

Forum:[Hack Forums](#)

Thread: [what can you do with open ports?](#)

boleii466 - June 6, 2024, 7:16 am

lets say that you port scan a network and you find out that port 21 ftp, 22 ssh, 23 telnet, 80 http, 443 https.... are all open

what can you really do?

from all of the educational articles, videos and threads i read, everyone just stays at the topic of "exploiting unclosed / open ports", but how does that specifically work?

are there any scripts involved? do you just somehow exploit an unpatched vulnerability? how does the process, specifically, work?

BiNBo - June 6, 2024, 7:46 am

Well once you've discovered those ports, you can check and see what services and versions of those services are running. From there you can potentially exploit outdated services, or start staging different attacks like brute forcing logins for SSH, FTP, etc. That's just a quick rundown, but the enumeration stage is crucial, and one of the most important parts of it is identifying open ports which might have other vectors for you to compromise in your pursuit of a foothold.

P1N7 - June 6, 2024, 10:28 am

You could use a packet sniffer to download the data that is being transmitted via UPnP on those ports.

DramaKing - June 6, 2024, 1:27 pm

(Jun 6, 2024 07:16 AM)boleii466 Wrote: [\[CITE\]](#) lets say that you port scan a network and you find out that port 21 ftp, 22 ssh, 23 telnet, 80 http, 443 https.... are all open

what can you really do?

from all of the educational articles, videos and threads i read, everyone just stays at the topic of "exploiting unclosed / open ports", but how does that specifically work?

are there any scripts involved? do you just somehow exploit an unpatched vulnerability? how does the process, specifically, work?

There's no simple answer for exploiting vulnerabilities if any known ones exist. Or even a complicated answer. You need to know the five phases of hacking to begin with: reconnaissance & footprinting, scanning & enumeration, gaining access, maintaining access, and covering tracks. Once you enumerate services and grab banners, you will hopefully have the information that you can use to search for vulnerabilities and exploits.