

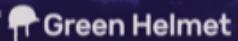
mindthesec[®]

/SÃO PAULO

MAIS UM
EVENTO:



REALIZAÇÃO:



Assumindo controle total da sua rede em menos de 1 hora, o ataque e suas principais defesas.

Helvio Junior (M4v3r1ck)

Analista de Cyber Segurança

mindthesec[®]
/SÃO PAULO



WHO
ARE
YOU?

mindthesec[®]
/SÃO PAULO



Helvio B. D. De Carvalho Junior

Malware and Security Researcher | Computer Forensics Investigator | OSCE | OSCP | CEHv9

- E-mail: helvio_junior@hotmail.com
- Twitter: @helvioju
- Mais de 20 anos de atuação com TI
- Apaixonado por Low Level Exploitation
 - Buffer Overflow
 - Binary Exploitation
- Foco de estudo e pesquisa:
 - Segurança ofensiva (Red Team)
 - Forense computacional
 - Bug hunting, Cyber threat hunting
 - Criação e engenharia reversa de Malware
- Analista em Cyber Security no Banco Original



mindthesec[®]
/SÃO PAULO

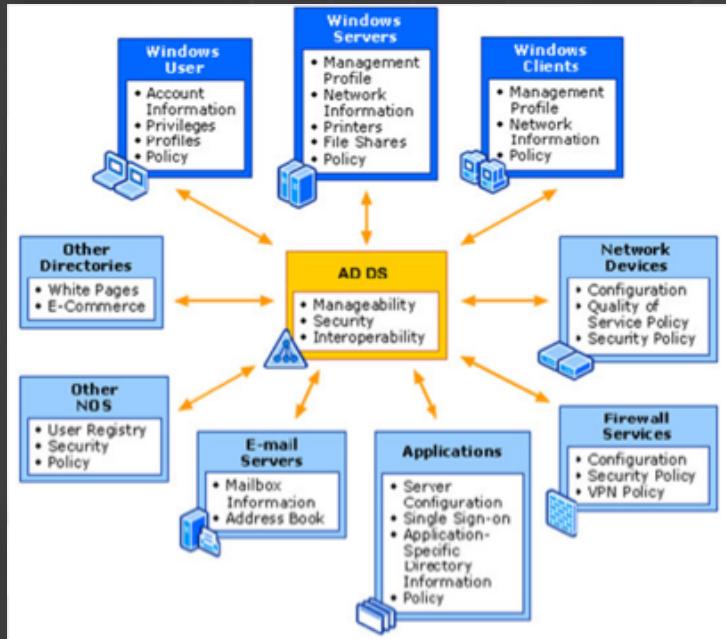


Motivações

Insider = Perigoso

Maior superfície de ataque

Acesso irrestrito a recursos e informações em caso de sucesso (Domain Controller)



Microsoft Active Directory:

Ambiente típico de instalação.





mindthesec[®]
/SÃO PAULO



```
PUSH 0x00000000  
PUSH 0x4633172  
PUSH 0x376344d  
PUSH ESP  
CALL printf
```

Domain Admin = Controle total

Em geral:

- Acesso a todos os computadores
- Acesso a todos os servidores
- Acesso a todos os bancos de dados
- Acesso a dados confidenciais

Passo 1

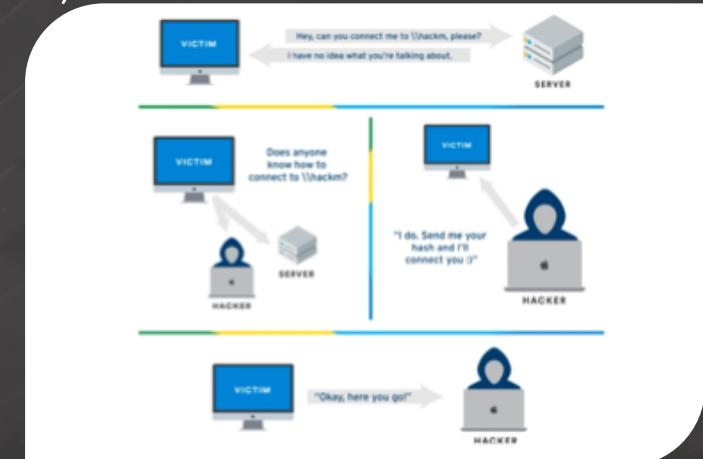
Captura do Hash NTLMv2 do usuário

Quebra do Hash usando ataque de força-bruta sobre o hash

Envenenamento LLMNR & NBT-NS

Comportamento padrão:

- Quando um Cliente Windows não consegue resolver um nome DNS, ele utiliza o protocolo LLMNR (Link-Local Multicast Name Resolution) para consultar aos outros hosts da rede sobre a requisição, se esse passo também falhar o cliente usa o NBT-NS (NetBios Name Service).
- Quando os protocolos LLMNR/NBT-NS são utilizados para resolver nomes, qualquer host da rede pode responder a estas requisições.



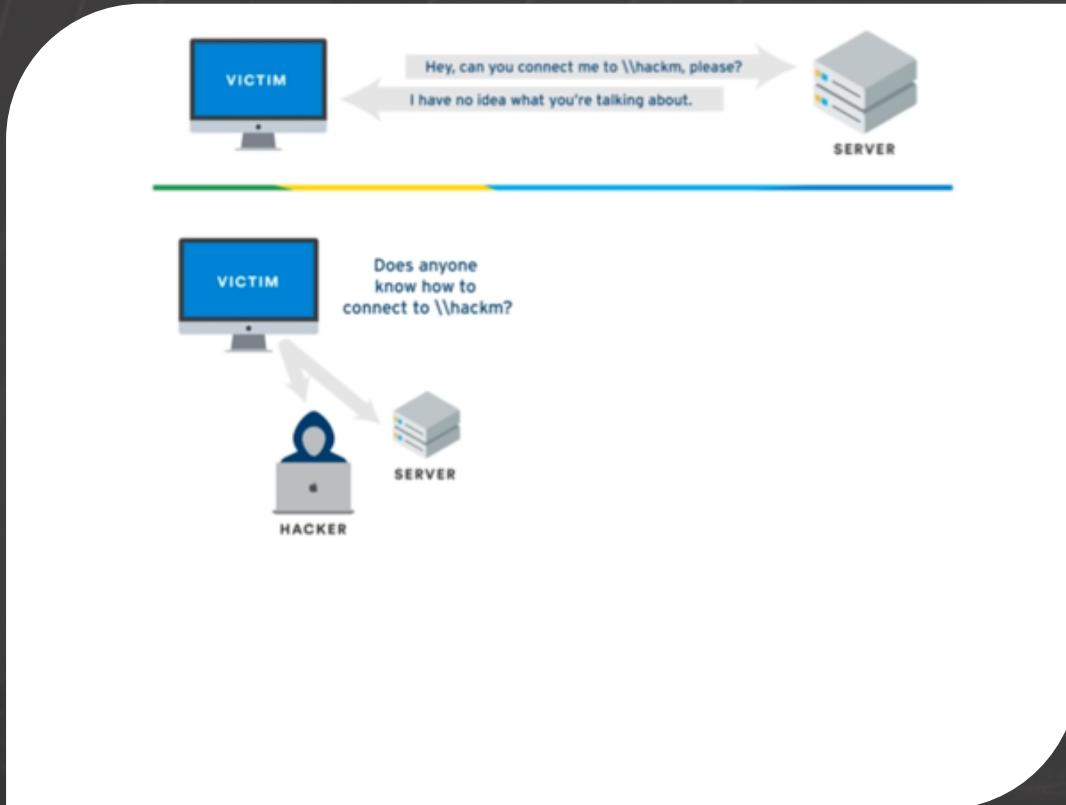
Fonte: <https://www.youtube.com/watch?v=Fg2gvk0qgJM>

Envenenamento LLMNR & NBT-NS



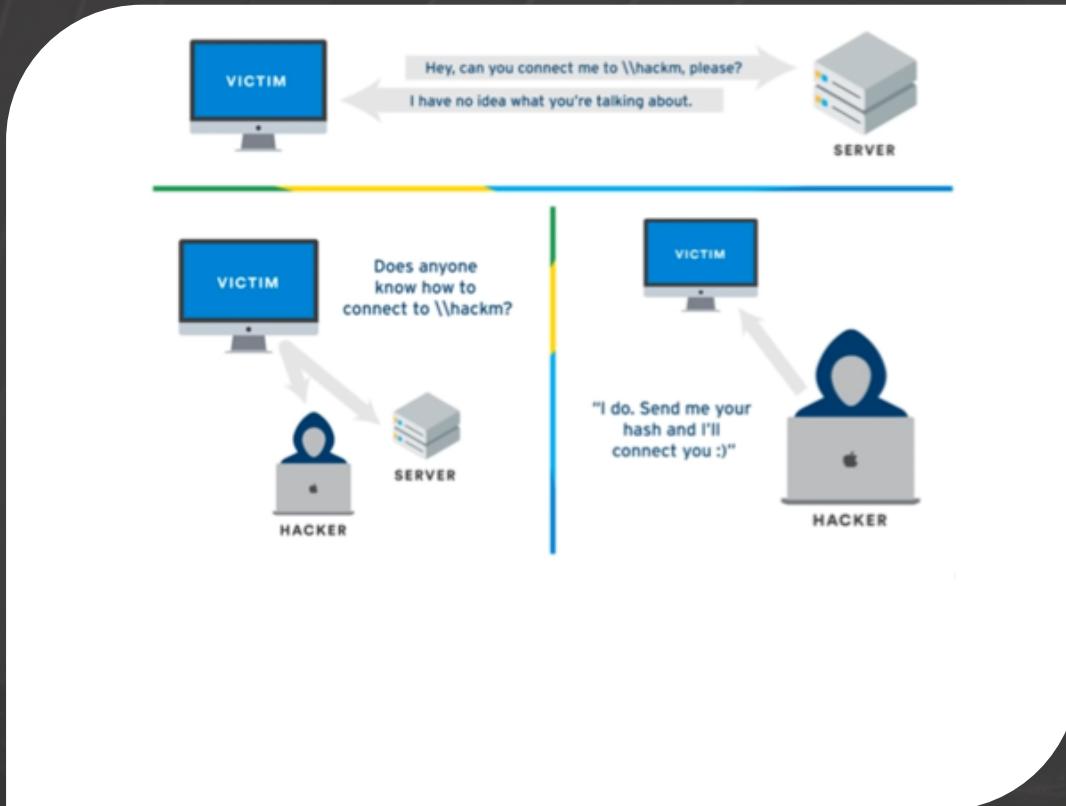
Fonte: <https://www.youtube.com/watch?v=Fg2gvk0qgjM>

Envenenamento LLMNR & NBT-NS



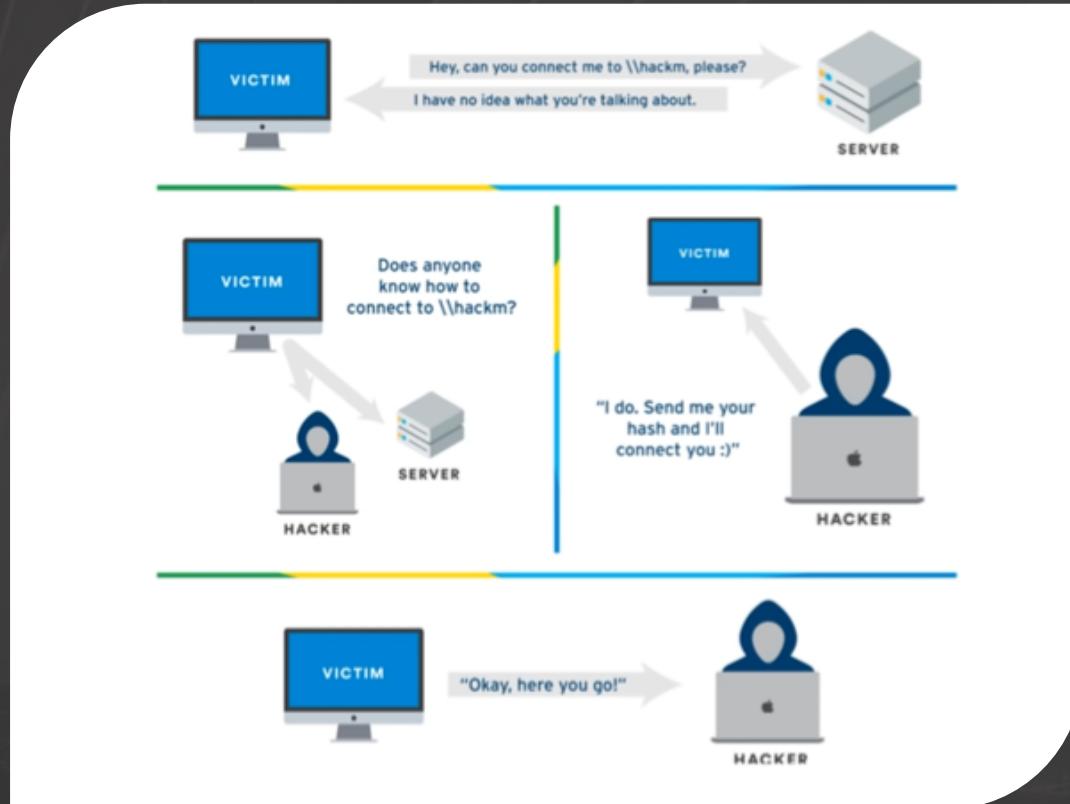
Fonte: <https://www.youtube.com/watch?v=Fg2gvk0qgjM>

Envenenamento LLMNR & NBT-NS



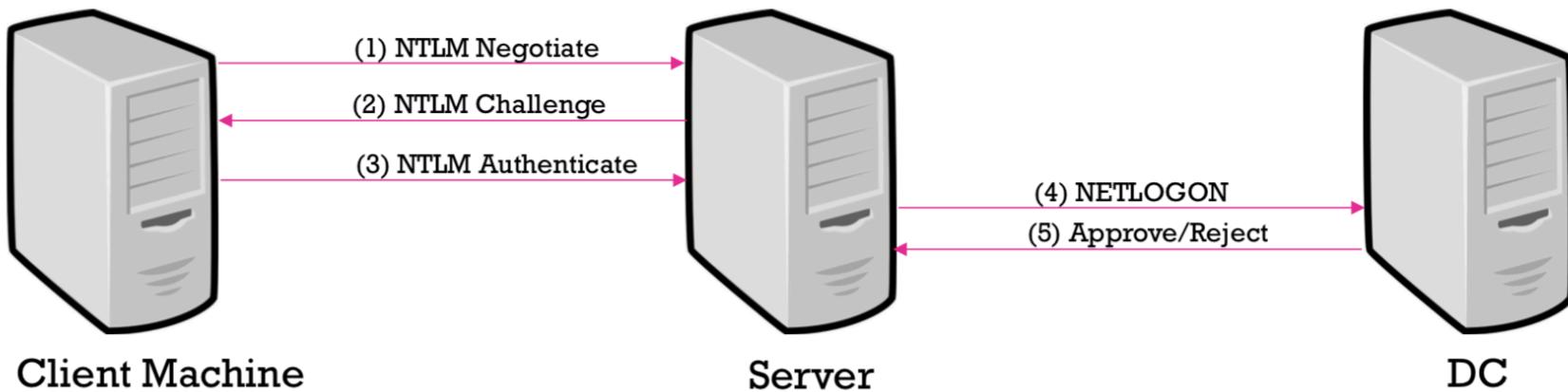
Fonte: <https://www.youtube.com/watch?v=Fg2gvk0qgjM>

Envenenamento LLMNR & NBT-NS



Fonte: <https://www.youtube.com/watch?v=Fg2gvk0qgjM>

Autenticação NTLM



00000000
0x4633172
0x376344d
ESP
CALL printf

O ataque

Aplicações:

- Responder: Envenenamento LLMNR & NBT-NS e Captura do NTLM Hash
- Hashcat: Quebra do Hash NTLM com ataque de força-bruta (Wordlist)

Demo Time

mindthesec[®]
/SÃO PAULO



```
PUSH 0x00000000
PUSH 0x4d633172*
PUSH 0x37634ed
PUSH ESP
CALL printf
```

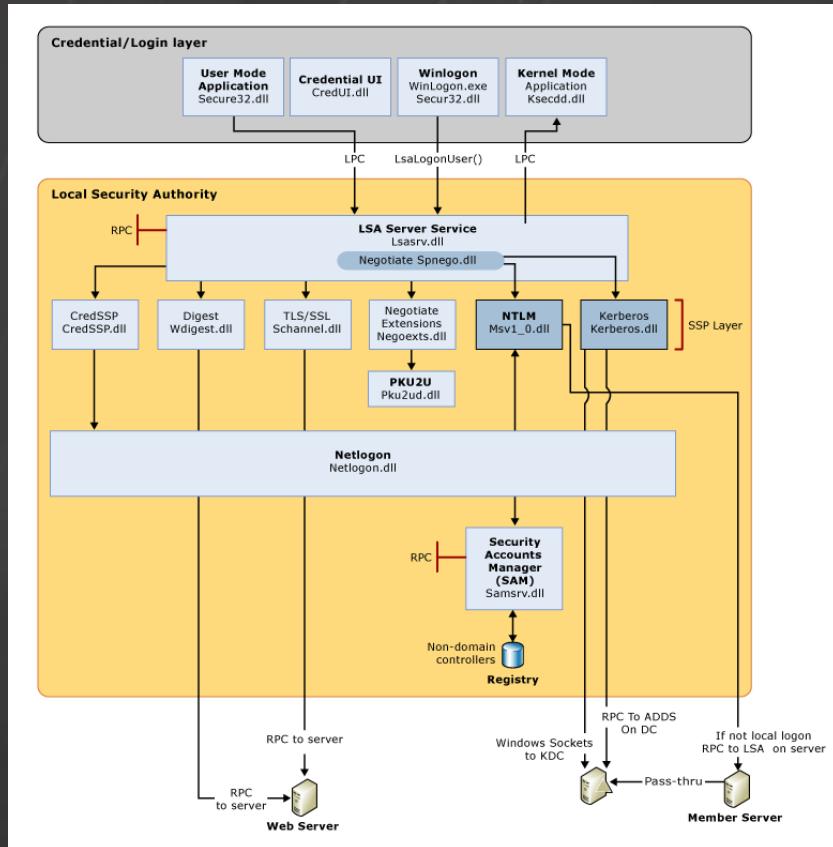
Mitigando envenenamento LLMNR & NBT-NS

- Desabilite os protocolos LLMNR e NBT-NS via registro do Windows ou GPO.
 - Para desabilitar LLMNR, selecione “Turn OFF Multicast Name Resolution” em Políticas Locais de Segurança (ou na GPO) > Configurações do Computador > Templates Administrativos > Rede > Cliente DNS dentro do Editor de Grupos de Segurança.
 - Para desabilitar NBT-NS, edite as configurações de rede em Propriedades TCP/IPv4 > Aba Avançado > WINS e selecione “Desabilitar NetBIOS sobre TCP/IP”.
- Habilite assinatura no protocolo SMB.
- Utilize políticas de alta complexidade de senha.
 - Tamanho mínimo de senha (Ex.: > 12 caracteres);
 - Black-list de palavras (Ex.: nome da empresa);
 - Caracteres especiais e etc...
 - Isso dificulta o processo de quebra da senha.

Passo 2

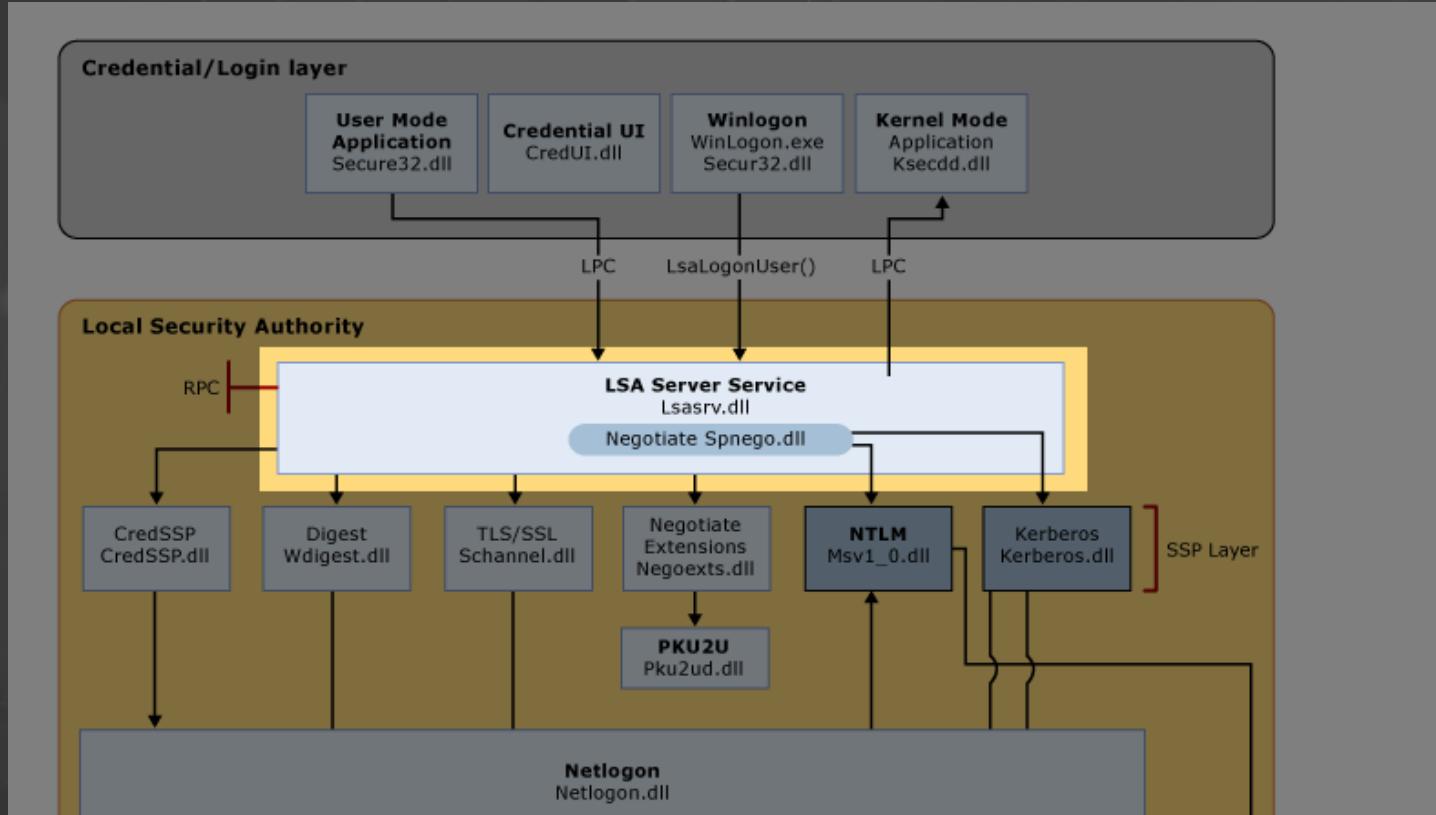
Escalando privilégios com Hashes/Senhas armazenadas em memória

Arquitetura LSASS



<https://docs.microsoft.com/en-us/windows-server/security/windows-authentication/credentials-processes-in-windows-authentication>

Arquitetura LSASS



<https://docs.microsoft.com/en-us/windows-server/security/windows-authentication/credentials-processes-in-windows-authentication>

O ataque

Aplicação:

- Mimikatz: Captura do Hash/Senha em memória

Demo Time

mindthesec[®]
/SÃO PAULO



```
PUSH 0x00000000
PUSH 0x4d633172*
PUSH 0x37634ed
PUSH ESP
CALL printf
```

Mimikatz

mimikatz 2.2.0 x64 (oe.eo)

```
.#####. mimikatz 2.2.0 (x64) #18362 Aug 14 2019 01:31:47
## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/
```

```
mimikatz # privilege::debug
```

```
Privilege '20' OK
```

```
mimikatz # sekurlsa::logonpasswords
```

```
Authentication Id : 0 ; 2641660 (00000000:00284efc)
Session          : Interactive from 2
User Name        : administrator
Domain          : HELVIOJUNIOR
Logon Server    : WIN-F5UEG9448DK
Logon Time      : 14/09/2019 22:42:57
SID              : S-1-5-21-3041531153-1085956979-1824583248-500
```

```
msv :
[00000003] Primary
* Username : Administrator
* Domain   : HELVIOJUNIOR
* NTLM     : 64f12cddaa88057e06a81b54e73b949b
* SHA1     : cba4e545b7ec918129725154b29f055e4cd5aea8
* DPAPI    : 0ee88bf6d368500f0478934d71971245
```

```
lspkg .
```



```
PUSH 0x00000000
PUSH 0x4633172
PUSH 0x376344d
PUSH ESP
CALL printf
```

Mitigando dump LSASS

- Desabilite senhas em texto-claro na memória.
 - Defina o parâmetro DWORD como 0 em HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/SecurityProviders/WDigest /UseLogonCredential.
- LSASS.exe protected mode
 - Defina o parâmetro DWORD como 1 em HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/Lsa
- Restrinja os acessos dos usuários ao mínimo necessário para suas atividades

Passo 3

Criando usuário com permissões de Domain Admin

O ataque

Aplicações:

- Mimikats: Pass-the-hash (Autenticação utilizando o Hash e não a Senha)
- Comando NET: Criação de um usuário com permissões de Domain Admin

Demo Time

mindthesec[®]
/SÃO PAULO



```
PUSH 0x00000000
PUSH 0x4d633172*
PUSH 0x37634ed
PUSH ESP
CALL printf
```

Recomendações Gerais

- NAC – Network Access Control
 - Não permita dispositivos não gerenciados conectarem em sua rede.
- Monitore o seu ambiente
 - Monitore e correlacione os eventos do seu ambiente (Exemplo: Autenticação, criação de credenciais, Pass-the-Hash e etc...)
 - Tenha uma metodologia de detecção e resposta de incidentes ativa.
- Teste os seus controles
 - Realize testes de invasão contínuos
 - Realize exercícios como War-Games (Ataque versus Defesa).

AGRADECIMENTO

helvio_junior@hotmail.com

@helvioju

<https://github.com/helviojunior/Presentations/tree/master/2019/MindTheSec>