

Forum:[Hack Forums](#)

Thread: [I scanned my target via Metasploit community and got 0 vulnerabilities, now what?](#)

the lone sherrif - September 10, 2017, 1:35 pm

the title explains what is my problem

dbasejob1 - September 10, 2017, 2:09 pm

first is it on wan or on lan

can scan port to see what are all service on network, if is lan

if is wan you can send mail or link

need more info on your target to say what to do

but for sure, do scanning searching for all service working on network

can do a man in the middle, exploit(because you can add exploit)

give more detail please

with respect

peace

LD_PRELOAD - September 10, 2017, 2:26 pm

The problem is in the title.

the lone sherrif - September 10, 2017, 2:32 pm

(Sep 10, 2017 02:09 PM)dbasejob1 Wrote: [\[CITE\]](#) first is it on wan or on lan

can scan port to see what are all service on network, if is lan

if is wan you can send mail or link

need more info on your target to say what to do

but for sure, do scanning searching for all service working on network

can do a man in the middle, exploit(because you can add exploit)

give more detail please

with respect

peace

thank you for trying to be so helpful but i'm talking about a generic case when i scan and get no vulnerabilities

(Sep 10, 2017 02:26 PM)LD_PRELOAD Wrote: [\[CITE\]](#) The problem is in the title.

when the guys who hacked the pentagon scanned it they also got 0 vulnerabilities and yet they did hack it, meaning the system was hackable, my question is how to find more ways to hack a device when MSFC failed

tetra - September 10, 2017, 2:51 pm

OP relying on scanners is never gona evolve you out of the script kiddie stage. I would suggest setting up vulnerable VM's (google virtualbox or vmware) using this site <https://www.vulnhub.com> and practice on them to gain some important skills before trying them in the wild. They have walkthroughs incase you ever need a hint.

dbasejob1 - September 10, 2017, 2:53 pm

ok now you expose the target = WAN = mean over internet = now i can try to resolve your question maybe

ok so what is an exploit ?

is a mechanisme doing a command without the will of the owner of the system

(sorry i gonna try to make a picture exemple to get what i want to explain to you)

from where internet come = Router = the box giving and adress like a nodes on coast
over it is traffic = different language = mean what tool communicate like goods transport from boat to coast
so first thing, looking at traffic paket = sniffing = we can determine what systeme or tool are use
if is potato is for potato market, if is tomato is for tomato market
so here is the first place of a network
so how we can operate for this case, we can try to login inside the router, by typing public ip of the router and port
how we found it = exemple with nmap, we can scan ip and port, so service....
ok we know that NsANfLCiAHsBc.com = 56.98.65.23 "ip is invented not existing"
this ip have port open to give access to some service, like user out connection, but even for service working on it, like pos terminal for stores, printer, fax, computer, etc
So first of all is a router or a server.....
let's say is a server of the site NsANfLCiAHsBc.com, site is on port 80, but have a php door to connect, or other service, with nmap and port scanning, we can determine service
first exploit would be to look the version use of the service, of the server use....
second if is possible, try a bruteforce with hydra or burpsuite for exemple...
next would be to try to found a user of this service like a worker. over internet you can found a lot...
try to attack user's login, is always a solution
can attack phone of worker, control it, obtain some mail or other superior phone number in the companie, can do an irl attack on user...
is really depend on the target and the will...
can kick like boxe, like karate, like aikido, all work, but depend of the will and the ability and possibility to do it
with respect
peace
contact = dbasejob@jabbb.im

LD_PRELOAD - September 11, 2017, 12:14 am

(Sep 10, 2017 02:32 PM)the lone sherrif Wrote: [\[CITE\]](#) thank you for trying to be so helpful but i'm talking about a generic case when i scan and get no vulnerabilities

when the guys who hacked the pentagon scanned it they also got 0 vulnerabilities and yet they did hack it, meaning the system was hackable, my question is how to find more ways to hack a device when MSFC failed You change your mindset out of thinking that a single tool is everything there is to hacking. Go and learn the craft. You don't know what you don't know.