COMPUTERWORLD

HackerVåben, Værktøj eller Redningskrans. Lav en Live XP CD med forskellige værktøjer

Live CD'ere har længe været kendt og brugt i linux verdenen. Her kan du se hvordan du laver en Live (bootbar) windows CD, der kan redde dig når, Din PCer gået ned med virus, spyware, eller uoprettelige fejl. Live CD'ere bruges af hackerne, administratore

Skrevet den **03. Feb 2009** af **bufferzone** I kategorien **Sikkerhed / Generelt** | ★★★☆☆

Alle der arbejder med Windows maskiner ved at sådan nogle, nogen gange går ubehjælpeligt ned og skal reddes. I dag med alt den spyware, malware og virus der florere, sker det oven i købet at maskinen er så død, at ikke engang en korrekt udført repair fra originalmedier kan rede maskinen, og eneste løsning er formatering og efterfølgende geninstallation fra sikre rene mediet, herunder total updatering og patching før maskinen igen tilkobles nettet. Denne løsning har ofte betydet at harddisken skulle afmonteres og placeres i en anden maskine først, for at redde dokumenter, billeder og anden vital data inden diskene formateres. Jeg vil endda påstå at jeg har reddet ægteskaber ved at fiske 4 års digitale billeder at børnene ud af en disk der var døden nær af virus.

Løsningen på dette og en række andre problemer og opgaver er en såkaldt Live CD. Normalt hører begrebet Live CD'ere til linux verdenen, hvor man kan få rigtig mange forskellige Live CD'ere hed forskellige værktøjer alt efter hvilken opgave man ønsker at løse med CD'en. Denne artikel beskriver hvordan du laver en Windows Live CD, der ikke bare indeholder selve Windows (XP, 2000 eller 2003) men også forskellige værktøjer, f.eks. antivirus scanner, anti spyware programmer og administrations værktøjer, der kan bruges til meget forskelligt nyttigt og også unyttigt hvis de er i de forkerte hænder. Mere herom senere.
Der vis sikkert være flere der kender det gode værktøj fra Winternal, der hedder ERD commander. Dette værktøj er rigtig godt, men dels koster det en del, og endeligt har det heller ikke den nødvendige tredjeparts plugin support

Værktøjet vil skal bruge er Bart's PE Builder, og det giver bl.a. følgende muligheder for funktionalitet i vores live CD:

- Anti-Spyware tools som Ad-Aware Pro SE eller HiJackThis.
- MSConfig så du kan ændre hvilke programmer der starter ved login.
- Mulighed for at skrive til og læse fra NTFS og FAT partitioner.
- Mulighed for at rette I registreringsdatabasen lokalt på maskinen.
- Mulighed for at kopiere filer fra en syg maskine til andre drev over netværk.
- Access ti USB drev.
- brug af MMC og Disk Manager så du kan arbejde med partitionerede drev .
- Ændring af lokale passwords.
- Defragmentering af diske uden af boote disse. Dette giver et bedre resultat da ingen filer.
- Mulighed for brug af SSH, Remote Desktop Client eller VNC så man f.eks. kan bruge Live CD'en som arbejdsstation eller tilgå ressourcer sikkert.
- genskabe slettede eller skjult data fra slack space og dermed anvende Live CD'en I forensic øjemed.
- Gennemfører wiping af diske (bit for bit) og dermed slette data med en højere grad af sikkerhed ofr at det ikke kan genskabes.
- Read event logs off the hard drive.
- tilbagefører efter Syskey og hente hashede passwords så de senere kan crackes.

 bruge Internet Explorer eller Firefox fra Live CD'en så du kan surfe og hente ting fra nettet.
 Kører forskellige security tools og dermed f.eks. scanne netværk og maskiner, også andre maskiner end den der bootes på..
 Lave totalt låste web terminaler til gæster og besøgende. Da en live CD er et read only media, er der få eller ingen muligheder for at ændre eller ødelægge maskinen. Vi bestemmer funktionaliteten og alt kan genskabes med en reboot.
 Og meget meget mere, se links herunder

Som du kan se af ovenstående, er der mulighed for at lave Boot CD'ere med mange forskellige formål. Et formål, som jeg vil bruge som eksempel, er en Boot CD, der indeholder værktøjer til at fjerne spyware fra en inficeret maskine med.
Den farligeste del af den spyware der florerer kan være rigtig sejlivet, og næsten umuligt at komme af med, hvis man arbejder med 'Windows boot'et fra harddisken. Noget af denne type spyware, vil oven i købet geninstallerer sig selv slige så hurtigt som du kan slette filer og registry keys. Noget at spywaret, kan du fjerne ved at kører værktøjerne fra fejlsikker tilstand, men det mest sejlivede forsvinder ikke en gang her.
Ved at boote fra en Live CD og ved at køre værktøjerne herfra, kan du fjerne alt den spyware der er derude i øjeblikket, og jeg ha svært ved at forestille mig, hvordan man skulle kunne lave skidt der ikke kan fjernes helt på denne måde.

Lad os gå i gang med forberedelserne

Først er vi selvfølgelig nødt til at hente Bart's PE builder, dette kan du gøre fra dette link:

http://www.nu2.nu/pebuilder/

I øjeblikket (pr. 12 januar 2006) hedder versionen 3.1.9. Det letteste er at downloade en selvudpakkende exe fil og lade den udpakke til default placering (C:\pebuilder319).

Herefter skal du kopiere setup filerne fra din Windows SP med SP2 til din harddisk. Hvis du ikke allerede har en Windows XP med SP2 slipstreamet ind, så kopiere du bare den CD du har og bruger Source->Slipsteam menu optionen i PE Builder, så vil den Live CD du laver være med SP2.

Jeg har her valgt at kopiere mine XP filer til c:\xpCD\ og det vil være den sti jeg anvender I resten af eksemplet.

Hvis du har kikket grundigt på ovenstående link til Bart's PE Builder, hard u allerede opdaget af der allerede er inkorporeret en masse nyttig funktionalitet I form af plugins. I dette tilfælde downloader vi dog endnu nogle nogle pugins til vores Live CD og disse skal lige downloads så vi har dem klar.

Fra http://oss.netfarm.it/winpe/ skal du hente:

[v1.0.4] Windows XPE plugin der håndterer ChangeLog og
[v1.3] Nu2XPE ShortCuts Converter

Download CAB filerne da ZIP filerne oftest indeholder source kode, der skal kompileres før de kan anvendes.

Fra http://www.paraglidernc.com/6901.html skal du hente

Plugin For Lavasoft Adaware SE Personal
Plugin For RunScanner Registry Redirector

Begge disse plugins kommer ned som CAB filer. PE buideren har Ad-Aware indbygget, men pluginnet fra

paraglider er bare bedre. RunScanner pluginnet er nødvendig for at andre plugins kan læse registry fra den lokale disk

Fra http://www.irongeek.com/i.php?page=security/pebuilder skal du hente
HiJackThis og
MSConfig
Begge disse plugins kræver at RunScanner pluginnet er installeret for at virke ordentligt.

Vi skal nu forberede selve bygningen af CD'en

Når du har hentet alt det du ønsker, skal du udpakke dine plugin filer til C:\pebuilder319\plugin\. I dette tilfælde har vi primært hentet CAB filer, som de færreste har udpakkeprogrammer til, det er heller ikke nødvendigt, vi burger I stedet Add optionen når vi vælger plugins I PE builder.
Ofte vil du finde en html fil, når du udpakker plugins, der fortæller hvordan den installeres, hvilke filer der skal kopiere fra din pc (hvis dette er nødvendigt og det er det ofte), hvorfra ting skal downloades og hvor ting skal placeres for at virke.

Du skal installerer Paraglider's Ad-Aware SE Pro og for at få fat I de nødvendige filer er du nødt til at installerer Ad-Aware på din maskine og kopiere filerne fra "c:\Programmer\Lavasoft\Ad-Aware SE Plus\" (eller der hvor du har installeret den) til "Files" mappen som du finder i Ad-Aware plugin's mappen.
HiJackThis plugin kræver at du downloader HiJackThis executable (exe filen) fra http://www.spychecker.com/program/hijackthis.html eller anden placering på nettet og ligger den I HiJackThis plugin's mappen.

Vi er nu færdige med at downloade, kopiere og udpakke og kan starte PE builderen ved at dobbeltklikke C:\pebuilder313\pebuilder.exe. Vælg stien til Win XP source filer(c:\xpCD.

klik "Plugins" knappen og add alle de plugins der kom ned som CAB filer. Du skal også enable de plugins du ønsker at installerer, I hvert tilfælde alle den du downloatede før. Du er også nødt til at disable nogle plugins for at XPE kan virke ordentligt. Disse er:

- nu2Shell
- PE Loader
- PENETCFG: Automatically start PE Network configurator
- PENETCFG: PE Network configurator (theTruth)
- Profiles folder

Du vil sansyneligvis have to Ad-Aware plugins. Den der angives som "Ad-Aware SE Pro" skjal du bruge den anden der f.eks. kunne hedde "Ad-Aware SE" SKAL disables. Når dette er gjort kan du klikke "Close" knappen.

Så skal vi konfigurere

Før vi fortsætter skal enkelte ting tilrettes. Dette kan ved første øjekast godt se lidt langhåret ud, men fortvivl ikke, det er i virkeligheden relativt enkelt. Åben c:\pebuilder319\plugin\xpe-1.0.4mappen og rename "z_xpe-custom.inf.sample" til "z_xpe-custom.inf".

Åben z_xpe-custom.inf med Notepad eller en anden teksteditor hvis du hellere vil det. Du skal nu ændre i z_xpe-custom.inf for at tilrette mange af de options XPE giver mulighed for at ændre. Her er nogle muligheder:

Vi kan starte med at ændre startup navnet:

[SetValue]

"txtsetup.sif","SetupData","loaderprompt","""Starting Windows XPE [The Horse Power]..."""

Ændres til:

[SetValue]
"txtsetup.sif","SetupData","loaderprompt","""Live XP AntispywareCD..."""

Herefter kunne vi f.eks. ændre IE's startup side:

; IE Start Page
0x1,"Software\Microsoft\Internet Explorer\Main","Start Page","about:blank"
0x1,"Software\Microsoft\Internet Explorer\Main","Default_Page_URL","about:blank"

ændre "about:blank" til f.eks. www.eksperten.d.

Vi ønsker selvfølgelig også at kunne starte You will want to add some shortcuts to start menuen og til skrivebordet. Find nedestående linie:

; XPEinit startup menu & desktop

Og indsæt nedenstående lige under denne linie (det er vigtigt at linieskiftene er som linierne er her og mellemrummene også):

0x2,"Sherpya\XPEinit\Programs","Anti-Spyware\Run Adaware on C","%SystemDrive%\programs\adaware\Ad-AwareScan.cmd||%SystemDrive%\Programs\adaware\Ad-Aware.exe,0"

0x2,"Sherpya\XPEinit\Desktop","Run Adaware on C","%SystemDrive%\programs\adaware\Ad-AwareScan.cmd||%SystemDrive%\Programs\adaware\Ad-Aware.exe,0"

Til sidst skal du vælge hvor taskBaren skal vises. Dette gøres i bunden af z_xpe-custom.inf filen. Jeg har vlagt at udkommenterer nedenstående linier:

Fra dette
; TaskBar on Top - Autohide
0x3,"Software\Microsoft\Windows\CurrentVersion\Explorer\StuckRects2","Settings",\
  28,00,00,00,ff,ff,ff,ff,03,00,00,00,01,00,00,00,3c,00,00,00,1e,00,00,00,fe,\
  ff,ff,ff,fe,ff,ff,ff,02,04,00,00,1c,00,00,00

til dette, hvor jeg udkommenterer med semikolloner:

; TaskBar on Top - Autohide
;0x3,"Software\Microsoft\Windows\CurrentVersion\Explorer\StuckRects2","Settings",\
; 28,00,00,00,ff,ff,ff,ff,03,00,00,00,01,00,00,00,3c,00,00,00,1e,00,00,00,fe,\
; ff,ff,ff,fe,ff,ff,ff,02,04,00,00,1c,00,00,00

Og fra dette:

; TaskBar on Bottom - No Autohide
;0x3,"Software\Microsoft\Windows\CurrentVersion\Explorer\StuckRects2","Settings",\

```
;  28,00,00,00,ff,ff,ff,ff,02,00,00,00,03,00,00,00,3f,00,00,00,1e,00,00,00,fe,\
;  ff,ff,ff,e4,02,00,00,02,04,00,00,02,03,00,00
```

til dette, hvor jeg fjerner udkommenteringer:

```
; TaskBar on Bottom - No Autohide
0x3,"Software\Microsoft\Windows\CurrentVersion\Explorer\StuckRects2","Settings",\
  28,00,00,00,ff,ff,ff,ff,02,00,00,00,03,00,00,00,3f,00,00,00,1e,00,00,00,fe,\
  ff,ff,ff,e4,02,00,00,02,04,00,00,02,03,00,00
```

Brænding af CD'en

Når du er færdig med at sætte PE Builder op og fifle med filer, så skal du til at lave en ISO fil der kan brændes ud på en CD. Dette kan du gøre med PE builder ved at afkrydse "Burn to CD" checkboxen og derefter vælge din brænder. Du kan også bruge Nero og for den sags skyld de fleste andre brænderprogrammer på marked.
Det vil være en rigtig god ide at bruge en CD-RW. Dels kan du lave det hele om, hvis du laver småfejl her første gang, og dels kan du senere opdaterer diskene, hvis der kommer nye service packs, updates, patches eller plugins, eller hvis du ønsker at indføje nye plugins for at få mere funktionalitet.
I PE Builder afkrydses "Create ISO image" checkboxen, hvorefter du klikker "Build" knappen, svare "Yes" og "I agree" ved de to pupup vinduer. Herefter

Sådan burger du CD'en

Det er let. Placer din live CD i dit drev (her har du selvfølgelig sørget for at din maskine booter fra CD drevet) og tænd for strømmen, så sker resten af sig selv. Du bør selvfølgelig teste din Live CD med alle de funktionaliteter du har inkorporeret i den.

Licenser

Her skal jeg straks indrømme at jeg ikke er jurist, og derfor ikke kan være 100% sikker, men sådan som jeg læser licensafsnittet på Bart'CD hjemme side og sådan som jeg tolker de svar jeg har fået hos både Microsoft Danmark og de jurister jeg har adgang til, så hører den licens du bruger ikke til det der er på CD'en, men til det der er på maskinen. Dette betyder formelt at du kun må boote din Windows Live CD på en maskine med et windows styresystem. Du bør dog hele tiden holde øje med windows licensbestemmelser, da de jo sagtens kan ændre sig. Som en medarbejder hos MS i danmerk sagde "Hvis der havde været helt generelle problemer med disse teknikker, så havde MS fået Bart's sider lukket"

Dødningehoved og korslagte knogler

Her har jeg valgt at lave en spyware Live CD, men jeg kunne lige så godt have lavet en penetrations test CD eller en forensic CD og dermed kan en sådan Live CD også bruges til grimme ting. Hvis en hacker har fysisk adgang til dine maskiner, vil han med en Live CD kunne gøre grimme ting. Disse muligheder har længe eksisteret med forskellige Linux Live CD'ere, nu kan alle der kan bruge en Windows maskine gøre det samme. Se nogle af de mange muligheder herunder.

Sådan sikre du dig
Hvis du er blevet lidt skræmt af de muligheder jeg her lister, så er det forståeligt, men fortvivl ikke, der er faktisk muligheder.

Først og fremmest skal du have styr på dine stik. Sørg for at der ikke er ledige stik rund om i lokaler hvor folk kan tilkoble sig og side i ro og fred og arbejde, uden at du ved at de er på. Alle ledige stik skal patches ud af dit net og først tilsluttet når du positivt ved hvem der skal bruge dem og til hvad, dette gælder i

principippet alle ledige stik.

Herefter bør alle offentlige computere, dvs computere der er opstillet til gæster og andet have CD drevene afmonteret. Skal en gæst bruge et CD drev, kan man udlåne et løst USB drev efter at man har kontrolleret hvad der skal læses fra dette drev.

Sørg for at bootsekvenserne er sat sådan, at maskinerne ikke kan boote fra CD drevene og beskyt denne indstilling med bios password. Hvis du har gjort dette, vil en Live CD ikke være til nytte.

Ovenstående ganske enkle råd vil faktisk kunne fjerne truslen fra disse værktøjer og de er alle ganske gratis, lige som CD'en

Andre brugbare plugins:

Der findes andre og flere plugins end den jeg her har brugt, herunder filder du flrskellige lister og hjemmesider, der har plugins, kik forbi en gang imellem, der kommer hele tiden nye.

Angry-IP-Scanner, Netstumbler, AirSnare, Norton-Prescan, XoftSpy, Tauscan-1.7, Grisoft-AVG-7.0-Antivirus, diverse wireless drivere og mange flere.
http://www.drowaelder.de/winpe/PEIndex.htm
Her er mulighed for både anti virus/spyware, Wireless penetration testing og mere.

Spybot Search and destroy, AVG6, Avast!, Kaspersky AntiVirus Personal 5.0.156, Eraser og meget meget mere
http://www.bootcd.us/BartPE_Plugins_Repository.php
EN utrolig velordnet og komplet samling plugins til mange forskelige formål.

Firefox-2.3 and Firefoxflash-1.2
http://oss.netfarm.it/winpe/
Fuld firefox browsing support på din Live CD

HWPnP
http://www.paraglidernc.com/6901.html
Normalt vil en Live CD kun kikke efter hardware under startup, hvorfor USb diveces ikke virker. Med HWPnP kan du også bruge USB

SAMInside v 2.5.2. og PasswordsPro v2.0.0.0,
http://www.insidepro.com/eng/index.shtml
ER det passwords der skal hentes/crackes så er dette stedet. Sammen med programmer L0phtCrack og Rainbow Crack er alle Windows maskiner nu frit tilgængelige

Keyfinder-PE og Network Security Scanner 6.0
http://www.drowaelder.de/winpe/PEIndex.htm
Registreringsnøgler og sikkerhedsanalyse og meget mere.

Registry Editor PE v0.9c
http://regeditpe.sourceforge.net/
Mange antospyware programmer kan håndterer registry entryes, men nogle gange har man brug for manuel editering. Her er muligheden for dette

Sam Spade og RemoteAnything
http://www.gonetiq.com/winpe
Sam Spade er en samling som alle spamfighters skal kende. Nu også på Live CD

Windows Password Renew 1.1 BETA og Win003 Optimize Tool
http://www.sala.pri.ee
Password Renew kan ændre password på den locale administrator og lave nye konti med admin rettigheder. Nyttigt og farligt I de forkerte hænder. Optimering af Windows 2003

Andre ressourcer findes her:

911 Rescue CD Forums,
http://www.911cd.net/forums/

Adrian's PE Builder Website:
http://www.irongeek.com/i.php?page=security/pebuilder

Bart's PE Builder Homepage:
http://www.nu2.nu/pebuilder/

Sherpya's XPE og plugin samling:
http://oss.netfarm.it/winpe/

PE Builder plugins:
http://www.bootcd.us

Step by step tutorial om PE Builder og XPE:
http://xpe.collewijn.info/index.php

Kommentar af cyberfinn d. 24. Jan 2006 | 1

En kvalitets artiker fra bufferzone..(Som altid)

Kommentar af steen_hansen d. 24. Jan 2006 | 2

Som altid veldokumenteret, gennemtestet og uhyre grundig. Flot, og 11 på en skala fra 1-10 :o)

Kommentar af radion d. 30. Jan 2006 | 3

Glimrende fin artikel :) skal jeg da til at lege med...

boxer, ziox: En af de største forcer som administrator / alm sikkerhedsinteresseret er da at vide hvilke ting der kan bruges til at stresse / ødelægge / cracke dit system.
Ellers ved du jo heller ikke hvordan du skal beskytte dig mod det..
Alle de foredrag / seminarer jeg har været på med sikkerhed som hovedemne, beskæftiger sig ca. halvdelen af tiden med at fortælle om hvordan man cracker systemer, hvilke værktøjer der er hotte osv osv... man skal have kendskab til tingene inden man kan forebygge dem.

Kommentar af amikk d. 24. Jan 2006 | 4

Genialt

Kommentar af john_stigers (nedlagt brugerprofil) d. 03. Feb 2006 | 5

Tjah... yderst brugbart ;)

Kommentar af tofferman d. 27. Jan 2006 | 6

Som sædvanlig en gang totalt gennemarbejdet kvalitetsarbejde ;)

Kommentar af ronni112 d. 26. Jan 2006 | 7

God artikel!

Kommentar af falster d. 06. Feb 2006 | 8

To spørgsmål er "der ikke bare indeholder selve Windows (XP, 2000 eller 2003)" korrekt f.s.v. angår 2000?. Skal det ikke være med XP eller 2003?

"Normal" slip streaming af SP 2 skulle ikke virke med OEM XP-CD'er. Virker det med Barts?

"Citat "This type of CD's will usually be from larger OEM suppliers (like Dell, HP, or others). You cannot use this type of CD to create a slipstreamed SP2 install"

Kommentar af plazm d. 25. Jan 2006 | 9

Fin artikkel, og til jer andre som har noget imod at oplyse om mulighederne med at lave administrator kontoer og lign. Hvad er problemet? Tror I ikke at folk der vil det, kunne finde det andre steder på nettet? Han oplyser jer faktisk bare om, hvor nemt det kan gøres. Deres findes endda CD'er som er baseret på linux, kun med det formål at nedbryde windows installationer.

Kommentar af dilling-hansen d. 28. Feb 2006 | 10

http://www.irongeek.com/i.php?page=security/pebuildertutorial

ligner en del ;)
Men god alligevel, er selv igang nu :P

Kommentar af forevernewbie d. 25. Jan 2006 | 11

Rigtigt godt.

Kommentar af fedora d. 31. Dec 2007 | 12

God artikel. Har før hørt om Live Windows XP, synes ikke rigtig at jeg har kunne finde noget, og jeg synes du kommer godt omkring dette. Thumbs up.

Kommentar af boxer d. 08. Apr 2006 | 13

Kommentar af psycosoft-funware d. 25. Mar 2006 | 14

utrolig god artikel, flot arbejde!!! :D

/FunteX! :-)

Kommentar af ziox d. 25. Jan 2006 | 15

Den er god! Men som Boxer siger "Jeg er ikke i tvivl om at denne artikel vil blive brugt uhensigtsmæssigt." Har han helt ret i, men det kunne dog godt undværes at vide de ting med at cracke/hacke.

Kommentar af snooby d. 08. May 2006 | 16

Rigtig god artikkel, vil hjem og prøve at lave sådan en cd :)

Kommentar af st3ff d. 19. Feb 2006 | 17

Evt lidt mere forklarende til n00bs som gerne vil prøve dette... som mig(:

Kommentar af mascote d. 10. Aug 2006 | 18

Hmm synes den er god nok men kan du ikke gøre sådan at når man skal dl den her http://www.nu2.nu/pebuilder/ lav den som et link/url så man bare klikker på den og man dl den