ACTIVE DIRECTORY STUDY GUIDE

Preparing for Active Directory (AD) security is crucial for passing the OSCP exam and becoming a proficient penetration tester. Here's a comprehensive study guide that focuses on AD security and will help you on your journey to clear the OSCP certification:

VIEH GROUP
AKASH BASFOR

Basic Networking and Windows Fundamentals:

- Description: Start by building a strong foundation in networking concepts and Windows operating system fundamentals.
- Skills:
  - TCP/IP, OSI model, and network protocols.
  - Basic Windows administration and user management.

Introduction to Active Directory:

- Description: Understand the basics of Active Directory, its components, and how it works in a Windows environment.
- Skills:
  - Active Directory structure and objects.
  - User and group management.
  - Group Policy basics.

AD Enumeration and Enumeration Tools:

- Description: Learn how to enumerate Active Directory environments effectively.
- Skills:
  - Enumeration of AD users, groups, and computers.
  - Utilizing tools like BloodHound, ADExplorer, and PowerView.

Privilege Escalation in Active Directory:

- Description: Focus on privilege escalation techniques within Active Directory environments.
- Skills:
  - Identifying and exploiting misconfigurations for privilege escalation.
  - Understanding Kerberos attacks (Golden Ticket, Silver Ticket).

Kerberos Attacks and Defense:

- Description: Deep dive into Kerberos authentication and related attacks.
- Skills:
  - Kerberoasting and ticket-based attacks.
  - Implementing defenses against Kerberos attacks.

Pass the Hash and Pass the Ticket Attacks:

- Description: Learn about Pass the Hash (PtH) and Pass the Ticket (PtT) attacks.
- Skills:
  - Exploiting credentials without password cracking.
  - Implementing defenses against PtH and PtT attacks.

Lateral Movement in Active Directory:

- Description: Focus on moving laterally within an Active Directory network.
- Skills:
  - Exploiting trust relationships.
  - Utilizing tools like PowerShell Empire and CrackMapExec.

AD Persistence Techniques:

- Description: Explore techniques to maintain persistence in an AD environment.
- Skills:
  - Backdooring user accounts and service accounts.
  - Understanding and detecting AD persistence mechanisms.

Active Directory Domain Trusts:

- Description: Learn about domain trusts and their security implications.
- Skills:
    - Exploiting and mitigating trust relationships.

Defensive Techniques for Active Directory:

- Description: Understand defensive measures to secure Active Directory environments.
- Skills:
    - Implementing strong password policies and authentication mechanisms.
    - Active Directory monitoring and auditing.

Active Directory Red Team Operations:

- Description: Emulate red team operations within Active Directory environments.
- Skills:
    - Developing and executing red teaming scenarios.
    - Reporting findings and recommendations.

Practice Labs and CTF Challenges:

- Description: Engage in practical labs and Capture The Flag challenges focused on Active Directory security.
- Skills:
    - Applying knowledge to real-world scenarios.
    - Developing problem-solving skills.

Kerberos Ticket Attacks:

- Description: Deepen your understanding of Kerberos tickets and related attacks.
- Skills:
  - Exploiting Kerberos ticket renewal process (Kerberoasting).
  - Identifying and extracting Kerberos tickets for further exploitation.

Active Directory Enumeration and Exploitation Tools:

- Description: Familiarize yourself with a wide range of tools specifically designed for Active Directory enumeration and exploitation.
- Skills:
  - Learning and using popular tools like BloodHound, CrackMapExec (CME), PowerSploit, and more.

Forest Trusts and Cross-Forest Attacks:

- Description: Dive into the complexities of Forest Trusts and learn how to exploit cross-forest trust relationships.
- Skills:
  - Understanding trust relationships between AD forests.
  - Exploiting trust relationships for lateral movement.

Active Directory Backup and Recovery:

- Description: Learn about AD backup and recovery strategies to ensure business continuity.
- Skills:
    - Backing up and restoring AD data.
    - Recovering from AD security incidents.

Active Directory Delegation and Abuse:

- Description: Understand AD delegation and its security implications.
- Skills:
    - Identifying and abusing excessive permissions and delegation.
    - Mitigating delegation-related security risks.

Pass the Key (PtK) Attacks:

- Description: Expand your knowledge of Pass the Key (PtK) attacks and domain persistence.
- Skills:
    - Leveraging PtK attacks to maintain access to AD environments.

AD Enumeration and Exploitation in a Multi-Domain Environment:

- Description: Practice enumerating and exploiting Active Directory in complex multi-domain environments.
- Skills:
    - Understanding the challenges of multi-domain AD environments.
    - Leveraging trust relationships for privilege escalation.

Red Team Operations - Active Directory Edition:

- Description: Focus on emulating advanced red team operations with an emphasis on Active Directory exploitation.
- Skills:
    - Conducting full-scale red team engagements against AD environments.
    - Developing custom tools and scripts for AD exploitation.

Some commonly used Active Directory commands for managing and querying Active Directory (AD) objects:

dsquery

```
dsquery user -name John
```

Description: Used to search for AD objects that match specified criteria.

dsget

```
dsget user "CN=John Doe,OU=Users,DC=example,DC=com"
```

Description: Retrieves properties of AD objects.

dsadd

```
dsadd user "CN=NewUser,OU=Users,DC=example,DC=com" -samid NewUser -upn newuser@example.com -fn New -ln User -display "New User"
```

Description: Adds new AD objects to the directory.

dsmod

```
dsmod user "CN=John Doe,OU=Users,DC=example,DC=com" -disabled no
```

Description: Modifies AD object properties.

dsrm

```
dsrm "CN=ObsoleteUser,OU=Users,DC=example,DC=com"
```

Description: Deletes AD objects.

net user

```
net group "Group Name" /add
```

Description: Manages AD groups.

net groupmember

```
net group "Group Name" John /add
```

Description: Adds or removes members from AD groups.

repadmin

```
repadmin /showrepl
```

Description: Used for Active Directory replication management and monitoring.

ldifde

```
ldifde -f ExportedData.ldf -s servername -d "OU=Users,DC=example,DC=com"
```

Description: Import or export AD data in LDIF format.

csvde

```
csvde -i -f ImportData.csv
```

Description: Import or export AD data to or from a CSV file.

gpupdate

```
gpupdate /force
```

Description: Updates Group Policy settings on the local machine.

nltest

```
nltest /sc_verify:example.com
```

Description: Used to test network connectivity and trust relationships.