

Forum: [Hack Forums](#)

Thread: [Privilege escalation on a Windows server 2012 R2](#)

CryptoLayer - February 13, 2020, 2:12 am

Hello guys , I have managed to have a meterpreter session on windows server 2012 R2 box and tried multiple exploits from the local exploit suggester that is integrated in metasploit framework but still did not manage have a UAC bypass or privilege escalation .

Any one as some suggestions or exploits I could use to elevate privilege ?

Thanks in advance .

CyberStrike - February 15, 2020, 6:41 am

The real secret is enumerate, enumerate and then enumerate a few more times, sometimes the exploit suggester is not exact, manually look at autorunsc find orphaned dlls/exes also check what patches are applied, read/write/append files/directories, scheduled tasks everything. There are a few tutorials here on this forum for privesc against WIndows just search.

CryptoLayer - February 15, 2020, 1:36 pm

(Feb 15, 2020 07:41 AM)CyberStrike Wrote: [\[CITE\]](#) The real secret is enumerate, enumerate and then enumerate a few more times, sometimes the exploit suggester is not exact, manually look at autorunsc find orphaned dlls/exes also check what patches are applied, read/write/append files/directories, scheduled tasks everything. There are a few tutorials here on this forum for privesc against WIndows just search.

Hi there , thanks for the reply .

I'm going to do some research .

Brill - February 15, 2020, 3:38 pm

there are so many priv esc guides out there...

<https://www.fuzzysecurity.com/tutorials/16.html>

inf1nity - February 15, 2020, 7:44 pm

(Feb 13, 2020 03:12 AM)C0DeLeSs Wrote: [\[CITE\]](#) Hello guys , I have managed to have a meterpreter session on windows server 2012 R2 box and tried multiple exploits from the local exploit suggester that is integrated in metasploit framework but still did not manage have a UAC bypass or privilege escalation .

Any one as some suggestions or exploits I could use to elevate privilege ?

Thanks in advance .

AV might be holding you back. Did you try veil evasion or similar?

Bass_Reeves - February 15, 2020, 7:48 pm

(Feb 15, 2020 05:30 PM)M0HX Wrote: [\[CITE\]](#) thank me later bobo ?

<https://github.com/hfiref0x/UACME>

This looks awesome! Thanks for sharing.

CryptoLayer - February 17, 2020, 1:26 pm

(Feb 15, 2020 05:30 PM)M0HX Wrote: [\[CITE\]](#) thank me later bobo ?

<https://github.com/hfiref0x/UACME>

Hey there , compiling this project , will tell you if it worked :)

POLY MATH - February 24, 2020, 2:26 pm

(Feb 15, 2020 07:41 AM)CyberStrike Wrote: [\[CITE\]](#) The real secret is enumerate, enumerate and then enumerate a few more times, sometimes the exploit suggerter is not exact, manually look at autorunsc find orphaned dlls/exes also check what patches are applied, read/write/append files/directories, scheduled tasks everything. There are a few tutorials here on this forum for privesc against WIndows just search.

This guy is on the right track but before you do any of this. You'll first need to enumerate and enumerate.

Seriously though. Automated tools catch low hanging fruit more often then not but manual enumeration is almost always beneficial.

It helps to understand the environment also.