Active Directory Penetration Testing

Cheatsheet

DEFINITION

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. Penetration testing AD is crucial for identifying and mitigating security vulnerabilities.

RELATIONSHIP BETWEEN AD COMPONENTS

Forest

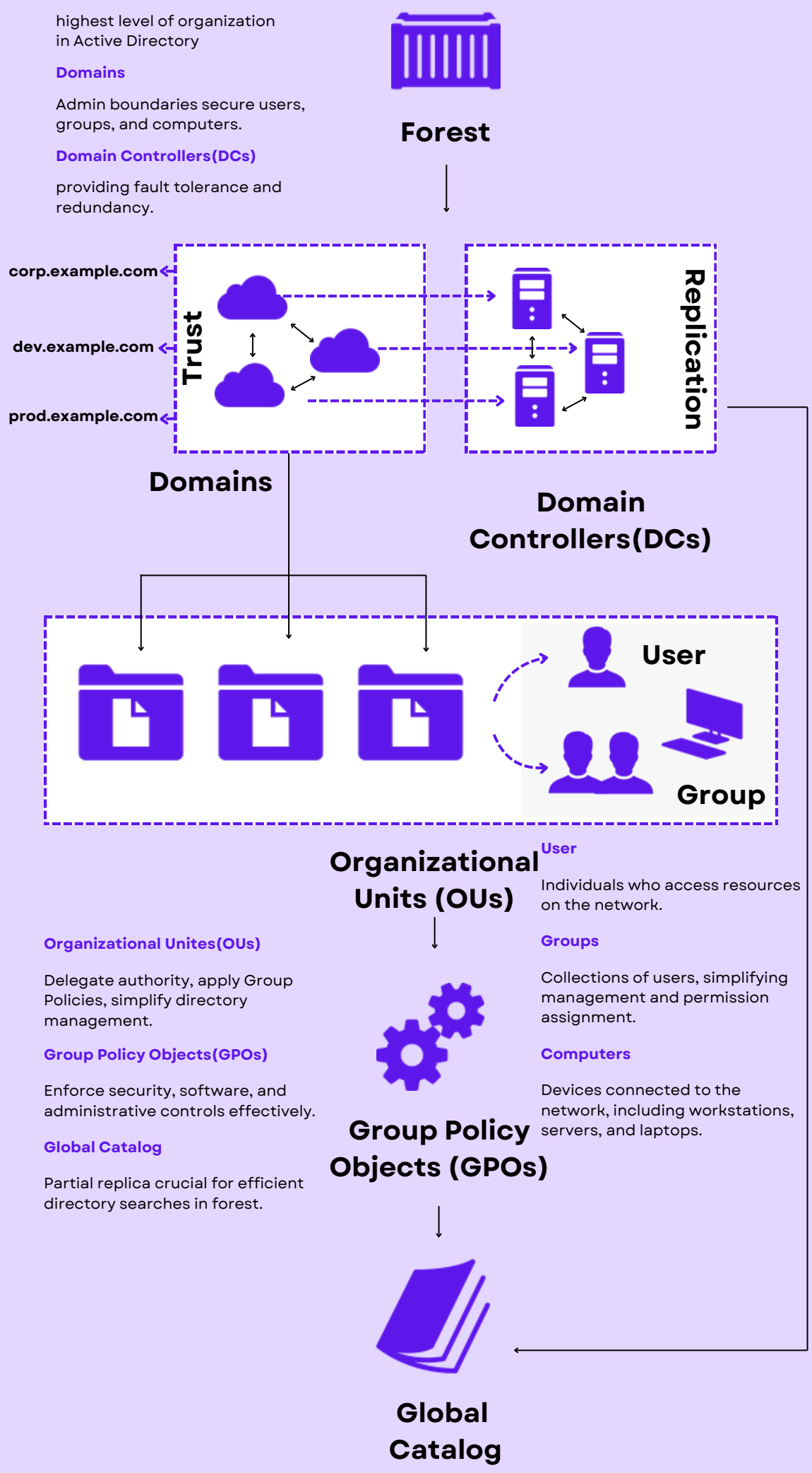
highest level of organization in Active Directory

Domains

Admin boundaries secure users, groups, and computers.

Domain Controllers(DCs)

providing fault tolerance and redundancy.



User

Individuals who access resources on the network.

Organizational Unites(OUs)

Delegate authority, apply Group Policies, simplify directory management.

Groups

Collections of users, simplifying management and permission assignment.

Group Policy Objects(GPOs)

Enforce security, software, and administrative controls effectively.

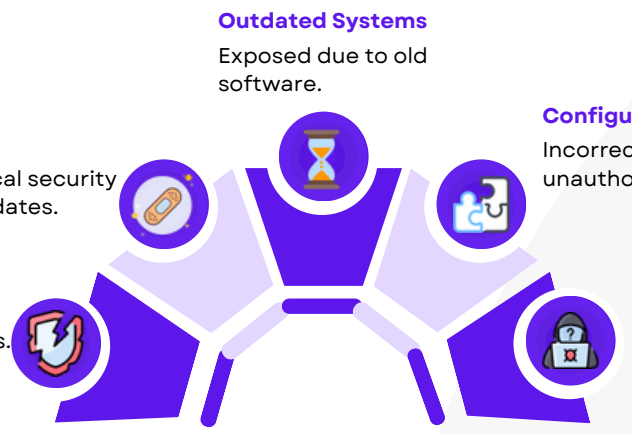
Computers

Devices connected to the network, including workstations, servers, and laptops.

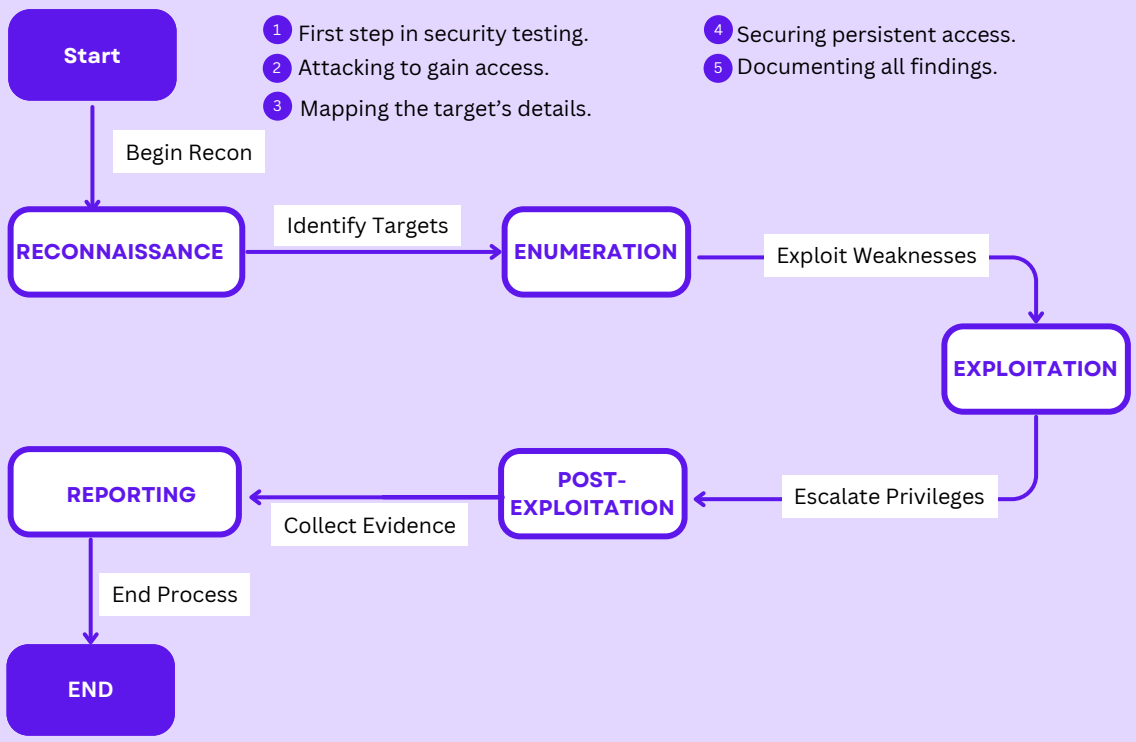
Global Catalog

Partial replica crucial for efficient directory searches in forest.

COMMON VULNERABILITIES



PENETRATION TESTING METHODOLOGIES



COMMAND SNIPPETS

POWERVIEW COMMANDS

Get domain computers	`Get-NetComputer -fulldata`
Find domain shares	`Invoke-ShareFinder -Verbose`
Enumerate domain users	`Get-NetUser | select cn`

IMPACKET COMMANDS

Get group members	`Get-NetGroupMember -GroupName "Domain Admins"`
Get user information	`Get-UserProperty -Properties pwdlastset`
List Kerberos tickets	`klist`

BLOODHOUND COMMANDS

Run BloodHound	`Invoke-BloodHound -CollectionMethod All`
Generate list of all domain admins	`Get-BloodHoundData -DomainAdmins`

WINDOWS COMMANDS

List local users	`net user`
View network connections	`netstat -ano`

MITIGATION STRATEGIES

SECURITY RISK ASSESSMENTS

Evaluate vulnerabilities and potential risks

INFORMATION SECURITY POLICIES

Develop strong, enforceable security guidelines

TRAINING AND AWARENESS

Educate staff on security practices

REGULAR PENETRATION ASSESSMENTS

Continuously test for system weaknesses

VULNERABILITY ASSESSMENTS

Identify and address security gaps

PERIMETER PROTECTION

Implement firewalls, intrusion detection systems

DNS SECURITY EXTENSIONS

Protect against DNS spoofing attacks

REGULAR SECURITY AUDITS

Identify weaknesses, enforce security controls