Ethical hacking and Penetration Testing

Infrastructure security. Reconnaissance

Author: Kutlymurat Mambetniyazov (@manfromkz)

Identifying the goals of lesson

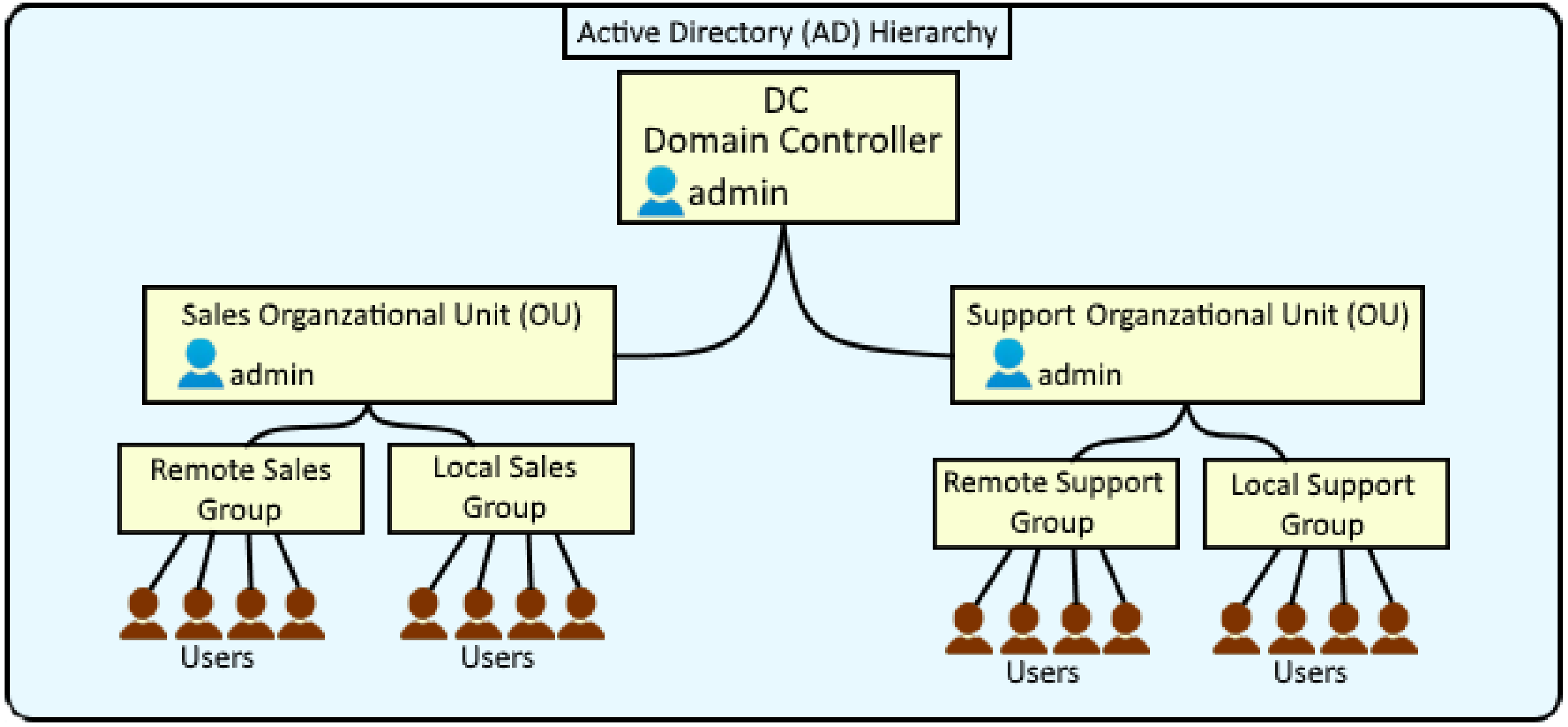
- Understanding basic terms and the way of hacking infrastructure
- Reviewing active information gathering methods
- Practicing Bloodhound

What is AD and DC, LDAP?

- **Active Directory (AD)** is a directory service developed by Microsoft for Windows domain networks.

- **A domain controller (DC)** is a server (most commonly Microsoft Active Directory) that manages network and identity security, effectively acting as the gatekeeper for user authentication and authorization to IT resources within the domain.

- **Lightweight directory access protocol (LDAP)** is a way (protocol) of speaking to Active Directory.


Active Directory (AD) Hierarchy
DC
Domain Controller
admin
Sales Organzational Unit (OU)
admin
Support Organzational Unit (OU)
admin
Remote Sales Group
Local Sales Group
Remote Support Group
Local Support Group
Users
Users
Users
Users

Active Directory analogies

- https://www.thewindowsclub.com/top-10-free-microsoft-active-directory-alternative-software

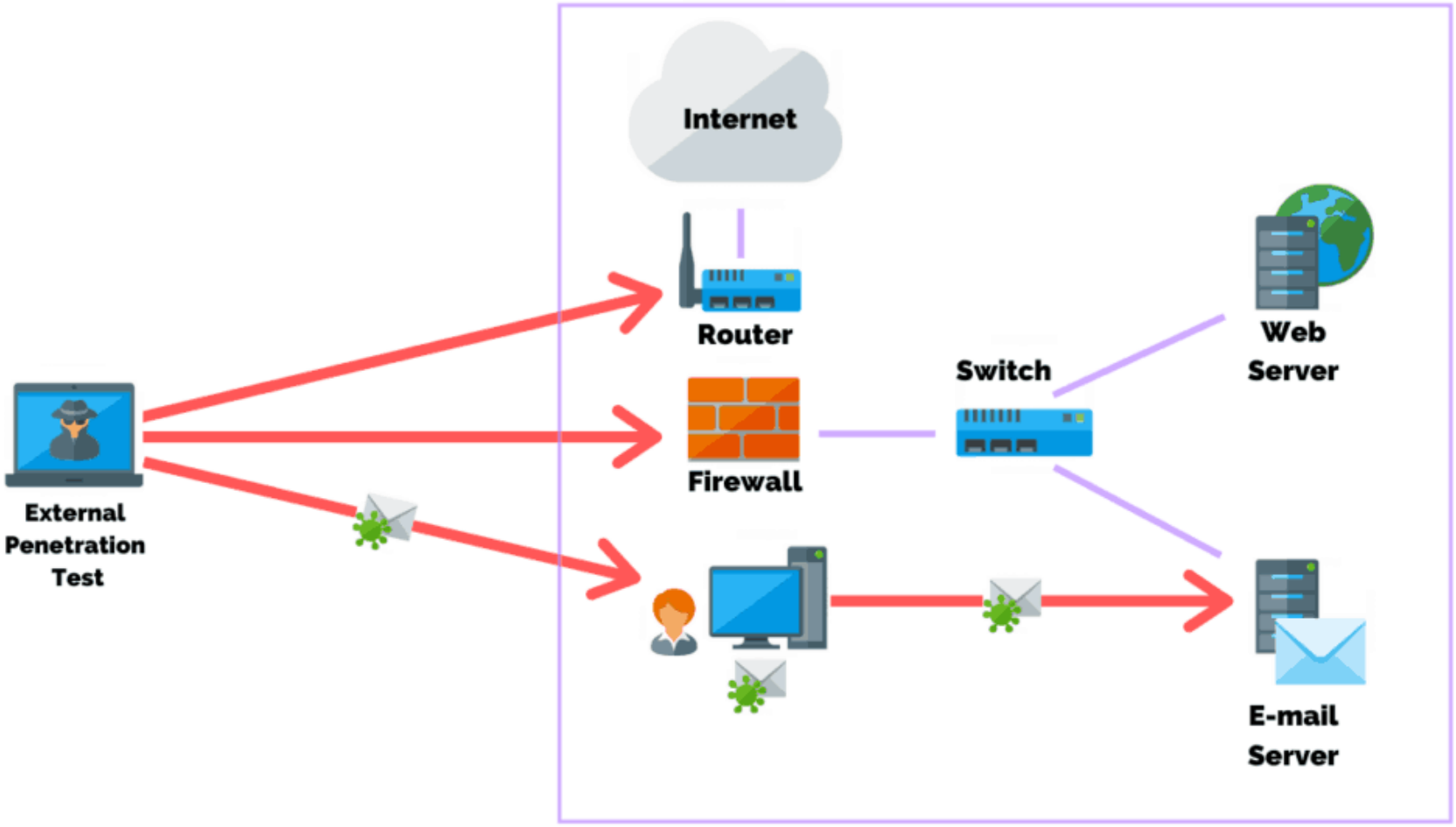
- Microsoft Active Directory is not the only directory software in the market.

Let’s start from beginning…

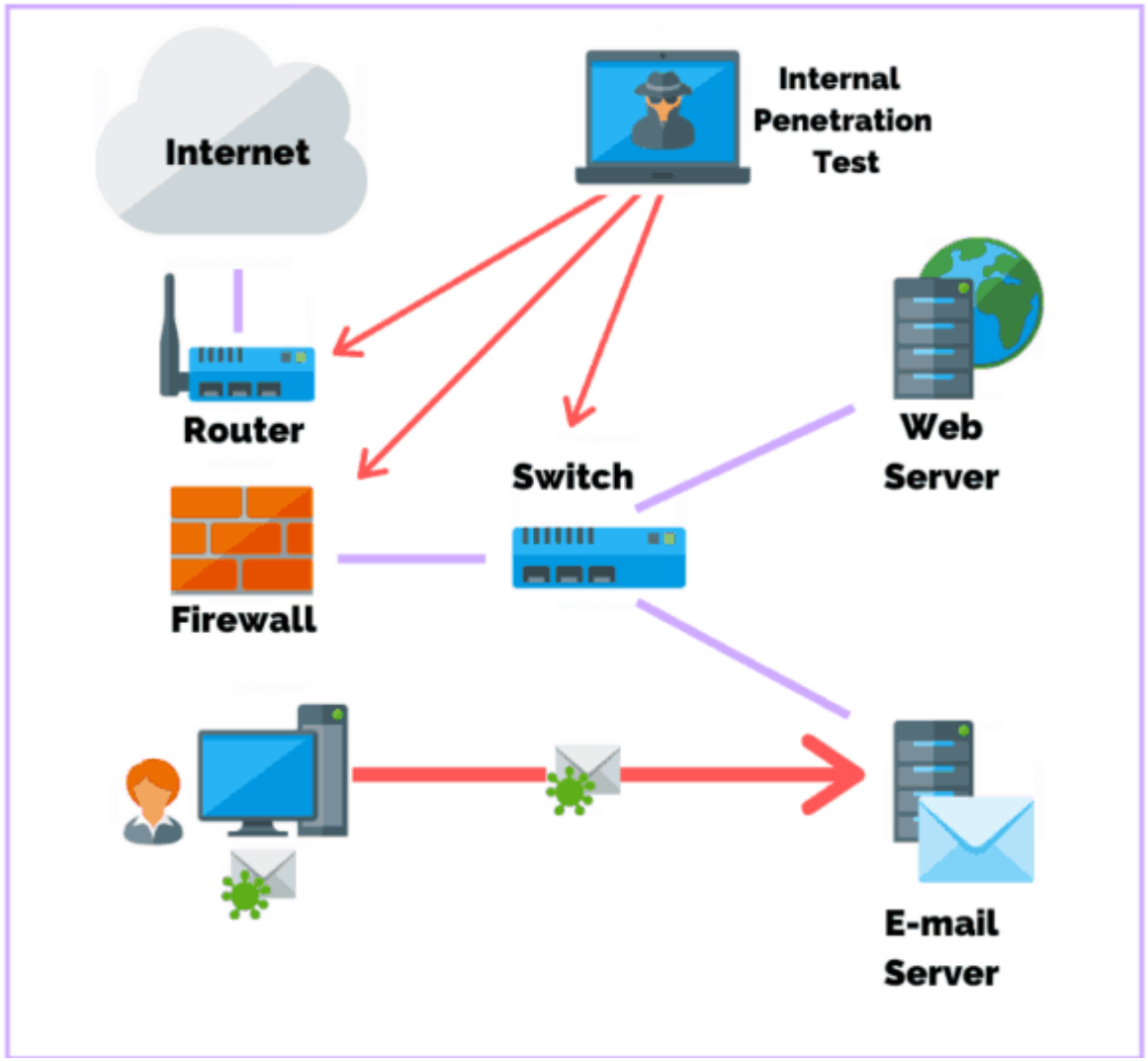
The classic way

- Step 1: getting foothold by hacking web / other service / phishing
- Step 2: escalating privilege on hacked host if possible, or starting scanning internal network
- Step 3: attacking internal network
- …
- Step N-1: ????
- Step N: getting sensitive info / domain admin / etc.

External attack to infrastructure



Internal attack to infrastructure



Information gathering

- Active Reconnaissance – you connect to the objects of scope
- Passive Reconnaissance – you don’t connect to the objects of scope

Nmap

- Site: https://nmap.org/

- Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing.

- Example:
  - nmap -p1-100 127.0.0.1-255
  - nmap -p- --script vuln* 127.0.0.1
  - nmap -p- -T4 --open -sV 127.0.0.1

In case of finding web ports

- Check version of installed software and try to use public exploits
- Search for custom scripts, hidden files/directories
- Try to bruteforce admin panel
- Gain shell
- When you have only IP address and you find some port (example, 443, 8443, etc.) with SSL certificate, you can view info (sslyze, sslscan, or just web browser) about this certificate and get the domain name (it is useful, for example for DNS enum)
- Search for 0day and register CVE :)
- Look for web hacking cheat sheets

In case of finding non-web ports

- Try to run nmap with -sV key to detect service version
- Try to run nmap with --script parameter
- Search for exploits and use them
- Try to use default passwords
- Gain shell
- Search for 0day and register CVE :)
- Look for cheat sheets about pentesting this service

DNS enumeration

- Tools: whois, dig, host, dnsenum or web services

- Usage:
  - whois domain-name-here.com
  - dig a domain-name-here.com @nameserver
  - dig axfr domain-name-here.com @nameserver

- Example:
  - https://digi.ninja/projects/zonetransferme.php

SMB enumeration

- smbclient
- smbmap
- enum4linux

- Example:
  - enum4linux -a -u "" -p "" <DC IP>
  - smbmap -u "" -p "" -P 445 -H <IP>
  - smbclient -U '%' -L //<IP>

FTP enumeration

- nmap --script ftp-anon,ftp-bounce,ftp-libopie,ftp-proftpd-backdoor,ftp-vsftpd-backdoor,ftp-vuln-cve2010-4221,tftp-enum -p 21 10.0.0.1

SMTP enumeration

- nmap --script smtp-commands,smtp-enum-users,smtp-vuln-cve2010-4344,smtp-vuln-cve2011-1720,smtp-vuln-cve2011-1764 -p 25 10.0.0.1
- nc -nvv INSERTIPADDRESS 25
- telnet INSERTIPADDRESS 25

NFS file shares enumeration

- Show:
  - showmount -e IPADDR

- Mount:
  - mount 192.168.1.1:/vol/share /mnt/nfs -nolock

??? enumeration

- Search in Google detected service name in this context “SOMESERVICE pentest”, “SOMESERVICE exploit”, “SOMESERVICE vulnerabilities”, etc.
- Install the same version of SOMESERVICE on your local environment to perform tests without additional noise
- Create final exploit and try on real target
- If nothing gained, move to the next service

Gaining shell

- If you get code execution, then you should get interactive shell for convenience work

- Reverse shells:
  - https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md

- C2 agents (in other word - trojan to control host remotely):
  - Merlin C2
  - Covenant C2
  - etc.

Bloodhound

- **Bloodhound** is a **post-exploitation** tool that uses graph theory to reveal the hidden and often unintended relationships within an Active Directory or Azure environment.

- https://github.com/BloodHoundAD/BloodHound
- https://tryhackme.com/room/postexploit

- Attacker should start SharpHound (client of BloodHound) on target host to collect information about AD.

Cloud security

- https://mitechnews.com/guest-columns/aws-penetration-testing-cheat-sheet/
- https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Methodology%20and%20Resources
- https://github.com/dafthack/CloudPentestCheatsheets

Any questions?

Homework for the next lesson

- Scan Metasploitable for all ports using -sV parameter
- Repeat yourself Bloodhound usage at Tryhackme Post-Exploit room https://tryhackme.com/room/postexploit

Feedback: did we achieved the goals of our lesson?

- Discussion 5-10 minutes

Useful links

- https://purplesec.us/external-vs-internal-network-penetration-tests/
- https://book.hacktricks.xyz/windows/active-directory-methodology
- https://www.varonis.com/blog/the-difference-between-active-directory-and-ldap
- http://www.freekb.net/Article?id=741