Active Directory

DNOSCP | NULL VILLUPURAM | 12/06/2022

Hello!

I am Dhanesh Sivasamy

- Offensive Security Certified Professional (OSCP)
- 4+ Yrs. in Information Security
- Acknowledged by Oracle
- Expertise in Application Security
- Student @ AURCC
- Analyst at Aujas Cybersecurity

“Opportunity does not waste time with those who are unprepared.

1.What is AD ?

Introduction to Active Directory

Active Directory

- Directory Service that makes the stored information available to everyone on the network
- Benefits Network Administrators
- Easy to audit
- Available locally and in cloud

Use Case

Active Directories and Cloud AD’s are widely adopted across the organizations for easy access and control of the users

Active Directory (Contd..,)

Users

- Multiple users accessing files across multiple systems

Computers

- When a computer is suspcted as compromised, detech it form the server

Groups

- Managing and providing certain permissions for certain group members (Interns, Employees, Managers, BoD..,)

Active Directory Heirarchy

Forest → College

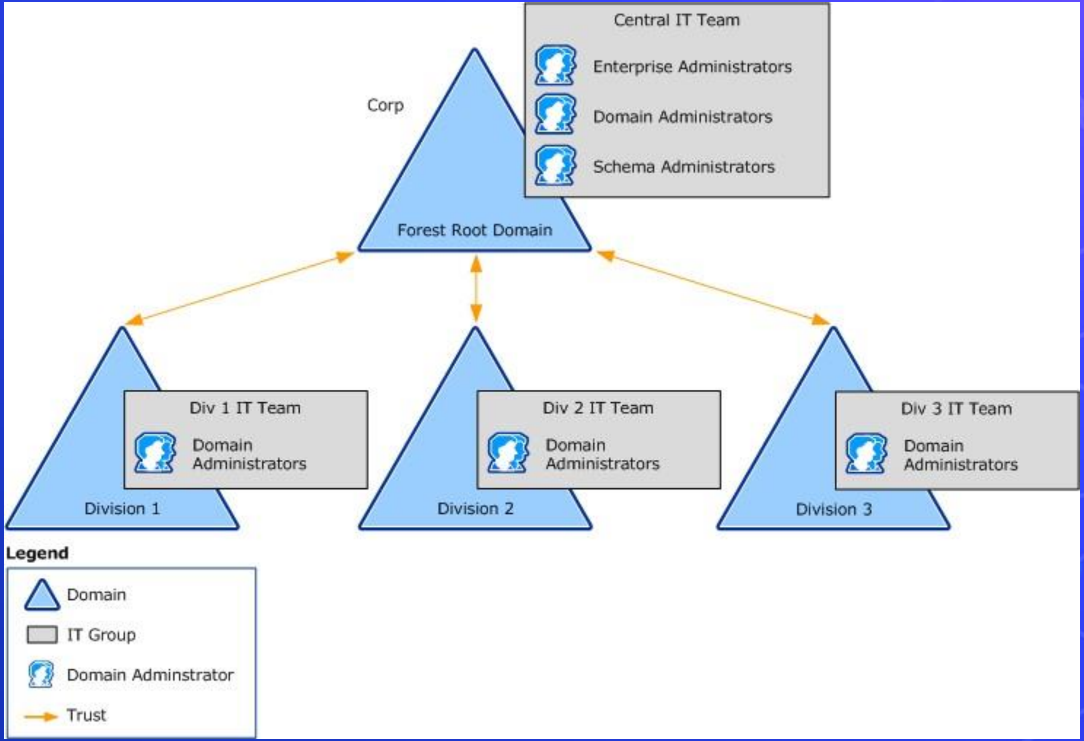
Domains → Departments

Domain Controllers → HoD's

OU's → Staffs and Students

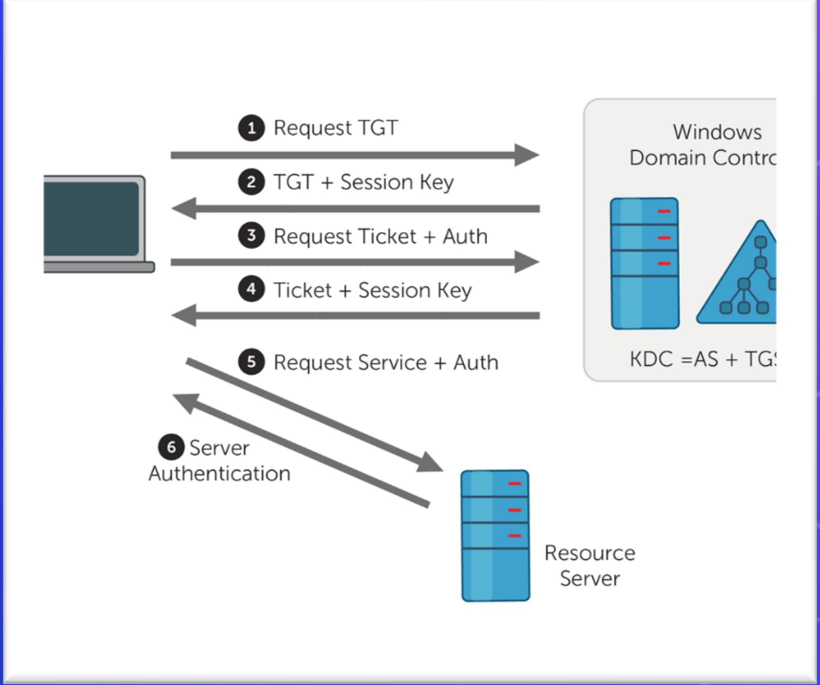
- Forest is a collection of Domains
- Each domains have Domain Controller
- The objects in domains are referred as Organizational Units

Active Directory Hierarchy (Contd..,)

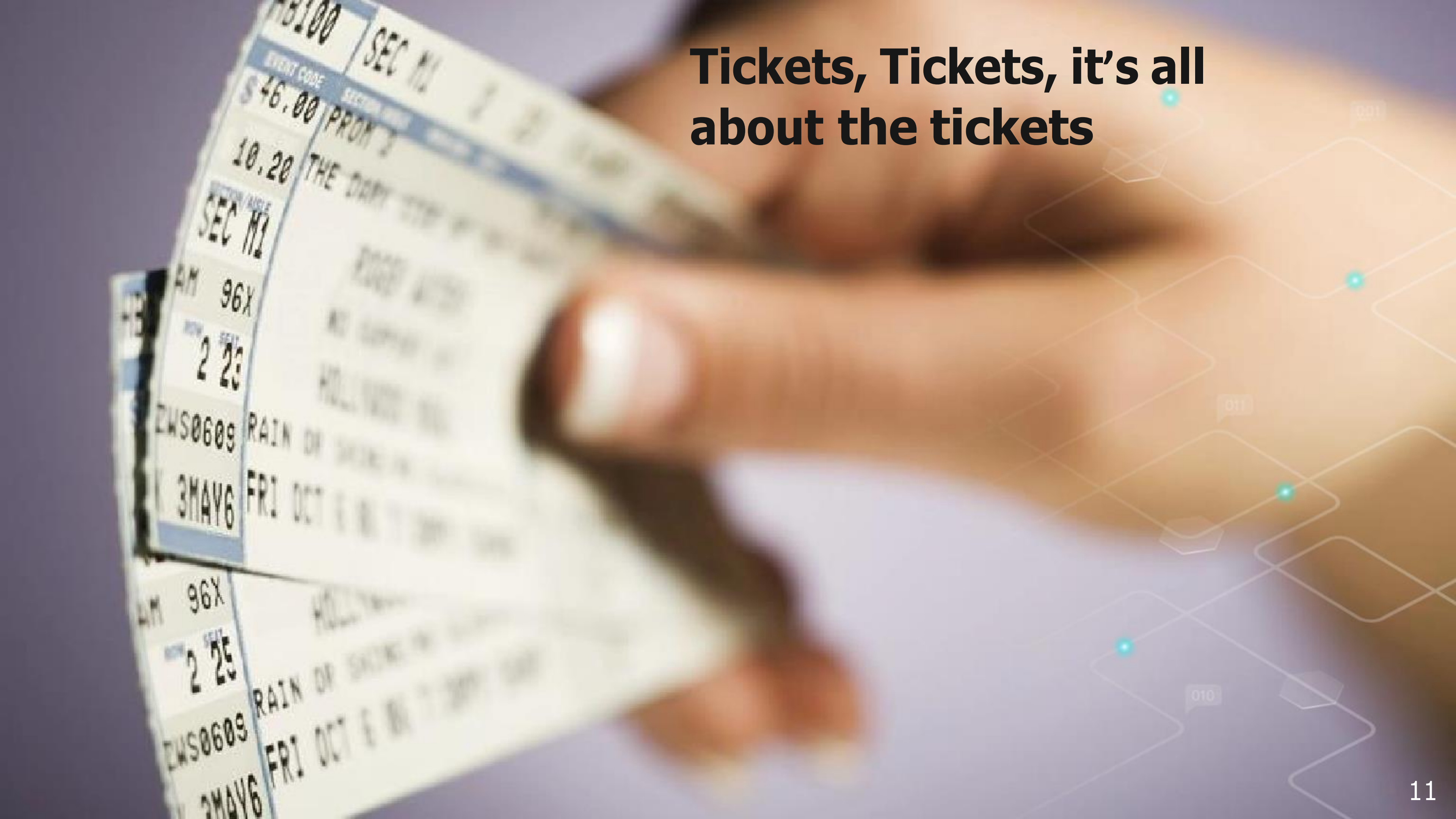


AD Authentication

- Uses Kerberos Protocol to authenticate users
- Same as web but password encrypted tickets instead of cookies



Tickets, Tickets, it’s all about the tickets



Authentication Process

- The user sends the time stamp encrypted with his / her password to the domain controller
- The domain controller decrypts the encrypted request and checks the timestamp, if it’s same the DC responds with a Ticket-Granting-Ticket (TGT) which is also encrypted by the user’s password

Authentication Process (Contd..,)

- With the TGT, the user requests for access for a service from the DC
- The DC provides the Ticket-Granting-Service to the user which he will use it to access the service
- When accessing the service, the user can just present the TGS ticket obtained from the DC and use it

2. Common AD Attacks

For OSCP and CTF’s

Attack Types

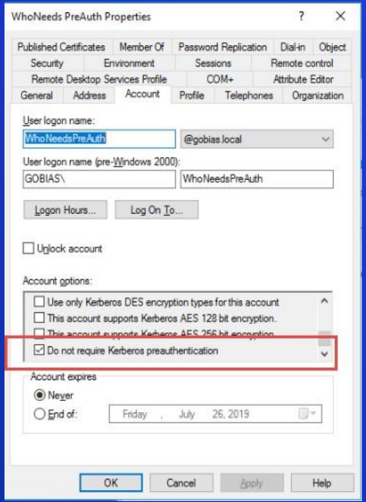
- ASREP Roasting
- Kerberoasting
- Silver and Golden Ticket attacks

ASResproasting

- ASResproasting occurs in the first two stages of the Kerberos authentication
- The attacker will send a request to the DC requesting a TGT for a user
- The Domain Controller (*when DONOTRequire Kerberos PreAuth* is disabled*)* will provide the TGT to the attacker
- Which can be cracked offline to obtain the password of the user

ASResproasting

- CANNOT BE FOUND IN PRODUCTION SERVERS
- Only in CTFS and in OSCP exams



WhoNeeds PreAuth Properties

User logon name: WhoNeedsPreAuth @gobias.local

User logon name (pre-Windows 2000): GOBIAS\ WhoNeedsPreAuth

□ Unlock account

Account options:

□ Use only Kerberos DES encryption types for this account
□ This account supports Kerberos AES 128 bit encryption.
□ This account supports Kerberos AES 256 bit encryption.
☑ Do not require Kerberos preauthentication

Account expires

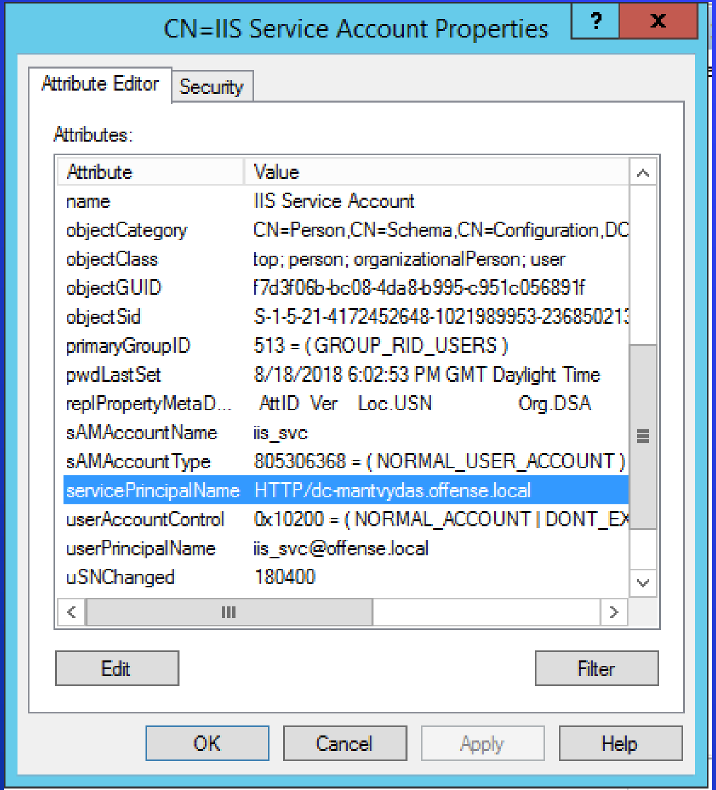
● Never
○ End of: Friday , July 26, 2019

```
Get-ADUser -Identity “sky.tate" | SetADAccountControl -
DoesNotRequirePreAuth:$true
```

Kerbroasting

- Abuses the Service Principal Name of active directory
- SPNs are used by Kerberos to associate a service instance with a service logon account which allows a client application to authenticate the resource
- In this attack, the attacker requests the DC to get the password hashes of the accounts with ServicePrincipleNames

Kerbroasting



Attributes:

Attribute	Value
name	IIS Service Account
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC
objectClass	top; person; organizationalPerson; user
objectGUID	f7d3f06b-bc08-4da8-b995-c951c056891f
objectSid	S-1-5-21-4172452648-1021989953-23685021
primaryGroupID	513 = (GROUP_RID_USERS)
pwdLastSet	8/18/2018 6:02:53 PM GMT Daylight Time
replPropertyMetaD...	AttID Ver Loc.USN Org.DSA
sAMAccountName	iis_svc
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT)
servicePrincipalName	HTTP/dc-mantvydas.offense.local
userAccountControl	0x10200 = (NORMAL_ACCOUNT | DONT_EX
userPrincipalName	iis_svc@offense.local
uSNChanged	180400

```
Set-ADUser -Identity "jon.snow" -
ServicePrincipalNames
@{Add='HTTP/thewallserver'}
```

Ticket Attacks

- Golden Ticket Attack
- Silver Ticket Attack

Golden Ticket Attacks

- Forged with the *krbtgt* account’s hash
- Once gained game over
- Provides persisting on a domain with access to EVERYTHING!

```
kerberos::golden /admin:ADMIINACCOUNTNAME /domain:DOMAINFQDN /id:ACCOUNTRID
/sid:DOMAINSID /krbtgt:KRBTGTPASSWORDHASH /ptt
```

Silver Ticket Attacks

- Forged with the service accounts hash
- Allows attacker to access any service on a domain

```
kerberos::golden /admin:LukeSkywalker /id:1106 /domain:lab.adsecurity.org
/sid:S-1-5-21-1473643419-774954089-2222329127
/target:adsmswin2k8r2.lab.adsecurity.org /rc4:d7e2b80507ea074ad59f152a1ba20458
/service:cifs /ptt
```

Lab Setup

Hands on AD lab setup

Thank You