Lägg dina svar från samtliga uppgifter i hemuppgiften i en mapp, komprimera mappen och lämna in den packade filen.

Table of Contents

1 Open source forensics

Vi ska i denna hemuppgift bekanta oss med gratisprogramvaror av hög kvalite för forensiska utredningar. De flesta av lösningarna är operativsystemsoberoende. Uppgifterna är enkla och skall mest ge ökad förståelse och träning i fria verktyg.

Ditt jobb är som bekant att utreda och analysera digitala kriminaltekniska bevis. Bevisningen är i detta fall en spegelavbild av en hårddisk.

Innan du börjar med uppgiften det är nyttigt att läsa polisanmälan m.m. för att få del bakgrundsinformation (precis som i alla andra undersökningar). Nu är bakgrundsinformationen i detta fall inte så omfattande utan all information är beskrivet i nedanstående scenario.

1.1 Scenario

De datasäkerhetsansvariga på ett företag har relativt starka misstankar om att en anställd dataanvändare sysslat med otillåtna aktiviteter på jobbet enligt följande lista:

1. Sniffat datatrafik på företagets nätverk
2. Installerat bakdörrar på sin egen PC
3. Stulit och kopierat en CD-ROM med konfidentiellt innehåll
4. Laddat ner copyright skyddad musik
5. Använt ett pen-test tutorial dokument för att utföra en del av sina aktiviteter

När de datasäkerhetsansvariga beslagtog användarens PC var den avslagen och saknade den bootbara systemdisken. De tog dock en dd kopia på den hårddisk som satt kvar i datorn och sände den till dig för analys och utredning.

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

Du hittar spegelkopian här (7zip file): http://users.du.se/~hjo/cs/dt1035/lab/hdb1.7z
MD5 för spegelkopian är: 988654A1C7CC5AA5FB2FBBCA8A34504D

1.2 Rapportering

Försök att hitta så många bevis som möjligt av varje misstänkt aktivitet. Ge en beskrivning av de verktyg och den analys/process du använde för att finna dina bevis. Tänk på att bevisen kan vara maskerade på en rad olika sätt. Sammanställ de hittade bevisen enligt listan i scenariot.

1.3 Förutsättningar och referenser

En förutsättning för denna hemuppgift är att enbart jobba med forensiska open source, gratis eller demo verktyg som FTK imager, The Sleuth Kit och Autopsy Browser, Pyflag och PTK (båda har The Sleuth Kit i botten), ProDiscover Basic Edition, ASR Data SMART, OSForensics - http://www.osforensics.com mm. Sök på produkternas namn så hittar du senaste versionen.

En av de ledande tillverkarna av forensisk programvara i Europa, X-Ways Software har ett verktyg, WinHex som även finns i en forensic edition med ungefär samma funktionalitet, då vid namn X-Ways Forensics - http://www.x-ways.net/. På [server]\tools\x-ways.net-winhex finns guider för hur man kommer igång med detta verktyg. Tex.' X-Ways Forensics' Video Clips The beginners playground to using X-Ways Forensics: http://xwaysclips.blogspot.se/.

Andra systemverktyg som tex. montering av dd/raw till diskenhet med FTK Imager, Mount Image Pro/Paraben P2 eXplorer i kombination med specifika Perl/Python script, antivirusprogram etc. osv. kan även vara aktuella att använda.

Kolla tex. på YouTube efter beskrivande videor i hur man använder dessa verktyg, det finns guider tex. för avancerad användning av WinHex.

1.3.1 VMware

En bra VMware image som SANS (http://www.sans.org/) använder under sina forensiska kurser har lagts upp på [server]\vmware\SIFT Workstation 2.14. Fullständiga namnet är SANS Investigative Forensic Toolkit (SIFT) Workstation och innehåller många forensiska verktyg, bl.a. PTK (http://ptk.dflabs.com/). Se readme.txt på [server] eller: http://computer-forensics.sans.org/community/downloads för login och användning etc. och bloggen nedan.

SIFT Workstation kanske är det bästa alternativet för din undersökning?!

Bli gärna medlem hos SANS de har mycket läsvärt och användbart inom säkerhet och forensics speciellt på deras forensiska blogg: http://computer-forensics.sans.org/blog/

1.3.2 Slutord

Se till att gå igenom manualerna för mjukvarorna ordentligt så du förstår hur du ska använda dem effektivt.

Lycka till!

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE
Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

2 Lösenordsåterställning

Vi skall i denna hemuppgift återställa lösenord med gratisprogramvaror av hög kvalite. De flesta lösningarna är operativsystemsoberoende. Uppgifterna är enkla och skall mest ge ökad förståelse och träning i fria verktyg.

Redovisning:
Besvara frågorna i uppgifterna och redovisa dina resultat i en liten rapport.

2.1 Referenser

Exempel på några verktyg eller resurser vi kan använda för lösenordsåterställning är:

- Cain, http://www.oxid.it/cain.html - kan göra det mesta, hanterar även rainbow tables!
- fgdump, http://www.foofus.net/fizzgig/fgdump/ - dumpar NT hashar och användarkonton.
- Jack The Ripper, http://www.openwall.com/john/ - snabb, kompetent och multi-plattform, Foundstone http://www.foundstone.com/us/resources-overview.asp har ett fritt GUI till John som heter FSCrack.
- ophcrack, http://ophcrack.sourceforge.net/ - kanske snabbaste CPU baserade lösenordscrackern, använder något som kallas ”rainbow tables”, se mer: http://www.rainbowtables.net/ (kika på tutorials delen som visar användning av Cain) och http://project-rainbowcrack.com/
- Eller verktyg fritt valda av er själv, speciellt om du har andra operativsystem än Windows. http://sectools.org/ har topplistor.
- Anti-Hacker Tool Kit, Third Edition har ett fritt kapitel 8 om password cracking. http://users.du.se/~hjo/cs/common/books/
- De sista åren har det dykt upp GPU (grafikprocessor) baserade lösningar som är mycket snabba på att knäcka lösenordshashar. Se t.ex. IGHASHGPU http://golubev.com/ som bl.a. klarar NT hashar. **GPUn är ca: 100-1000 ggr. snabbare än CPUn beroende på GPUns prestanda!**
- Hashcat/oclhashcat: http://hashcat.net/oclhashcat/ med GUI i Windows http://www.md5decrypter.co.uk/hashcat-gui.aspx
- Det absolut senaste är att använda OpenCL kompatibel hårdvara i distribuerade lösningar för att knäcka lösenord. Ett exempel är mjukvaran Virtual OpenCL: http://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/

2.2 Exempel på tillvägagångssätt och förklaringar

Dumpa ut användarkonton och lösenordshashar från en Windows dator med fgdump. Ladda in dem i en lämplig passwordcracker som ni valt själv (obs! detta moment behövs ej om Cain är installerat på datorn). Man måste vara administratör för att kunna dumpa användaruppgifter ur SAM-delen i registret.
Installera och starta Cain, gå till fliken Cracker och högerklicka, välj ”Add to list” för att addera NT Hashes from text file (filer från verktyg som fgdump) eller Import Hashes from local system. När vi importerat användaruppgifterna så ska de synas i listan.

Utför en ”brute force” attack genom att högerklicka på ett användarkonto. Obs! Vilken metod du bör välja beror på versionen av Windows och ditt lösenords längd. Laborera med olika val

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE
Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

på lösenordslängden och ”keyspace”. En fil med beräkningsformel (keyspace_password.xls) ligger i lab mappen som du även kan använda för dessa beräkningar.

Har du ett grafikkort som stödjer något av beräknings-API:erna Cuda (Nvidia) eller OpenCL (AMD/Nvidia) så använd gärna det tillsammans med IGHASHGPU eller oclHashcat-*. Ofta har vanliga CPUn numera stöd för OpenCL också. För att det ska fungera måste du ha en Cuda/OpenCL kompatibel drivrutin vilket oftast bundlas med grafikkortdrivrutinen.

Russian Password Crackers har en hel del information om olika attacker mot svagheter i kryptosystem och lösenordsåterställning: http://www.password-crackers.com/

Frågor:

a) Välj en passande lösenordslängd och ”keyspace” för ditt nuvarande lösenord i gränssnittet (modifiera standard inställningen efter hur långt lösenord du har). Hur lång tid tar det som längst att cracka ditt lösenord med ”brute force” (du behöver inte vänta, programmet talar om worst case tiden om Cain används)?

b) Förklara begreppen SAM, LM hash, LM hash + challenge, NTLM hash, NTLM hash + challenge och NTLM session security hash?

c) Utför en dictionary attack, se hjälp http://www.rainbowtables.net/tutorials/dictionary.php
Några fria dictionaries/wordlists finns här: http://www.apasscracker.com/dictionaries/, http://www.openwall.com/mirrors/, ftp://ftp.ox.ac.uk/pub/wordlists/ eller sök med Google.
Cain har även en liten wordlist med i cain\wordlists mappen.
Hur lång tid tar det att cracka ditt lösenord nu (du måste ha bytt ditt lösenord till ett lösenord som är med i dictionariet/wordlisten eller lagt till ett nytt lösenord i wordlisten)?

d) Vilken lösenordslängd och ”keyspace” skulle du rekommendera som säkert i t.ex. Windows, motivera ditt svar?

e) Testa Ophcrack eller Cain med rainbow tables och jämför mot ”brute force”. Vilket resultat får du?
I Cain kan man t.ex. bygga sin egen rainbow table med programmet Winrtgen som medföljer, se: http://oxid.netsons.org/phpBB2/viewtopic.php?t=911. Även http://project-rainbowcrack.com/ har en mycket bra dokumentation hur man går tillväga för att bygga sin egen rainbow table.
Något man får vara beredd på är att detta kan ta mycket mycket lång tid och kräver många GB med plats, speciellt för långa lösenord och lösenord med möjlighet till många olika tecken (charset).

Det ligger därför några enklare färdiga rainbowtables på [server]:\rainbowtables\lm-nt. Läs dokumentationen i LSO-RainbowCrack.pdf för hur du kan använda dessa tabeller ifrån t.ex. Cain eller rainbowcrack.

f) Försök dig nu på att enkelt/kortfattat förklara begreppet rainbow tables med några meningar och vad är det som gör rainbow tables så snabbt?

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE
Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

3 File carving och säker lagring med TrueCrypt

Vi skall i denna hemuppgift kryptera/dekryptera en systemdisk, volym eller fil samt prova på lite file carving med gratisprogramvaror av hög kvalite. De flesta lösningarna är operativsystemsoberoende. Uppgifterna är enkla och skall mest ge ökad förståelse och träning i fria verktyg.

Redovisning:
Ta en skärmdump på en monterad enhet och TrueCrypt dialogruta ifrån din dator. Besvara frågorna nedan och redovisa dina resultat i en liten rapport.

3.1 Carving

Vi skall använda några fria carving verktyg i denna hemuppgift. Se en lista på några fil karvningverktyg och deras prestanda i examensarbetet ”Measuring and Improving the Quality of File Carving Methods.pdf ” under [server]\forensics\docs\Examensarbeten. Rapporten finns även på nätet om ni söker på filnamnet, t.ex. här:
http://www.forensicswiki.org/wiki/File_Carving_Bibliography.

Förbered ett USB minne eller annat minne/partition av mindre storlek (det är bra om det är så litet som möjligt för att snabba upp momenten nedan).

a) Börja med att lägga lite olika filer, t.ex. jpg, gif, etc. (sådan media ditt valda file carving verktyg stödjer) på din minnesenhet. **Quick formatera** sedan enheten och testa filkarvning med t.ex. PhotoRec http://www.cgsecurity.org/wiki/Main_Page eller annat/flera verktyg. Hittade du något?

b) Formatera nu din minnesenhet ordentligt (ta bort ”Quick Format” check box) och gör om karvningen. Hittade du något?

c) Lägg nu ytterligare på några bilder etc. på din enhet och skriv sedan ”sönder” din enhet med en wipe programvara som t.ex.
Active Killdisk Free - http://www.killdisk.com/ ,
Darik's Boot And Nuke - http://www.dban.org/ ,
dd med ”dd if=/dev/zero of=/dev/usbdisk bs=4096” (detta är ett exempel och är lite olika under Windows) eller liknande verktyg och gör om karvningen. Hittade du något?

3.2 Truecrypt

Med verktyget TrueCrypt kan en enhet/volym som t.ex. en hårddisk (t.om. system/boot disken), en partition eller innehållet i en fil skyddas via kryptering ”on-the-fly” på ett säkert och väldigt smidigt sätt. Se referenser nedan för dokumentation och hjälp.

a) Kryptera nu din minnesenhet och lägg återigen på blandad media, data etc. och prova om det går att karva ut något från enheten på samma sätt som tidigare? Obs! TrueCrypt enheten ska vara avmonterad när du karvar.

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

b) Sätt dig nu in i begreppet ”plausible deniability” som utvecklarna talar om på TrueCrypts hemsida. Är det enligt dig möjligt för forensiker upptäcka att du använder denna funktion med något verktyg och hur fungerar det egentligen?

c) Den forensiska imagen: http://users.du.se/~hjo/cs/dt1035/lab/tc70a.E01 är en image av en TrueCrypt enhetsvolym ifrån ett flash-minneskort. Din uppgift är att dekryptera enhetsvolymen och tala om vilka filer som finns på den samt enhetsvolymens lösenord. Lösenordet består endast av två tecken och du kan använda dig av Passware Kit Forensic Demo för att lösa uppgiften. Demot tillåter endast 1 minuts arbete åt gången så du måste konfigurera verktyget korrekt för att lösa uppgiften.

Ett annat mycket bättre alternativ om man har hårdvarusupport (i princip alla datorer idag har stöd för OpenCL via CPU/GPU - http://en.wikipedia.org/wiki/OpenCL) är att använda oclhashcat http://hashcat.net/oclhashcat/ vilket har stöd för flera av TrueCrypts krypteringsalgoritmer.

d) Nämn minst två anledningar till varför det är så svårt att dekryptera TrueCrypt volymer? Några exempel (legal cases) att tänka på och hjälp i uppgiften:
http://en.wikipedia.org/wiki/Truecrypt#Operation_Satyagraha

3.2.1 Referenser

TrueCrypt hemsida - http://www.truecrypt.org/
TrueCrypt wiki - http://en.wikipedia.org/wiki/Truecrypt
Kryptera hårddisken med TrueCrypt (på Svenska men för en äldre version av TrueCrypt) - http://www.wladimir.se/krypto.htm
Security Now! Pod Cast om TrueCrypt - http://www.grc.com/SecurityNow.htm episode #41 och #133
Tekniska detaljer om TrueCrypt volymer: http://www.truecrypt.org/docs/?s=volume-format-specification

3.2.2 Trucrypt forensiska verktyg

TCHunt - Quickly Find Most Encrypted TrueCrypt Volumes - http://16s.us/TCHunt/
Passware Kit Forensic - http://www.lostpassword.com/kit-forensic.htm
hashcat - http://hashcat.net/oclhashcat/

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE
Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/