Table of contents

Executive Summary

Overview

Fixed solution mentors asked mourad company to perform Penetration testing (as assessment) on their LAN. The company will also provide estimates of how susceptible LAN is to data exploitation or breach.

High-level Test Outcomes

no. of issues: 6

Severity	Critical	High	Medium	Low	Information
# of issues	3	1	0	1	1

Severity scoring:

- **Critical** -Immediate threat to key business processes. CVSS[9:10]
- **High**– Direct threat to key business processes. CVSS[7:9]
- **Medium** – Indirect threat to key business processes or partial threat to business processes. CVSS[4:7]
- **Low**– No direct threat exists. Vulnerability may be exploited using other vulnerabilities. CVSS[0:4]
- **Informational** – This finding does not indicate vulnerability, but states a comment that notifies about design flaws and improper implementation that might cause a problem in the long run.

Performed Tests:

Performed Tests	**Status**(done or not)	**criteria**
Host and service enumeration	Done	Failed
Weak passwords attack and brute-force	Done	Failed
Identification of configurations	Done	Failed
Vulnerability identification and system exploitation	Done	Failed
Weak Authorization Mechanisms testing	Done	Failed
Outdated services	Done	Failed
Search Engine Discovery and Reconnaissance for Information Leakage	Done	Passed
Database compromising, sensitive information stealing	Done	Failed
S3 bucket enumeration	Not Applicable	

Security Tools Used:
- rustscan
- dirsearch
- kerbrute
- smbclient
- GetNPUsers.py
- hashcat

Recommendations

- Patch and update applications/services continuously. You can use Updates management Center for this.

- Enforce strong password policies.

- do vulnerability assessment weekly/monthly.

- make restrictions on sensitive/dangerous resources.

Scope

this engagement done on internal windows machine. IP: 192.168.137.82

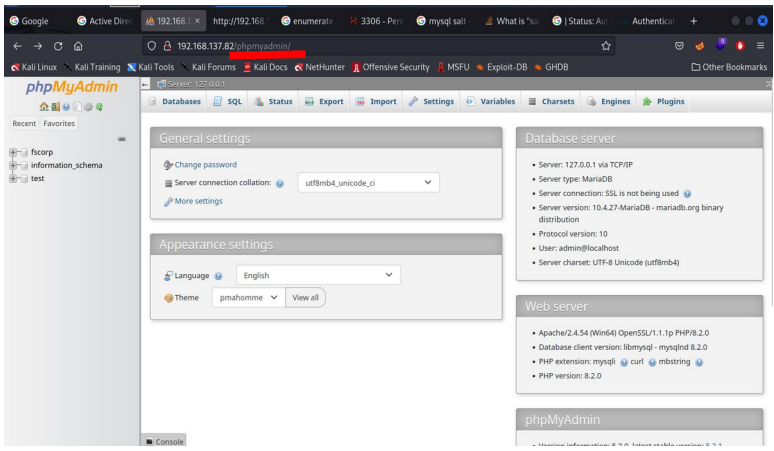
Team

Team: Mohamed Mahmoud Mourad

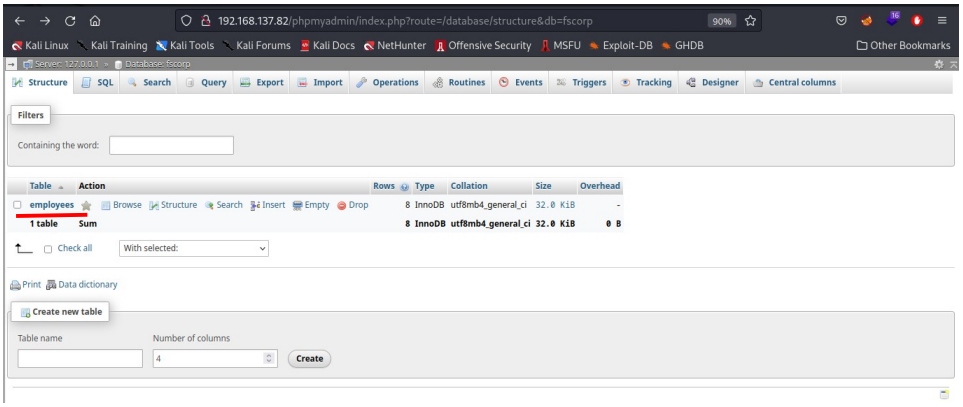
Technical Detailed Findings

Getting user1 account(flag1)

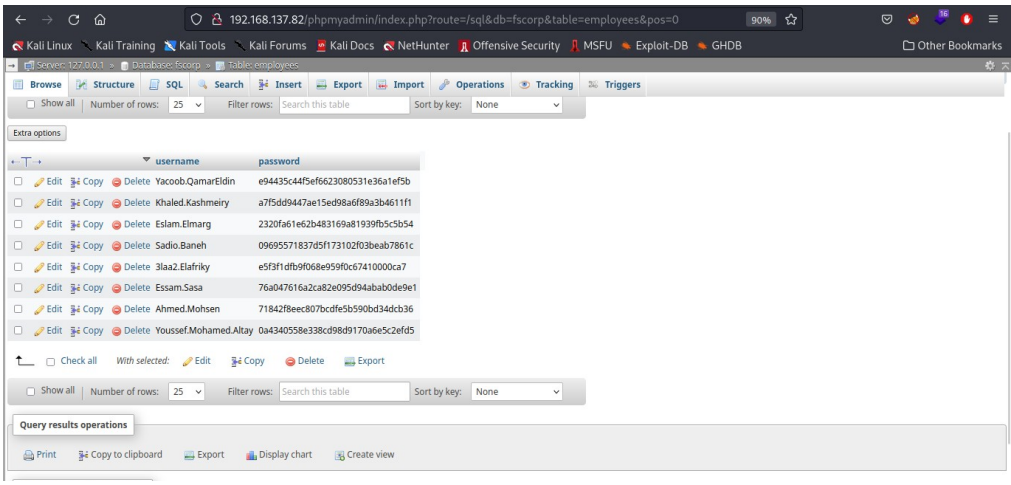
severity: **Critical**
cvss: 9.2
impact: attacker can access db and successfully login to active directory domain.
steps to reproduce:
1. open: http://192.168.137.82/phpmyadmin/
2. login page will be shown, login with admin:admin. Admin panal will be shown



3. in admin panal, in above bar. Visit: database then structure. Db tables will be shown

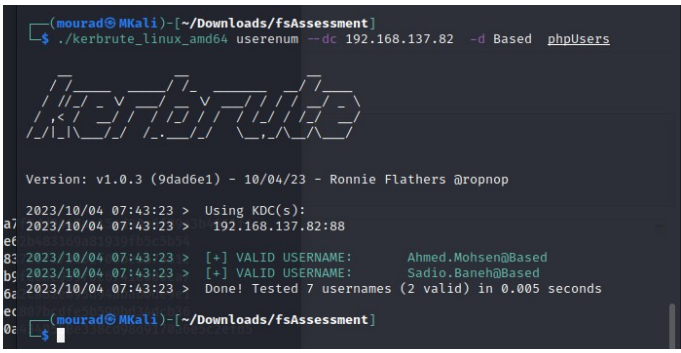


4. click employee table. Usernames, passwords hashes will be shown.

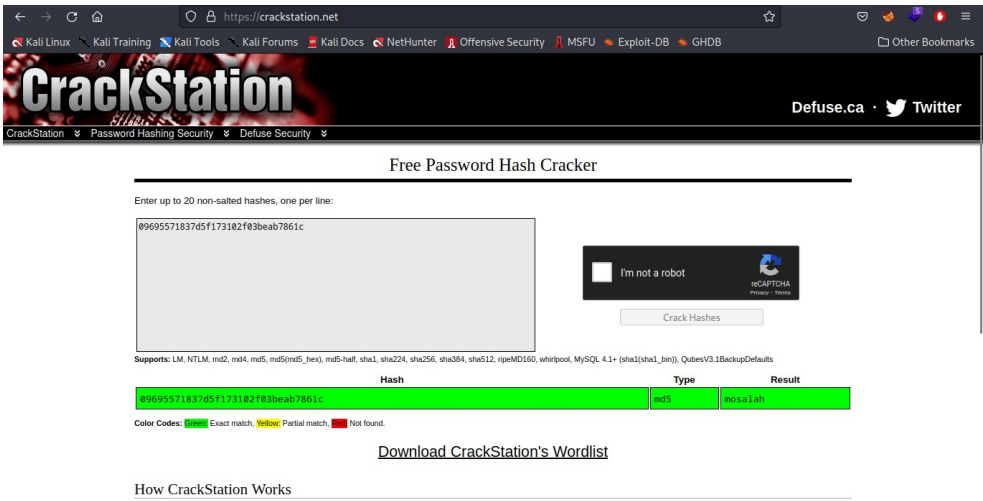


5. put these usernames in wordlist(i called it phpUsers).

6. using kerbrute tool, check any of these usernames is valid as active directory account through Kerberos Pre-Authentication.



7. after getting valid usernames, crack their hashes.
   *) visit https://crackstation.net/ put each hash.
  *)Hash of sadio.baneh username is crackable(mosalah) while ahmed.mohsenn not crackable.



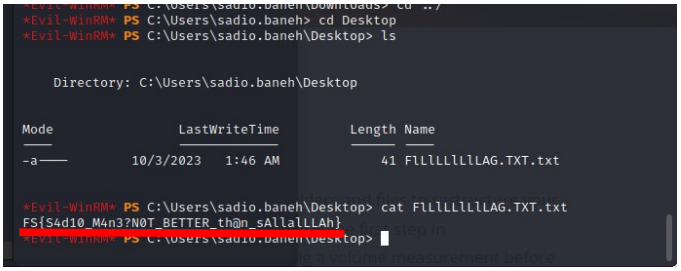
8. now, we have valid credential=> sadio.baneh:mosalah. Login using them via evil-winrm tool

prompt: `evil-winrm -i 192.168.137.82 -u Sadio.Baneh  -p mosalah`

   you logged in successfully *)now, we foot held on the machine via user account

9. go to Desktop dir., open flag file via cat tool.

   Now, we got the first flag.



Recommended remediation: **restrict admin page and don't use default credential for login.**

AS-REP roasting attack (Getting user2 account(flag2))

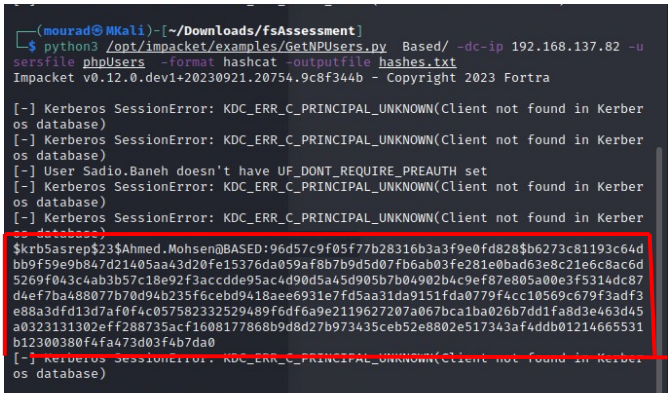
severity: Low
cvss:3.7
impact: attacker can access active directory domain as user account.
steps to reproduce:

Lets get other flags
1. go to C:\Users\ahmed.mohsen\Desktop. You will find flag file open it => access denied

lets try find way to login via ahmed.mohsen. Really we have its uesername. Reminded to login in is password

2. get hashes of users that have 'pre-authenticated flag is disabled'
prompt: `python3 /opt/impacket/examples/GetNPUsers.py  Based/ -dc-ip 192.168.137.82 -usersfile phpUsers  -format hashcat -outputfile hashes.txt` (**AS-REP roasting attack**)

3. hash of ahmed mohsen will be shown crack it via hash cat method.
   Result of hash: 'pewpew24'



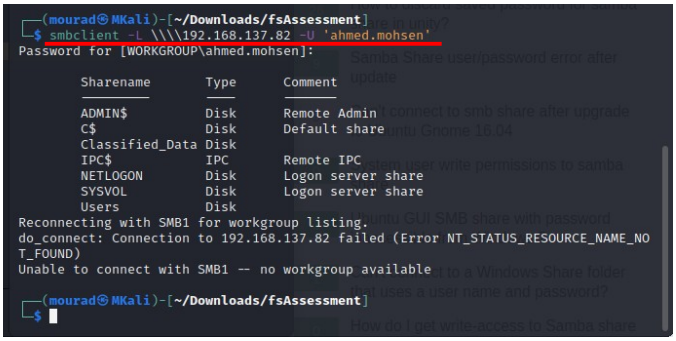
4. login with via ahmed mohsen cred=> ahmed.mohsen: pewpew24 using evil-winrm tool. Prompt: `evil-winrm -i 192.168.137.82 -u ahmed.mohsen  -p pewpew24`

5. go to Desktop dir. Open the flag file .
flag2: FS{P3W_P3W_P3W_4HM3D_M0HS3N_P3W_P3W_P3W}

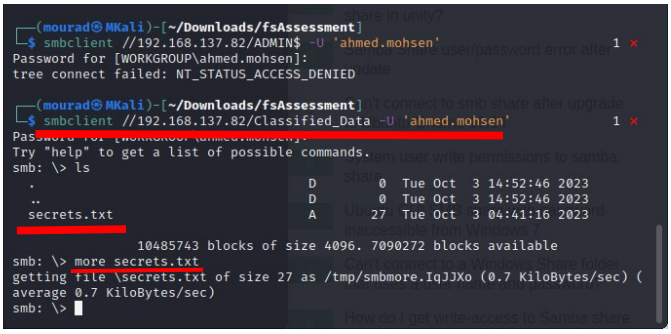
Recommended remediation: **Enforce robust password policies for service accounts.**

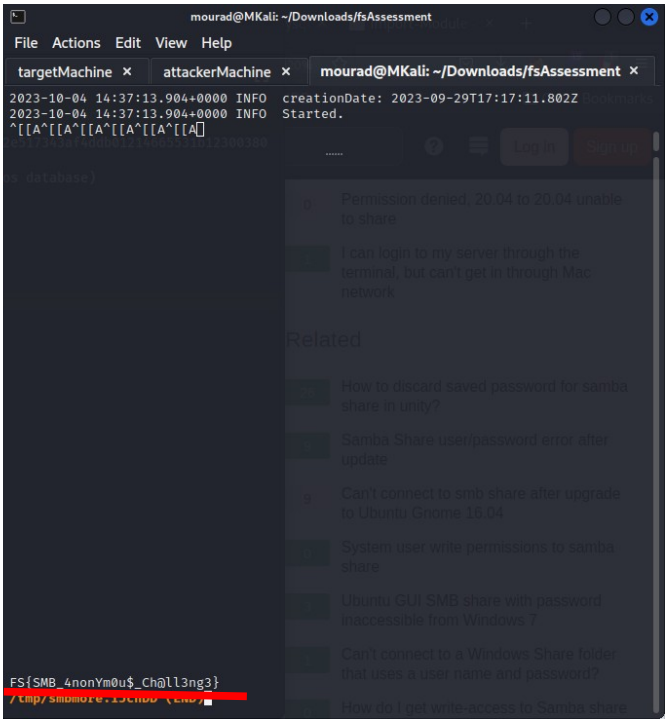
Getting flag3

1. enumerate smb shared folders via smbclient and using ahmed.mohsen credential



2. open Classified_Data dir., Then read secret file.





you got the flag:
flag3: FS{SMB_4nonYm0u$_Ch@ll3ng3}

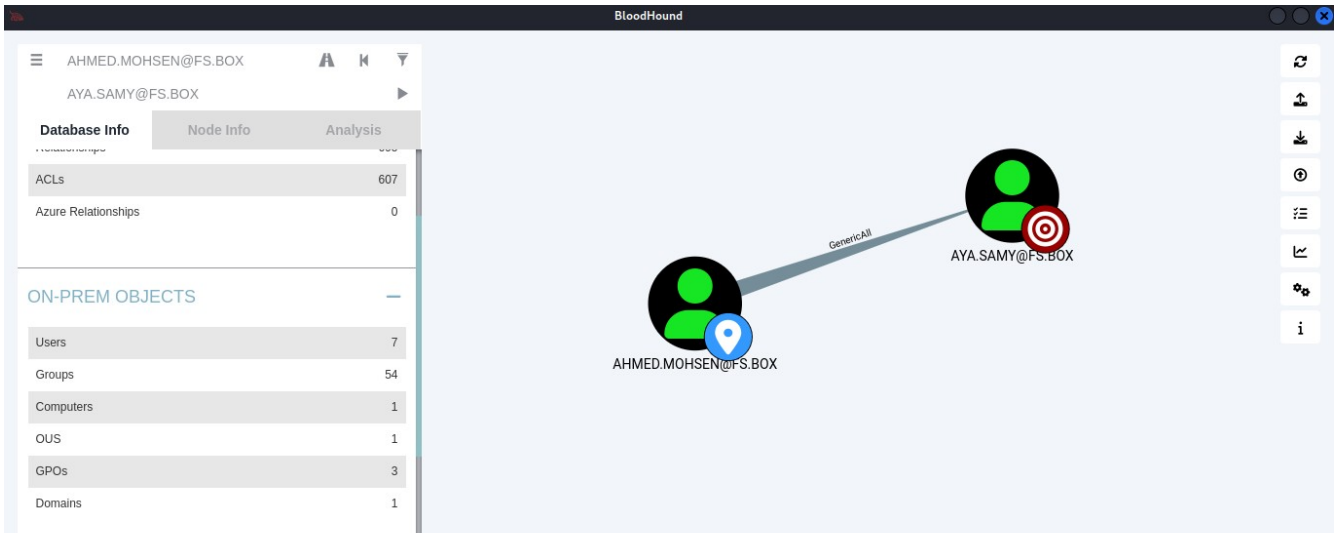
Privilege Escalation from user account to admin account(flag4)

severity: **High**
cvss: 7.5
impact: attacker can get admin account then has full control on the active directory domains.

steps to reproduce:

1. collect data via bloodhound.py
  prompt: ` bloodhound-python -u ahmed.mohsen -p 'pewpew24' -ns 192.168.137.82 -d fs.box -c all`

2. open bloodhound gui to identify your path to admin(from ahmed.mohsen@fs.box to aya.samy@fs.box)



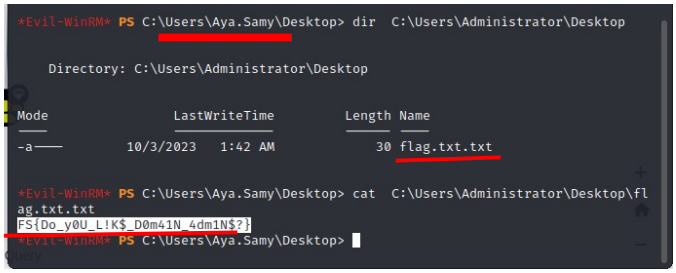
*)The GenericAll right is the same as Full Control on the object.
I abused GenericAll permission to change password of admin.

3. login via evil-winrm again using ahmed mohsen credential.

4. change password of admin(aya.samy). prompt: `Set-ADAccountpassword aya.samy -reset - Newpassword (ConvertTo-SecureString -AsPlainText 'Pass123!' - Force() *`

5. logout then login via aya.samy credential. (aya.samy:Pass123).

6. read flag file. Prompt: `cat C:\Users\Administrator\Desktop\flag.txt.txt`

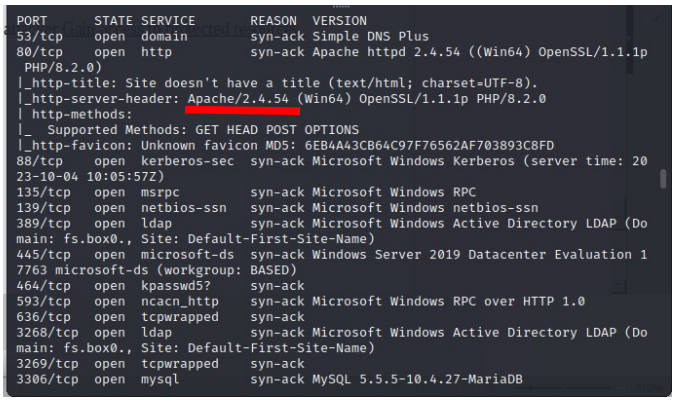


Recommended remediation: remove GenericAll permission from normal users.

Using vulnerable version from apache server for web application

description: Apache 2.4.54 version has critical vulnerabilities.
severity: **Critical**
cvss: 9.8
impact: apply request smuggling attack, that may make attacker Gain access to protected resources, such as admin consoles.

steps to reproduce:
scan services using rustscan



```
PORT      STATE SERVICE       REASON  VERSION
53/tcp    open  domain        syn-ack Simple DNS Plus
80/tcp    open  http          syn-ack Apache httpd 2.4.54 ((Win64) OpenSSL/1.1.1p
 PHP/8.2.0)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/8.2.0
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: 6EB4A43CB64C97F76562AF703893C8FD
88/tcp    open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time: 20
23-10-04 10:05:57Z)
135/tcp   open  msrpc         syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Do
main: fs.box0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds  syn-ack Windows Server 2019 Datacenter Evaluation 1
7763 microsoft-ds (workgroup: BASED)
464/tcp   open  kpasswd5?     syn-ack
593/tcp   open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped    syn-ack
3268/tcp  open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Do
main: fs.box0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped    syn-ack
3306/tcp  open  mysql         syn-ack MySQL 5.5.5-10.4.27-MariaDB
```

CVEs affects on this product:
CVE-2023-25690
CVE-2022-36760

Recommended remediation: update to at least version 2.4.56 of Apache HTTP Server.

Not restricted admin page

severity: **Info**

Steps to reproduce:
1. open: http://192.168.137.82/phpmyadmin/

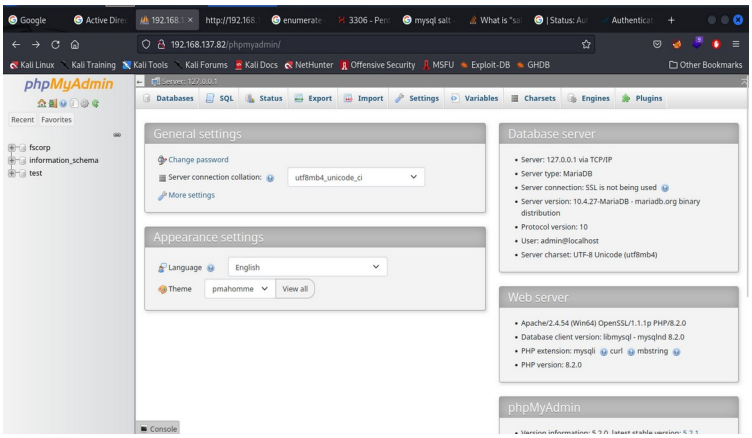
Recommended remediation: restrict users that can access this page. You can use ACL for this.

Accessing admin page via default credential

severity: **Critical**
cvss: 9.8

impact: attacker has full control on the db.

steps to reproduce:
1. open: http://192.168.137.82/phpmyadmin/
2. login via cred=> admin:admin



Recommended remediation: don't use default credential for login. Use strong passwords for login.

Special Thanks To:

Eng. Aya Samy

Eng. Omar Karam