

[14] Föreläsningar av Martin Sörensson i kursen Säkerhet på EC-Utbildning, maj 2014.

[15] Wikipedia.org, *Human Intelligence (intelligence collection)*, http://en.wikipedia.org/wiki/Humint
Läst 2014-05-04

[16] Linus Vallej (2000), *Copyright Finns Inte,* http://www.df.lth.se/~triad/book/

[18] Lennart Alexandrie, Lennart Persson (2001), *Svensk Säkerhet 2001,* AR Media AB. ISSN: 1401-8314.

[19] Scanner.nu, *Digitala radiosystem i Sverige – 1200Bd,* http://www.scanner.nu/faq_digital.htm.
Läst 2014-05-07

[20] Wikipedia.org, *Personsökare*, http://sv.wikipedia.org/wiki/Persons%C3%B6kare
Läst 2014-05-07

[21] Generic Mobile, *Minicall tjänster,* http://genericmobile.se/minicall-tjanster
Läst 2014-05-07

[22] Wikipedia.org, *Wardialing,* http://sv.wikipedia.org/wiki/Wardialing
Läst 2014-05-08

[23] Hacklabs, *Wardialing Penetration Test,* http://www.hacklabs.com/war-dialing-penetration-test/
Läst 2014-05-08

[24] SecureState, *Wardialing,* http://www.securestate.com/Services/Risk%20Management/Pages/War-Dialing.aspx
Läst 2014-05-08

[25] Kevin Mitnick (2002), *Bedrägerihandboken,* Pagina Förslags AB, Sundbyberg.
ISBN: 91-636-0764-6

[26] Wikipedia.org, *Wired Equivalent Privacy,*
http://sv.wikipedia.org/wiki/Wired_Equivalent_Privacy
Läst 2014-05-09

[27] Wikiepdia.org, *WPA* → http://sv.wikipedia.org/wiki/WPA
Läst 2014-05-09

[28] HowToGeek, HTG *explains the difference between wep wpa and wpa2 wireless encryption and why it matters* →
http://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/
Läst 2014-05-09

[29] PaloAltoNetworks, *Attacks on WPA/WPA2,*
http://researchcenter.paloaltonetworks.com/2013/09/risks-to-wireless-networks-attacks-on-wpawpa2/
Läst 2014-05-09

[30] NyTeknik, *Lätt avlyssna trådlös telefon,*
http://www.nyteknik.se/nyheter/it_telekom/allmant/article258109.ece
Läst 2014-05-10

[32] Computer Sweden, *Penetrationstester - Varför blir det så fel?,*
http://computersweden.idg.se/2.29373/1.526204/penetrationstester--varfor-blir-det-sa-fel
Läst 2014-05-09

[33] Craig S. Wright (2007), *A Taxonomy of Information Systems Audits, Assessments and Reviews,*
http://www.sans.org/reading-room/whitepapers/auditing/a-taxonomy-of-information-systems-audits-assessments-and-reviews-1801?show=1801.php&cat=auditing