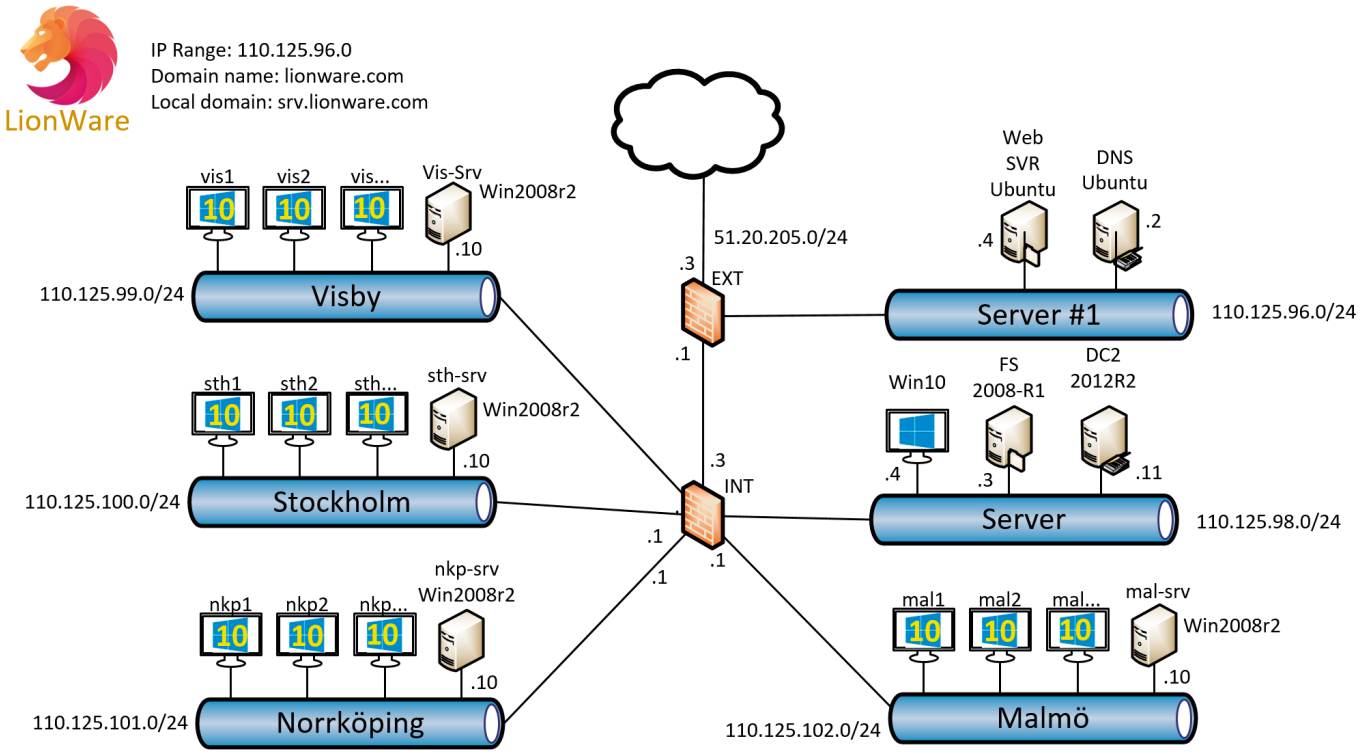
Självstudieuppgift
Behörighetskontroll

Den här självstudieuppgiften är framtagen för att ge dig som arbetar med cybersäkerhet möjlighet att träna på att upptäcka och hantera incidenter. På första sidan finner du det övergripande scenariot med en beskrivning av miljön och av vad som har hänt. På nästa sida hittar du de uppgifter som du på egen hand löser med hjälp av de filer som tillhandahålls. Du hittar också tips som du kan använda om du kör fast, samt förslag på hur uppgifterna kan lösas.

IT-avdelningen på Lionware har upptäckt att någon har lagt till användarkonton i deras domän. De aktuella kontona har dessutom fått höga rättigheter. Ingen på IT-avdelning har lagt till dessa användarkonton och inga säkerhetsmekanismer har slagit larm. Det är oklart vad som har hänt. Lionware:s ledning har valt att klassa händelsen som en incident och har anlitat dig för att utreda vad som har hänt. De vill också att du ger tre rekommendationer för hur de kan undvika liknande incidenter i framtiden.

Lionware har en IT-miljö med ett femtiotal datorer fördelade på fyra verksamhetsorter. Nätverket består av sex segment implementerade med hjälp av två brandväggar, samt en domän (se nedanstående bild). En initial analys av nätverkstrafiken tyder på att datorn nkp1 (110.125.101.110) i Norrköping har varit inblandad i angreppet. Dessutom verkar även nkp-srv samt dc2 vara inblandade. IT-enheten har säkrat ramminnesdumpar från dessa datorer.



Instruktioner

På denna sida beskrivs de frågor som ledningen vill ha svar på i form av deluppgifter. Svaren erhålls genom att ladda ned och analysera de ramminnesdumpar som tillhandahålls i zip-filen https://download.iwlab.foi.se/uppgifter/behorighet.zip (MD5: e80b7186b99b1425c25034a053cda0d4).
På sidorna 3 hittar du tips som syftar till att hjälpa dig hitta svaren på uppgifterna, men inte ger dig hela lösningen. På sidorna 4-5 hittar du lösningsförslag och på sista sidan hittar du svaren på frågorna i uppgifterna

Uppgift 1

Vilka metoder har angriparen använt för att extrahera lösenord och för att förflytta sig mellan datorer i IT-miljön? Skapa om möjligt en tidslinje av angreppet genom att lista vilka datorer och processer som har varit inblandade.

Uppgift 2

Vilka konton har utnyttjats av antagonisten under angreppet? Går det att hitta lösenord eller lösenordshashar till några konton?

Uppgift 3

Vilka tre konton har angriparen skapat i domänen?

Uppgift 4

Vad behöver företaget göra för att återställa säkerheten i sin IT-miljö?

Uppgift 5

Ge tre rekommendationer på säkerhetsåtgärder som företaget kan införa för att undvika liknande incidenter i framtiden.

Återkoppla!

Din återkoppling gör det möjligt för oss att ta fram fler självstudieuppgifter. Så återkoppla gärna genom att besvara formuläret på https://survey.crate.foi.se/index.php/712587

Tips

Ett sätt att lösa uppgifterna är att använda en dator med ett Linuxoperativsystem och programmet Volatility[1] för att bearbeta ramminnesdumparna. Därefter kan kommandon eller verktyg såsom cat, grep och strings användas för att analysera de bearbetade filerna. Första steget är att ladda ner lionware.zip och packa upp filen med kommandot ”unzip lionware_forensics.zip”.

Första tipset är att utforska programmet Volatility och se vilken typ av information som kan läsas ut. En viktig del i uppgiften är att identifiera processer som angriparen kan ha startat. Fundera över vilka processer som kan hjälpa en angripare att ta reda på inloggningsuppgifter och förflytta sig mellan datorer i nätverket.

Efter att intressanta processer har identifieras kan minnesinnehållet för de processerna extraheras med hjälp av Volatility. Detta resulterar i en fil för varje process som kan analyseras var och en för sig. Fundera dels över hur processerna fungerar under huven. Till exempel vilka protokoll, autentiseringsalgoritmer och typer av lösenordshashar som används. Fundera även över vilka kommandon som kan ha körts i de olika processerna.

Filerna som har extraherats med hjälp av Volatility kan innehålla tidsstämplingar för när saker skedde. Sätt ihop en tidslinje som innehåller tidpunkter och händelser. Fundera på hur och när angriparen gjorde vad, samt med vilket verktyg. Försök lista ut vilken känd attack som har använts för att fjärrstyra datorer, vilka datorer som har fjärrstyrts, med vilka inloggningsuppgifter, samt vilka användarkonton som har lagts till.

Tips uppgift 1

Antagonisten har troligtvis använt ett verktyg som extraherar lösenord ut ramminnet och därefter ett verktyg för att ansluta mellan olika datorer. Om antagonisten använt samma verktyg vid flera tillfällen är det bra att anteckna namn och processidentifikationsnummer för att skilja på processerna. Använd vid behov internet för att leta efter vanliga verktyg och därefter Volatility för att extrahera en lista över processer som körts i datorerna. Sök sedan efter verktygen bland de processer som har körts på datorerna.

Tips uppgift 2

För att fjärrstyra nya datorer måste antagonisten först autentisera sig. Utifrån tidslinjen i föregående uppgift är det känt vilket verktyg som använts för att fjärrstyra datorer. Sök igenom ramminnesdumparna för de verktygsprocesserna. Använd eventuella kunskaper om verktyget för att hitta rätt söksträngar. Genom att göra strängsökningar i ramminnesdumparna för de processer som identifierades i uppgift 1 går det att hitta konton, lösenord och lösenordshashar som kan ha utnyttjats under angreppet.

Tips uppgift 3

Angriparen har skapat tre egna domänanvändare med hjälp av ett dos-kommando i ett försök att skapa ett permanent fotfäste i domänen. Lista ut vilket kommando som har använts och se om det går att hitta spår av det i ramminnesdumparna för de processer som identifierades i uppgift 1. Tänk på att det är en Windows Server 2012 när sökningarna efter kommandot görs. Går det att se några tecken på att angripare även har lagt till de nya användarna i några grupper?

Tips uppgift 4

De tidigare uppgifterna har gett den kunskap som behövs för att lösa den här uppgiften. Använd den och bestäm vad som behöver rensas ut från datorerna som har nyttjats i angreppet.

Tips uppgift 5

Vilka verktyg har använts under angreppet och hur kan det säkerställas att dessa inte är möjliga att använda i systemet i framtiden?

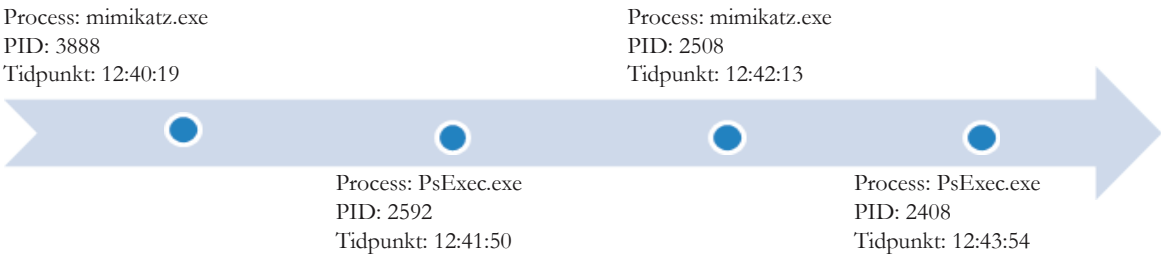
[1] https://github.com/volatilityfoundation/volatility

Lösningsförslag

I det här avsnittet ges förslag på lösningar till uppgifterna. Notera att det finns flera olika sätt, så använd gärna ramminnesdumparna för att se vad som mer kan hittas.

Uppgift 1

Svaret till uppgift 1 finns ramminnesdumparna för nkp1 och nkp-srv. Dumparna analyseras med hjälp av Volatility med vars hjälp till exempel aktiva processer kan visas. I ramminnesdumpen för nkp1 syns att antagonisten använt verktyget Mimikatz[2] följt av två processinstanser av verktyget PsExec. I ramminnesdumpen för nkp-srv finns också en Mimikatzprocess, vilket tyder på att en körning av Mimikatz upprepades på nkp-srv. Med hjälp av denna information kan den tidslinje för angreppet som visas i figur 1 skapas.



Figur 1: Tidslinje angrepp

Genom att söka efter ”psexec” i processminnet för PsExec-processerna syns det att datorerna nkp-srv samt dc2 har fjärrstyrts. Informationen extraheras med följande kommandon:

```
# nkp1
$ volatility imageinfo –f nkp1.nkp.lionware.com.memdump
$ volatility pslist --profile Win10x64_10586 –f nkp1.nkp.lionware.com.memdump
$ volatility memdump –p 2592 --profile Win10x64_10586 –f nkp1.nkp.lionware.com.memdump –dump-dir .
$ strings 2592.dmp | grep psexec
$ volatility memdump –p 2408 --profile Win10x64_10586 –f nkp1.nkp.lionware.com.memdump –dump-dir .
$ strings 2408.dmp | grep psexec

# nkp-srv
$ volatility imageinfo –f nkp-srv.nkp.lionware.com.memdump
$ volatility pslist --profile Win10x64_Win2008R2SP1x64_23418 –f nkp-srv.nkp.lionware.com.memdump
```

Uppgift 2

Svaret på Uppgift 2 finns i processminnet för de två PsExec-processerna. Genom att göra en strängsökning efter ”ntlm” i den första processen kan flera användare, lösenord i klartext samt lösenordshashar identifieras. Mimikatz ”pass-the-hash” kommando har använts för att fjärransluta till datorerna som annan användare och autentiseringen har skett med användarens NTLM-hash. Genom att göra strängsökningar efter ”sekurlsa::pth” avslöjas vilka användare och lösenordshashar som har använts. För att extrahera informationen kan följande kommandon användas:

```
# nkp1
$ strings 2592.dmp | grep –i ntlm –A 3 –B 3
$ strings 2592.dmp | grep sekurlsa
$ strings 2408.dmp | grep sekurlsa
```

[2] https://gitlab.com/kalilinux/packages/mimikatz

Att lösenord lagras i klartext i vissa datorer beror dels på inställningar i operativsystemet och dels på inställningar i domänen. Detta är viktigt att känna till vid konfiguration av system och det påverkar även hur länge en organisation bör tillåta äldre operativsystem i sin domän. Det är också ett exempel på att det ofta är den svagaste länken i kedjan som brister.

Uppgift 3

Svaret på uppgift 3 finns i PsExec-processen från nkp1 till dc2. Angriparen har skapat användarna ”UberAdmin”, ”UberAdm” och ”UberNimda”. Dessa kan hittas genom att söka efter strängen ”dsadd” i PsExec-processens minnesdump (den med processidentifikationsnummer 2408). Notera att även dsmod addmbr har används för att lägga till dessa användare i gruppen Domain Admins, vilket ger dem administrativa rättigheter i hela IT-miljön. För att extrahera informationen kan följande kommandon användas:

```
# nkp1
$ strings 2408.dmp | grep dsadd
$ strings 2408.dmp | grep addmbr
```

Uppgift 4

Baserat på svaren på uppgift 1 till 3 behöver företaget åtminstone göra följande för att återställa säkerheten i sin IT-miljö:

- Ta bort de tre konton som angriparen har skapat
- Byt lösenord på de konton som har använts under angreppet
- Ta bort Mimikatz från de angripna datorerna.

Notera att dessa åtgärder utgör ett minimum av åtgärder som företaget behöver göra. I ett riktigt fall är det svårt att säkerställa att dessa åtgärder är tillräckliga utan en mer omfattande analys av IT-miljön.

Uppgift 5

Det finns många olika säkerhetsåtgärder som helt eller delvis kan skydda mot den typ av angrepp som används i scenariot. Exempel på åtgärder som kan hjälpa är:

- Inför kontroll på hur domänadministratörskonton skapas och används
- Inför regelbunden revision av konton och deras rättigheter
- Följ Microsofts rekommendationer avseende privilegierad åtkomst (ofta kallad Microsoft Privileged Access Management[3])
- Inför detektion av icke-önskvärd mjukvara såsom Mimikatz
- Se över er segmentering. Det bör inte vara möjligt att genomföra administrativa arbetsuppgifter utanför en kontrollerad zon.

Notera att valet av säkerhetsåtgärder och hur de skall konfigureras är beroende av hur företagets IT-miljö är uppbyggd. I detta fall hade det till exempel inte hjälpt med så kallad flerfaktorsautentisering eftersom angreppet missbrukar operativsystemets autentiseringsfunktionalitet.

[3] Microsoft (2022). Privilegierad åtkomst: Strategi. https://docs.microsoft.com/sv-se/security/compass/privileged-access-strategy, hämtad 2022-02-07

Facit

Svar uppgift 1

Vilket program används för att stjäla lösenord?

- Mimikatz

Vilket program används för att fjärransluta till NKP-SRV och DC2?

- PSexec

Vilket kommando används för att skapa användare i domänen?

- Dsadd och dsmod

Svar uppgift 2

Vilka konton har utnyttjats av antagonisten under angreppet? Kan du hitta lösenord eller lösenordshashar till några konton?

- Användarnamn: admhanden
- Lösenord: GulleFjun2013
- NTLM-hash: 2fd0a1e978a52b55205d1a4a218eff22

Svar uppgift 3

Vilka tre konton har angriparen skapat i domänen?

- UberAdmin, UberAdm och UberNimda

Svar uppgift 4

Vad behöver företaget göra för att återställa säkerheten i sin IT-miljö?

- Ta bort de tre konton som angriparen har skapat
- Byt lösenord på de konton som har använts under angreppet
- Ta bort Mimikatz från de drabbade datorerna.

Notera att dessa åtgärder utgör ett minimum av åtgärder som företaget vill göra. I ett riktigt fall är det svårt att säkerställa att dessa åtgärder är tillräckliga utan en mer omfattande analys av IT-miljön.

Svar uppgift 5

Ge tre rekommendationer på säkerhetsåtgärder som företaget kan införa för att undvika liknande incidenter i framtiden.

- Inför kontroll på hur domänadministratörskonton skapas och används
- Inför regelbunden revision av konton och deras rättigheter
- Följ Microsofts rekommendationer avseende privilegierad åtkomst (ofta kallad Microsoft Privileged Access Management[4])
- Inför detektion av icke-önskvärd mjukvara såsom Mimikatz
- Se över er segmentering. Det bör inte vara möjligt att genomföra administrativa arbetsuppgifter utanför en kontrollerad zon.

Notera att dessa bara är exempel på åtgärder som kan hjälpa. Vilka säkerhetsåtgärder som bör införas och hur de skall konfigureras behöver anpassas baserat på företagets IT-miljö.

[4] Microsoft (2022). Privilegierad åtkomst: Strategi. https://docs.microsoft.com/sv-se/security/compass/privileged-access-strategy, hämtad 2022-02-07

Crate – Totalförsvarets cyberanläggning för ett säkrare Sverige

Denna självstudieuppgift är gjord med hjälp av Crate, Sveriges nationella cyberanläggning för totalförsvaret. Crate ökar totalförsvarets förmåga i cyberdomänen genom forskning, utbildning, träning, övning och utvärdering med fokus på samhällsviktig verksamhet och cyberfysiska system. Crate är ett samarbete mellan Försvarsmakten, Myndigheten för samhällsskydd och beredskap samt FOI. Läs mer om cyberanläggningen och dess verksamhet på www.foi.se/crate.

FOI Totalförsvarets forskningsinstitut

FÖRSVARSMAKTEN

MSB Myndigheten för samhällsskydd och beredskap