Offensive Red Teaming

WhoAmI

Ajay

- 4+ Years of experience.
- Certs - Certified Red Teaming Expert, OSCP, CREST (CPSA, CRT), CEH, ITIL V4.
- Acknowledgment from Google drive addon Editey, Microsoft, GM, Acunetix.
- H1-212 Challenge coin reward
- CVE -2018-20341 author.
- https://www.koolacac.blogspot.in

Nitesh

- 5+ Years of experience.
- Certs - OSCP, Offensive IoT and AWS Security Fundamentals.
- Speaker at Null Mumbai and Corporate Trainer.
- https://resources.infosecinstitute.com/author/niteshmalviya/

GOAL

- Understanding Red Teaming adversarial Tactics, Techniques and Procedure (TTPs)
- Getting familiar with Active Directory (AD) basics, AD components and various attacks on AD.
- PowerShell - Fundamentals and role in Red Teaming Activity.
- Insider Attack Simulation - Privilege Escalation, Domain and AD Recon, Lateral movement and Pivoting, Gaining Domain Admin Access, Persistence.
- Attacks to be covered – Privilege Escalation Techniques, Dumping credentials from remote system, Credentials Replay, Kerberoasting, Silver ticket, Golden ticket attack

So what is Red Teaming ?

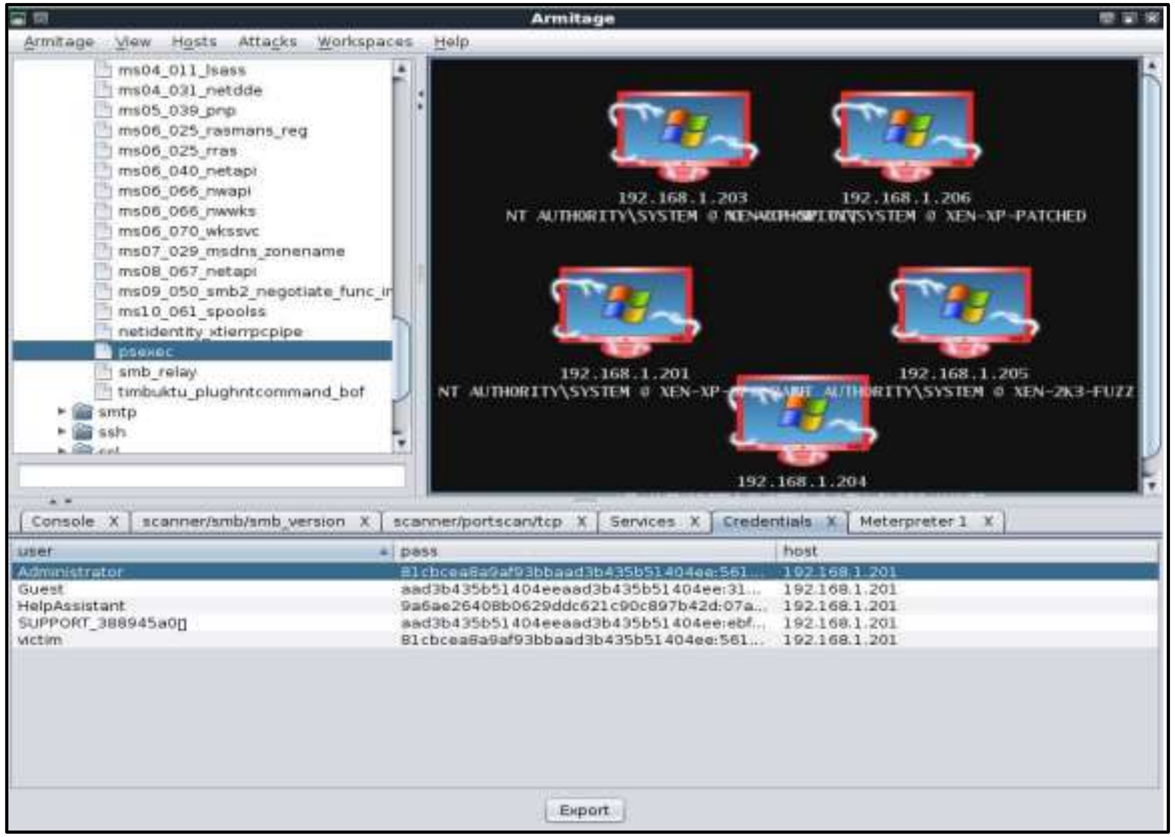
Continued….

Some we have heard –

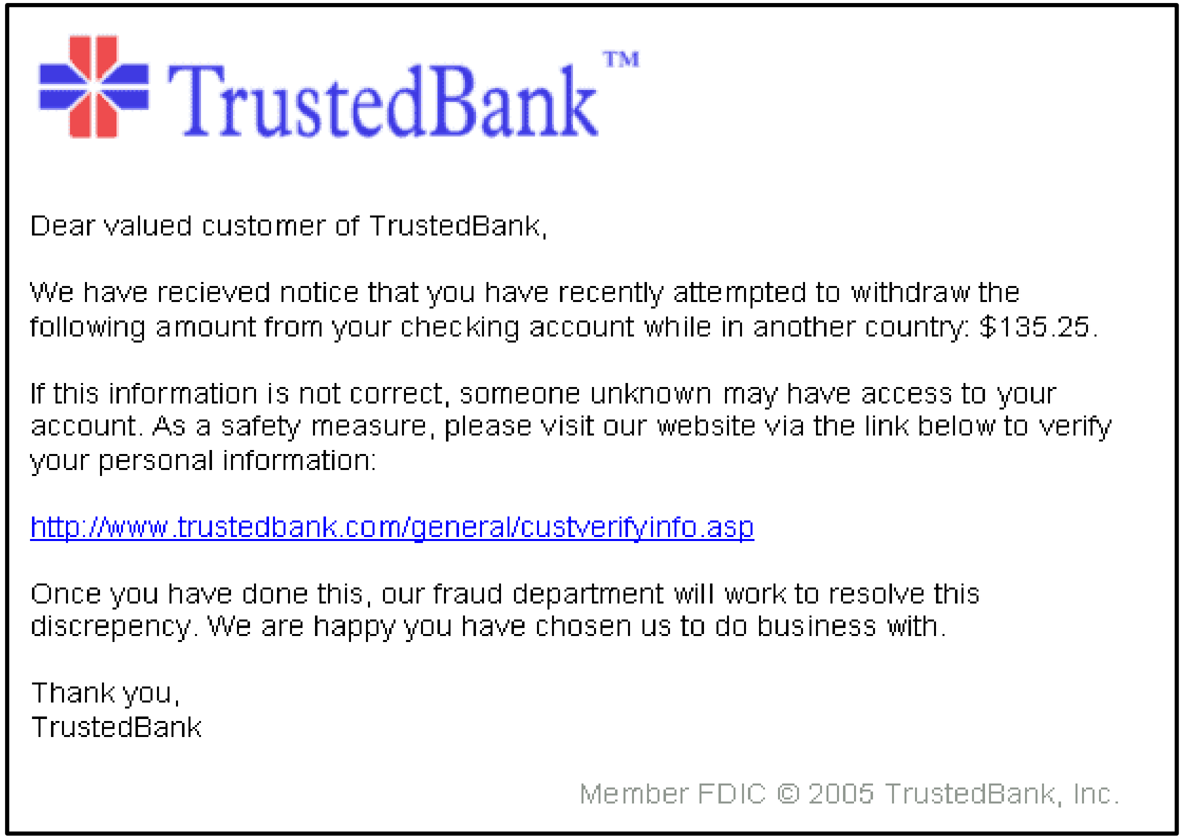
- No-restriction Pen Testing
- No-scope Penetration Testing
- From system to Domain Controller

Our Setup ??

From access to any device in the network to gaining access to Domain Controller



user	pass	host
Administrator	81cbcea8a9af93bbaad3b435b51404ee:561...	192.168.1.201
Guest	aad3b435b51404eeaad3b435b51404ee:31...	192.168.1.201
HelpAssistant	9a6ae26408b0629ddc621c90c897b42d:07a...	192.168.1.201
SUPPORT_388945a0▯	aad3b435b51404eeaad3b435b51404ee:ebf...	192.168.1.201
victim	81cbcea8a9af93bbaad3b435b51404ee:561...	192.168.1.201



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Pentesting vs Red Teaming

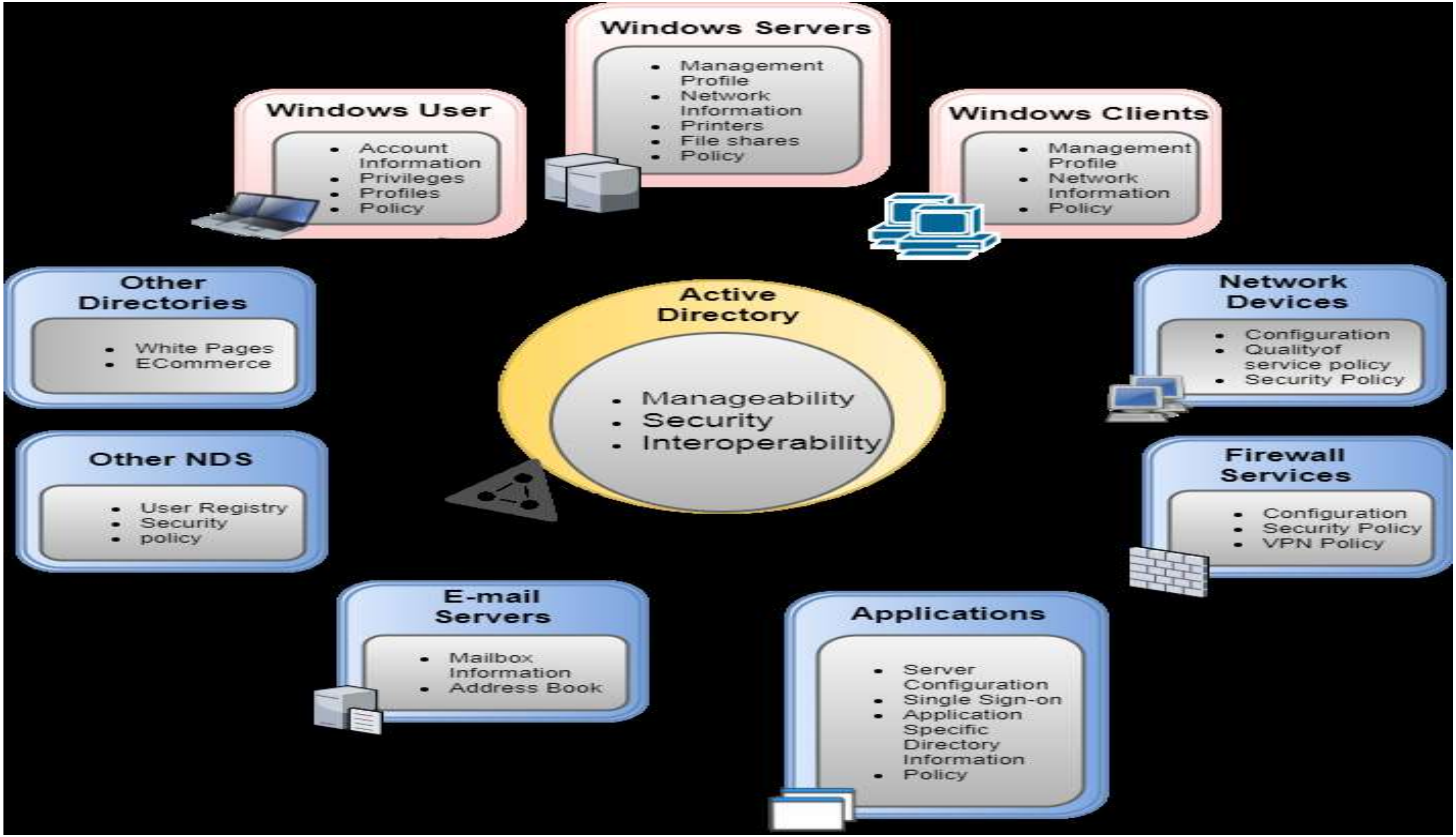
Active Directory Fundamentals

Active Directory

- Directory service which acts as a centralized repository that holds all the data related to users, computers, servers, resources etc. of an organization and it makes administration & management very easy for System administrators

- Enables centralized, secure management of an entire network, which might span a building, a city or multiple locations throughout the world.

- Stores information about objects on the network and makes it easily available to users and admins.



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

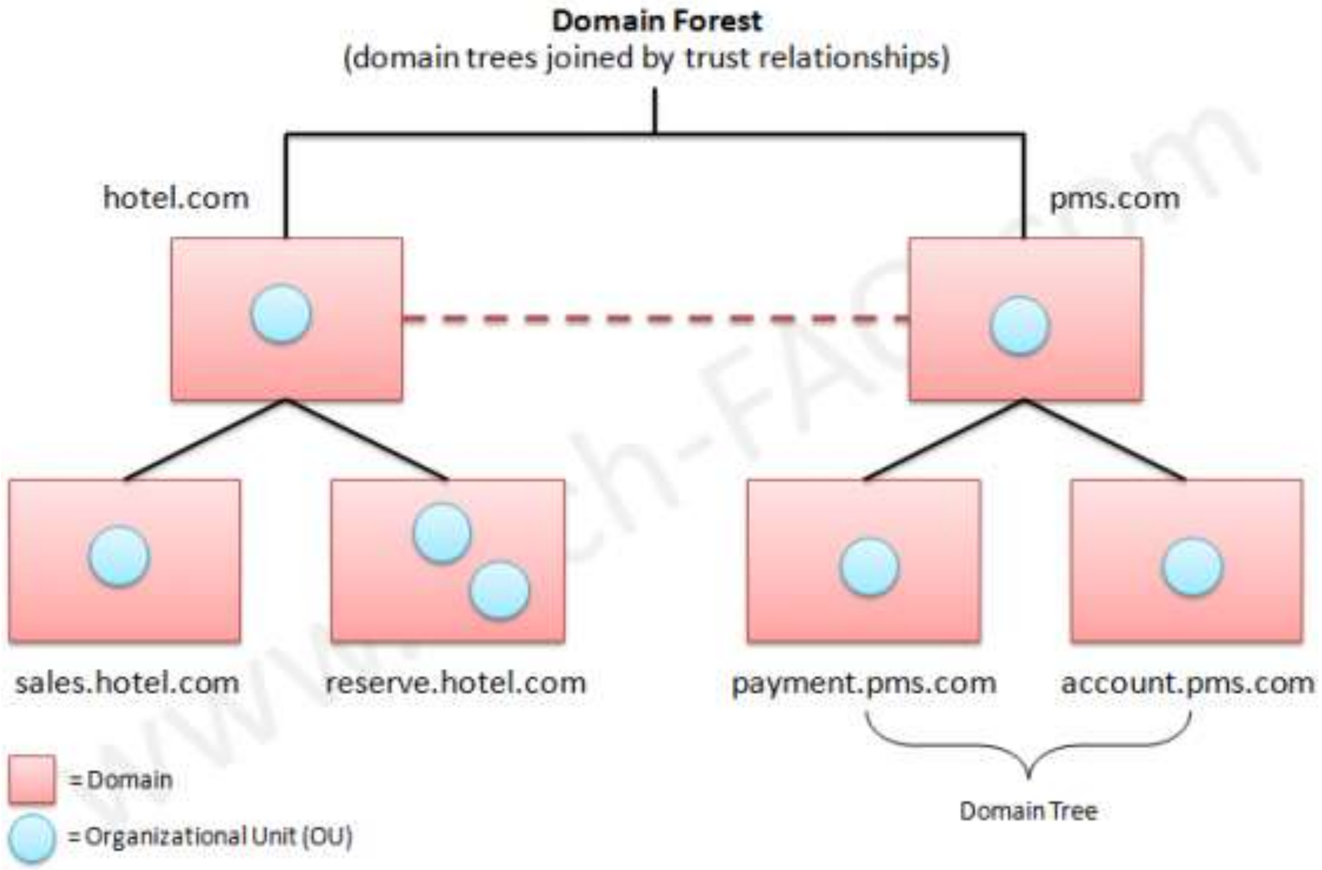
- Configuration
- Security Policy
- VPN Policy

E-mail Servers

- Mailbox Information
- Address Book

Applications

- Server Configuration
- Single Sign-on
- Application Specific Directory Information
- Policy



- OU - An **organizational unit** (**OU**) is a subdivision within an Active Directory into which you can place users, groups, computers, and other organizational unit

- Domain – Represents logical partitions within Active Directory. Domain is always referred to by its unique name and has a proper domain name structure. (hotel.com, sales.hotel.com, pms.com and so on)

- Trees - Collection of one or more domains.

- Forest - Collection of Trees is Forest.

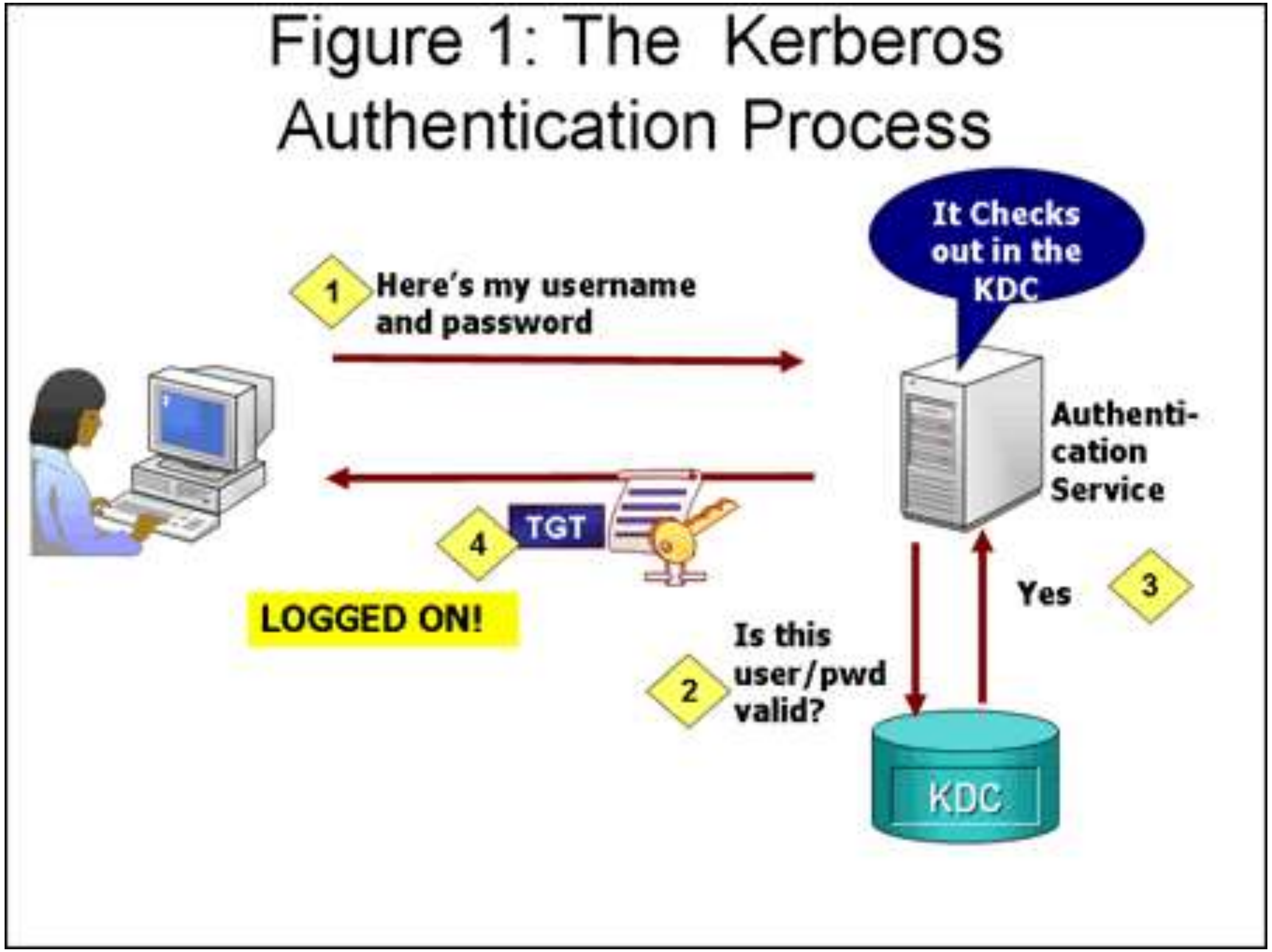
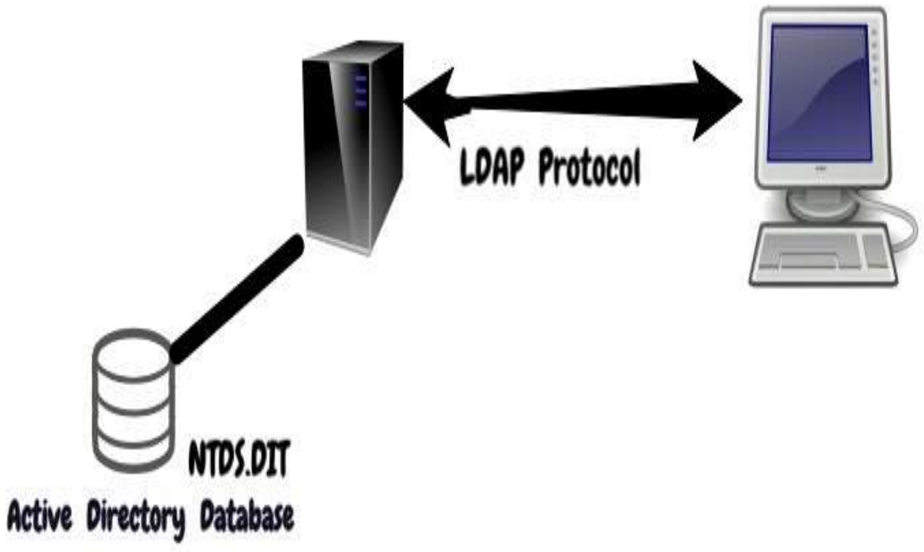


Figure 1: The Kerberos Authentication Process

Active Directory Domain Controller

AD Domain Controllers host the service that authenticates user and computer accounts when they log on to the domain, so all users and computers must connect to AD Domain Service (AD DS) domain controllers when signing into the network



AD Database - The information on user identity, computers, groups, services and resources etc. is stored in Active Directory database which is made up of a single file named **ntds.dit**. By default, it is stored in the %SYSTEMROOT%\NTDS folder.

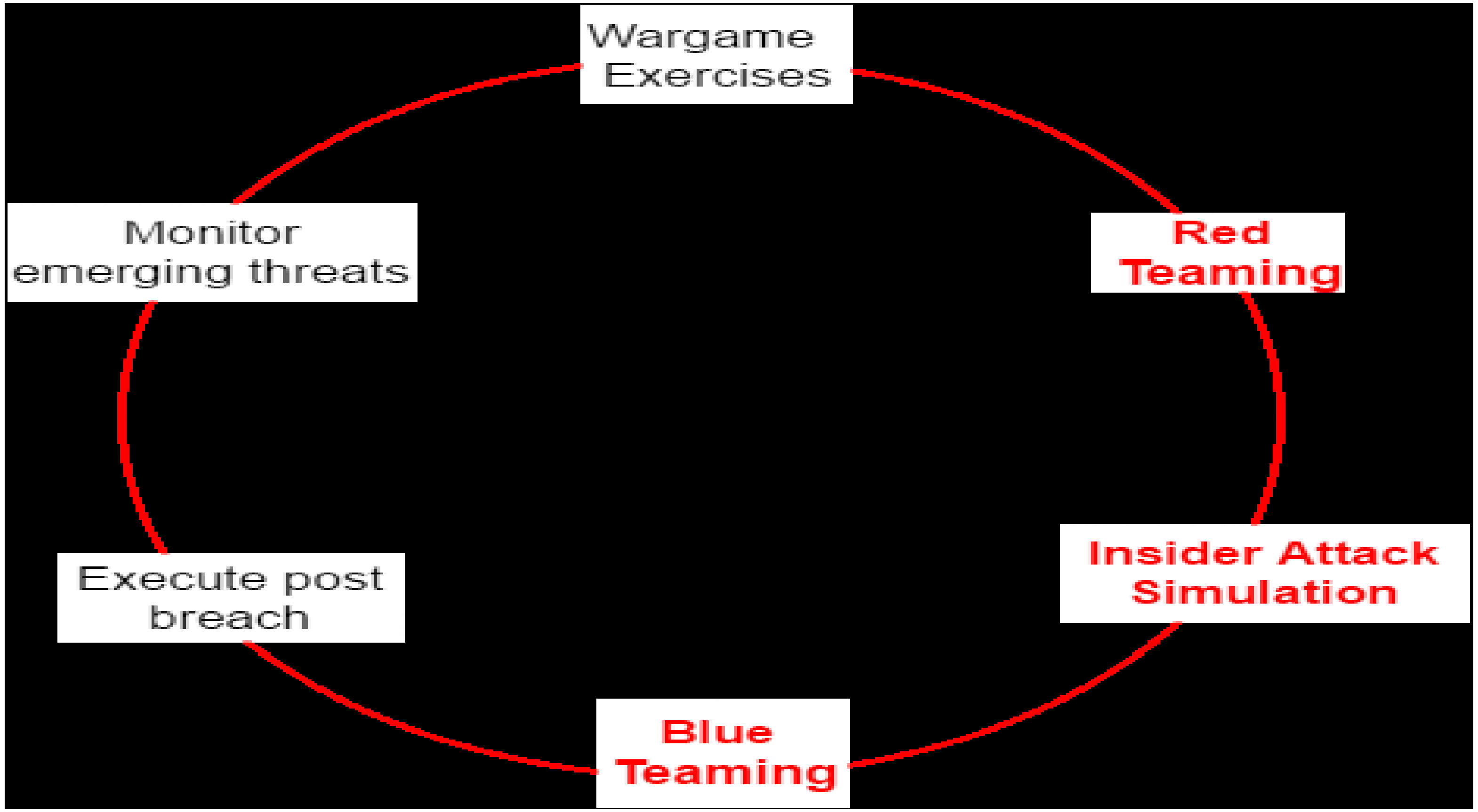
LDAP - LDAP stands for Lightweight Directory Access Protocol. This service is responsible for keeping track of what is on the network.

Kerberos - Kerberos is the services that allows you to use one username and password to log into multiple computers throughout the domain. It basically handles Single Sign On throughout the domain.

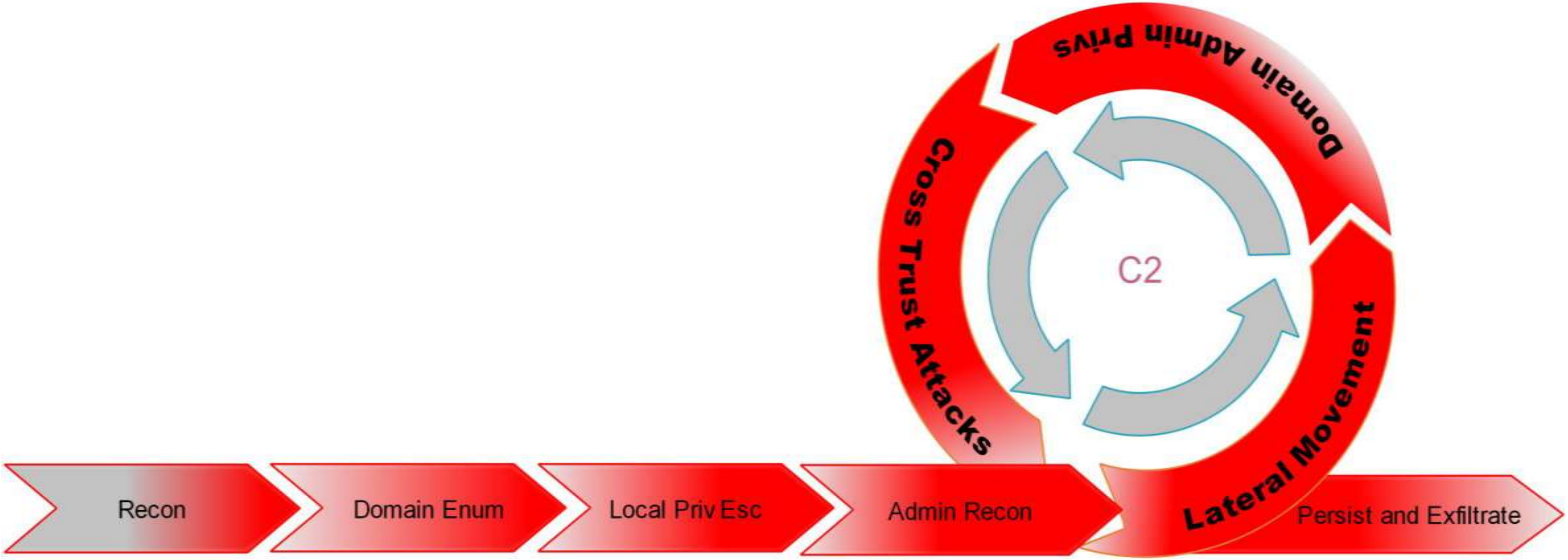
Group Policies - Group Policy is used to define user, security and networking policies at the machine level. Administrators can apply group policies from a centralized location to the whole domain or few computers/users.

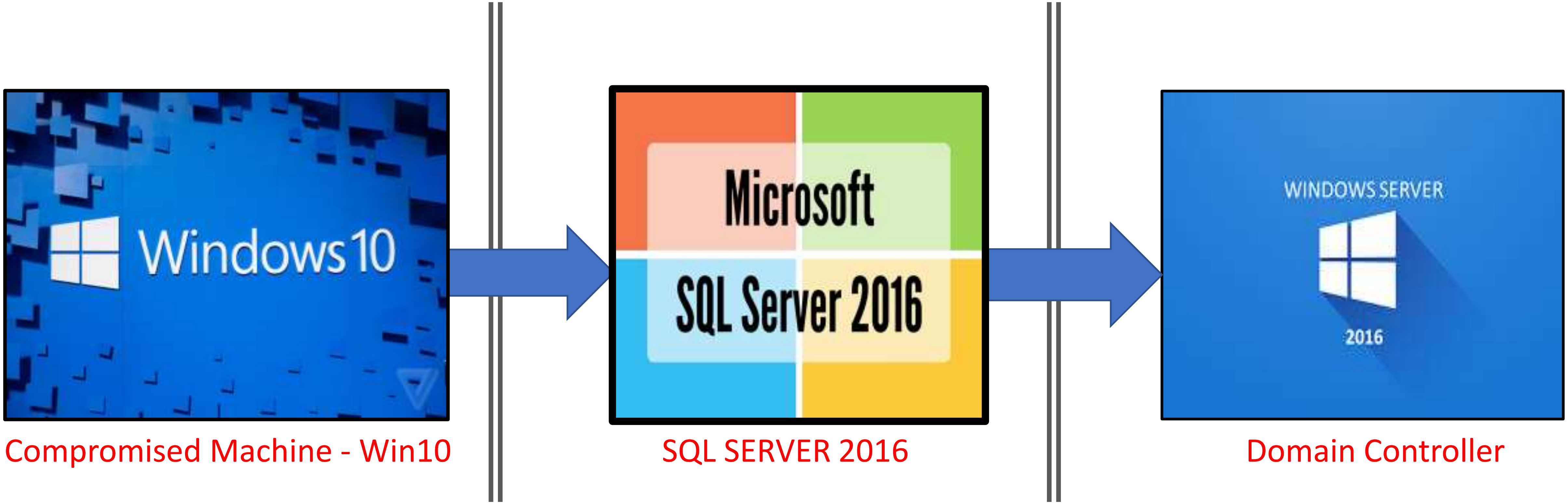
Methodology – Assume Breach

In this class, we are going to use the Assume Breach Methodology on an Active Directory Environment and use internal access available with an adversary to perform further attacks.



Insider Attack Simulation





Compromised Machine - Win10

SQL SERVER 2016

Domain Controller

Lab Setup

Theory and Explanation

- We have 3 machines – Win10, SQL Server 2016 and Win 2016 server.

- Win 2016 server is Domain Controller

- Assumption – Windows 10 has already been compromised by attacker with low privilege shell.

- On Win10 we escalate our privilege to become admin. Through lateral movement, we compromise SQL Server 2016 and then pivot to Domain Controller for gaining domain admin privilege.

Powershell

- What shell script is to Linux, Powershell is to Windows.

- Based on .NET framework and tightly integrated with Windows.

- Has the ability to run completely from memory. Thus, making difficult for blue teamers to detect on their network.

- Powershell script cannot be blocked, they can just be monitored. Also, there are myriads of techniques to bypass powershell restrictions.

- Widely used resources –
  1. Powersploit - https://github.com/PowerShellMafia/PowerSploit
  2. Powershell Empire - https://github.com/EmpireProject/Empire
  3. Nishang - https://github.com/samratashok/nishang

Information Gathering and Privilege Escalation

- Assumption – we already have access to the system.
- Let's enumerate and gather more info about it.
- Manually too much time consuming. Here comes Powerup.ps1 – https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1
- Enumerate and look for following for Windows 10 Machine :
  - **Missing Patches**
  - **Misconfigured Service**
  - **DLL Hijacking**
  - **AlwaysInstallElevated and more…..**
- Attack and become admin of the system. Congratulations, you are admin now!!!
- Manual Exploitation - https://www.fuzzysecurity.com/tutorials/16.html

Domain Enumeration

- Let's start with Domain Enumeration and map various entities, trusts, relationships and privileges for the target domain.

- The enumeration can be done by using Native executables and .NET classes:

```
$ADClass= [System.DirectoryServices.ActiveDirectory.Domain]
$ADClass::GetCurrentDomain()
```

- To speed up things we can use PowerView:

https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1

- Enumerate following for the offensive.local domain :

  - Users

  - Computers

  - Groups

  - Domain Administrators

  - Shares

PowerUpSQL

- MS SQL servers are generally deployed in plenty of Windows Environment/Domain.

- SQL Servers provide very good options for lateral movement as domain users can be mapped to database roles.

- For MSSQL and PowerShell hackery, lets use PowerUpSQL - https://github.com/NetSPI/PowerUpSQL

- Enumerate following for the offensive.local domain :

  - SQLInstances and check the accessibility

  - Gather Information about SQL Instances

  - SQL Server configuration

  - Database Links

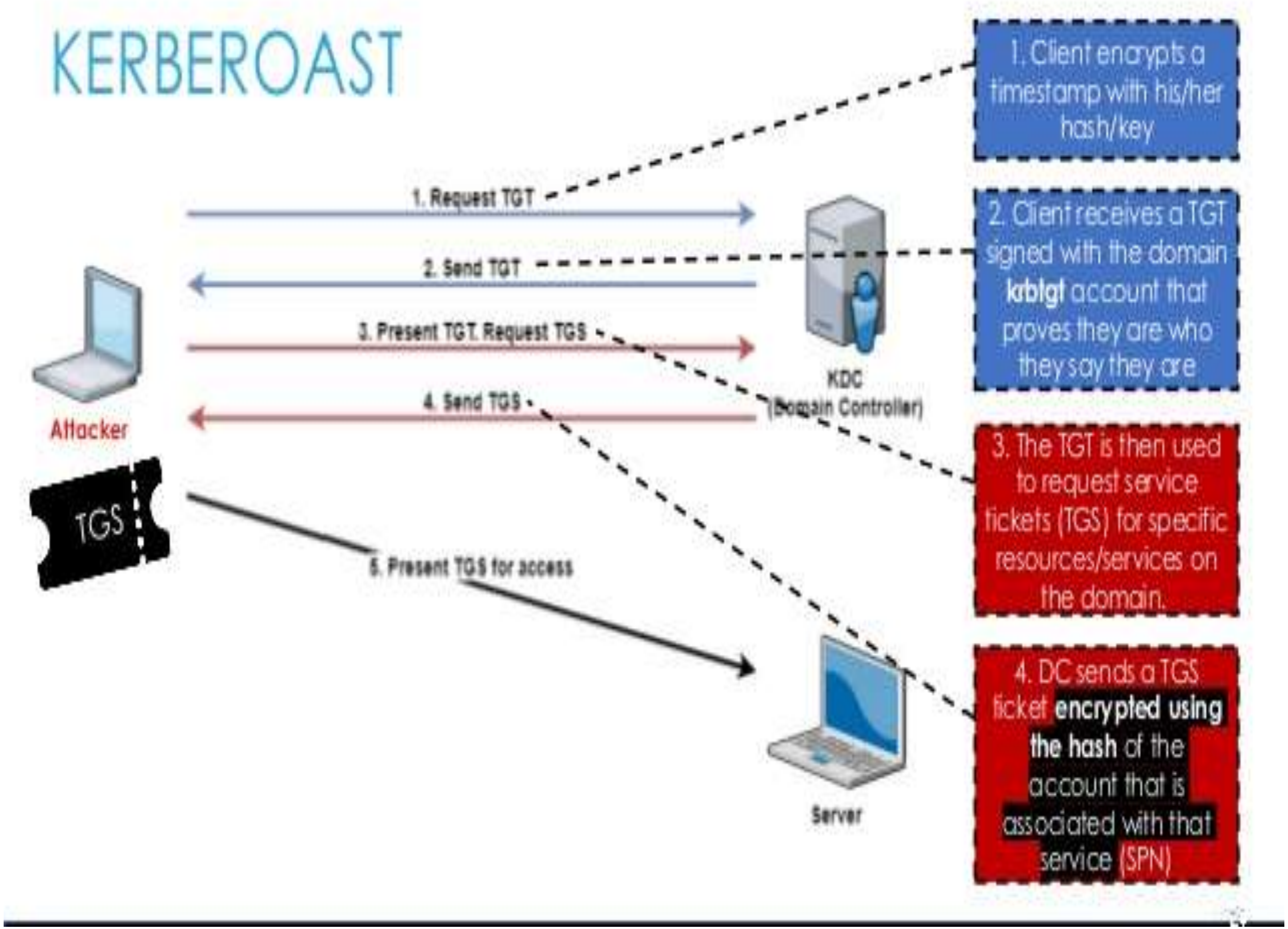
Lateral Movement

- Did you get anything interesting from PowerUpSQL ??

- Obtain reverse shell through HeidiSQL.

- Perform Following Attack :
  - **Run Mimikatz for dumping credentials and hashes**
  - **Over Pass the hash**
  - **Pivot to DC using PowerShell Remoting**
  - **Gaining Domain Admin**
  - **Dumping ntds.dit**

Kerberoasting



KERBEROAST

1. Client encrypts a timestamp with his/her hash/key

2. Client receives a TGT signed with the domain **krbtgt** account that proves they are who they say they are

3. The TGT is then used to request service tickets (TGS) for specific resources/services on the domain.

4. DC sends a TGS ticket **encrypted using the hash** of the account that is associated with that service (SPN)

Silver Ticket Attack

Silver Tickets enable an attacker to create forged service tickets (TGS tickets) that are used to access compromised service accounts.

Parameters to be passed in Mimikatz
Domain Name
Domain SID
Target Host Name
Service Name
NTLM Password Hash of Service Account
User Name
Group Information

- Invoke-Mimikatz-Command'"kerberos::golden /domain:<domain_name> /sid:<domain_sid> /target:<target_hostname> /service:<service_name> /rc4:<NTLM_Hash_Of_Service_Account> /user:<user_name> /id:<group_id> /ptt"'

Golden Ticket Attack

- By obtaining the password hash for the most powerful service account in AD – the KRBTGT account – an attacker is able to compromise every account within AD, giving them unlimited and virtually undetectable access to any system connected to AD.

Parameters to be passed in Mimikatz
KRBTGT account password hash
Domain name
Domain SID
User Name and Group ID (optional)

- Invoke-Mimikatz-Command'"kerberos::golden /domain:<domain_name> /sid:<domain_sid> /rc4:<NTLM_Hash_Of_KRBTGT_Account> /user:<user_name> /id:<group_id> /ptt"'

Defence Against Attacks

Monitoring Powershell

- Enable Module Logging
- Enable Script block Logging
- Enable Transcription logging

Dumping Ntds.dit folder

- The best way to mitigate the risks of a successful attack against your Ntds.dit file is to limit the number of users who can log onto Domain Controllers.
- If possible, monitoring and alerting software that can detect and/or prevent users from extracting files from Volume Shadow Copies should also be leveraged to reduce the attack surface.

Defence Against Attacks

Kerberoasting:

- Ensure your service accounts that use Kerberos with SPN values leverage long and complex passwords.If possible, rotate those passwords regularly.
- Service accounts traditionally should be used from the same systems in the same ways, so it is possible to detect authentication anomalies.
- Monitor for service ticket requests in Active Directory to look for spikes in those requests.

Silver Ticket:

- Enforce proper security over service accounts to avoid having these accounts compromised to begin with
- Monitoring for logon anomalies using local logon events.

Golden Ticket

- The most important protection against golden tickets is to restrict domain controller logon rights. There should be the absolute minimum number of Domain Admins, as well as members of other groups that provide logon rights to DCs such as Print and Server Operators.
- In addition, a tiered logon protocol should be used to prevent Domain Admins from logging on to servers and workstations where their password hashes can be dumped from memory and used to access a DC to extract the KRBTGT account hash.

References

- https://www.slideshare.net/CTruncer/pen-testing-red-teaming-and-more
- https://scriptdotsh.com/
- http://www.tech-faq.com/tree-and-forest-in-active-directory.html
- https://www.pentesteracademy.com/activedirectorylab
- https://image.slidesharecdn.com/carlosgarcia-slides-180312234839/95/carlos-garca-pentesting-active-directory-rooted2018-39-638.jpg?cb=1520899303
- https://attack.stealthbits.com/