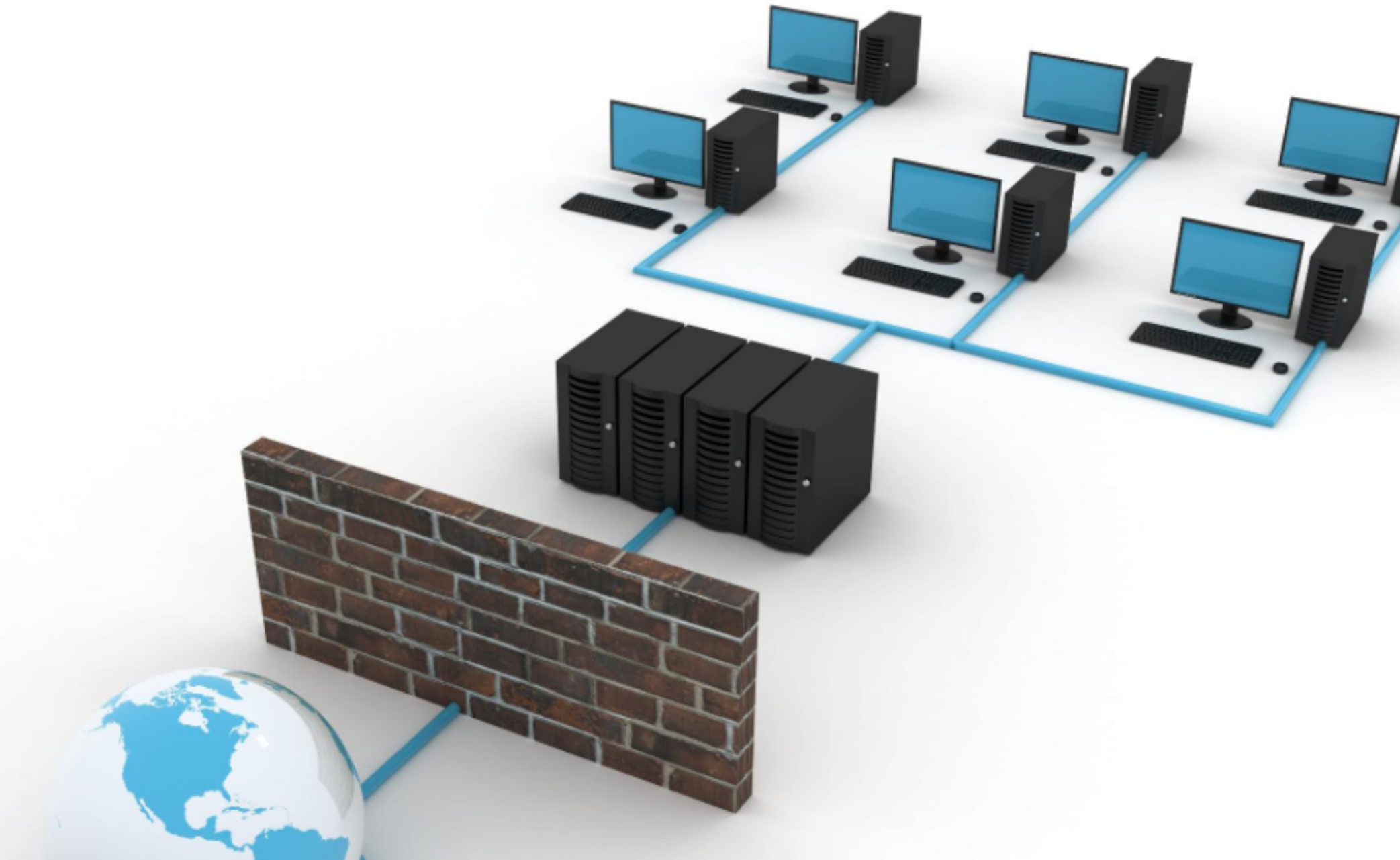
@NoorMaryam16

Active Directory PenTesting Tools



There are various tools and techniques that penetration testers and security professionals can use to assess the security of an Active Directory environment. Here are some of the commonly used tools for Active

Directory penetration testing:

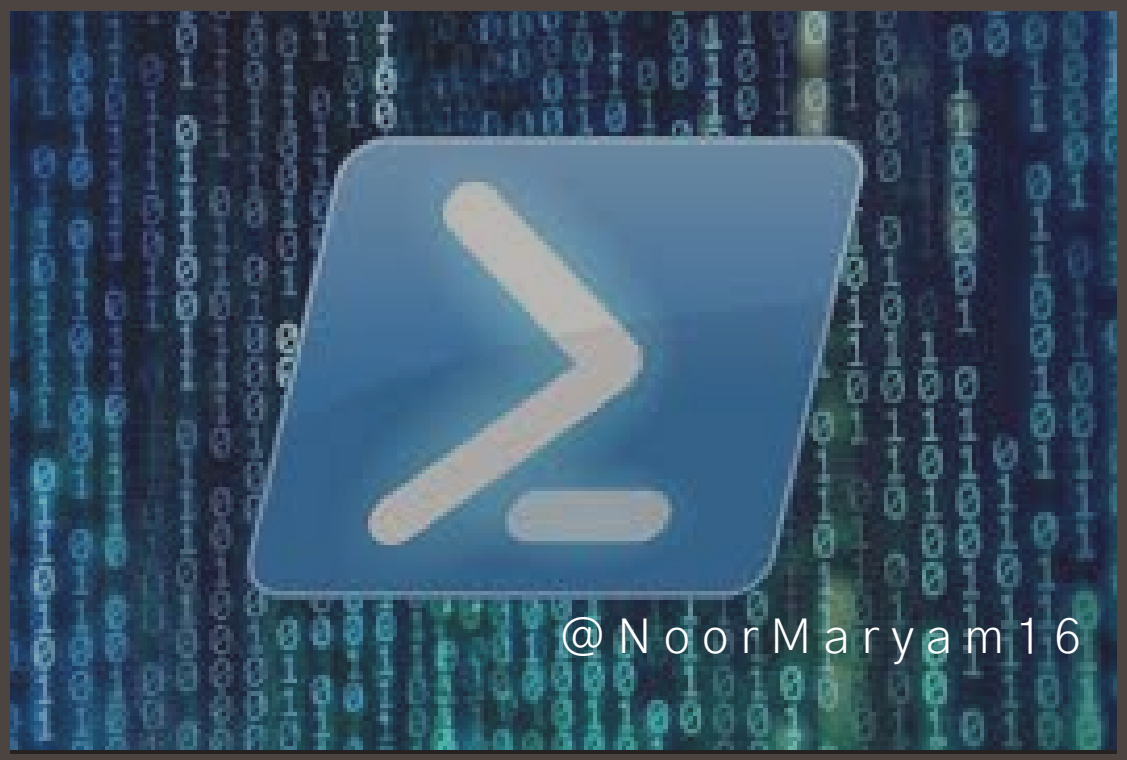
@NoorMaryam16

BloodHound

BloodHound is a popular open-source tool for mapping and analyzing an Active Directory environment. It helps identify attack paths, privilege escalation opportunities, and other security issues.

PowerShell

PowerShell, especially with the PowerView module, is a powerful tool for Active Directory penetration testing. It allows you to interact with AD and perform various reconnaissance and exploitation tasks.



Impacket

Impacket is a collection of Python classes for working with network protocols. It can be used for various Active Directory-related attacks, such as pass-the-hash, pass-the-ticket, and more. It is a powerful tool that can be used to perform a wide variety of penetration testing tasks.

Mimikatz

Mimikatz is a well-known tool for extracting plaintext passwords, hashes, PINs, and Kerberos tickets from memory. It is often used for post-exploitation activities in Active Directory environments.

PowerView

PowerView is a PowerShell tool for enumerating and attacking Active Directory. It is a powerful tool that can be used to perform a variety of penetration testing tasks.

SharpHound

SharpHound is part of the BloodHound project and is used to collect data from Active Directory environments. It helps identify security risks and vulnerabilities. SharpHound is a tool for enumerating Active Directory and creating graphical representations of possible attack paths.

Rubeus

Rubeus is a tool for Kerberos ticket extraction, injection, and manipulation. It can be used for various Kerberos-related attacks in Active Directory environments.

CrackMapExec (CME)

CrackMapExec is a post-exploitation tool that can be used for a variety of tasks related to Active Directory penetration testing, including enumeration, lateral movement, and more.

Empire

Empire is a post-exploitation framework that can be used for lateral movement and privilege escalation in Active Directory environments.

LAPSTool

LAPSTool (LAPS - Local Administrator Password Solution) is used to audit and extract the LAPS password of a target machine. It can be helpful for privilege escalation.

Grouper2

Grouper2 is a tool for identifying the relationships between groups in Active Directory. It can be helpful for understanding access control and potential privilege escalation paths.

@NOORMARYAM16

Was this helpful?

Ask any questions in the comments.

Like, share and save for later