

Forum:[Hack Forums](#)

Thread: [Privilege Escalation Windows](#)

tacobella2 - October 30, 2024, 9:46 am

Hi

when it comes to linux there are numerous misconfigurations or exploits to run and use and most likely no antivirus

as for windows, most users are very limited and isolated not just by the system default but mostly by the antivirus

aside from windows services misconfigurations. my question is. people who still take advantage of tools like mimikatz, localpotato .. etc.

how do they allow these files to get in without disabling antivirus (which requires higher access they trying to gain)

for what i know mostly obfuscation is the only way but eg windows defender is very updated and patches bypasses pretty quick and some even automatically.

are such tools too dirty to be used or obfuscated now in 2024?

is this the best it gets?

DramaKing - October 30, 2024, 10:08 am

(Oct 30, 2024 09:46 AM)tacobella2 Wrote: [\[CITE\]](#) Hi

when it comes to linux there are numerous misconfigurations or exploits to run and use and most likely no antivirus

as for windows, most users are very limited and isolated not just by the system default but mostly by the antivirus

aside from windows services misconfigurations. my question is. people who still take advantage of tools like mimikatz, localpotato .. etc.

how do they allow these files to get in without disabling antivirus (which requires higher access they trying to gain)

for what i know mostly obfuscation is the only way but eg windows defender is very updated and patches bypasses pretty quick and some even automatically.

are such tools too dirty to be used or obfuscated now in 2024?

is this the best it gets?

Mimikatz is going to be difficult to crypt. Its behavior is too well known, and LSASS has too many protections since Microsoft increased the security baseline.

tacobella2 - October 30, 2024, 11:04 am

(Oct 30, 2024 10:08 AM)DramaKing Wrote: [\[CITE\]](#) Mimikatz is going to be difficult to crypt. Its behavior is too well known, and LSASS has too many protections since Microsoft increased the security baseline.

what would be doable or accessible with antivirus active and windows defender filtering ps cmds. basic obfuscation trials like msfvenom meterpreter obfuscated n singed with ScareCrow .. etc are still blocked

im wondering cause some people claim there's so much to do on such a closed environment

DramaKing - October 30, 2024, 11:15 am

(Oct 30, 2024 11:04 AM)tacobella2 Wrote: [\[CITE\]](#) what would be doable or accessible with antivirus active and windows defender filtering ps cmds. basic obfuscation trials like msfvenom meterpreter obfuscated n singed with ScareCrow .. etc are still blocked

im wondering cause some people claim there's so much to do on such a closed environment
Pop UAC prompts on a loop until access is granted.