

Forum:[Hack Forums](#)

Thread: [What are your strategies?](#)

slagalica - May 3, 2014, 2:28 am

What are your strategies to gain shell access on Windows 7?

I'm pretty new to hacking and while I was researching I noticed that so many tutorials described here on hackforums rely too much on social engineering.

I mean, if I want to target a specific person on the network and that person doesn't open any suspicious links or run .exe files, how would I approach him?

Are there ways that I can force him to run malicious files or gain access to his shell without him knowing it?

If I understood right, exploiting windows xp is very easy and doable without the victim knowing it, but most people here use windows 7 so I would appreciate any help regarding this.

DrDinosaur - May 3, 2014, 2:53 am

Because most people aren't running vulnerable services on a Windows 7 machine. On a LAN? Try MITM or DNS spoofing.

mudasir007 - May 3, 2014, 6:36 am

(May 3, 2014 02:28 AM)slagalica Wrote: [\[CITE\]](#) What are your strategies to gain shell access on Windows 7?

I'm pretty new to hacking and while I was researching I noticed that so many tutorials described here on hackforums rely too much on social engineering.

I mean, if I want to target a specific person on the network and that person doesn't open any suspicious links or run .exe files, how would I approach him?

Are there ways that I can force him to run malicious files or gain access to his shell without him knowing it?

If I understood right, exploiting windows xp is very easy and doable without the victim knowing it, but most people here use windows 7 so I would appreciate any help regarding this. yes there are ways to hack a persons windows 8.1 machine with metasploit, a simple tool like netcat can give you a shell but you have to try harder, you have to look at weakness in target system like browser, networkshare, openports, services, etc to attack it if you are unable to attack it please give us a summary of target machine we may be able to help

hahdbwoannniabs - May 3, 2014, 7:13 am

Use nmap and scan the target machine, look for any un-obvious services running on it, look up exploits for them.

Sundrop - May 3, 2014, 8:05 am

I agree with him ^

That's a good method unless you have physical access, in which you could easily just bind System32 to a port using netcat.

slagalica - May 3, 2014, 11:35 am

(May 3, 2014 02:53 AM)DrDinosaur Wrote: [\[CITE\]](#) Because most people aren't running vulnerable services on a Windows 7 machine. On a LAN? Try MITM or DNS spoofing.

(May 3, 2014 06:36 AM)mudasir007 Wrote: [\[CITE\]](#) yes there are ways to hack a persons windows 8.1 machine with metasploit,a simple tool like netcat can give you a shell but you have to try harder,you have to look at weakness in target system like browser, networkshare,openports,services,etc to attack it if you are unable to attack it please give us a summary of target machine we may be able to help

(May 3, 2014 07:13 AM)ThatExploitTho Wrote: [\[CITE\]](#) Use nmap and scan the target machine, look for any un-obvious services running on it, look up exploits for them.

Thank you guys for answering. I will look into those methods. Although I'm quite familliar with MITM/DNS spoofing I haven't tryed netcat and nmap yet.

SIM-5561 - May 3, 2014, 11:45 am

(May 3, 2014 06:36 AM)mudasir007 Wrote: [\[CITE\]](#) yes there are ways to hack a persons windows 8.1 machine with metasploit,a simple tool like netcat can give you a shell but you have to try harder,you have to look at weakness in target system like browser, networkshare,openports,services,etc to attack it if you are unable to attack it please give us a summary of target machine we may be able to help

You know, there are times I think, is this guy any good? Then there are times I think, yeah this guy knows his shit - this is one of those times.

You should write up a proper tutorial, step by step of you hacking into a Windows 7 machine via services or open ports. That kind of stuff would boost your rep massively (providing it was your own work). Plus it'd be good for everyone to learn from.

mudasir007 - May 3, 2014, 9:01 pm

(May 3, 2014 11:45 AM)9puzzles Wrote: [\[CITE\]](#) You know, there are times I think, is this guy any good? Then there are times I think, yeah this guy knows his shit - this is one of those times.

You should write up a proper tutorial, step by step of you hacking into a Windows 7 machine via services or open ports. That kind of stuff would boost your rep massively (providing it was your own work). Plus it'd be good for everyone to learn from.Thanks 9puzzles i will write a little tutorial on how to exploit windows With local privilege Escalation it is my own work, But I don't know how increase feedback for my thread