CONFIABILIDADE E SEGURANÇA CIBERNÉTICA
(DACYS)
PL07
Jorge Pinto Leite (***JPL***)
Pedro Sousa Rodrigues (***DCR***), *Nuno Peralta* (**NSP**)
{@isep.ipp.pt}

Exercise 1: Active Directory

Corporate environments host several services. They are inherently complex networks that are supported by several services ranging from email, file sharing and accounts management. With the intent to centralize the management of these services, the Active Directory [1] concept was created by Microsoft. It is important to understand how one is built and managed to understand fallacies and misconfigurations that can be abused by today's attackers.

1. Download a Microsoft Server ISO from Microsoft [2] https://www.microsoft.com/en-us/evalcenter/download-windows-server-2016
2. Install a new Virtual Machine.
3. Add the role of Domain Services and promote the server to a Domain Controller.
4. What services are required for a Domain Controller to function?

Exercise 2: BadBlood

As previously stated, an active directory centralizes several services. To prepare the environment run BadBlood [3].

1. Download the repository located at https://github.com/davidprowe/BadBlood.
2. Run the script.
3. What did the script do?

Exercise 3: BloodHound

Due to all the available vectors to exploit an Active Directory environment automation is mandatory to scan the environment. BloodHound [4] [5] is a tool that is used to enumerate all available paths to compromise an Active Directory environment.

1. Clone the bloodhound git repository. https://github.com/BloodHoundAD/BloodHound.
2. Run a collector to retrieve data. Make sure to read the documentation at https://bloodhound.readthedocs.io/en/latest/index.html.

3. Install the necessary Neo4J [6] database engine https://neo4j.com/download/.
4. Run BloodHound with a new Neo4J database and import the collectors' data.
5. Determine a path of exploitation.
6. Investigate on new Vectors [7] and Custom queries.

References

[1] Iainfoulds, "Active directory domain services overview." [Online]. Available: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

[2] "Windows server 2016: Microsoft evaluation center." [Online]. Available: https://www.microsoft.com/en-us/evalcenter/download-windows-server-2016

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

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

[5] "Bloodhound six degrees of domain admin - wiki." [Online]. Available: https://bloodhound.readthedocs.io/en/latest/index.html

[6] "neo4j desktop," Feb 2022. [Online]. Available: https://neo4j.com/download/

[7] C. Polop, "Hacktricks." [Online]. Available: https://book.hacktricks.xyz/welcome/readme