Hacking / Hacker

En hacker er egentlig en person som er usedvanlig flink innenfor et spesielt fagområde. I dag derimot, forbindes en hacker med en som har kunnskaper og ferdigheter innenfor informasjonsteknologi og datasystemer som bruker disse til å utforske og manipulere datasystemer på en kreativ og som oftest uautorisert måte.

Hacking er derfor prosessen som en hacker gjør, nemlig det å være kreativ, utforske og manipulere datasystemer ved hjelp av ulike verktøy eller teknikker. I dag blir hacking sett på som å utnytte sårbarheter i programvare for å gjennomføre sosial manipulasjon (Social Engineering), som eksempelvis kan lede videre til å lure folk til å avsløre passord eller annen informasjon.

Motivasjonen bak hacking er ulik, og man har forskjellige typer hackere.

Første type er bare «hacker», og er en person som prøver seg fram, men vil ikke gjøre noe skade, kun utforske.

Andre type er «cracker». Denne har ofte et mål, men har ikke kunnskapene til å nå målet sitt. Den bruker derfor ferdige verktøy for å nå målet.

Tredje type er «white hat». Denne er en vennlig hacker som ofte gjør selskaper en tjeneste ved å teste systemene deres for sikkerhetshull.

Fjerde type er «grey hat». Her stammer navnet fra «gråsone» som betyr at denne gjør ting som er litt «på kanten». En «grey hat» gjør noe ulovlig, men med «gode» intensjoner, ofte for å fremheve et poeng. Eksempelvis: “Jeg så du hadden en dårlig dørløs, så jeg brøt med inn. Har ikke rørt noe, men ville bare vise hvor dårlig låsen din er. Fiks låsen din!”

Femte type er «script kiddie». Denne ligner på «cracker», men har ingen mål. «script kiddie» bruker ferdige verktøy, grunnet sin manglende kompetanse, men bruker sin begrensende kompetanse og ferdige verktøy for å teste for «gøy».

Sjette og siste type er «hacktivist» og er nesten selvforklarende, men er en som hacker for å oppnå et mål og for å synliggjøre sin sak. Eksempelvis: Politiske og ideologiske mål.

I senere tid har man funnet «oppskrifter» hvor man slår sammen flere av disse. Man har derfor fått begreper som scammers og social engineering, hvor social engineering spiller på psykologi, overtaling og manipulering og scammers som er script kiddies, men som bruker social engineering i tillegg.

Social Engineering / Sosial manipulasjon:

Social Engineering er argumenterbart den største trusselen i dagens IT-sikkerhet. Social engineering er en teknikk som brukes av hackere for å manipulere mennesker. I stedenfor at en hacker skal hacke seg frem til informasjon ved å finne sårbarheter i et datasystem, kan man heller bare «spørre» om den. Noen metoder for social engineering finnes under.

Phishing: Dett er en form for SE hvor man sender ut falske e-poster, tekstmeldinger eller andre former for skriftlig kommunikasjon hvor man later som man er en pålitelig kilde, for å lure mottakeren til å avsløre passord, betalingskort eller annen info.

Preteksting: Denne innebærer å få brukeren til å gjøre en handling ettersom avsender er «troverdig» og det vil «løse et problem». Eksempelvis det som skjedde i starten av semesteret. «Feide systemet virker ikke, så vi må lage vårt eget utenom. Bare skriv inn brukernavn og passord her..»

Bating: Innebærer å lokke offeret med noe som er fristende eller et løfte/belønning. Eksempelvis legge ut en minnepinne på et tilfeldig, men velplassert sted hvor noen vil bli nysgjerrig og plukke den opp. Hvis noen da plugger denne inn i en datamaskin vil hackeren få tilgang til systemet, med et ferdigkodet script som ligger på minnepinnen.

Tailgating: Er en mer praktisk manipulasjon, men innebærer å følge etter en autorisert person inn i et sikret område, ved å late som man hører til. Eksempelvis: Følg etter noen inn et sted hvor man egentlig trenger nøkkelkort for å komme inn.

Nettsider og sikkerhet

URL eller Uniform Resource Locator sier noe om hvor en ressurs er. En URL inneholder flere deler.

Protokoll er den første delen av en URL og spesifiserer hvilken protokoll som skal brueks for å hente resursen du vil se. De vanligste protokollene er http og https, men man har også ftp for filoverføring og mailto for e-post.

Vert: Dette er den andre delen av en url som spesifiserer nettadressen til serveren. Eksempelvis: [www.example.com](http://www.example.com)

Sti: Denne spesifiserer banen eller plasseringen på hvor man vil på serveren. Dette kan være en underside på en nettside eller en bestemt fil. Eksempelvis: /folder/file.html

Http vs https:

Http er en grunnleggende kommunikasjonsprotokoll hvor informasjon blir sendt i klartekst, som vil si at alt du skriver inn på siden blir sendt som en tekstfil, og kan leses av. Informasjon sendes via GET eller POST, hvor GET foregår gjennom URL og POST sendes i forespørselspakker, som ikke er sikkert.

Https er en krypert kanal som tilbyr bedre sikkerhet. Https beskytter derimot kun mot overføring, altså «man in the middle»-attacks. Informasjonen er derfor sikret når den sendes fra A til B, og kan ikke snappes opp og leses av, endres eller liknende. Den har derimot ingen garanti mot svindel.

Ulemper med https:

https blir stemplet som en trygghet noe som gjør at vi mennesker stoler mer blindt på de sidene som har dette. Det skaper dermed en falsk trygghet, ettersom svindlere også kan benytte seg av https, hvor den sensitive informasjonen går rett til svindleren.

Cookies:

Cookies eller informasjonskaplser er noe som lagres på brukerens maskin og brukes til å skreddersy innhold til brukeren. Cookies sporer all aktivitet, som f.eks. hvor du er på en nettside, hva du ser på, hvor lenge du ser på det, og gir deg videre forslag.

Cookies har også en Session ID som er en idenfitikator på DEG, som brukes på f.eks. innlogging, og kan holde deg innlogget i et visst tidsrom, hvis du er på samme nettleser.

Skadevare:

Skadevare kan være veldig mye, men det omhandler det å få tilgang til en maskin og hente ut data, eller alternativt overvåke data. Skadevare kan også ta utnytte at pcen den har infisert ved å bruke en porsjon av resursene på den (CPU, GPU, RAM, SSD etc.) til f.eks. filserver eller webserver. Skadevare kan også være ren hæreverk, hvor skadevaren gjør deler av pcen utilgjengelig for brukeren, for å deretter kreve penger fra offeret, for å få tilgang til dette igjen (ransom).

Skadevare kan også bruke tilkoblede enheter til å spionere på deg, ved å f.eks. ta opp lyd og/eller bilde, alternativt overvåke hva du skriver på tastaturet ditt, for deretter snappe opp passord, e.l.

Skadevare kan også hente ut informasjon som ligger på maskinen, som f.eks. besøkte websider, hemmelig filer eller annen personlig informasjon.

Oppbygging av skadevare:

Spredningen av skadevare skjer i flere faser og metoder. Dette er en generell oppbygging for hvordan skadevare opptrer.

Stridshode: All skadevare må komme seg inn i et system, enten det er via en minnepenn som offeret plugger inni pcen sin, eller en fil som offeret laster ned. Som oftest kommer stridshodet til pcen til offeret via Social Engineering. Her kan en hacker eller scammer lure offeret til å laste ned noe som virker troverdig, men som viser seg å være noe helt annet. Alternativt har hackeren utvidet installasjonspakken til et troverdig program, hvor stridshodet er en del av det legitime programmet. Dette hjelper med kamuflasje, som er en annen fase.

Spredning: Er prosessen hvor stridshodet «pakkes ut» og sprer seg på maskinen til offeret.

Kamuflasje: Er fasen hvor skadevaren må prøve å «gjemme seg» eller kamuflere seg blant andre filer på maskinen, for å ikke bli oppdaget av enten offeret eller programmer som søker etter skadevare.

Nyttelast: Nyttelast er siste fase, og er når skadevaren gjør skaden den ble programmert til å gjøre.

Skadevare er med andre ord veldig mye, og det er derfor kun en samlebetegnelse for mye annet. Under spesifiseres noen skadevare-typer.

Ormer:

* Kan sammenliknes med en bakterie. Den er nemlig «levende» og selvstendig. Ormer er selvstendig, og selvspredende/selvrepliserende. De sprer som regel via nettverk (mail, web, LAN, fildeling eller sosial medier). Ormer baserer seg som regel på bakdører, og feilkonfigureringer som standardpassord og åpne porter.
* Ormer skiller seg fra virus ved at disse sprer seg selv, er selvstendige (bruker ikke noe program), og infiserer nettverk, fremfor maskiner.

Virus:

* Virus er i motsetning til ormer avhengig av å bli aktivert. Virus er selv en sekvens av programkode, som igjen knytter seg til en annen programkode, hvor virusdelen er programmert til å gjøre skade. Virus blir sjeldene oppdaget av offeret, ettersom det jobbet over tid (sakte), hvor den tar over den ufarlige programkoden.
* Virus infiserers forskjellig, men dette er noen av metodene som finnes.
  + Overwriting: Erstatter innhold i exe-fil med ny kode
  + Prepending: Legge til viruskode først i den ufarlige exe-fila (virus+original)
  + Appending: Legge til viruskode sist i den ufarlige exe-fila (original+virus)

Makrovirus:

* Lesbart virus i høykode
* Eksempel: «Melissa»
* Skrives i egen «enkle» scriptspråk
* Kopierer seg inn i word f.eks.
  + Kan utføre kommandoer som «delete», «sendmail» osv.

Scriptvirus:

* Ikke-kompilert kode = ren tekst

Trojanere/webtrojanere

* En trojaner er skadevare som utnytter tillitten som vi har til et program eller nettside.
* Eksempelvis kan en trojaner installeres samtidig som du installerer en oppriktig og troverdig applikasjon, da du har trykket deg inn på google.com/chróme og lastet ned derifra. Nettsiden ser ordentlig ut, og du får også den ordentlige versjonen av chrome, men pluss denne trojaneren som har lurt seg i installasjonsmappen. Denne trojaneren kan videre gjør masse skade på din maskin, samt overvåke det du gjør.
* Eksempelvis kan gå inn på komplett.no for å handle. Her trykker du ja cookies og logger deg inn samtidig. På grunn av en svakhet i Komplett sitt system har nå en trojaner fått tilgang på din innloggingsinformasjon og på grunn av cookiene får den også tilgang til dine preferanser og kan bruke dette til å lokke deg en annen gang med social engineering.

Spyware:

* Spyware kommer av ordet spion og er skadelig programvare laget for å spionere og overvåke det du gjør. Dette kan være alt fra nettleseraktivitet, til å spionere på deg gjennom kameraet på laptopen din, og overvåke alt du skriver på tastaturet ditt.
* Typisk mer plagsomt enn farlig.

Drive-by-download:

* Typisk skadevare som automatisk lastes ned når du som bruker trykker deg inn på en link (nettside, mail, e.l.)

Rootkits:

* Rootkits kommer av navnet root-tilgang og er en form for skadevare hvor målet er å gi angriperen rot-tilgang til systemet. Tilgangen er som oftest

Ransomware:

* Skadevare hvor angriperen typisk låser brukeren ute fra systemet, eller holder igjen filer, eller sensitive filer/bilder/videoer. Angriperen ber som oftest om penger fra brukeren for at den skal få tilgang til dette igjen.

Hoax:

* Hoax = bløff
* Hoax er når man blir lurt til å tro at man har et problem som MÅ fikses.
* Det kan for eksempel være en mail; «Du har virus! Trykk på denne linken for å laste ned et virusprogram som vil ordne dette for deg»

Botnets:

* Botnest er skadevare som sendes som alle andre skadevarer, via e-post, lenker eller gjennom andre sårbarheter. Det som gjør disse annerledes fra annen skadevare, er at disse kan fjernstyres
* Typisk vil en angriper ha muligheten til å navigere seg fritt rundt på datamaskinen din uten at du vet om det.

Begreper:

Bakdører:

* Bakdører er kort sagt en annen vei inn i et system, som vanligvis er skjulte. Disse kan være laget med vilje, eller ikke. Er det ikke laget med vilje, er det generelt en sikkerhetsrisiko som kan utnyttes av hackere. Lager man en bakvei med vilje, har man som oftest tenkt litt gjennom sikkerheten.
* En bakdør er som sagt en annen vei inn i et system, hvor som oftest hackere kan få tilgang til et system uten å måtte autentiserer seg ved bruk av påloggingsinformasjon eller liknende. Dette kan videre tillate angriperen å utføre skadelige handlinger, som å stjele data, installere skadevare, eller utføre andre angrep.
* For å sette det i perspektiv kan jeg trekke fram et eksempel-scenario. «En tyv skal bryte seg inn hos deg og stjele noe verdifult imens du er på ferie. Tyven bryter seg ikke inn hoveddøren ettersom den har en dørløs med smartfunksjoner som kan avsløre han hvis den tukles med, og hovedsakelig for at den er låst. Alle vinduer er lukket og gardiner er trukket for, på hovedsiden. Tyven går videre rundt huset og ser at et vindu står på gløtt i andre etasje på baksiden av huset. Tyven finner en stige som ligger på eiendommen og klatrer inn vinduet, og har nå fri tilgang til huset».
* Her ser man at hovedinngangen til huset er godt sikret, hvor døren er låst og tyven har ingen mulighet til å komme seg inn. Men da tyven går på baksiden og ser seg godt om, finner han en svakhet i sikkerheten til husstanden og utnytter den.
* Her kan det da tenkes at familien uviten dro på ferie uten å vite at vinduet sto åpent. Hadde dette vært med vilje, ville de kanskje satt vinduet i låsestilling for å lufte, noe som ville vært sikrere.

Signatur:

* Signatur refererer til en bestemt type skadevare, eller de ulike mønstrene de følger. Signaturer brukes av antivirusprogrammer for å identifisere og blokkere kjente trusler. Signatur kan være mye forskjellig. Alt fra filnavn, til filstruktur, og kodestruktur. Antivirusprogram sammenlikner derfor strukturen i det du laster ned, med det de har i sin egen database

Heuristikk:

* Heuristikk refererer til analysen som blant annet antivirusprogrammer gjør mot signaturer og mønstre.

Sandkasse:

* Sandkasse eller sandbox er mye av det samme som i videospill. Det er rett og slett et sted hvor man tester, utforsker og kjører operasjoner før man bruker det i den «ordentlig verden». En sandkasse blir sett på som et kontrollert miljø, hvor man ikke kan gjøre noen skade.

Tripwire:

* Tripwire er en «detektor» for å oppdage uautoriserte endringer i noe man ikke vil skal komme på avveie. En tripwire vil si ifra hvis endringer eller sikkerhetsbrudd oppstår.

Dos-angrep:

* DoS eller Denial of Service angrep oppstår når en angriper overbelaster en tjeneste eller enheten til brukeren.
* Eksempelvis kan dette være at angriperen laster opp en kjempestor fil til systemet/enheten som den vil prøve å gjøre utilgjengelig.

Spoofing:

* Spoofing vil si å fremstå som noe/noen du ikke er.
* Eksempelvis kan dette være e-postspoofing, hvor avsender prøver å være en kjent kleskjede som sender ut sin ukentlige kundeavis, men hvor linkene sender bruker til en falsk nettside. Her er det da en blanding mellom spoofing og phising.

Maskinvare:

Angrep ved fysisk tilgang:

* Dette vil si at noen får tilgang til en fysisk datamaskin, server eller annet for å gjøre skadelige handlinger som stjeling av data, installere skadevare eller andre ondsinnede handlinger.
* Et eksempel på angrep ved fysisk handling er å installere skadevare gjennom en minnepinne.

Remote desktop:

* Remote dekstop gjør det mulig for noen/en angriper å koble seg til en datamaskin fra en annen datamaskin over nettet, og får dermed full tilgang til den, som om personen skulle vært der selv. Remote dekstop brukes ofte som et kundeservice verktøy ved å bruke applikasjonen TeamViewer, noe som lar en kyndig person hjelpe den som er mindre kyndig. Dette kan derimot utnyttes gjennom social engineering, spoofing, eller hoax, hvor angriperen tilbyr seg å hjelpe for å deretter ta kontroll over datamaskinen.

**Finne og utforske maskiner/systemer**

Sikkerhetshull/oppdateringer

* Sikkerhetshull viser til svakheter i et system som kan utnyttes av angripere. Dette kan f.eks. være en bakdør, eller en bug.
* Oppdateringer inneholder vanligvis rettelser for slike sårbarheter.

Backup

* Backup refererer til å lage en kopi av data hvis noe skulle skje med originalfilen. Har man backup har man muligheten til å gjenopprette filene senere.

Sletting av data (formatering)

* Slette data er ikke så lett som man skulle tro. Når man sletter data, sletter man egentlig ikke selve innholdet, bare plassen som var satt av til innholdet, eller med andre ord, man sletter referansen til filen, som gjør at man ikke finner den igjen uten avanserte verktøy.
* Ønsker man å slette noe fullstendig, bør man bruke sletteverktøy, eller ødelegge lagringsenheten fysisk.
* Man kan også formatere disken hvor filene ligger lagret. Ved å formatere flere ganger, vil man overskrive den originale plassen og øke sjansen for at det orignale innholdet blir borte. Men ettersom alt blir tildelt en tilfeldig plass, må man i så fall formatere mange ganger.

Metadata

* Metadata er informasjon som beskriver andre data, eller data om data. Metadata beskriver selve informasjonen som lagres. Eksempelvis i et bilde vil noen av metadataene si noe om; filstørrelse, GPS-plassering, filtype, kamera/telefon-modell, ISO, lukkeråpning, blenderåpning osv.

Skytjenester

* Skytjenester er tjenester som tilbys over nettet. Skytjenestene er mange, hvor noen tilbyr lagrings av filer, bilder og videoer, andre tilbyr databaser og andre servere for nettsider. Eksempel på førstenevnte er Google Drive, Google Photo, OneDrive, Dropbox og iCloud.

Utstyr / IOT

* IoT eller Internet of Things refererer til all småutstyr innenfor IT. Noen eksempler på IoT er; routere, skrivere, datamaskiner, smartlys, smartkontakter, sporingsbrikker m.m.

Mobile enheter:

* Mobile enheter referer til enheter som er bærbare, hvor disse er noen; smarttelefoner, nettbrett, bærbar pc,

Hackere – Hacking (23.04)

Hvem er hackere – Hva vil de?

Hvorfor feiler datasikkerhet

Sosial manipulering

* Teknikker
* Spoofing, phising, finne info
* AI/KI

Nettsider:

* Parametere
* GET/POST
* HTTPS
* Coockies/Sessions
* Sporing/Overvåkning
* Validering av input (Hvorfor + typer)
* SQL-injection (Ideen om at input blir til kode)
* XSS
* CSRF/Webtrojanere
* DoS
* CMS-systemer