BMC Discovery Schwerpunkt Security

BMC Discovery User Group

München

07.11.2018

Dipl.-Ing. Karim Ibrown
Freelancer

Karim@Ibrown.de
+491799476150
www.xing.com/profile/Karim_Ibrown/

Dipl.-Inf. Viktor Marinov
Freelancer

viktor.marinov@outlook.com
+491797608602
www.linkedin.com/in/vmmware

Agenda

Projekt

Security

Empfehlungen

Nächste Schritte…

Agenda

Projekt

1. Stakeholder
2. Ausgangslage
3. Projekt-Ziele
4. Aktuelles Ergebnis
5. Vermeidbare Fehler

Security

Empfehlungen

Nächste Schritte…

Stakeholder

- Lizenzmanagement
  - Inventarisierung Microsoft Windows Lizenzen
    - Betriebssystem
    - Anwendungen (sonstige MS Produkte)
  - Inventarisierung Oracle Datenbanken Lizenzen
  - Reporting
- Configuration Management
- Schwachstellenmanagement

Projektverlauf

- Ausgangslage
  - manuell erfasste und gepflegte Serverdaten in
    - 7 Datenbanken
    - diverse Excel- und CSV-Listen

Projektverlauf

- Ausgangslage
  - manuell erfasste und gepflegte Serverdaten in
    - 7 Datenbanken
    - diverse Excel- und CSV-Listen

- Projekt-Ziele
  - Inventarisierung 100% der Ausgangslage (SOLL)

Projektverlauf

- Ausgangslage
  - manuell erfasste und gepflegte Serverdaten in
    - 7 Datenbanken
    - diverse Excel- und CSV-Listen
- Projekt-Ziele
  - Inventarisierung 100% der Ausgangslage (SOLL)
- Aktuelles Ergebnis
  - Erfolgreich gescannt 100% (SOLL)
  - +50% dank BMC Discovery (150% IST)

Vermeidbare Fehler

- Planung und Implementierung **ohne Discovery Know-How**

Vermeidbare Fehler

- Planung und Implementierung **ohne Discovery Know-How**
  - Versuche Windows Systeme ohne Admin zu scannen

Vermeidbare Fehler

- Planung und Implementierung **ohne Discovery Know-How**
  - Versuche Windows Systeme ohne Admin zu scannen
  - Firewall-Portfreischaltung für alle Ports aus der BMC Dokumentation

Vermeidbare Fehler

- Planung und Implementierung **ohne Discovery Know-How**
  - Versuche Windows Systeme ohne Admin zu scannen
  - Firewall-Portfreischaltung für alle Ports aus der BMC Dokumentation
  - Offline Scanner

Vermeidbare Fehler

- Planung und Implementierung **ohne Discovery Know-How**
  - Versuche Windows Systeme ohne Admin zu scannen
  - Firewall-Portfreischaltung für alle Ports aus der BMC Dokumentation
  - Offline Scanner
  - Einzelne IP-Adressen, statt IP-Adressen Bereiche (Ranges) gescannt

Vermeidbare Fehler

- Planung und Implementierung **ohne Discovery Know-How**
  - Versuche Windows Systeme ohne Admin zu scannen
  - Firewall-Portfreischaltung für alle Ports aus der BMC Dokumentation
  - Offline Scanner
  - Einzelne IP-Adressen, statt IP-Adressen Bereiche (Ranges) gescannt
  - Oracle Inventarisierung starten ohne UNIX/Linux Inventarisierung

Agenda

Projekt

Security

1. Risikoanalyse
2. Sicherheitskonzept
3. Windows Discovery Fall A und Fall B
4. Maßnahmen

Empfehlungen

Nächste Schritte…

Schwerpunkt: Security

Risikoanalyse
(Standard BSI 100-3)

Gefährdungskatalog

Risikoanalyse
(konsolidiert)

Schwerpunkt: Security

Risikoanalyse (Standard BSI 100-3)

Sicherheitskonzept

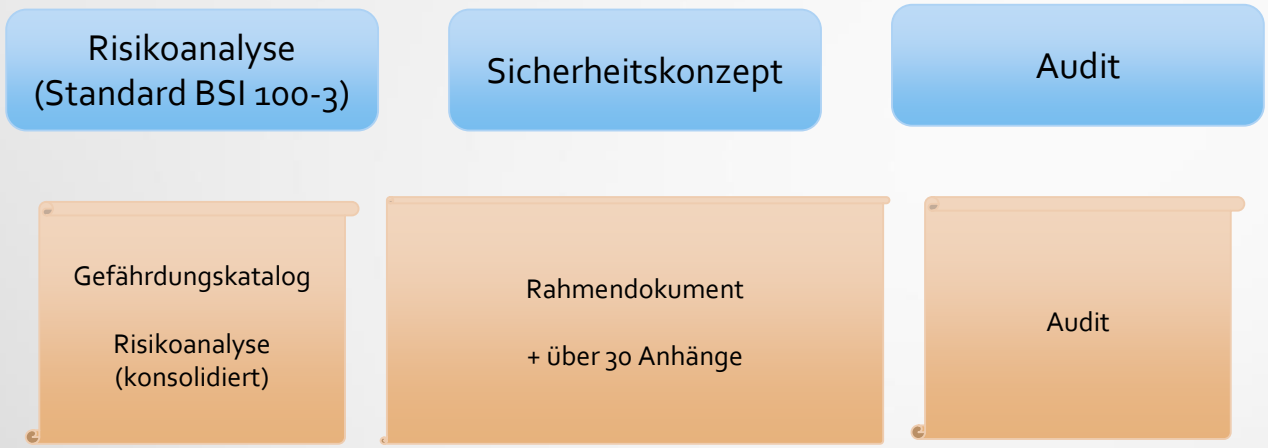
Gefährdungskatalog

Risikoanalyse (konsolidiert)

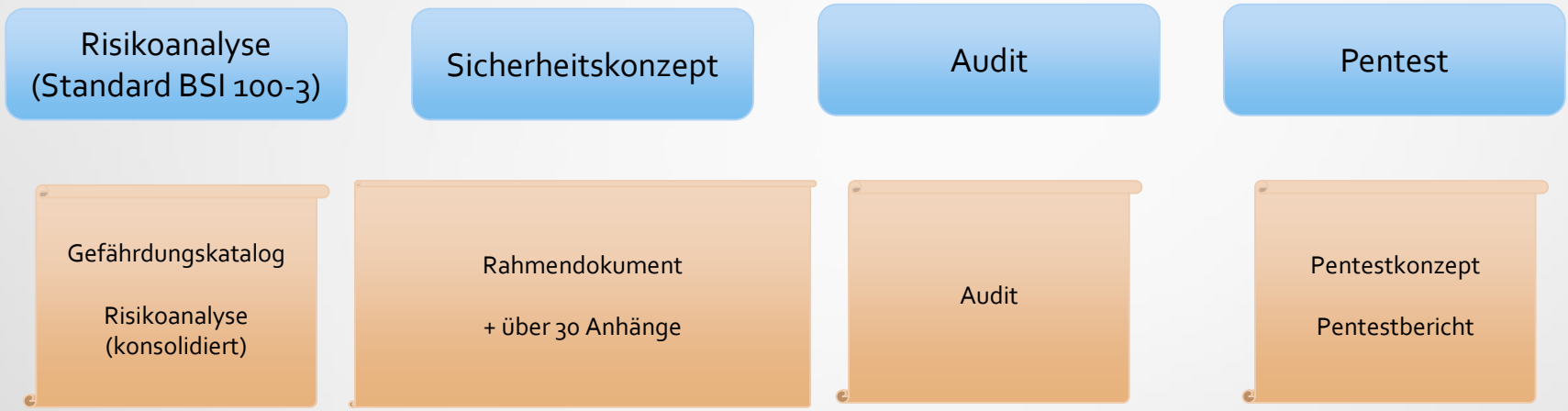
Rahmendokument

+ über 30 Anhänge

Schwerpunkt: Security



Schwerpunkt: Security



Windows Discovery
Fall A

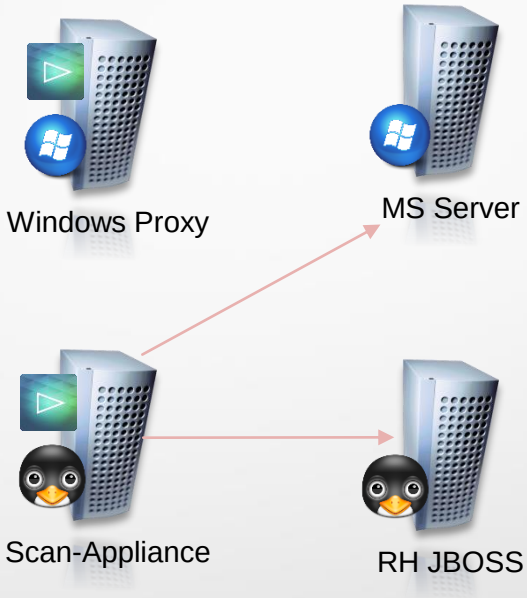

Windows Proxy


MS Server

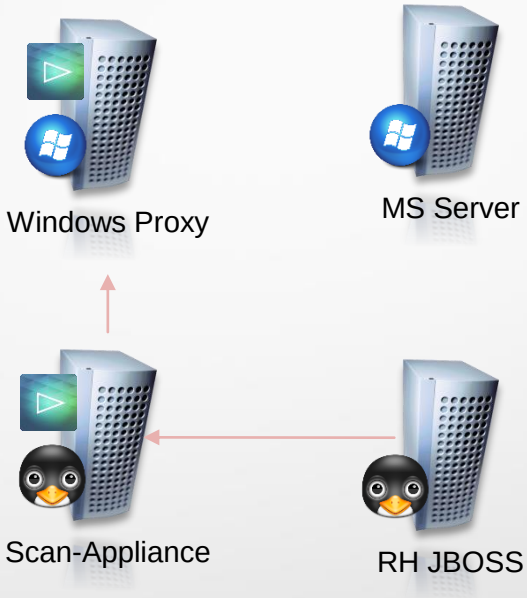

Scan-Appliance


RH JBOSS

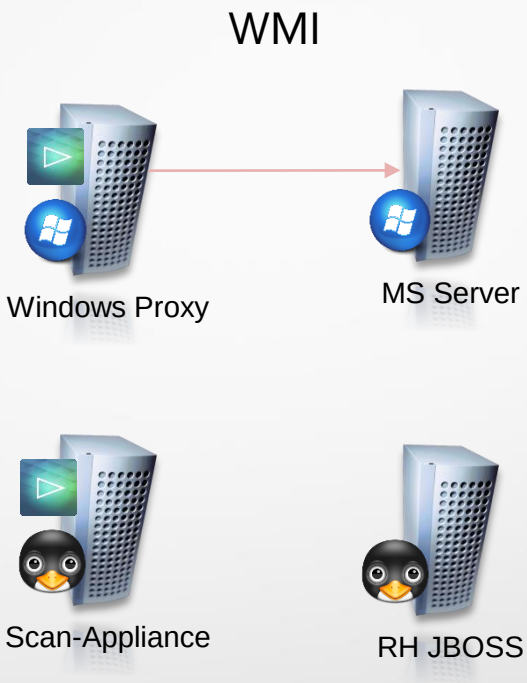
Windows Discovery
Fall A



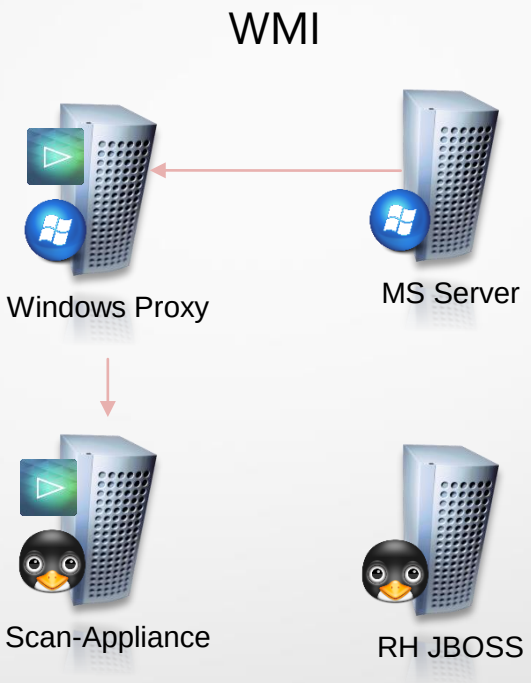
Windows Discovery
Fall A



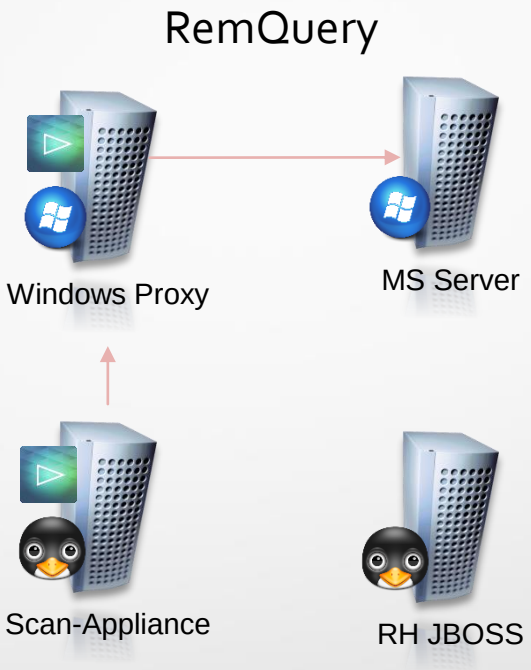
Windows Discovery
Fall A



Windows Discovery
Fall A



Windows Discovery
Fall A



Windows Discovery
Fall A

ADDMRemQuery_x86_v2.exe

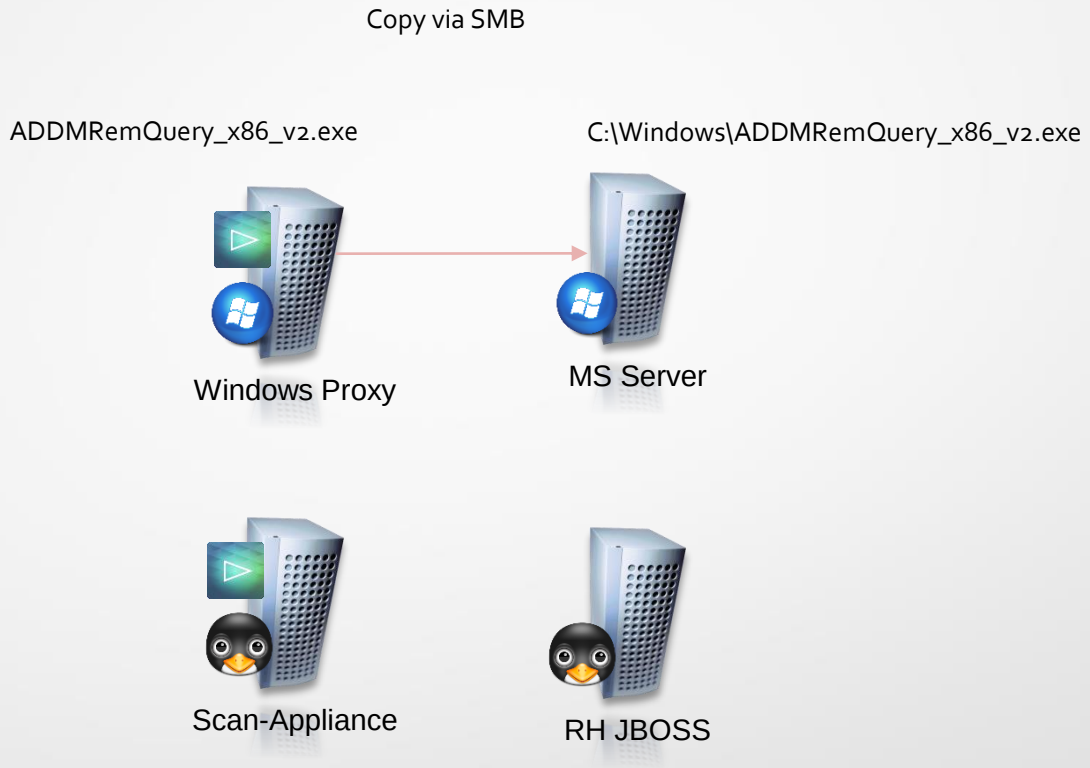
Windows Proxy

MS Server

Scan-Appliance

RH JBOSS

Windows Discovery
Fall A

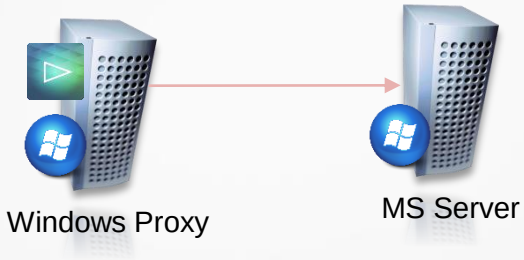


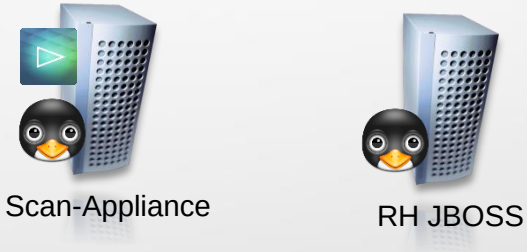
Windows Discovery
Fall A

Execute as **ADMIN**

ADDMRemQuery_x86_v2.exe

C:\Windows\ADDMRemQuery_x86_v2.exe





Windows Discovery
Fall A

ADDMRemQuery_x86_v2.exe

Windows Proxy

MS Server

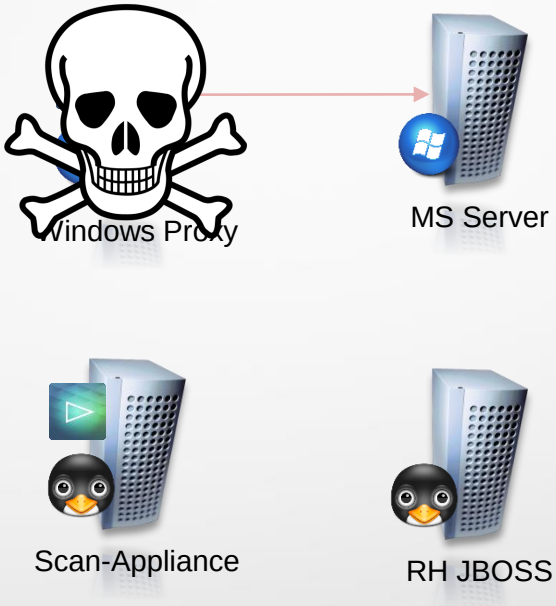
Scan-Appliance

RH JBOSS

Windows Discovery Fall A

Copy via SMB?

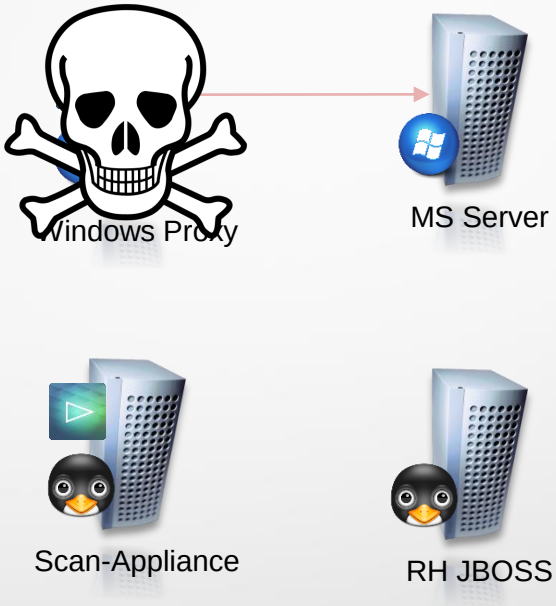
ADDMRemQuery_x86_v2.exe



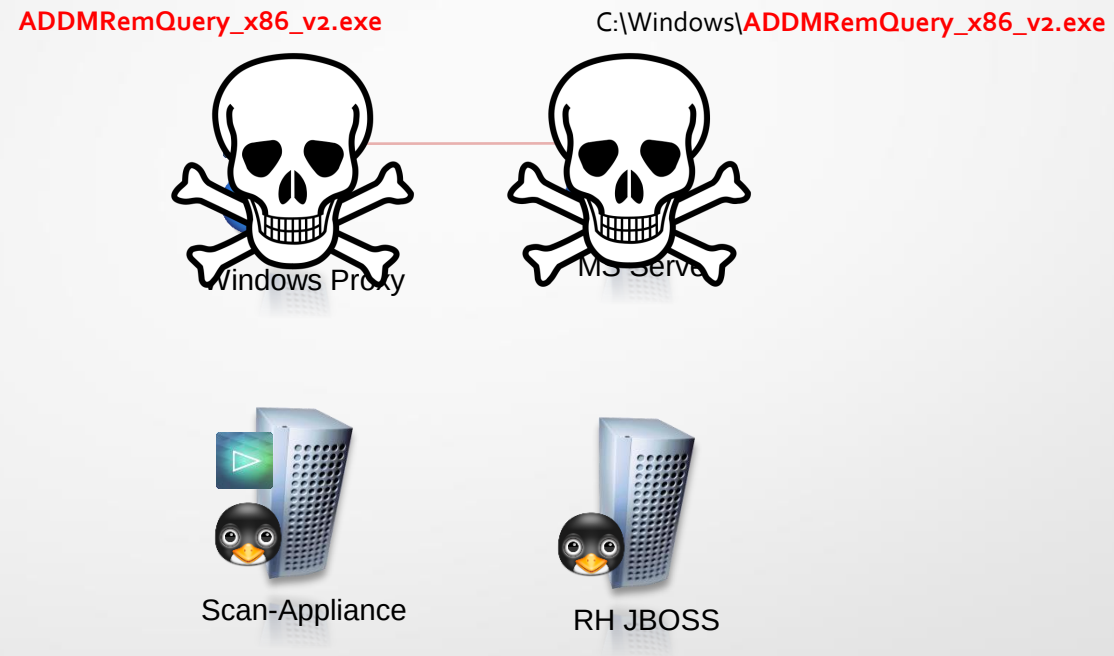
Windows Discovery
Fall A

Integrity Check?

ADDMRemQuery_x86_v2.exe



Windows Discovery
Fall A

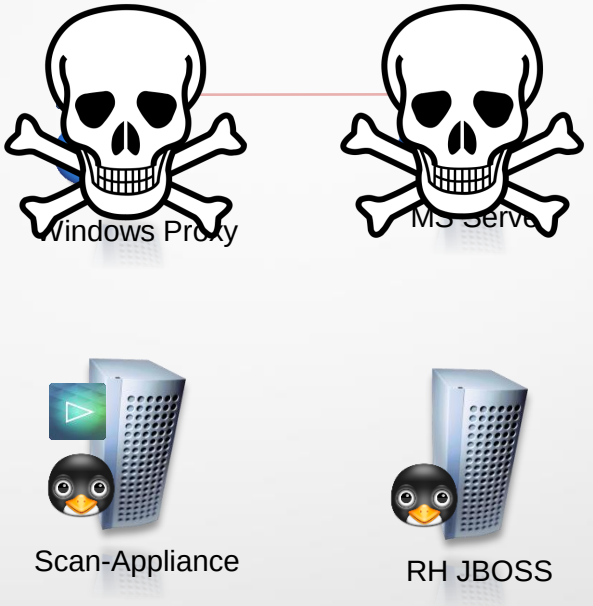


Windows Discovery
Fall A

Execute as ADMIN

ADDMRemQuery_x86_v2.exe

C:\Windows**ADDMRemQuery_x86_v2.exe**



Windows Discovery
Fall A

Windows Discovery
Fall B

C:\Windows**ADDMRemQuery_x86_v2.exe**

Windows Proxy

MS Server

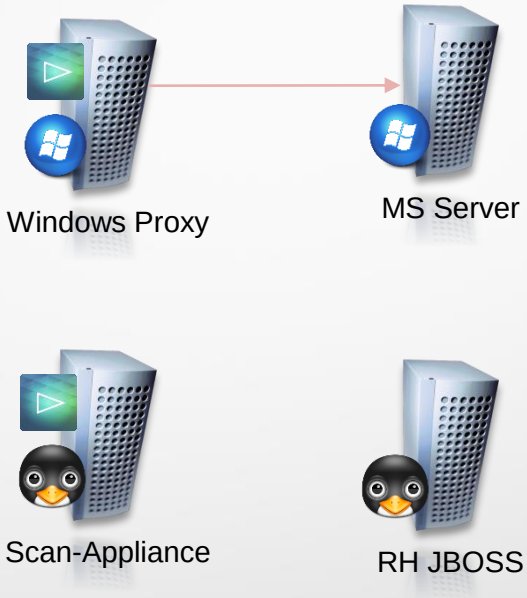
Scan-Appliance

RH JBOSS

Windows Discovery
Fall B

Integrity Check

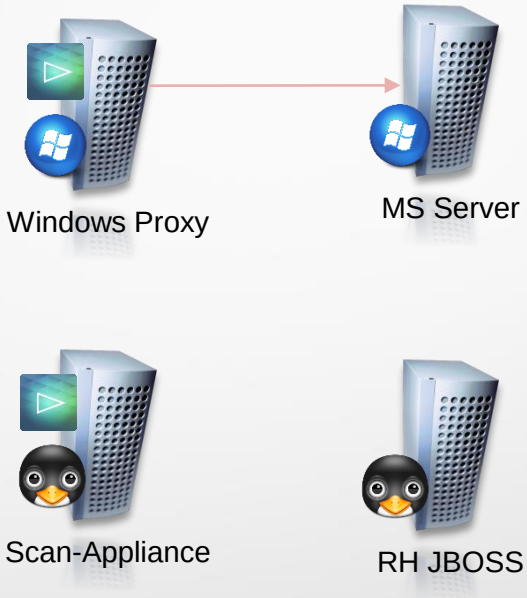
C:\Windows\ADDMRemQuery_x86_v2.exe



Windows Discovery
Fall B

Execute as **ADMIN**

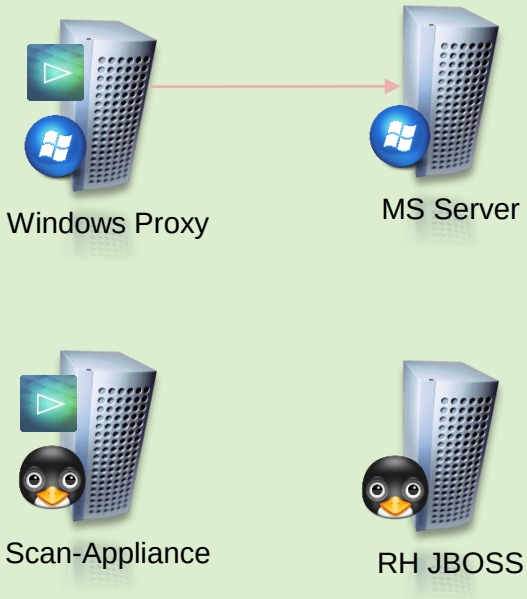
C:\Windows\ADDMRemQuery_x86_v2.exe



Windows Discovery
Fall B

Execute as **ADMIN**

C:\Windows\ADDMRemQuery_x86_v2.exe



Maßnahmen

- Logmanagement
  - Appliances
  - Windows Proxies
  - Zielsysteme

Maßnahmen

- Logmanagement
  - Appliances
  - Windows Proxies
  - Zielsysteme
- Antivirus
- Monitoring

Maßnahmen

- Logmanagement
  - Appliances
  - Windows Proxies
  - Zielsysteme
- Antivirus
- Monitoring
- Windows Discovery automatisierte
  - Benutzer Aktivierung/Deaktivierung
  - Passwort-Änderung lokal und AD

Maßnahmen

- Logmanagement
  - Appliances
  - Windows Proxies
  - Zielsysteme
- Antivirus
- Monitoring
- Windows Discovery automatisierte
  - Benutzer Aktivierung/Deaktivierung
  - Passwort-Änderung lokal und AD
- Firewall Ports für Windows Discovery minimiert
  - ALL_DCE_RPC (1024-65535 => 135)

Maßnahmen

- Logmanagement
  - Appliances
  - Windows Proxies
  - Zielsysteme
- Antivirus
- Monitoring
- Windows Discovery automatisierte
  - Benutzer Aktivierung/Deaktivierung
  - Passwort-Änderung lokal und AD
- Firewall Ports für Windows Discovery minimiert
  - ALL_DCE_RPC (1024-65535 => 135)
- Zahlreiche Prozesse implementiert

Agenda

Projekt

Security

Empfehlungen

1. Security
2. Allgemein

Nächste Schritte…

Empfehlungen Security

- RemQuery Integrity Check (Windows Discovery Fall A)

Empfehlungen Security

- RemQuery Integrity Check (Windows Discovery Fall A)
- Zertifikate für interne Kommunikation Gültigkeitsprüfung

Empfehlungen Security

- RemQuery Integrity Check (Windows Discovery Fall A)
- Zertifikate für interne Kommunikation Gültigkeitsprüfung
- Unverschlüsseltes Dateisystem
- Unverschlüsselte Dateien des Offline-Scanners

Empfehlungen Security

- RemQuery Integrity Check (Windows Discovery Fall A)
- Zertifikate für interne Kommunikation Gültigkeitsprüfung
- Unverschlüsseltes Dateisystem
- Unverschlüsselte Dateien des Offline-Scanners
- Sensitive Data Filters mit MD5 Hash

Empfehlungen Security

- RemQuery Integrity Check (Windows Discovery Fall A)
- Zertifikate für interne Kommunikation Gültigkeitsprüfung
- Unverschlüsseltes Dateisystem
- Unverschlüsselte Dateien des Offline-Scanners
- Sensitive Data Filters mit MD5 Hash
- SMB Version konfigurierbar

Empfehlungen Security

- RemQuery Integrity Check (Windows Discovery Fall A)
- Zertifikate für interne Kommunikation Gültigkeitsprüfung
- Unverschlüsseltes Dateisystem
- Unverschlüsselte Dateien des Offline-Scanners
- Sensitive Data Filters mit MD5 Hash
- SMB Version konfigurierbar
- Checks für BMC
  - Pattern Änderung => geloggt in Baseline?
  - Zertifikat-Tausch => funktioniert die Datenübertragung noch?

Empfehlungen Allgemein

- Mehr Platz auf Mount-Points

Empfehlungen Allgemein

- Mehr Platz auf Mount-Points
- Logmanagement Schnittstelle

Empfehlungen Allgemein

- Mehr Platz auf Mount-Points
- Logmanagement Schnittstelle
- Start Discovery Run geloggt nur in DEBUG?

Empfehlungen Allgemein

- Mehr Platz auf Mount-Points
- Logmanagement Schnittstelle
- Start Discovery Run geloggt nur in DEBUG?
- REST API read-only Security Permissions

Empfehlungen Allgemein

- Mehr Platz auf Mount-Points
- Logmanagement Schnittstelle
- Start Discovery Run geloggt nur in DEBUG?
- REST API read-only Security Permissions

- Model Change gewisse Sicherheit
- Lifecycle auch für Databases/Database Details

Empfehlungen Allgemein

- Mehr Platz auf Mount-Points
- Logmanagement Schnittstelle
- Start Discovery Run geloggt nur in DEBUG?
- REST API read-only Security Permissions

- Model Change gewisse Sicherheit
- Lifecycle auch für Databases/Database Details

- Bessere Fehler-Protokollierung CyberArk Interface

Empfehlungen Allgemein

- Mehr Platz auf Mount-Points
- Logmanagement Schnittstelle
- Start Discovery Run geloggt nur in DEBUG?
- REST API read-only Security Permissions

- Model Change gewisse Sicherheit
- Lifecycle auch für Databases/Database Details

- Bessere Fehler-Protokollierung CyberArk Interface

- LVM und Multipath Support

- Timezone über Cluster (WebUI) konfigurierbar und repliziert

- Datastore Compaction zuverlässig machen

- IPV6 Range Scans

Agenda

Projekt

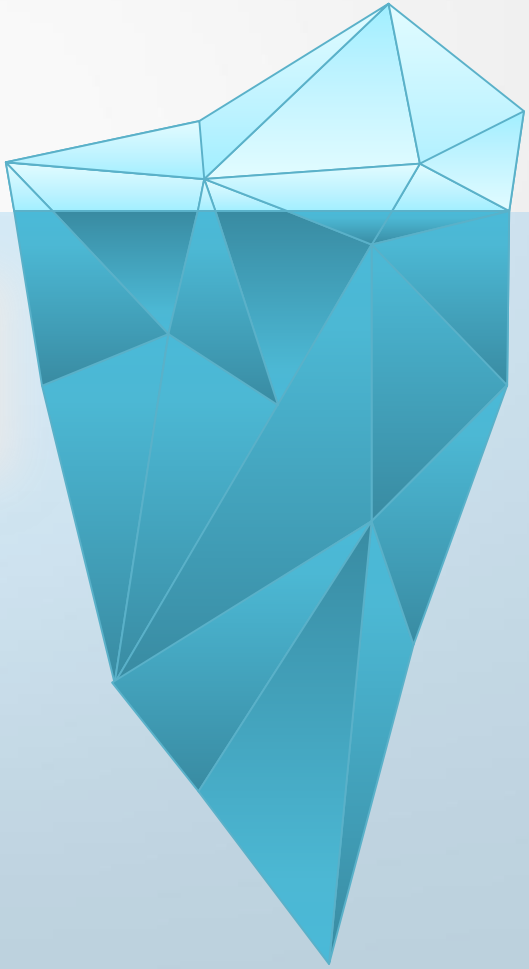
Security

Empfehlungen

Nächste Schritte…

Nächste Schritte…

- Audit
  - Sicherheitskonzept Maßnahmen
- Pentest
  - Appliances
  - Evil-Host
  - Userrechte Eskalation
  - Verschlüsselungsmethoden Prüfung
  - Integritätsprüfung
  - Schnittstellenprüfung
    - Lizenzmanagement
    - Schwachstellenmanagement
    - CMDB
  - REST API
  - XML API
- Rollout und Einbindung von neuen DCs bzw. Standorten
- Upgrade 11.3



Vielen Dank!

viktor.marinov@outlook.com
www.linkedin.com/in/vmmware

Karim@Ibrown.de
www.xing.com/profile/Karim_Ibrown/