Advanced Windows Security Course for 2019: Module 3 - Advanced Attacks on Active Directory

Krystian Zieja
CQURE: Systems Architect and Solutions Expert
CQURE Academy: Trainer
krystian@cqure.pl
www.cqureacademy.com

CQURE CONSULTING

CQURE ACADEMY

@CQUREAcademy

Module 3:
Advanced Attacks on Active Directory

CQURE CONSULTING

CQURE ACADEMY

@CQUREAcademy

Active Directory: Fundamentals

- Data stored within Active Directory is presented to the user in a hierarchical fashion similar to the way data is stored in a filesystem.

- Each entry is referred to as an *object*

- We have two types of objects: containers and non-containers (aka leaf nodes)

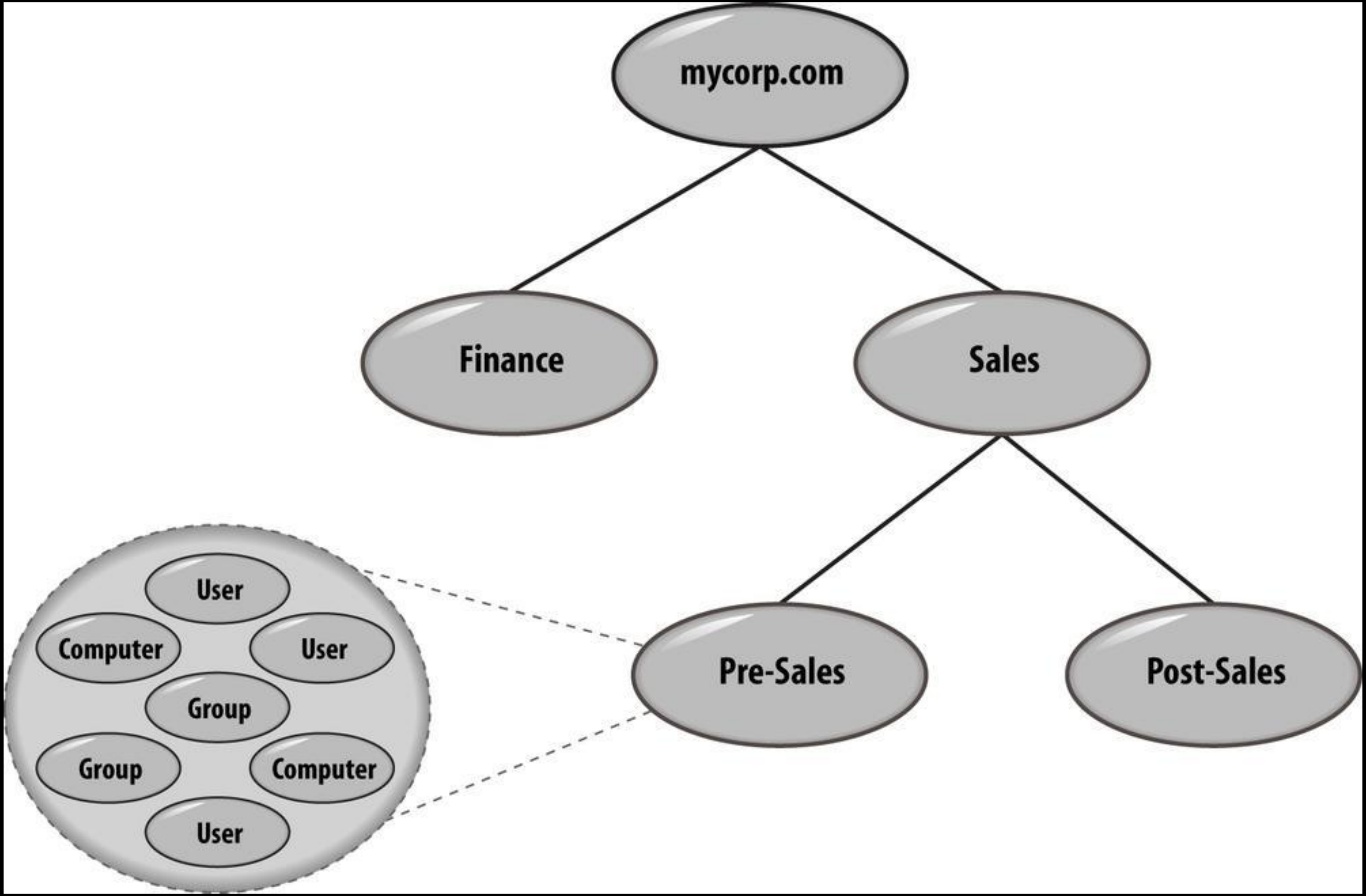
- Containers can contain other objects, while leaf nodes cannot

Active Directory: Fundamentals

- Although the data in Active Directory is presented hierarchically, it is actually stored in flat database rows and columns.

- The directory information tree (DIT) file is an Extensible Storage Engine (ESE) database file.

Active Directory: Fundamentals



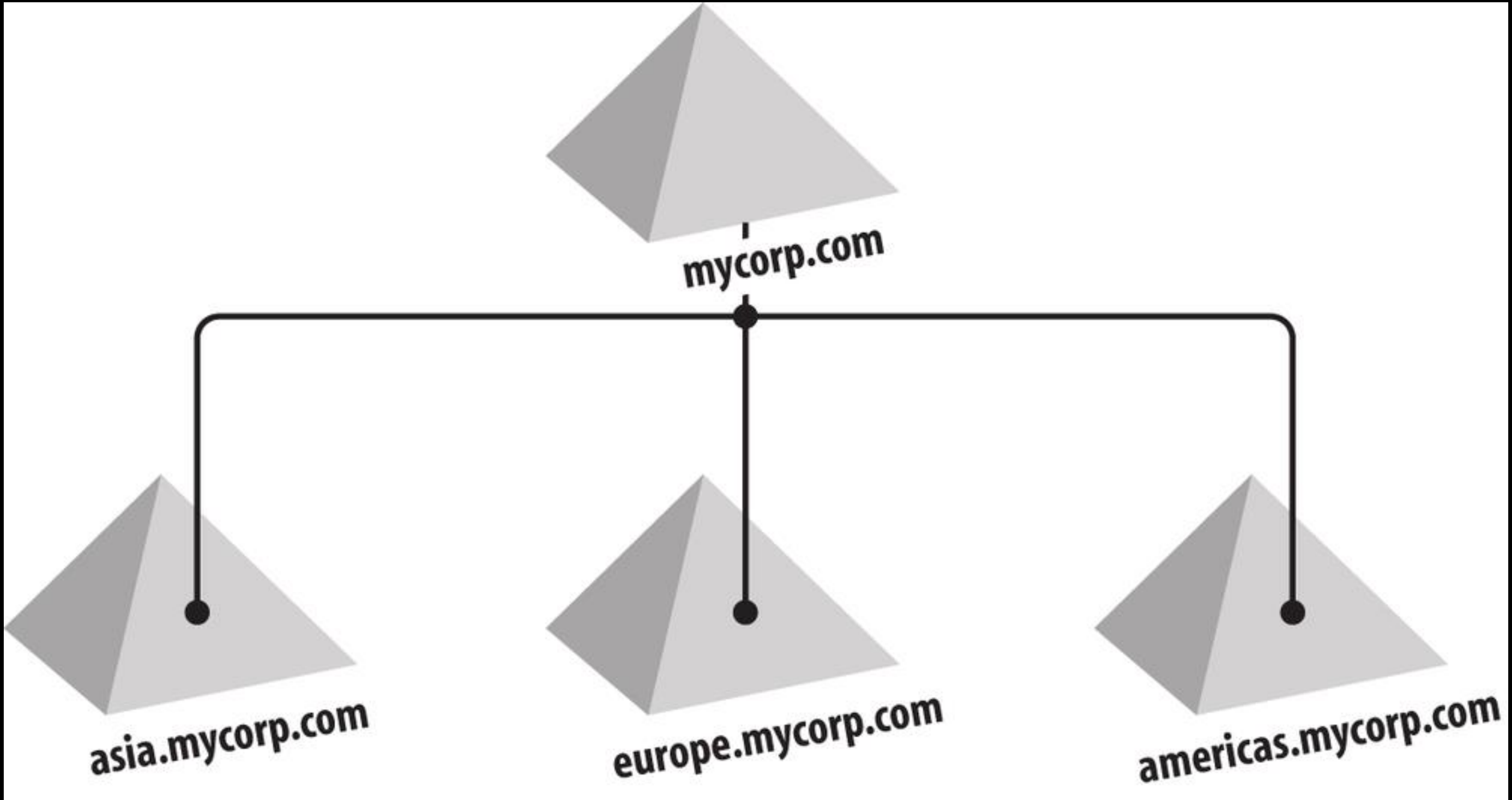
Active Directory: Fundamentals

- Objects have a globally unique identifier (GUID) assigned to them by the system at creation
- The object's GUID stays with the object until it is deleted, regardless of whether it is renamed or moved within the directory information tree (DIT).
- The object's GUID will also be preserved if you move an object between domains within a multidomain forest.
- Distinguished names represent hierarchical path in Active Directory - cn=John Doe, ou=Employees,dc=cqure,dc=lab

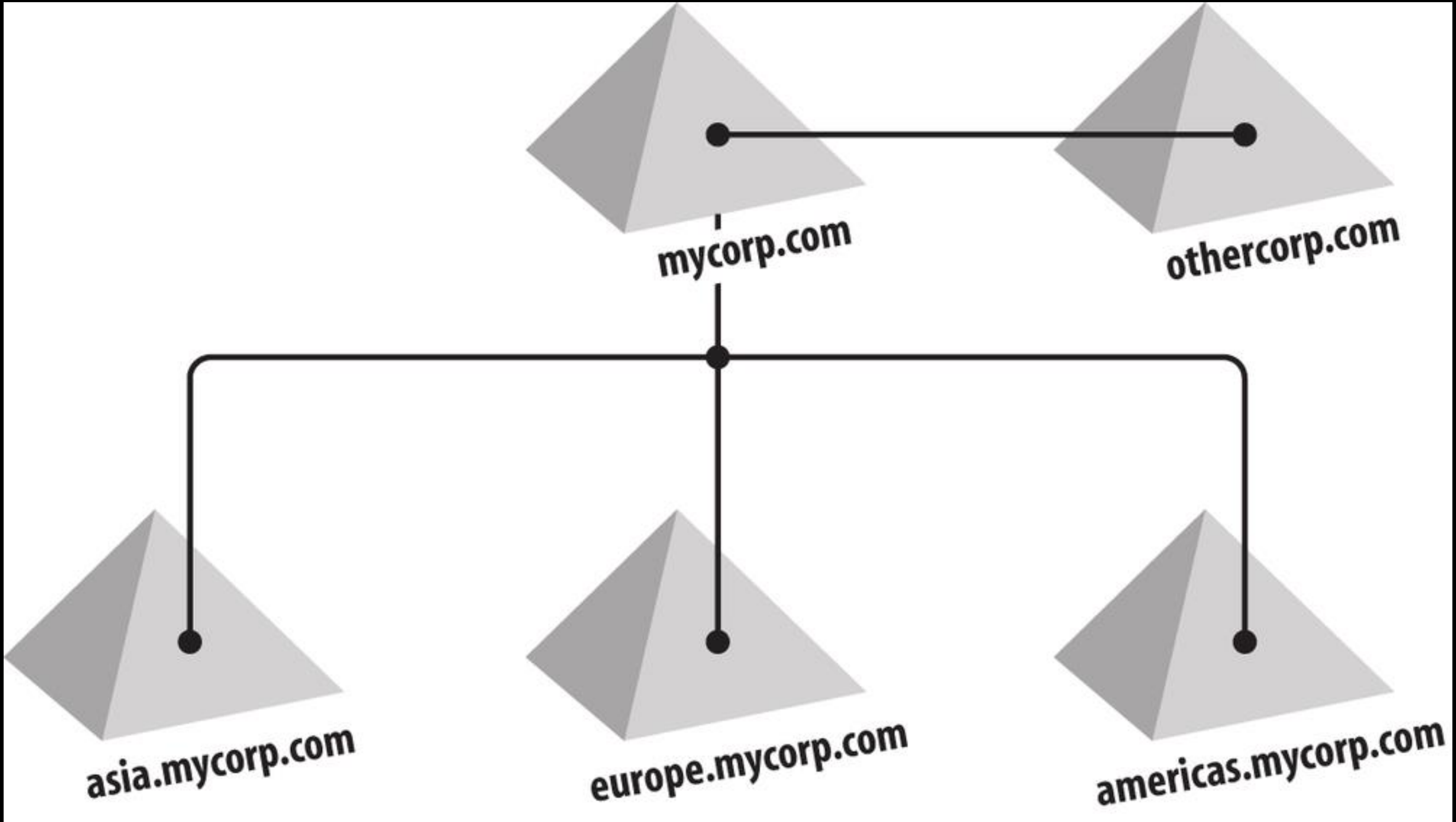
Active Directory: Fundamentals

- Active Directory's logical structure is built around the concept of domains. Each domain is build from:
- An X.500-based hierarchical structure of containers and objects
- A DNS domain name as a unique identifier
- A security service, which authenticates and authorizes any access to resources via accounts in the domain or trusts with other domains
- Policies that dictate how functionality is restricted for users or machines within that domain

Active Directory: Fundamentals



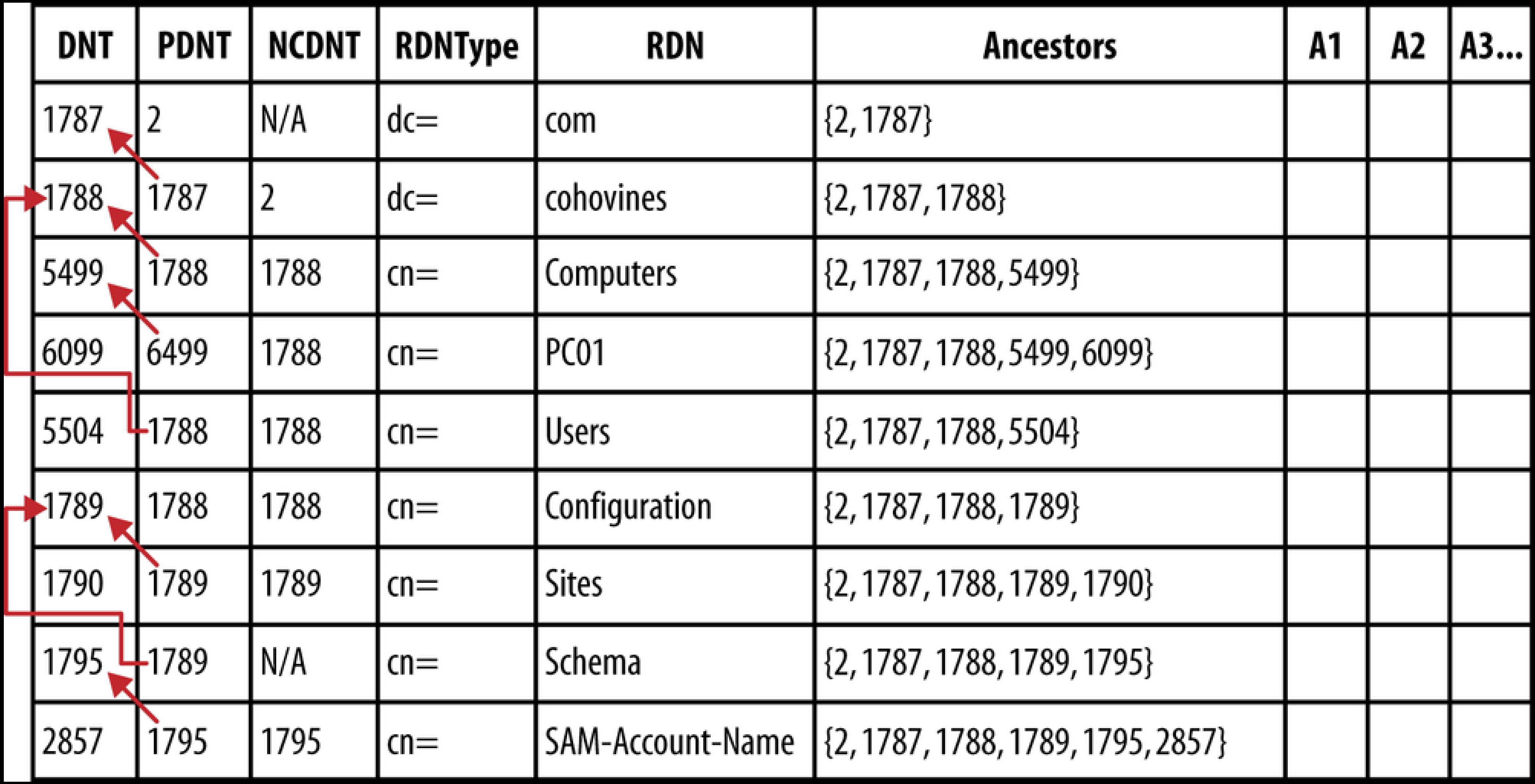
Active Directory: Fundamentals



Active Directory: Database

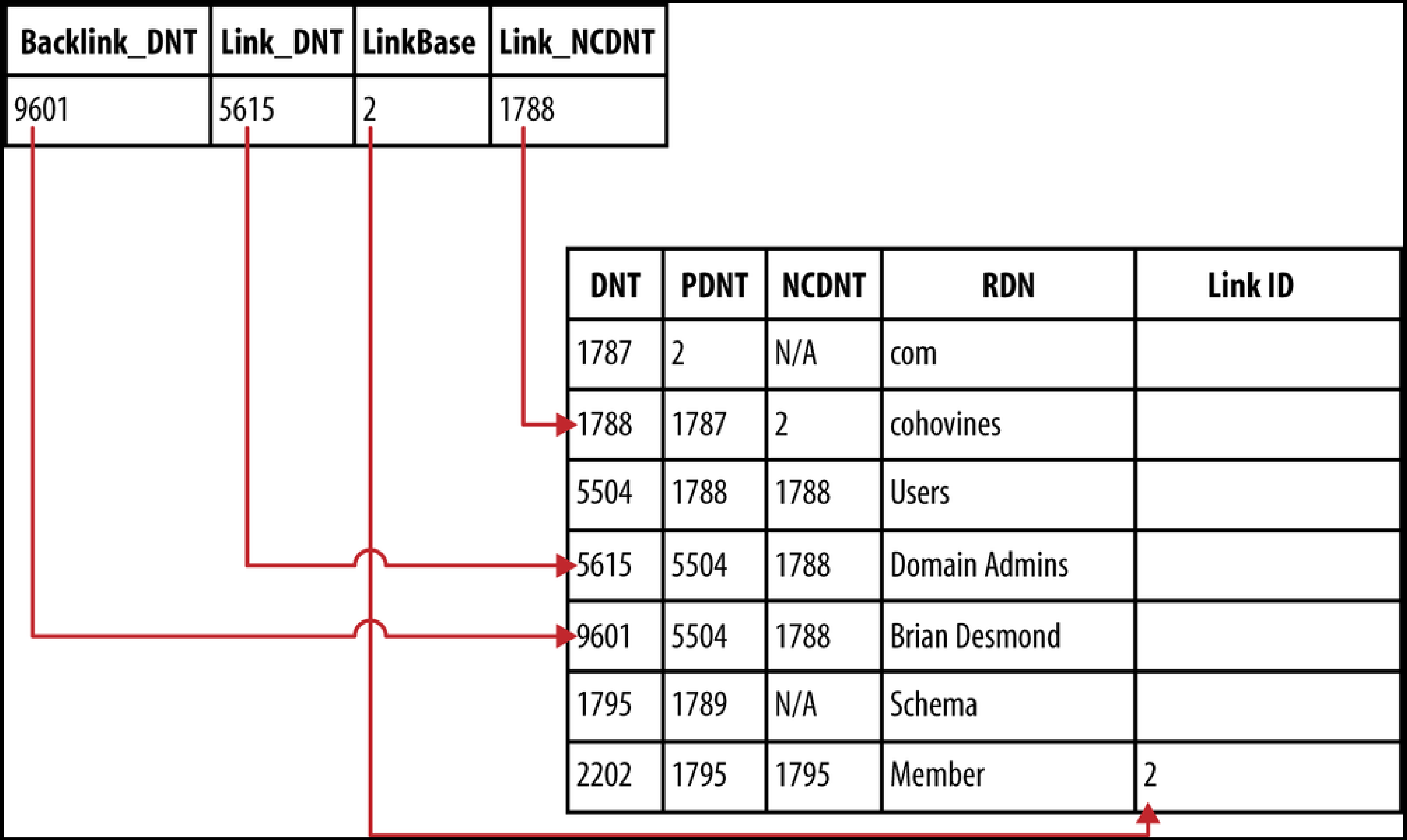
- Active Directory stores its database on each domain controller in the *ntds.dit* file
- DIT – Directory Information Tree
- Key tables in DIT are:
  - Data Table
  - Link Table
  - Hidden Table
  - Security Descriptor Table

Active Directory: Data Table



DNT	PDNT	NCDNT	RDNType	RDN	Ancestors	A1	A2	A3...
1787	2	N/A	dc=	com	{2,1787}			
1788	1787	2	dc=	cohovines	{2,1787,1788}			
5499	1788	1788	cn=	Computers	{2,1787,1788,5499}			
6099	6499	1788	cn=	PC01	{2,1787,1788,5499,6099}			
5504	1788	1788	cn=	Users	{2,1787,1788,5504}			
1789	1788	1788	cn=	Configuration	{2,1787,1788,1789}			
1790	1789	1789	cn=	Sites	{2,1787,1788,1789,1790}			
1795	1789	N/A	cn=	Schema	{2,1787,1788,1789,1795}			
2857	1795	1795	cn=	SAM-Account-Name	{2,1787,1788,1789,1795,2857}			

Active Directory: Link Table



Backlink_DNT	Link_DNT	LinkBase	Link_NCDNT
9601	5615	2	1788

DNT	PDNT	NCDNT	RDN	Link ID
1787	2	N/A	com	
1788	1787	2	cohovines	
5504	1788	1788	Users	
5615	5504	1788	Domain Admins	
9601	5504	1788	Brian Desmond	
1795	1789	N/A	Schema	
2202	1795	1795	Member	2

First phase: The reconnaissance

- People are concerned about giving out information about AD
- How many of them really checks what is accessible to every user in AD by default
- Every Windows system also contains a bunch of tools that can help us
- Using built-in tools is beneficial because it makes our endeavors more stealthy

The reconnaissance: WMI

- Retrieve user accounts with Win32_UserAccount
- With a simple query we can retrieve all accounts from AD with some information like:
  - Username
  - SID
  - Password Expires
  - Lockout account

The reconnaissance: LDAP

- Retrieve information about AD structure
- Almost undetectable
- Easy to construct your own set of queries

The reconnaissance: LDAP Filters and Booleans

Operator	Description
=	Equal
<=	Less than or equal to
>=	Grater than or equal to
!	Not

Operator	Description
&	And
|	Or
>=	Grater than or equal to
!	Not

The reconnaissance: SAMR

- Standard protocol for performing operations in Active Directory
- Built-in tools available on every workstation – NET commands
- Can be used in reconnaissance but also later

The reconnaissance: NLTEST

- Available on all machines
- Get a list of domain controllers
- Get Domain Trusts
- and more …

The reconnaissance: AD Explorer

- Part of Sys Internals toolkit

- Signed by MS

- Get Domain Trusts

- and more …

Demo

- Combining everything in to get initial information about AD

The reconnaissance: AD Explorer

- Part of Sys Internals toolkit
- Signed by MS
- Get Domain Trusts
- and more …

Assess AD Security: PingCastle

- Quickly asses the security of AD
- Find something worth attacking
- Map AD environment
- Helpful for Red and Blue Team

Assess AD Security: PingCastle

Staled Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	ACL Check	Old trust protocol	Backup
Network topography	Admin control	SID Filtering	Certificate take over
Object configuration	Irreversible change	SIDHistory	Golden ticket
Obsolete OS	Privilege control	Trust impermeability	Local group vulnerability
Old authentication protocols		Trust inactive	Network sniffing
Provisioning			Pass-the-credential
Replication			Password retrieval
Unfinished migration			Reconnaissance
Vulnerability management			Temporary admins
			Weak password

BloodHound: Unintended relationships

- BloodHound uses graph theory to reveal the hidden and relationships within an Active Directory
- Attackers can use BloodHound to easily identify highly complex attack paths
- Defenders can use BloodHound to identify and eliminate those same attack paths
- Gain a deeper understanding of privilege relationships

TODAY'S SECURITY CHALLENGE

PASS THE HASH ATTACKS

Access to one device can lead to access to many

1.

Single IT Pro's machine is compromised

IT Pro manages kiosks/shared devices on network

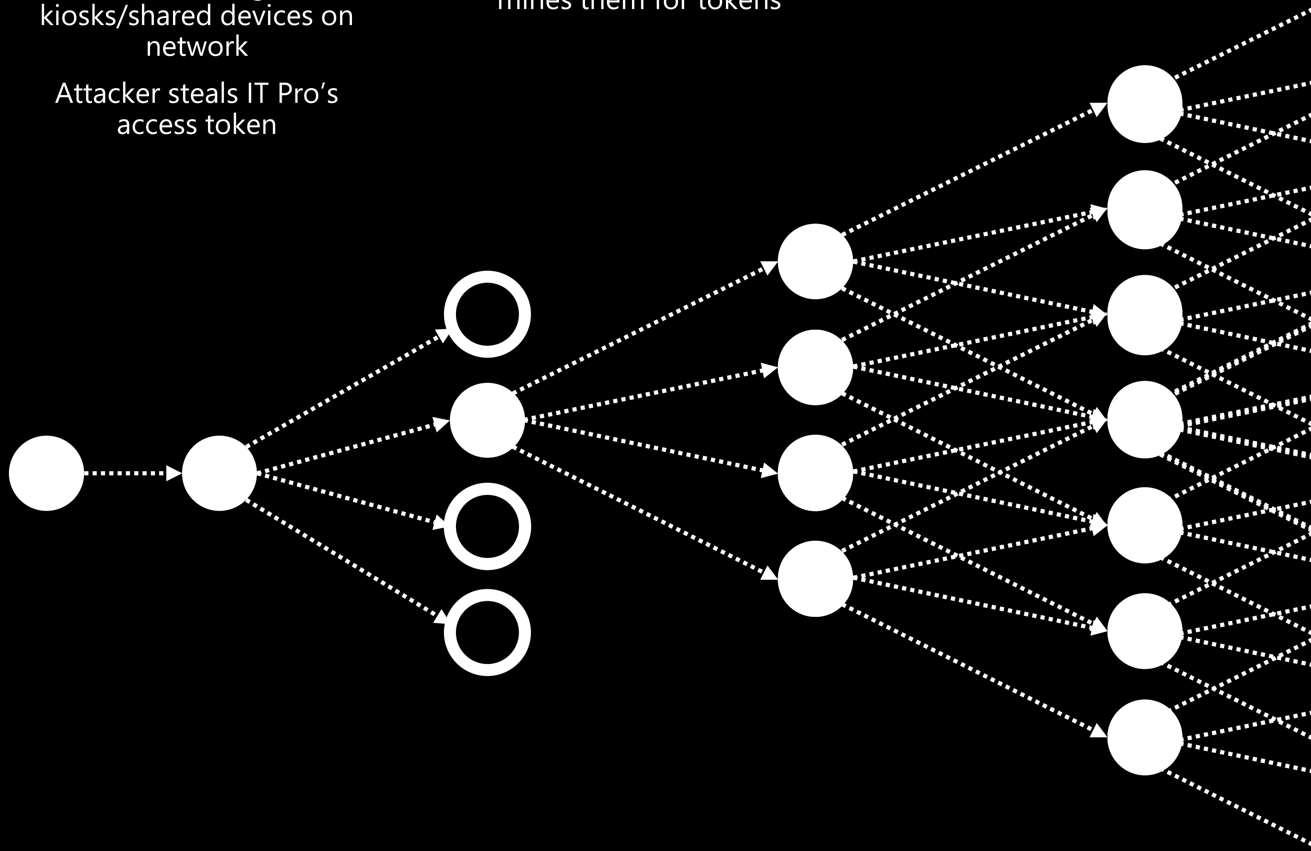
Attacker steals IT Pro's access token

2.

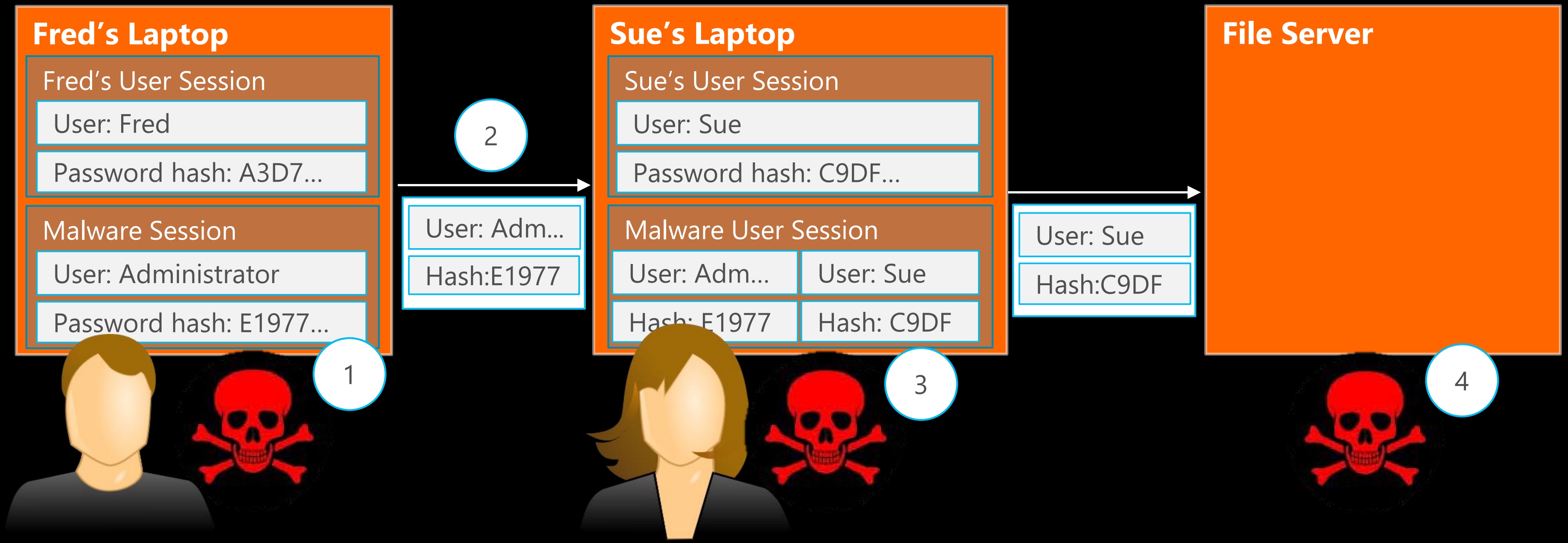
Using IT Pros access token attacker looks for kiosk/shared devices and mines them for tokens

3.

Repeat



Pass-The-Hash Technique



1. Fred runs malware, he is a Local Administrator
2. There is a Pass the Hash
3. Malware infects Sue's laptop
4. Malware infects File Server

Attack on a ticket: Kerberosting

- No admin rights required
- Relays on Kerberos protocol
- Once ticket is generated it can be taken away
- and crack at leisure of your home ☺

Abusing delegation flow

- Use information gathered by PingCastle, BloodHound, custom scripts
- Get access to user/s account with the path to Domain Admins
- Attack!!!
- In some cases you can use one more neat trick – after performing an attack reset the password back

Pass the Ticket and Golden Ticket

- Passing the ticket works on the same principal as PtH
- But there are also ….
- Golden Tickets
- and they are so much better ☺

Pass the Ticket and Golden Ticket

- Passing the ticket works on the same principal as PtH
- But there are also ….
- Golden Tickets
- and they are so much better ☺

Golden Ticket

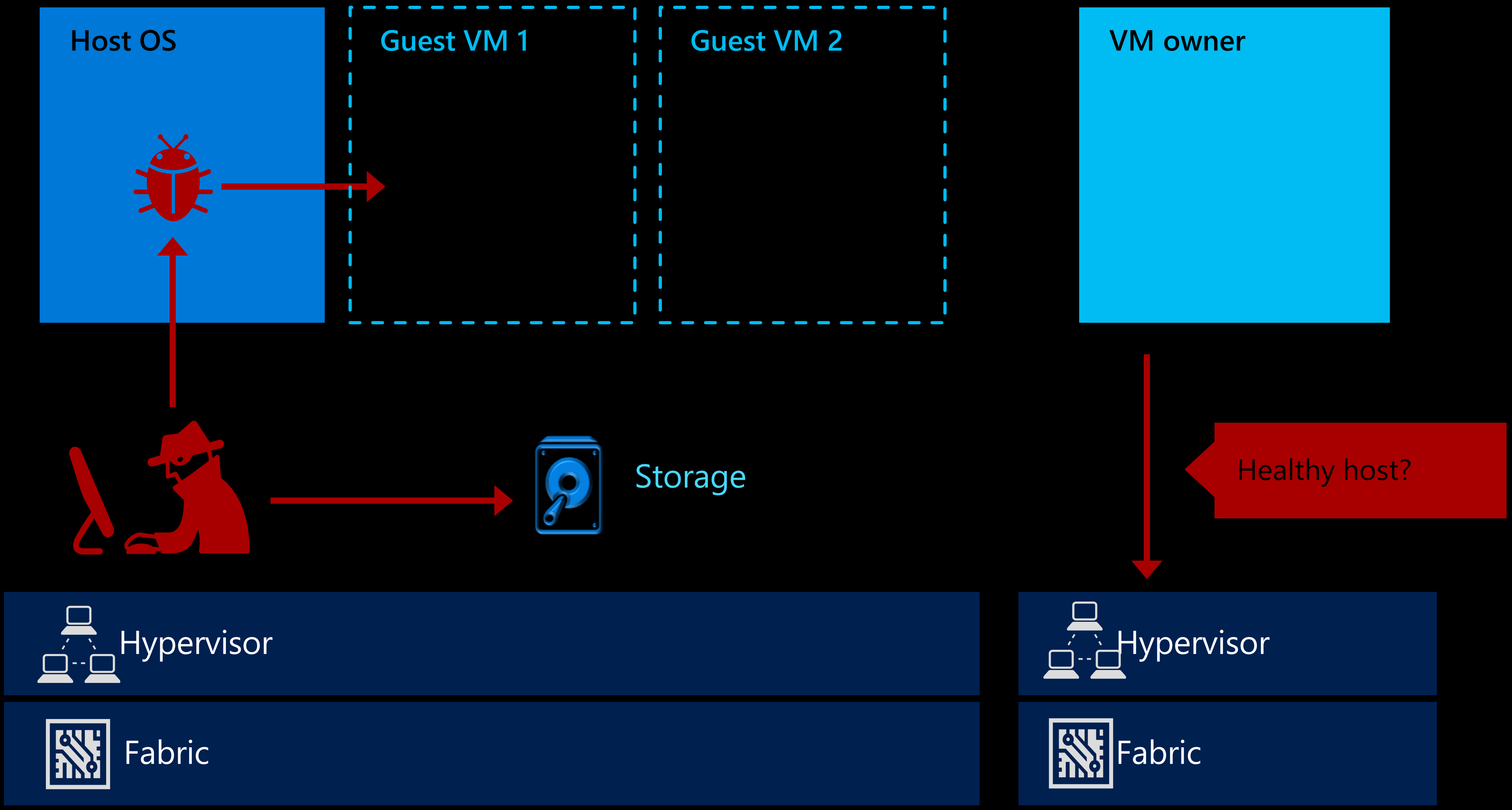
- Valid for your lifetime (default is 10 years)
- You do not need to be admin to generate it
- Can be exported and you can re-use it
- Very hard to detect
- One known defense is reset krbtgt account password twice

Golden Ticket – why it works?

- Leverages the lack of validation on the Kerberos authentication protocol in order to impersonate a particular user valid or invalid

- This is due to the fact that users that have a TGT (ticket granting ticket) in their current session will consider trusted for Kerberos and therefore can access any resource in the network.

Attack Vectors – Virtualization Fabric



QUESTIONS?

Thank You!

If you have questions email us at
info@cqureacademy.com

You can also chat us up on the page
https://cqureacademy.com/

Advanced Windows Security Course for 2019: Module 3 - Advanced Attacks on Active Directory

Krystian Zieja

CQURE: Systems Architect and Solutions Expert

CQURE Academy: Trainer

krystian@cqure.pl

www.cqureacademy.com

CQURE CONSULTING

CQURE ACADEMY

@CQUREAcademy