Segurança de Sistemas e Informação

(SEGSI)
PL03

*Jorge Pinto Leite (**JPL**)*
*Pedro Sousa Rodrigues (**DCR**)*
{@isep.ipp.pt}

Exercise 1: Active Directory

Active Directory came to light as an evolution from Windows NT. It was created to support scaling business and to adapt to the necessities of the workplace making changes and integrations work seamlessly within the environment.
In order to prepare for the next exercises please accomplish the following:

1. Download a Trial image from Microsoft Download Center of Windows 2019 [1]
2. Install it on a Virtual Machine
3. Update the installation with all patches
4. Promote your server to Domain Controller

Exercise 2: Active Directory Domain Services

Having a functional active directory, you can now play around with their services. It is imperative to understand how the services work and how they integrate with your environment to provide correct AAA services.

1. Create a new Linux Virtual Machine and add it to the newly created Domain
2. Create the necessary Group Policies to ensure that Auditing is correctly implemented
3. Harden your Authentications services
   (a) Block insecure ciphers from encrypting Kerberos Tickets
   (b) Ensure that LDAP sign and seal is applied
   (c) Verify that your Linux server can still connect

Exercise 3: Attacks on Active Directory/Kerberos

Due to its expansion and adoption Active Directory environments have a huge attack surface [2]. In order to understand how can we abuse it try to accomplish the following

- Deploy **BadBlood** on your testing domain [3]

- Download and run Bloodhound [4]
- Install Neo4J Desktop [5] and load your results into the Database using the BloodHound binaries
- Try to trace a potential attack vector and how could you exploit it using the Hacktricks Database [2]

References

[1] Microsoft, "Windows server 2019: Microsoft evaluation center." [Online]. Available: https://www.microsoft.com/en-us/evalcenter/download-windows-server-2019

[2] C. Polop, "Active directory methodology." [Online]. Available: https://book.hacktricks.xyz/windows-hardening/active-directory-methodology

[3] D. Prowe, "Davidprowe/badblood: Badblood by @davidprowe, secframe.com." [Online]. Available: https://github.com/davidprowe/BadBlood

[4] BloodHoundAD, "Bloodhoundad/bloodhound: Six degrees of domain admin." [Online]. Available: https://github.com/BloodHoundAD/BloodHound

[5] Neo4J, "Download neo4j desktop," Jun 2023. [Online]. Available: https://neo4j.com/download/