



To Serve and Protect: Microsoft Advanced Threat Analytics

Dennis Rietveld



SECURITY



Dennis Rietveld

Freelance IT consultant

MCSA, MCSE, MCITP, CCA, VCP

activedirectory.nl

[@R33dfield](https://twitter.com/R33dfield) [#ExpertsLive](https://twitter.com/ExpertsLive)

dennis@rietveld-ict.nl





Agenda

- Wat is Microsoft ATA
 - Introductie
 - Architecture
 - Sizing, Planning & Deployment
- Attack Kill Chain
- Demo
- Mitigation



KIM ZETTER SECURITY 06.15.16 7:00 AM

THOUSANDS OF HACKED GOVERNMENT AND CORPORATE SERVERS SELLING FOR \$6 ON BLACK MARKET



Inverse Path's USB armory is a secure computer squeezed onto a USB device.



By Charlie Osborne for Zero Day | August 10, 2016 -- 10:26 GMT (11:26 BST) | Topic: Security

AtomBombing Code Injection can potentially hack all

Windows OS versions

October 28, 2016 By Pierluigi Paganini

Great Tesco Bank robbery: Hackers steal cash from 20,000 accounts as bosses freeze payments in 'emergency measure' amid fears fraudsters have cracked the codes to make new bank cards at will

- Bank CEO Benny Higgins freezes online transactions after hackers strike
- Under fire boss says 20,000 accounts have cash taken in weekend attack
- One customer says hackers may have created a new debit card in Brazil
- Another victim reported account was hit by £2,000 due to the attack
- Thousands of customers have found their bank cards have been stopped

created "golden keys" which unlock Windows devices
ot. [Updated]



SECURITY

Microsoft ATA



Wat is Microsoft ATA

- On-premise applicatie (nog wel)
- Onderdeel van EMS
- Gedragsanalyse
- Verschillende data bronnen
- Detectie
 - Reconnaissance
 - Compromised credentials
 - Lateral movement
 - Privilege escalation
 - Domain dominance





SECURITY

Reconnaissance

Account enumeration
Net Session verkenning
Verkenning DNS
Verkenning Active Directory (SAM-R)
Afwijkend gedrag toegang resources



Lateral Movement

Pass the ticket
Pass the hash
Over-pass the hash
Afwijkende authenticatie verzoeken
Afwijkend gedrag toegang resources

Domain Dominance

Skeleton key malware
Golden ticket
Remote execution
Malicious replication request

Brute force via NTLM, Kerberos, LDAP
Gevoelige accounts in plain text authentication
Service accounts in plain text authentication
Honey Token account verdacht gedrag
Unusual protocol implementation
Malicious Data Protection Private Info Request
Afwijkend gedrag (aanwezigheid medewerker)

MS14-068 exploit (Forged PAC)
MS11-013 exploit (Silver PAC)



Compromised Credential

Privilege Escalation

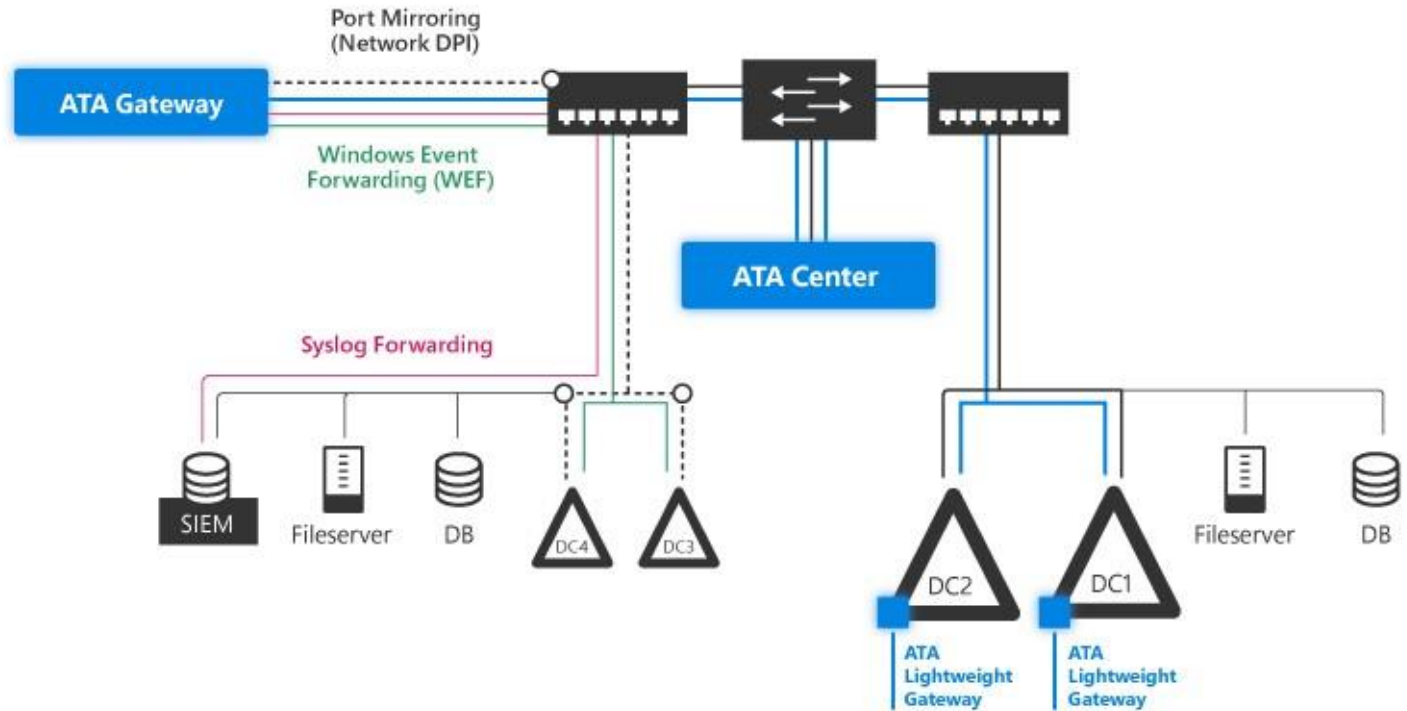


SECURITY

Architecture

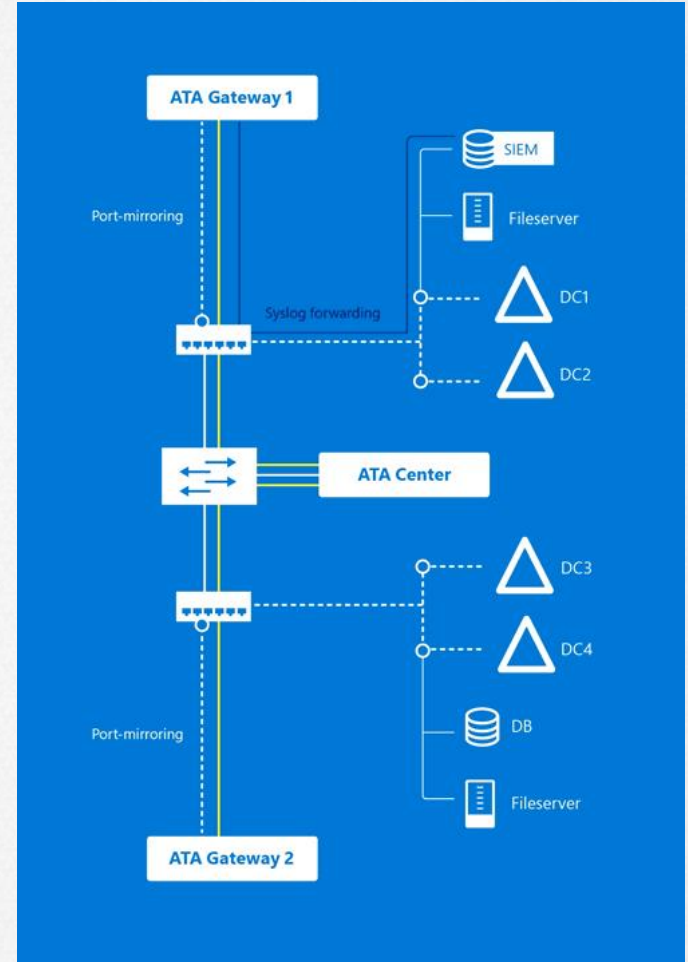


Architecture



Architecture

- ATA Center
- ATA Console
- ATA Gateway
- ATA Lightweight Gateway





SECURITY

Sizing, Planning & Deployment



System requirements

	2008 R2 SP1	2012	2012 R2	2016
ATA Center / Console			X	X
ATA Gateway			X	X
ATA Lightweight Gateway	X	X	X	X

ATA Center / Console	ATA Lightweight Gateway	ATA Gateway
ATA Center Service	ATA Gateway service	ATA Gateway service
.NET Framework 4.6.1	ATA Gateway updater service	ATA Gateway updater service
MongoDB	.NET Framework 4.6.1	.NET Framework 4.6.1
2 IP adressen	Microsoft Visual C++ 2013 redistributable	Microsoft Visual C++ 2013 redistributable
Certificaten	Certificaten	Certificaten
KB2919355	KB2919355	2 netwerk adapters
		KB2919355 en KB3047154



Sizing

- ATA sizing tool
- Baseline Domain Controller

Number of DCs	4				
Number of Samples	69				
Overall Start Time UTC	2016-07-21 10:41:54				
Overall End Time UTC	2016-07-21 10:43:09				
Display DC Times as UTC/Local	Universal Time (UTC)				
Center	Max Packets/sec	Avg Packets/sec	Busy Packets/sec	Busy Packets/sec Start UTC	Busy Packets/sec End UTC
Grand Total	1,616	1,184	1,184	10:41:55	10:43:08
DC	Max Packets/sec	Avg Packets/sec	Busy Packets/sec	Busy Packets/sec Start Time	Busy Packets/sec End Time
DC1	644	457	457	10:41:54	10:43:08
DC3	334	234	234	10:41:54	10:43:08
DC4	408	249	249	10:41:54	10:43:08
DC2	405	244	244	10:41:54	10:43:08
Total	1,792	1,184	1,184		



Sizing tool download: <https://gallery.technet.microsoft.com/Advanced-Threat-Analytics-7371c87f>

Sizing ATA Center

Packets per second *	CPU (cores**)	Memory (GB)	Database storage per dag (GB)	Database storage per maand (GB)	IOPS ***
1.000	2	32	0,3	9	30 (100)
10.000	4	48	3	90	200 (300)
40.000	8	64	12	360	500 (1.000)
100.000	12	96	30	900	1.000 (1.500)
400.000	40	128	120	1.800	2.000 (2.500)

* Totaal dagelijks gemiddelde aantal packets per seconde van alle domain controllers gemonitord door alle ATA Gateways

** Aantal fysieke cores, niet hyper-threaded

*** Gemiddelde (piek)



Sizing Gateway

Packets per second	CPU (cores)*	Memory (GB)
1.000	1	6
5.000	2	10
10.000	3	12
20.000	6	24
50.000	16	48

Sizing Lightweight Gateway

Packets per second	CPU (cores)**	Memory (GB)***
1.000	2	6
5.000	6	16
10.000	10	24

* Hyper-threading moet disabled zijn

** Aantal fysieke cores, niet hyper-threaded

*** Hoeveelheid geïnstalleerd geheugen in domain controller



Planning

- ATA Center Fysiek vs Virtueel
- ATA Center domain joined of workgroup?
- Disaster Recovery
- Gateway of Lightweight Gateway

Gateway	Voordelen	Kosten	Deployment	Domain controller resources
ATA Gateway	Out-of-band oplossing, lastig vindbaar door aanvaller	Hoger	Geplaatst naast domain controller (out-of-band)	Ondersteund tot 50.000 packets/sec
ATA Lightweight Gateway	Geen fysieke of virtuele dedicated server nodig en port mirroring	Lager	Geïnstalleerd op domain controller	Ondersteund tot 10.000 packets/sec



Planning

- Certificates, self signed of CA?
- Update strategie
- SIEM of WEF?
- ATA rol groepen

Groep	Permissies
ATA Admin	Alles
ATA Operator	Schrijf rechten maar kan geen aanpassingen maken aan de ATA configuratie
ATA Viewer	Alleen kijken





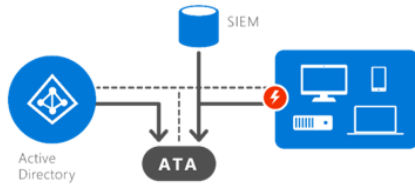
Deployment

- Active Directory forest is boundary
- Default domain user benodigd
- Deployment van ATA (lightweight) Gateway
 - Package download via ATA Center
 - Silent installatie mogelijkheden
- MongoDB



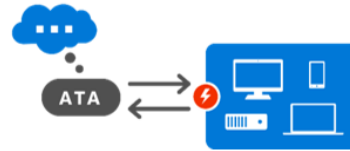
Done!

1 Analyze



Advanced Threat Analytics analyzes all Active Directory-related traffic and collects relevant events from SIEM

2 Learn



Advanced Threat Analytics automatically learns all entities' behaviors

3 Detect



ATA builds the organizational security graph, detects abnormal behavior, protocol attacks, and weaknesses, and then constructs an attack timeline





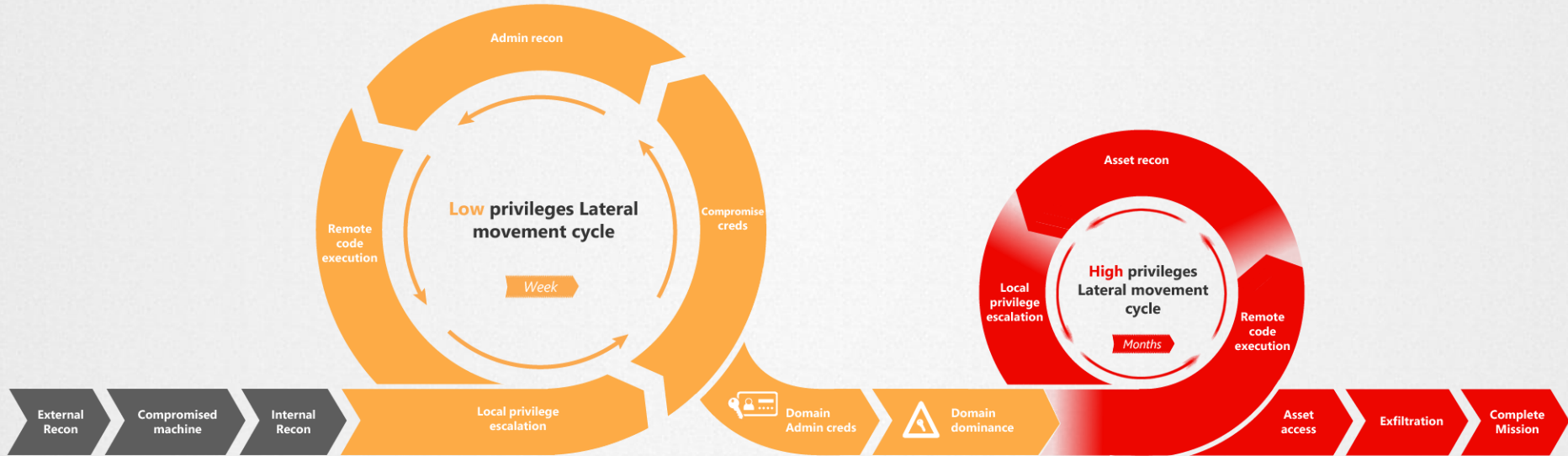
SECURITY

Attack Kill Chain





Attack Kill Chain





SECURITY

Demo





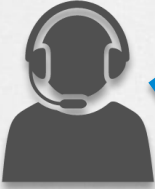
SECURITY

Overview woodgrovebank.com

Phillip



Angela



Elliot

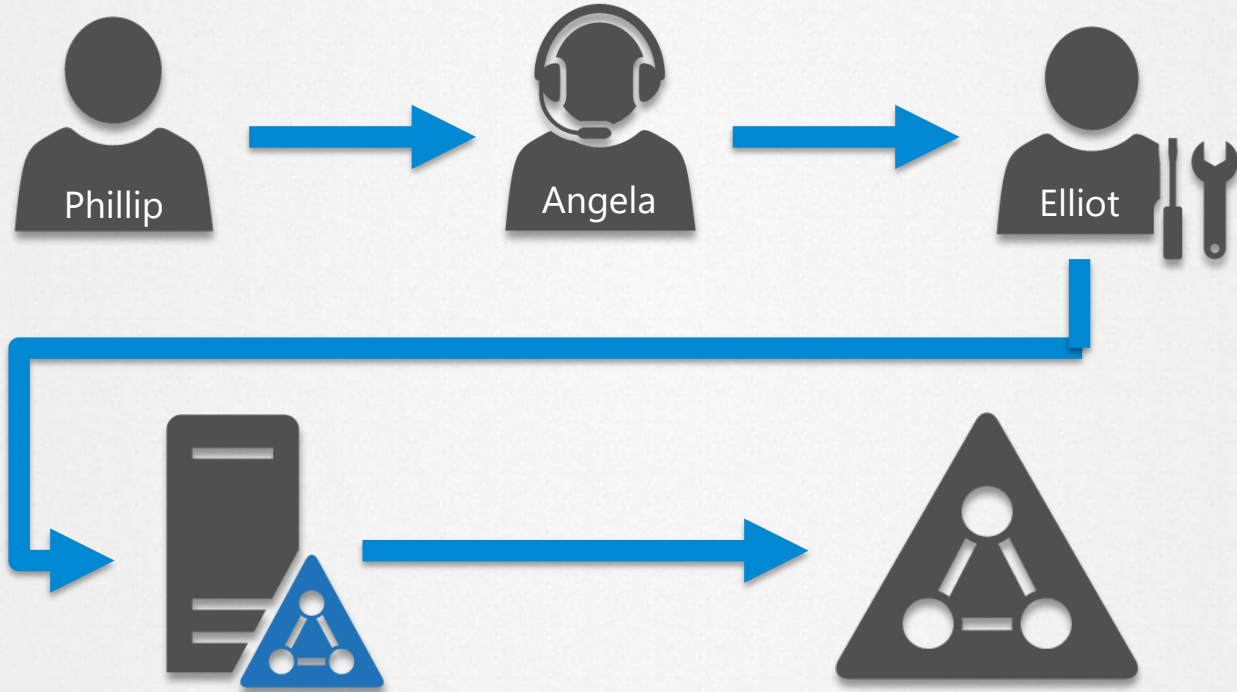


ATA Center





Doel? Domain Dominance





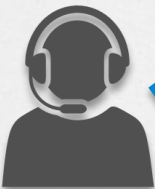
SECURITY

Startpunt

Phillip



Angela



Elliot



ATA Center





Verkenning (reconnaissance)

- Gebruiker en groep informatie (SAM-R)
- SMB sessies (Netsess)

Lateral Movement

- Privileges van support stelen
- Over-pass-the-hash



- Filter by
- All [18]
 - Open [0]
 - High [0]
 - Medium [0]
 - Low [0]
 - Resolved [18]
 - Dismissed [0]

EL_DEMO_CLIENT_ADMIN on PRECISION - Virtual Machine Connection

File Action Media Clipboard View Help

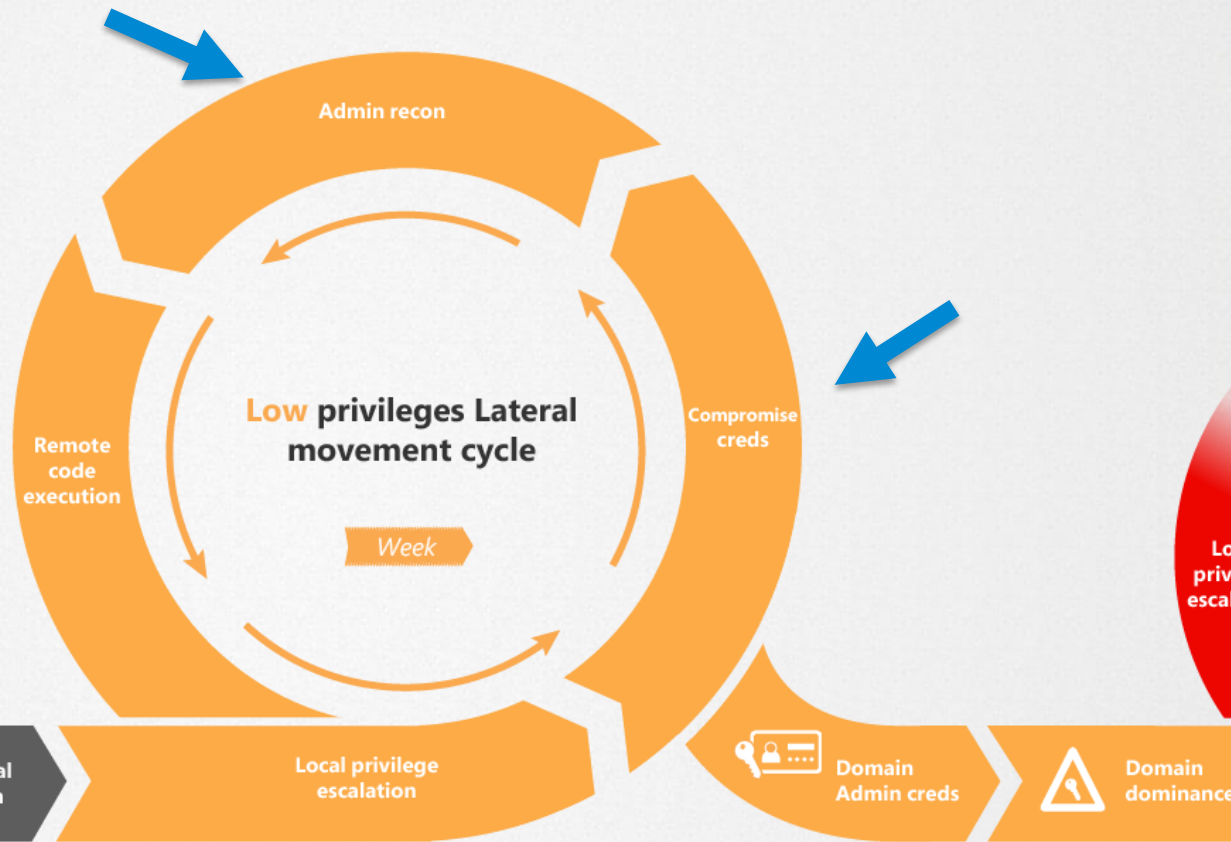
Status: Running

EL_DEMO_CLIENT_WIN8 on PRECISION - Virtual Machine Connection

No notifications



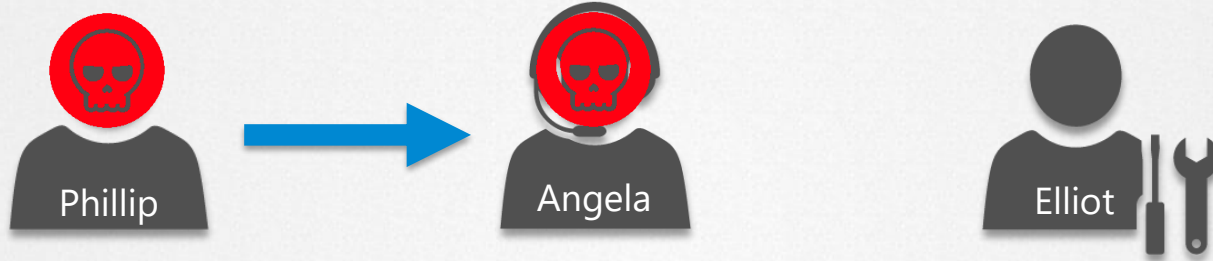
SECURITY





SECURITY

Bereikt tot zover





Lateral Movement

- Domain admin privileges stelen
- Pass-the-Ticket



Filter by

- All [18]
- Open [3]
 - High [0]
 - Medium [3]
 - Low [0]
- Resolved [15]
- Dismissed [0]

4:56 PM Monday, October 24, 2016

9:01 PM Friday, November 4, 2016

Reconnaissance using SMB Session Enumeration

SMB session enumeration attempts were successfully performed on WIN8.

Note Share Export to Excel Details



- Recommendations
- Disconnect WIN8 from the network, or move it into an isolated network.
 - Verify that all enumerated accounts use a strong password.

10:24 PM Thursday, November 3, 2016

10:56 PM

Unusual protocol implementation

Angela Moss successfully authenticated from WIN8 against the domain controller using Pass-the-Hash and brute force.

Note Share Export to Excel Details Input

EL_DEMO_CLIENT_WIN8 on PRECISION - Virtual Machine Connection

File Action Media View Help

Administrator: C:\Windows\SYSTEM32\cmd.exe

Recycle Bin

Administrator: C:\Windows\SYSTEM32\cmd.exe

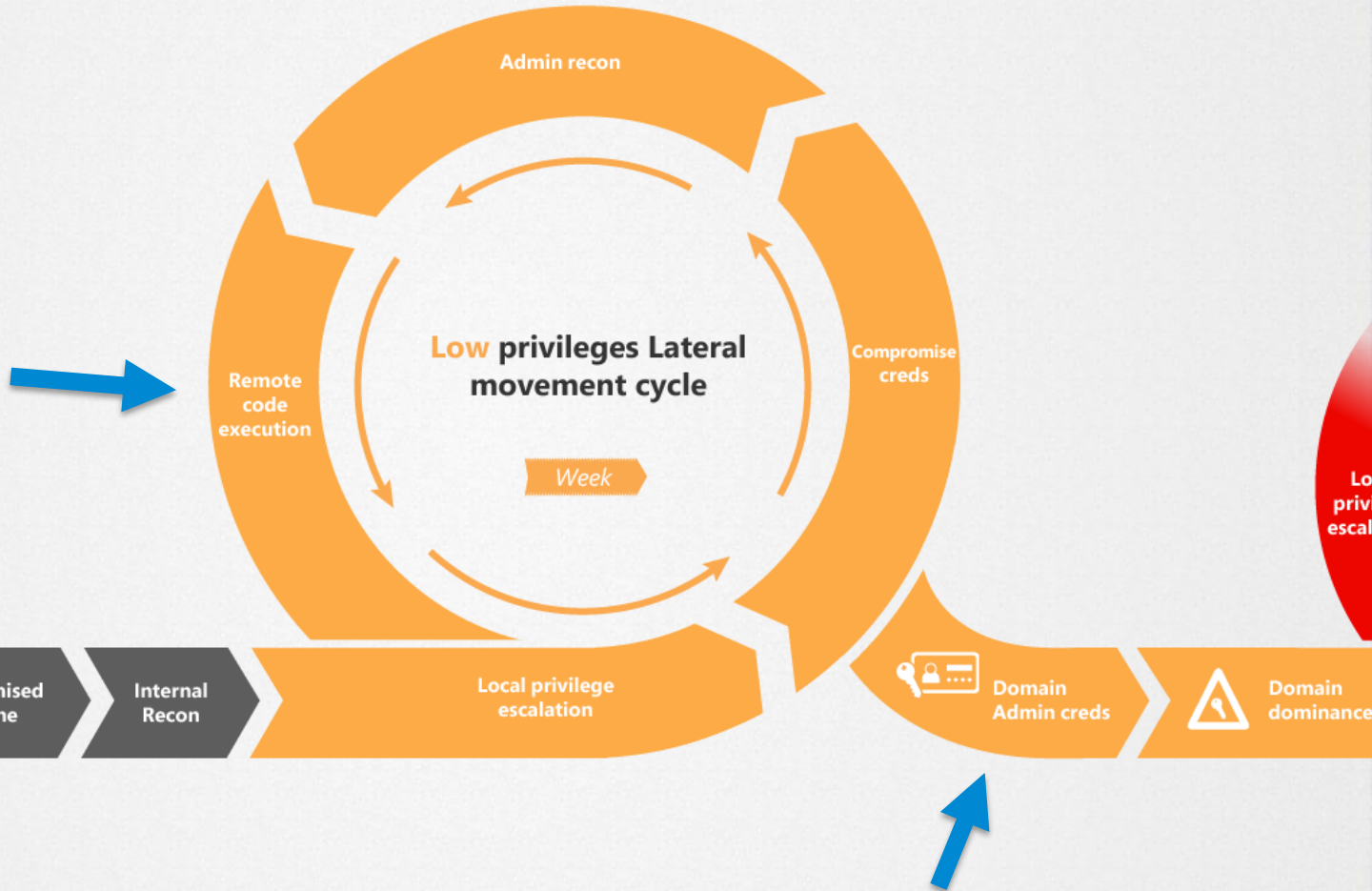
Status: Running

21:56 4-11-2016

- Suspicious Activity
- Unusual protocol implementation an hour ago
- Suspicious Activity
- Reconnaissance using SMB Session Enumeration an hour ago
- Suspicious Activity
- Reconnaissance using directory services enumeration an hour ago

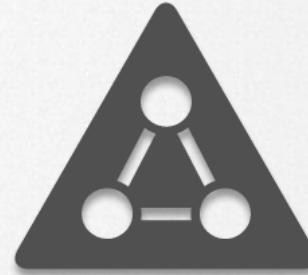
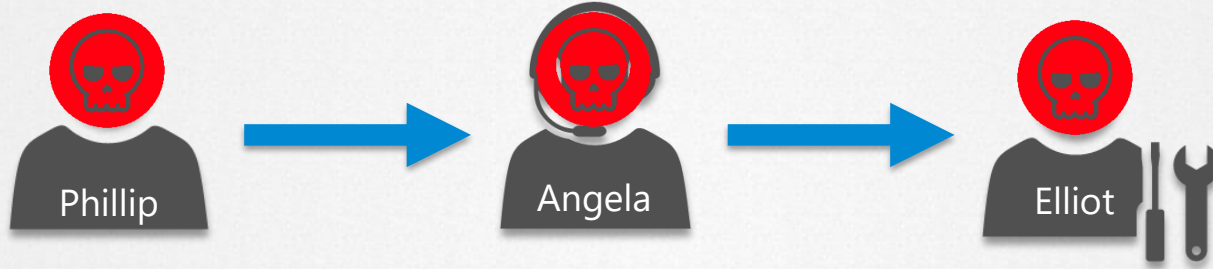


SECURITY





Bereikt tot zover





Domain Domination

- Dump hash KRBTGT account
- Creëren Golden Ticket
- Import Golden Ticket
- Toegang tot alle resources



Filter by

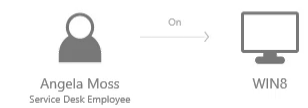
- All [18]
- Open [3]
 - High [0]
 - Medium [3]
 - Low [0]
- Resolved [11]
- Dismissed [4]

10:24 PM Thursday, November 3, 2016

Unusual protocol implementation

Angela Moss successfully authenticated from WIN8 again as Pass-the-Hash and brute force.

Note Share Export to Excel Details



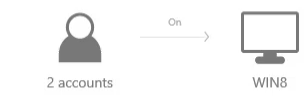
- Recommendations
- Disconnect WIN8 from the network, or move it into an isolated network.
 - Investigate the root cause on WIN8.
 - Reset Angela Moss's password.

4:56 PM Monday, October 24, 2016

Reconnaissance using SMB Session Enumeration

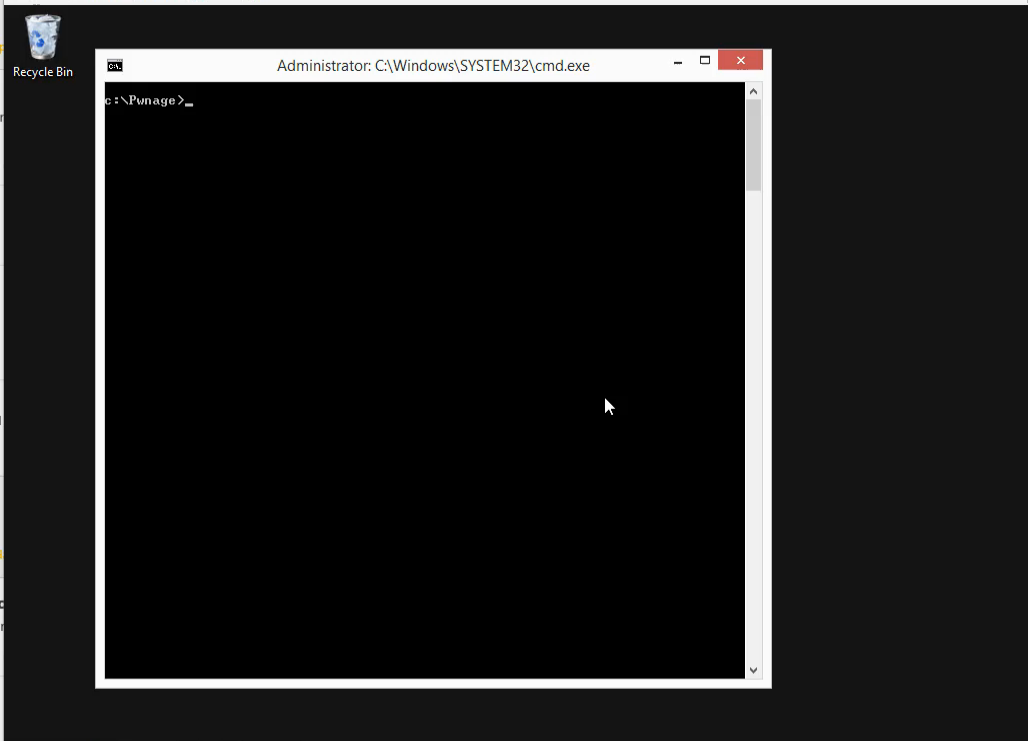
SMB session enumeration attempts were successfully performed.

Note Share Export to Excel Details



EL_DEMO_CLIENT_WIN8 on PRECISION - Virtual Machine Connection

File Action Media View Help

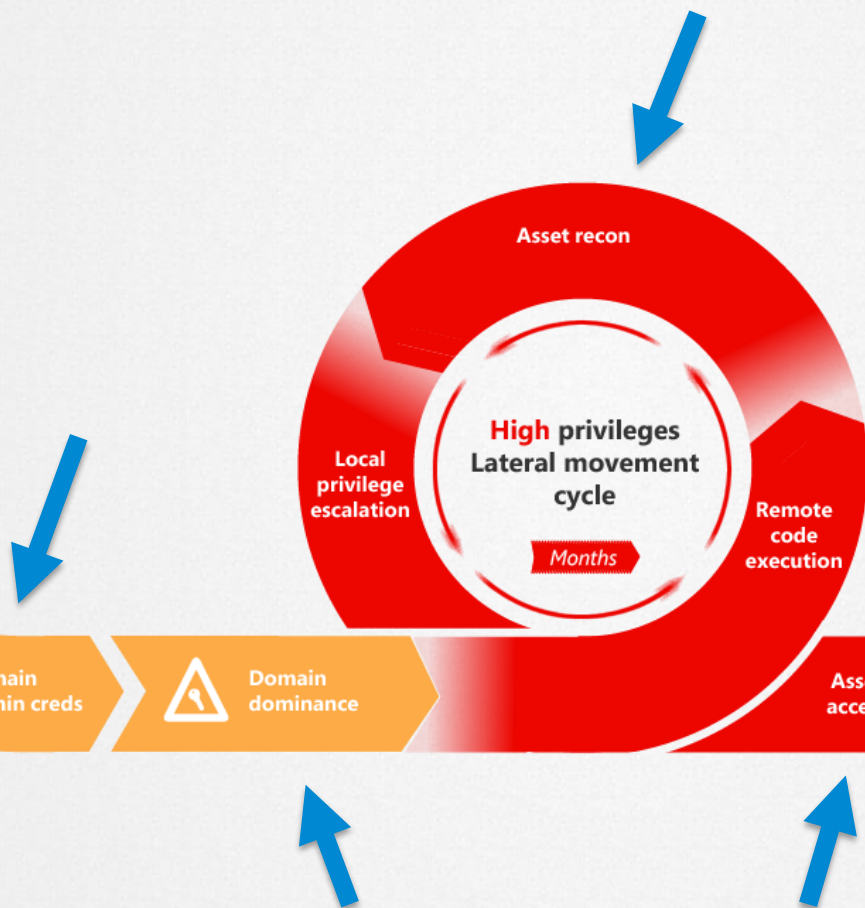
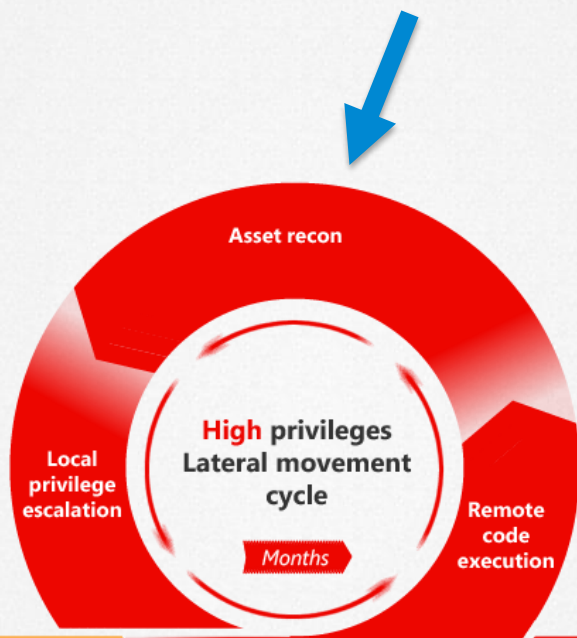
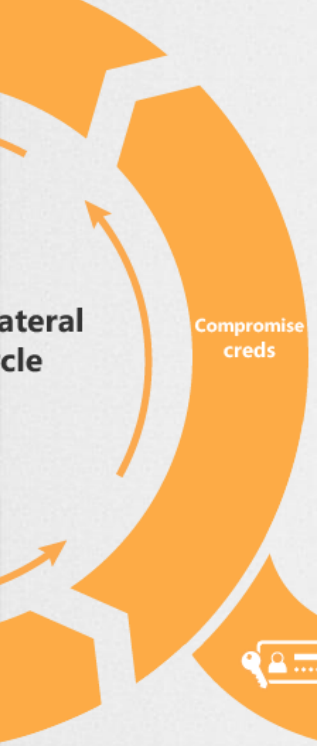


Suspicious Activity

- Unusual protocol implementation 2 hours ago
- Suspicious Activity Reconnaissance using SMB Session Enumeration 2 hours ago
- Suspicious Activity Reconnaissance using directory services enumeration 2 hours ago



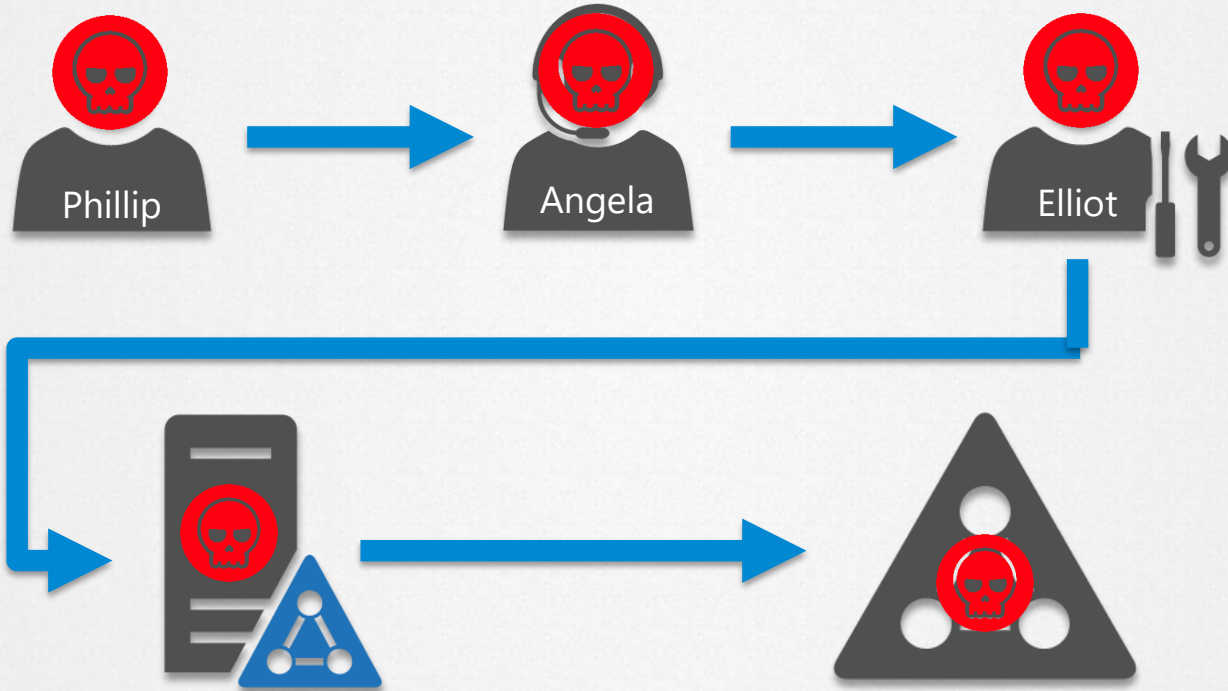
SECURITY





SECURITY

Pwnage! Mission Accomplished



- Filter by
- All [20]
 - Open [7]
 - High [2]
 - Medium [5]
 - Low [0]
 - Resolved [10]
 - Dismissed [3]

- angela on 10.0.0.11
- WIN8\$ on 10.0.0.11

Recommendations

- Disconnect WIN8 from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Verify that all enumerated accounts use a strong password.

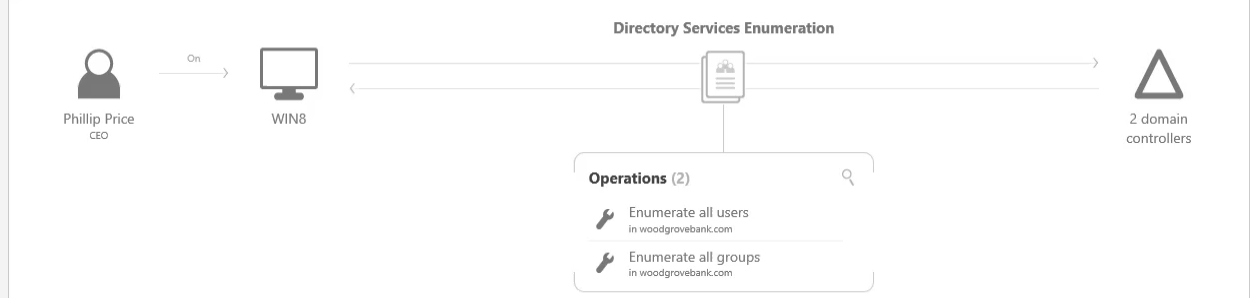
10:19 PM Thursday, November 3, 2016 > 10:19 PM Friday, November 4, 2016

Reconnaissance using directory services enumeration

The following directory services enumerations using SAMR protocol were attempted against 2 domain controllers from WIN8:

- Successful enumeration of all users in woodgrovebank.com by Phillip Price
- Successful enumeration of all groups in woodgrovebank.com by Phillip Price

Note Share Export to Excel Details Input Open



Recommendations

- Disconnect WIN8 from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more

1:17 PM Thursday, October 27, 2016

- Health Issue Gateway stopped communicating a few seconds ago
- Health Issue Gateway stopped communicating a few seconds ago
- Suspicious Activity Brute force attack using LDAP simple bind 4 minutes ago
- Suspicious Activity Encryption downgrade activity 4 minutes ago
- Suspicious Activity Identity theft using Pass-the-Ticket attack 4 minutes ago
- Suspicious Activity Malicious replication of directory services 4 minutes ago



SECURITY

Mitigation





SECURITY

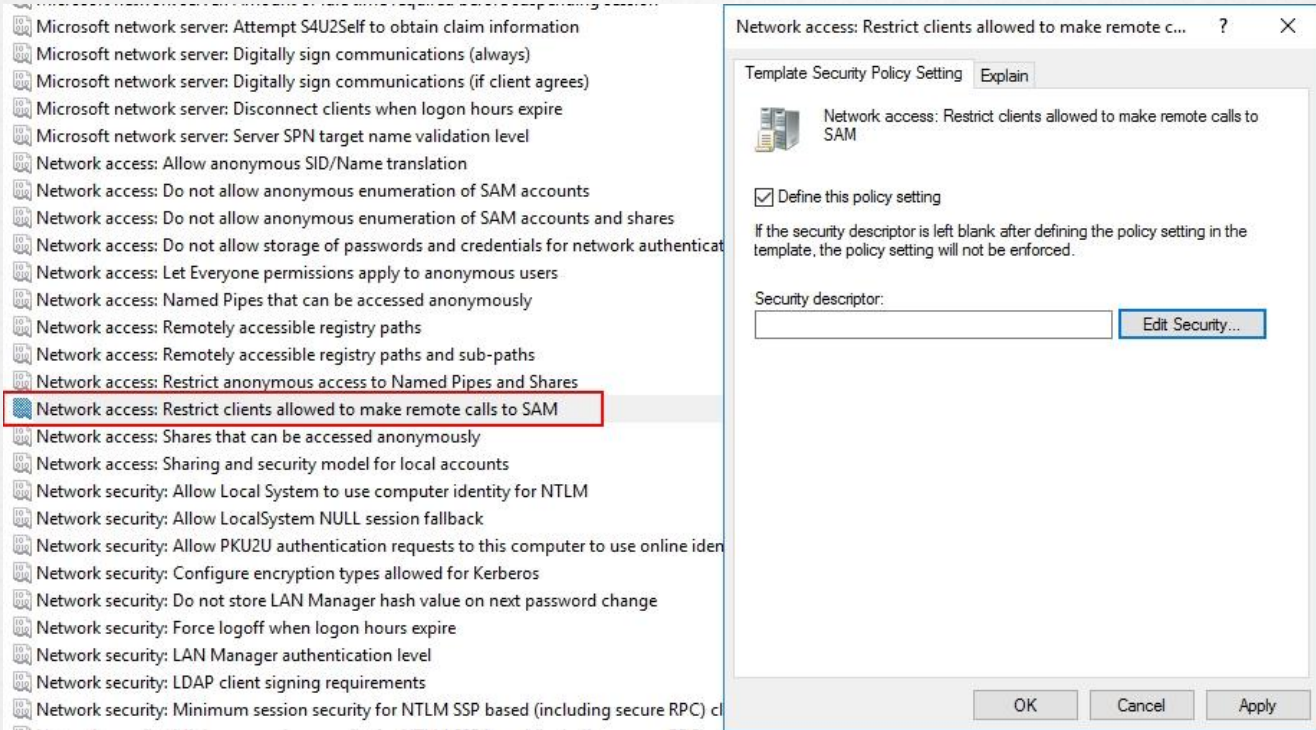
Verkenning (reconnaissance)

1. SAM-R



SAM-R

RestrictRemoteSAM registry (GPO) (Win10/Server 2016)



The image shows a screenshot of the Group Policy Editor window. The left pane displays a list of policy settings, with 'Network access: Restrict clients allowed to make remote calls to SAM' highlighted by a red box. The right pane shows the configuration for this policy. The 'Define this policy setting' checkbox is checked. Below it, there is a text box for the 'Security descriptor' and an 'Edit Security...' button. At the bottom of the right pane, there are 'OK', 'Cancel', and 'Apply' buttons.

Microsoft network server: Attempt S4U2Self to obtain claim information
Microsoft network server: Digitally sign communications (always)
Microsoft network server: Digitally sign communications (if client agrees)
Microsoft network server: Disconnect clients when logon hours expire
Microsoft network server: Server SPN target name validation level
Network access: Allow anonymous SID/Name translation
Network access: Do not allow anonymous enumeration of SAM accounts
Network access: Do not allow anonymous enumeration of SAM accounts and shares
Network access: Do not allow storage of passwords and credentials for network authentication
Network access: Let Everyone permissions apply to anonymous users
Network access: Named Pipes that can be accessed anonymously
Network access: Remotely accessible registry paths
Network access: Remotely accessible registry paths and sub-paths
Network access: Restrict clients allowed to make remote calls to SAM
Network access: Shares that can be accessed anonymously
Network access: Sharing and security model for local accounts
Network security: Allow Local System to use computer identity for NTLM
Network security: Allow LocalSystem NULL session fallback
Network security: Allow PKU2U authentication requests to this computer to use online identities
Network security: Configure encryption types allowed for Kerberos
Network security: Do not store LAN Manager hash value on next password change
Network security: Force logoff when logon hours expire
Network security: LAN Manager authentication level
Network security: LDAP client signing requirements
Network security: Minimum session security for NTLM SSP based (including secure RPC client authentication)

Network access: Restrict clients allowed to make remote calls to SAM

Template Security Policy Setting Explain

Network access: Restrict clients allowed to make remote calls to SAM

Define this policy setting

If the security descriptor is left blank after defining the policy setting in the template, the policy setting will not be enforced.

Security descriptor:

Edit Security...

OK Cancel Apply



get-aduser -filter {AdminCount -eq 1} -Properties Name,AdminCount,ServicePrincipalName>PasswordLastSet,LastLogonDate,MemberOf

```

Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\phillip> get-aduser -filter {AdminCount -eq 1} -Properties Name,AdminCount,ServicePrincipalName>PasswordLastSet,LastLogonDate,MemberOf

AdminCount           : 1
DistinguishedName    : CN=Administrator,CN=Users,DC=woodgrovebank,DC=com
Enabled              : True
GivenName            :
LastLogonDate        : 18-10-2016 07:53:32
MemberOf             : CN=Group Policy Creator Owners,CN=Users,DC=woodgrovebank,DC=com, CN=Domain Admins,CN=Users,DC=woodgrovebank,DC=com, CN=Enterprise Admins,CN=Users,DC=woodgrovebank,DC=com, CN=Schema Admins,CN=Users,DC=woodgrovebank,DC=com...}
Name                 : Administrator
ObjectClass          : user
ObjectGUID           : f06927e2-3947-460f-bf41-5d5213369977
PasswordLastSet      : 2-10-2016 20:58:44
SamAccountName       : Administrator
SID                  : S-1-5-21-3014657713-3602203707-3300139565-500
Surname              :
UserPrincipalName    :

AdminCount           : 1
DistinguishedName    : CN=krbtgt,CN=Users,DC=woodgrovebank,DC=com
Enabled              : False
GivenName            :
LastLogonDate        :
MemberOf             : {CN=Denied RODC Password Replication Group,CN=Users,DC=woodgrovebank,DC=com}
Name                 : krbtgt
ObjectClass          : user
ObjectGUID           : 555f5fd7-f436-4231-bbd0-e298b2e548d7
PasswordLastSet      : 11-10-2016 11:58:37
SamAccountName       : krbtgt
ServicePrincipalName : {kadmin/changepw}
SID                  : S-1-5-21-3014657713-3602203707-3300139565-502
Surname              :
UserPrincipalName    :

AdminCount           : 1
DistinguishedName    : CN=Elliot Alderson,OU=Users,OU=Corp,DC=woodgrovebank,DC=com
Enabled              : True
GivenName            : Elliot
LastLogonDate        : 18-10-2016 07:34:20
MemberOf             : {CN=Domain Admins,CN=Users,DC=woodgrovebank,DC=com}
Name                 : Elliot Alderson
ObjectClass          : user
ObjectGUID           : d0793a85-acae-462f-8ebb-713e5f7ab62e
PasswordLastSet      : 4-10-2016 13:07:22
  
```





Verkenning (reconnaissance)

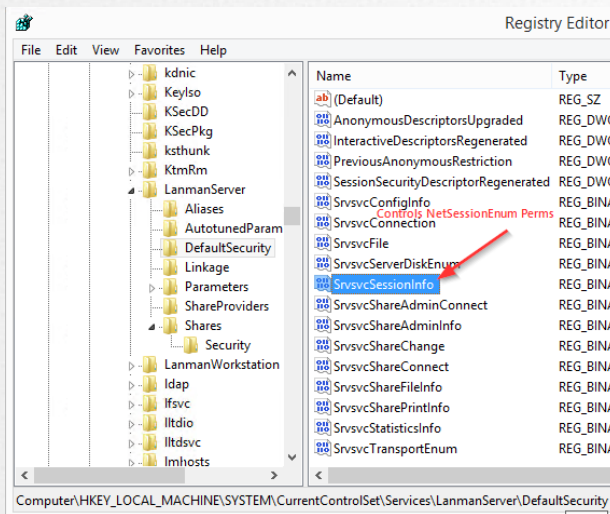
1. SAM-R
RestrictRemoteSAM registry (GPO)
2. NetSess



SMB Session Enumeration (NetSess.exe)

- Administrators group (Security Identifier (Sid) S-1-5-32-544)
- Server Operators group (Sid S-1-5-32-549)
- Power Users group (Sid S-1-5-32-547)
- Authenticated Users group (Sid S-1-5-11)

Net Cease download: <https://gallery.technet.microsoft.com/Net-Cease-Blocking-Net-1e8dcb5b>



Net Cease - Hardening Net Session Enumeration

"Net Cease" tool is a short PowerShell (PS) script which alters Net Session Enumeration (NetSessionEnum) default permissions. This hardening process prevents attackers from easily getting some valuable recon information to move laterally within their victim's network.

Download

NetCease.zip

Ratings

★★★★ (4)

Updated

10/18/2016

Downloaded

1,310 times

License

TechNet terms of use

Favorites

Add to favorites

Share

✉

Category

Security

Sub-category

DAACLs

Tags

Security, Powershell, Permissions, Domain Controllers, User sessions, NetSessionEnum



Verkenning (reconnaissance)

1. SAM-R

RestrictRemoteSAM registry (GPO)

2. NetSess

Verwijderen 'authenticated users' permissie

Lateral Movement

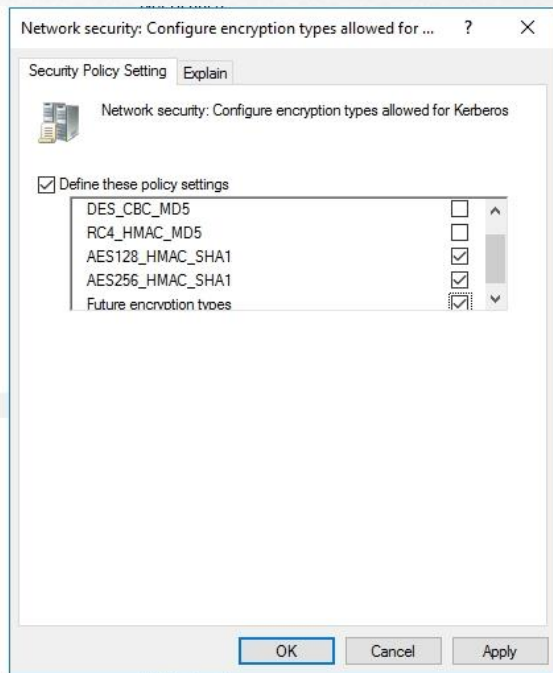
3. Over-pass-the-hash



Over-pass-the-hash

Zwakke Kerberos encryptie uitschakelen! DES, RC4. Enkel AES128/256 gebruiken

- Microsoft network server: Server-side target name validation level
- Network access: Allow anonymous SID/Name translation
- Network access: Do not allow anonymous enumeration of SAM accounts
- Network access: Do not allow anonymous enumeration of SAM accounts and shares
- Network access: Do not allow storage of passwords and credentials for network authentication
- Network access: Let Everyone permissions apply to anonymous users
- Network access: Named Pipes that can be accessed anonymously
- Network access: Remotely accessible registry paths
- Network access: Remotely accessible registry paths and sub-paths
- Network access: Restrict anonymous access to Named Pipes and Shares
- Network access: Restrict clients allowed to make remote calls to SAM
- Network access: Shares that can be accessed anonymously
- Network access: Sharing and security model for local accounts
- Network security: Allow Local System to use computer identity for NTLM
- Network security: Allow LocalSystem NULL session fallback
- Network security: Allow PKU2U authentication requests to this computer to use online identities.
- Network security: Configure encryption types allowed for Kerberos**
- Network security: Do not store LAN Manager hash value on next password change
- Network security: Force logoff when logon hours expire
- Network security: LAN Manager authentication level
- Network security: LDAP client signing requirements
- Network security: Minimum session security for NTLM SSP based (including secure RPC) clients
- Network security: Minimum session security for NTLM SSP based (including secure RPC) servers
- Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication
- Network security: Restrict NTLM: Add server exceptions in this domain
- Network security: Restrict NTLM: Audit Incoming NTLM Traffic
- Network security: Restrict NTLM: Audit NTLM authentication in this domain



Verkenning (reconnaissance)

1. SAM-R
RestrictRemoteSAM registry (GPO)
2. NetSess
Verwijderen 'authenticated users' permissie

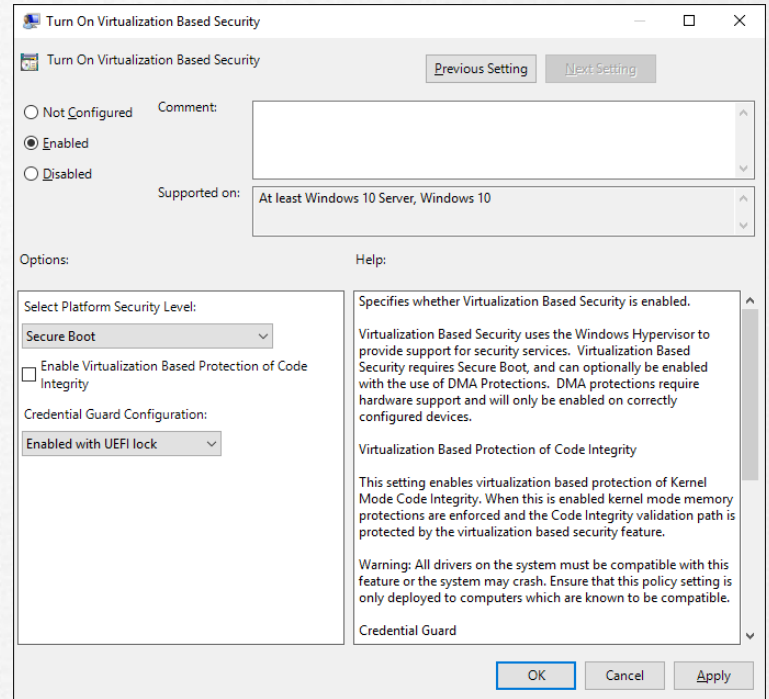
Lateral Movement

3. Over-pass-the-hash
Zwakke Kerberos encryptie uitschakelen!
4. Pass-the-Ticket



Pass-the-Ticket Credential Guard

- Hardware eisen
- Intel VT-D of AMD Vi IOMMU
- TPM 1.2 of 2.0
- UEFI 2.3.1c+
- UEFI Secure Boot
- Windows 10
- Lijst wordt langer



Verkenning (reconnaissance)

1. SAM-R
RestrictRemoteSAM registry (GPO)
2. NetSess
Verwijderen 'authenticated users' permissie

Lateral Movement

3. Over-pass-the-hash
Zwakke Kerberos encryptie uitschakelen!
4. Pass-the-Ticket
Credential Guard

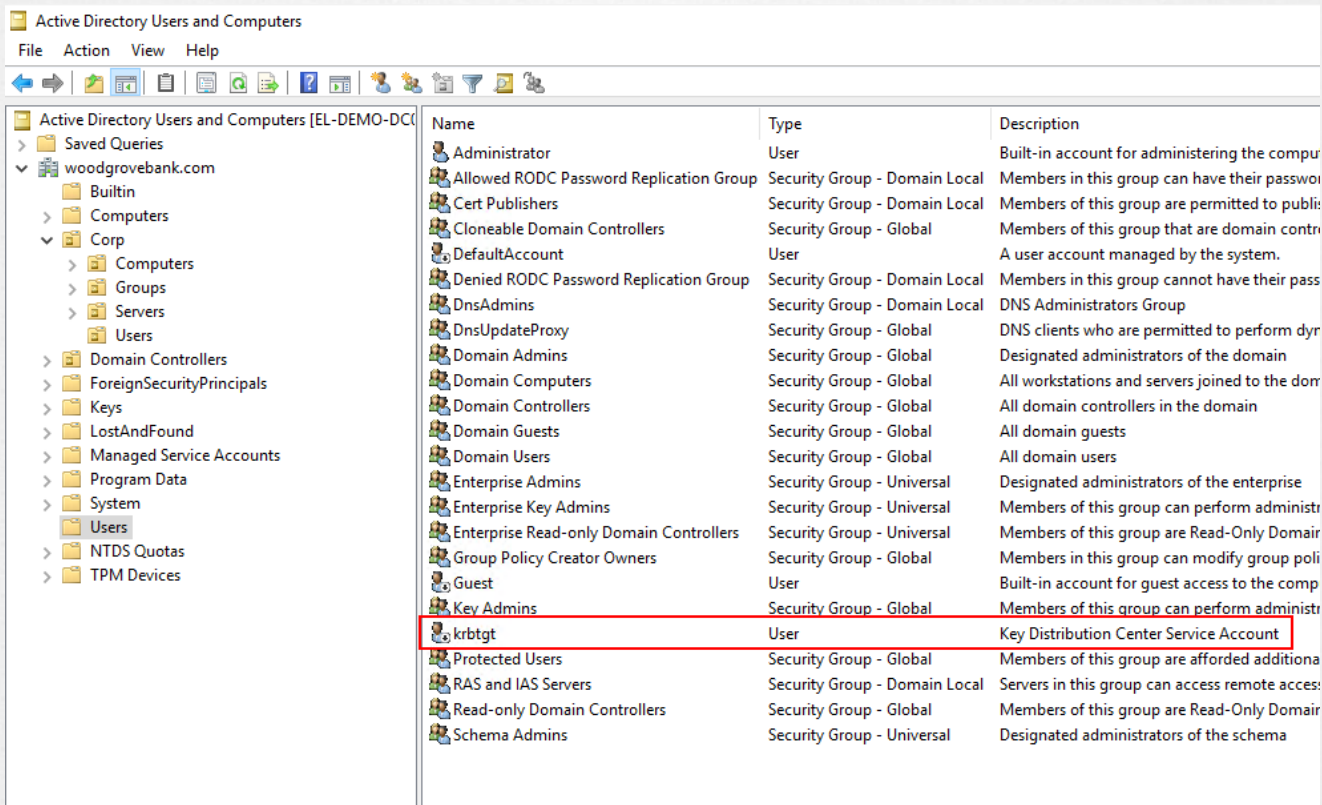
Domain Domination

5. Compromitteren KRBTGT account (DcSync)
6. Golden Ticket



KRBTGT account, Golden Ticket

Enkel detectie



The screenshot shows the Active Directory Users and Computers console for the domain woodgrovebank.com. The left pane shows the tree structure with 'Users' selected. The right pane displays a list of users and groups with columns for Name, Type, and Description. The 'krbtgt' user is highlighted with a red box.

Name	Type	Description
Administrator	User	Built-in account for administering the computer
Allowed RODC Password Replication Group	Security Group - Domain Local	Members in this group can have their passwords replicated to Read-Only Domain Controllers
Cert Publishers	Security Group - Domain Local	Members of this group are permitted to publish certificates
Cloneable Domain Controllers	Security Group - Global	Members of this group that are domain controllers can be cloned
DefaultAccount	User	A user account managed by the system.
Denied RODC Password Replication Group	Security Group - Domain Local	Members in this group cannot have their passwords replicated to Read-Only Domain Controllers
DnsAdmins	Security Group - Domain Local	DNS Administrators Group
DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to perform dynamic updates
Domain Admins	Security Group - Global	Designated administrators of the domain
Domain Computers	Security Group - Global	All workstations and servers joined to the domain
Domain Controllers	Security Group - Global	All domain controllers in the domain
Domain Guests	Security Group - Global	All domain guests
Domain Users	Security Group - Global	All domain users
Enterprise Admins	Security Group - Universal	Designated administrators of the enterprise
Enterprise Key Admins	Security Group - Universal	Members of this group can perform administrative tasks on Read-Only Domain Controllers
Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group are Read-Only Domain Controllers
Group Policy Creator Owners	Security Group - Global	Members in this group can modify group policy objects
Guest	User	Built-in account for guest access to the computer
Key Admins	Security Group - Global	Members of this group can perform administrative tasks on Read-Only Domain Controllers
krbtgt	User	Key Distribution Center Service Account
Protected Users	Security Group - Global	Members of this group are afforded additional protection
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can access remote access services
Read-only Domain Controllers	Security Group - Global	Members of this group are Read-Only Domain Controllers
Schema Admins	Security Group - Universal	Designated administrators of the schema



Verkenning (reconnaissance)

1. SAM-R
RestrictRemoteSAM registry (GPO)
2. NetSess
Verwijderen 'authenticated users' permissie

Lateral Movement

3. Over-pass-the-hash
Zwakke Kerberos encryptie uitschakelen!
4. Pass-the-Ticket
Credential Guard

Domain Domination

5. Compromitteren KRBTGT account (DcSync)
Enkel detectie
6. Golden Ticket
Reset KRBTGT account 2x





SECURITY

Pas bestaande technieken toe!



Protected Users Group



Kerberos Armoring (FAST)

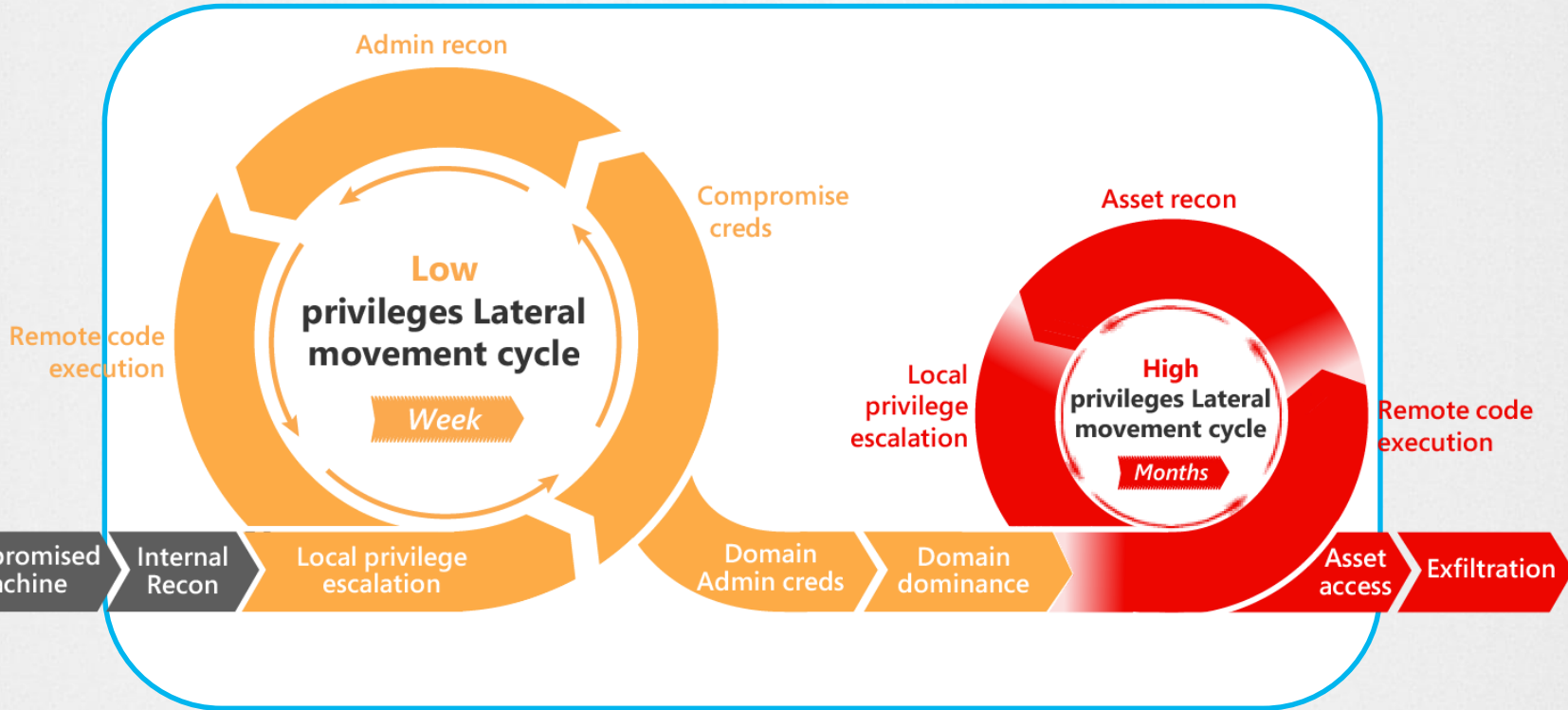


Authentication
Policies & Silos





Samenvatting





SECURITY

Q&A





Volgende sessie 9:00 – 10:00 uur

Keynote: “Reinvent IT infrastructure
for business agility”

Lorenzo Rizzi
Expo Theater

Experts  Live2016