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

Spyware:

Drive-by-download:

Rootkits:

Ransomware:

Hoax:

Botnets:

Begreper:

Bakdører:

Malware/Skadevare:

Signatur:

Heuristikk:

Sandkasse:

Tripwire:

Dos-angrep:

Spoofing:

CMS – systemer:

Standarder og prosedyrer for bedrifter

Nettverk

«Klassisk datasikkerhet»