JR. PENETRATION TESTER PATH + AD ROOMS

DEPI PROJECT

Expl0it3lit3

ABOUT US

AHMED HAMDY

Introduction to Cyber Security + Privilege Escalation + Lateral Movement and Pivoting

AHMED HAMDY

Network Security + Enumerating Active Directory

AHMED MAHER

Introduction to Web Hacking + Burp Suite+ Exploiting Active Directory

HASSAN MOLHAM

Vulnerability Research + Persisting Active Directory

MOHAMMED AHMED

Metasploit + Credentials Harvesting

INTRODUCTION TO WEB HACKING & BURP SUITE

Manual discovery
Favicon, Sitemap.xml, Wayback Machine, S3 Buckets

Authentication Bypass
Bruteforcing with ffuf

File Inclusion
types and filter bypasses

SSRF
places to look and Defeating Common SSRF Defenses

Burp Suite
comparer, Sequencer, Extensions, organizer

NETWORK SECURITY

Module Description:

The Network Security module provided me with a solid foundation in scanning techniques, network protocol analysis, and security tools. It covered essential methods for assessing and securing networks, with hands-on practice in various attack and defense strategies.

Gained Knowledge:

- Deep understanding of Nmap scanning with Wireshark analysis.
- Learned Xmas, Zombie, and Null scans.
- Acquired IP/MAC spoofing skills.
- Basic brute-forcing with Hydra.
- Strong grasp of network protocols.

METASPLOIT

Metasploit Pro & Framework

Commercial version with a GUI, automates and manages tasks for penetration testing. VS Open-source, command-line interface, used on penetration testing Linux distributions.

Modules

- Auxiliary
- Encoders
- Evasion
- Exploits
- NOPs
- Payloads
- Post

Database & Workspace

Database stores test data like scan results for tracking, while Workspaces organize data for multiple projects or environments in Metasploit.

PRIVILEGE ESCALATION

Types of Shell

- Reverse
- Bind
- Interactive
- Non-interactive

Socat Encrypted Shells

staged vs stageless payloads.

GTFOBins

Corn Jobs & Scheduled Tasks

Unquoted Service Paths

ACTIVE DIRECTORU ENUMERATION

Active Directory enumeration involves gathering information about users, groups, computers, and other resources in an AD environment. This process helps identify potential misconfigurations, vulnerabilities, and privilege escalation paths by using tools like PowerShell scripts, Cmd, MMC and Bloodhound to extract details such as user accounts, group memberships, and permissions. It's a crucial step in penetration testing to map out the structure and weaknesses within an organization's AD infrastructure.

WHAT ARE THE STEPS?

Getting Credentials

At first in order to use BloodHound and visualize information on it, we must use Sharphound. Sharphound is the enumeration tool of Bloodhound. It is used to enumerate the AD information that can then be visually displayed in Bloodhound.

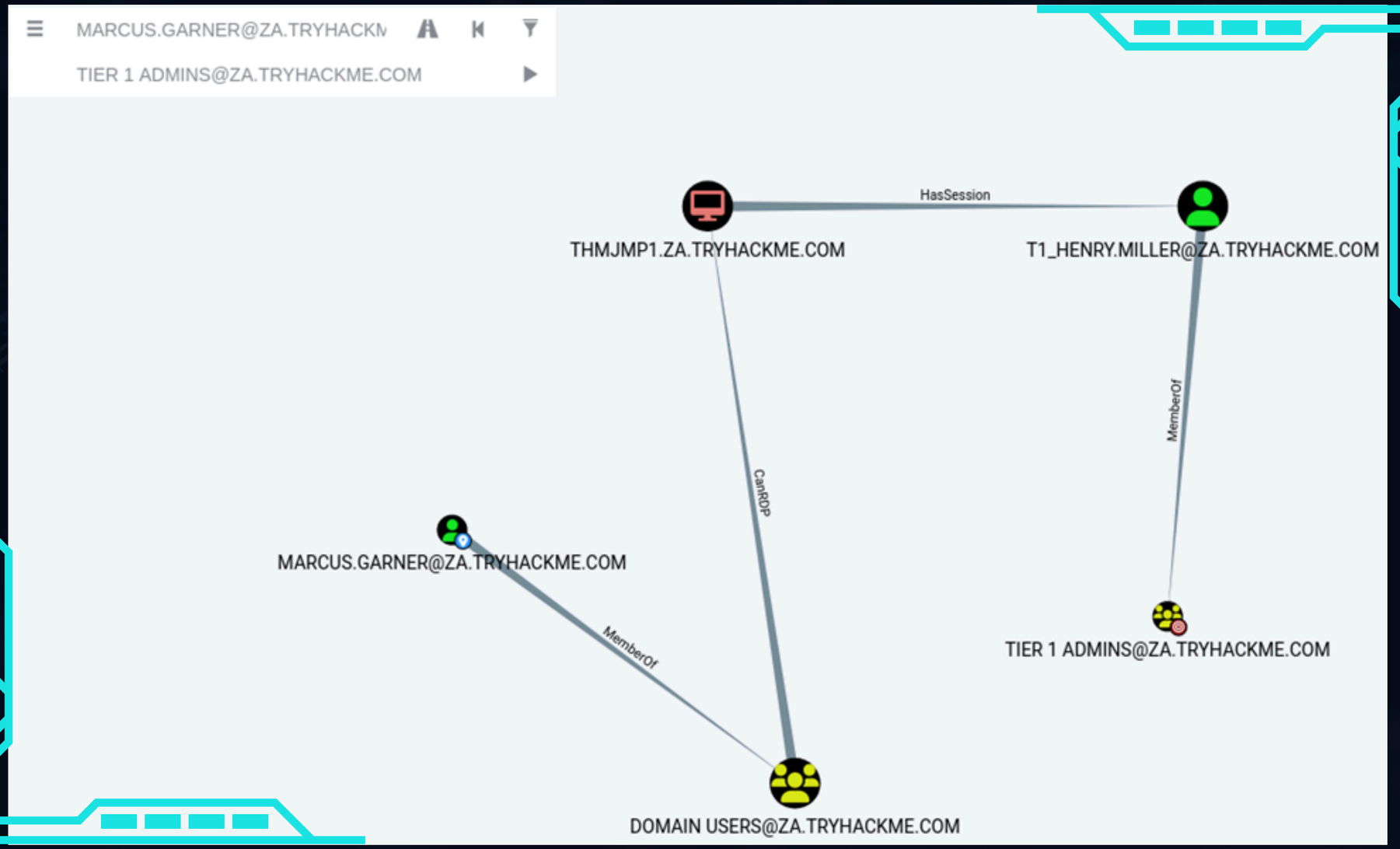
Visualizing Data

After uploading the data to bloodhound at the top left under the search bar we can see usefull and general information about our environment

Possible Attack Vectors

As we are currently having creds of a user called marcus.garner we will check for attack pathes to the admins groups in order to escalate our privileges and we will find that there is an available attack path to the Tier 1 Admins group

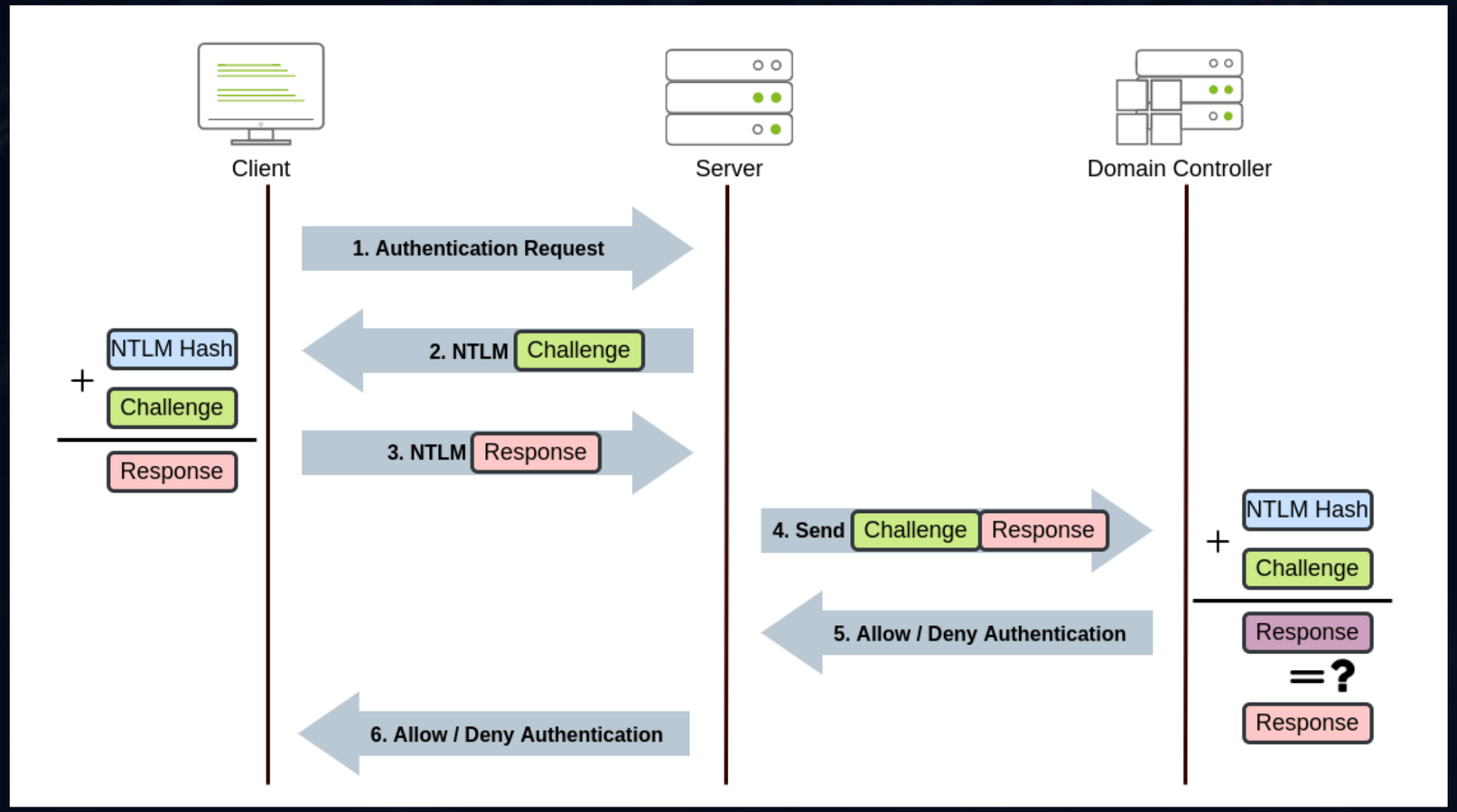
ATTACK PATH


MARCUS.GARNER@ZA.TRYHACKM
TIER 1 ADMINS@ZA.TRYHACKME.COM
HasSession
THMJMP1.ZA.TRYHACKME.COM
T1_HENRY.MILLER@ZA.TRYHACKME.COM
MemberOf
CanRDP
MARCUS.GARNER@ZA.TRYHACKME.COM
MemberOf
TIER 1 ADMINS@ZA.TRYHACKME.COM
DOMAIN USERS@ZA.TRYHACKME.COM

LATERAL MOVEMENT AND PIVOTING

lateral movement is the group of techniques used by attackers to move around a network. Once an attacker has gained access to the first machine of a network, moving is essential for many reasons, including the following: - Reaching our goals as attackers - Bypassing network restrictions in place - Establishing additional points of entry to the network - Creating confusion and avoid detection.

USING PASS THE HASH IN LATERAL MOVEMENT



EXPLOITING ACTIVE DIRECTORY

We will cover several methods that can be used to exploit AD misconfigurations. This is by no means a complete list, as available methods are usually highly situational and dependent on the AD structure and environment. However, we will cover the following techniques for exploiting AD:

AD Delegation
Forcing Authentication Relays
Group Policy Objects
Targeting AD Users
Domain Trusts
Silver and Golden Tickets

CREDENTIALS HARVESTING

Credentials harvesting is a technique used in penetration testing to gather sensitive information such as usernames, passwords, or tokens from a target system. This can be done by:

- Clear-text files
- Database files
- Memory
- Password managers
- Active Directory

THANK YOU

Expl0it3lit3