23 December 2014

Lidt at tænke over i Julen

Dette er noget jeg meget ofte støder på i forbindelse med mit job på den ene eller anden måde.

- Hosting af egen hjemmeside på eget net = DDOS og mulig fuld komprimentering af hele ens NET.
- Man er nem at finde når man har sit eget AS nummer (ip range) = Target .
- Almindelige NS lookups på A, MX osv afsløre hvor der skal angribes = Target.
- Email adresser = Target - phishing og spearphishing.
- Tilladte filtyer = traget attacks , virus komprimenteringer, hvornår har du sidst undersøgt hvad der kan sendes igennem din mail scannnings løsning ?
- NTP = Kan afsløre hvilket udstyr man har kørende = brug egen NTP serevr.
- Externe DNS serevrs = DDOS og andre DNS attacks som opstår ind imellem...har du forresten hørt om SPLIT DNS og "Rate Limiting" ?
- Web-admin interfaces til ANY på alle former for udstyr = Hacker forsøg og endelig komprimentering.
- RDP åben for ANY = Hacker angreb og endelig komprimentering, dejligt når der er etableret et grafik interface til hackerne !
- Bring you own device = Fucked up....Du vil blive komprimenteret ellers tillader du bare komprimenteret brugere på dele af dit net og har du styr på de ikke kan

komme igennem fra et net til et andet ?

- Wireless uden Radius implementering = Du kan hackes med tiden og brugen af WPA2 alene er mere "hacker friendly"

- Kasse apperater = Det er set at kasseekspedienten kan surfe fra et kasseapperat med windows systemer kørende....Hvad mon der kan ske ved det ?

- Brugerne kan benytte facebook fra dit virksomheds net = Hacker angreb og endelig komprimentering

- Brugerne kan benytte Dropbox fra dit virksomheds net = Dataloos data leaks, Benyttes ofte til at hoste malware i forbindelse med phishing og spearphishing kampanger. Men det er smart.....

- Brugen af java = Hacker angreb og endelig komprimentering - Du vil blive ramt af "Drive-by" attacks på et eller andet tidspunkt.

- Tillad java og java scripts i din browser = Hacker angreb, Drive-by og endelig komprimentering.

- Firewalls er ikke bedre end dem der sætter den op, mangler typisk regler for outbound trafik = Alle Botnets kan køre på dit net.

- Bruger du USB = Alle kan gå forbi og installere Trojans og andet i dit net, blot ved at have adgang i sekunder til ubeskyttet udstyr.

- Har du ingen beskyttet logs fra IDS, Netflow, Firewalls, Routers, Servers, mailservers osv. = Du lever i lykkelig uvidenhed, du har slet ikke styr på din sikkerhed og er sikkert allerede komprimenteret.

- Web-cams, NAS servers publiceret direkte på Internettet = Fucked up....Du vil blive komprimenteret på et eller andet tidspunkt.

- VPN forbindelser kun med opsatte preshared keys = Yndet vej ind igennem dit net når data skal xfilterers ud af det.

- Kender du alle IP enhder på dit net = Ikke....hvordan ved du sår, hvad du skal beskytte dig imod ?

- Vi bliver ikke ramt vi bruger kun linux = Idiot....alle nævnte ting her gælder også for Linux, unix, ios, windows of andet

- Vi bruger kun Open source software så vi er sikre = Tiden har vist dette ikke er tilfældet. Open Source er lige så usikkert som closed source. OpenSSL ?

- Vi bruger kun Iphone de er de sikreste = Nej...per defination kan de ikke være sikere fordi de bruger Internettet.

- Vi vil have stemme systemer til næste folketings valg = Idiot....alt elektronisk kan manipuleres. Systemet vil desuden være forældt imellem hvert folketings valg. 4år er evigheder i sikkerheds verden, hvem skal betale for et nyt system

hvert 4 år ? - Kun en tjener ved det system...ham der sælger det.

- Ingen styr på Smartphones i dit net = Big time dataloss, og du lever igen i lykkelig uvidenhed.

- Passwords under 14 karekterer = De kan gættes uden det helt store setup idag til at cracke med.

- Tillader du brugen af eksterne web-mail systemer fra dit eget net = Så kan du rammes af mange af de nævnte agreb listet her.

- Tillader du adgang til alle domæner i verden = Nye angreb kan opsættes imod DNS blacklistning løsninger af alle typer og kan omgås på 1 min. (brug whitelistning)

- Patch Management = Skal virke på alle dine systemer, Firewalls, Routers, klienter, servers, telefoner osv.

- Chefer der gerne vil have alting som de andre ikke kan få eller bare før de andre = Hvem er det lige en hacker gerne vil ramme ?

- Ved du hvordan al trafikken ser ud i hele dit net ? = Ikke...Hvordan kan du så sige at du ikke er komprimenteret nogen steder ?

- Vi benytter kun switches på vores net som er opsat som elmindelig falde switchs = Har du hørt om ARP Poisining ?

- Bruger du alle dine hosts i dit netværk, som små honypots med et HIPS system der kan afsløre om unormale ting foregår ? = Måske du burde oveveje dette

- Kan alle på dit lokal net tilgå alle servers ? = Måske du burde overveje en segmentering, men hackeren ville elske hvis du ikke gjorde det.

- Gemmer din printer en kopi af alt hvad der bliver sendt til den ? = Måske du burde slå det fra ? Hackeren ville igen elske hvis du ikke gør det.

- Tillader dine switchwes at der kan tilkobles yderligere ting (mac adresser) på en port ? = OK ikke... så kan hacking devises også tilkobles uden nogen ville vide at det skete !

- Jamen Anti-virus virker jo ikke = Jo det gør. Det tager det værste skrald som er kendt, hvilket er meget, men det tager ikke alt....det er rigtigt.

- Tillader brugen af URL Shorteners som goo.gl eller bit.ly = Vidste du at dette bruges til at tracke hvem der klikker på en url, eller til at skjule ondsindet urls, eller kan bruges til at holde styr på om et mål har klikket på et opsat ondsindet angreb.

- Har du et Samsung SMART TV med indbygget mikrofon og stemme genkendelse ? = Vidste du at det i mange tilfælde optager alle samtaler det kan høre !

- Vidste du at iphone har talt alle dine skridt du hat gået ? = Har gjort de siden

iphone 4.....man kan ikke slå dette fra !

- Har du hørt om bagdøre før i forbindelse med hacking ? = Vidste du at der findes bagdøre der kun kan lukkes op med en såkaldt "magic packet" som firewalls og IDS enheder ikke kan opdage !

- Tillader du SHODAN scanninger imod dit net = Tillykke du vil være blandt de første der bliver ramt.

- Har du ingen IT-Sikkerheds folk ansat = Nej vi har outsourcet det -> Nej du har outsourcet dit hovede == GAME OVER

Glædelig Jul og Godt Nytår