Introduction to Computer Security Module – G6077

-

Additional Nmap tools:

Ncrack, Nping and Ncat (part 1)

Warning: Attempting to crack any application or files that you do not have the permission is illegal. Ncrack and other tools must be used only on the applications that I used in my notes.

# Ncrack

One of the most aggressive tools included in the Nmap suite is Ncrack—a tool for aggressively brute-forcing (or "cracking") network services. While it's not unique in its functionality (as there are many software tools that can brute force network accounts), the ability to easily (and natively) integrate with Nmap (and Nmap results) makes it ideal for use after scans.

### Task

Find and open the Ncrack tool

### Task

The most straightforward way to run Ncrack is very simple; as shown in the preceding screenshot, one may simply run ncrack followed by the protocol URI and hostname (or IP address) of the targeted service. Used in this way, we can attack services (such as SSH) by running ncrack ssh://TARGET.

Run the following command. If it gives you installation related error, it means that Ncrack is not installed. To install see the next task and then comeback to do this task again.

ncrack –v ssh://localhost

If the command work, wait for five minutes and hit enter, what percentage of cracking is done. It took about 20 hours on my machine. After a little while, stop the cracking, no need to wait for that long.

Ncrack is most effective when used with a known username. For example, if we knew that a given system had a root login that allowed password authentication, we would run ncrack --user root ssh://TARGET to brute force against that username.

### Task.

### You need to do this task only if you find that Ncrack did not work in previous task due to installation. It will display a message like Ncrack not found etc.

Run the following scripts in the order they are listed

1. wget http://nmap.org/ncrack/dist/ncrack-0.4ALPHA.tar.gz
2. tar -xzf ncrack-0.4ALPHA.tar.gz
3. cd ncrack-0.4ALPHA
4. ./configure
5. make ; sudo mak

### Task

Although this functionality is very useful, it is by no means unique; many tools, such as **Hydra** and **Medusa** can run brute force attacks. The true benefits of Ncrack are revealed when Ncrack is run based on the results from an Nmap scan. Let's say that we are conducting a penetration test or security assessment on a series of hosts across a Class C (/24) network. If, for example, 200 hosts are online—and each one has between five and ten services listening—you're looking at a lot of different brute force attempts to implement over the command line. Ncrack, however, can do this for you.

Just as Nmap can export different log types, Ncrack can read them as input—and automatically attack the services in question. For example, if we have an -oX flag (XML output) from an Nmap scan, Ncrack can use -iX to input that same list as a target file:

Write a command that gives XML output of scanning the scanme.nmap.org application.

Note where you are saving the output

From the same drive run ncrack –iX nameOfTheXMLFile

// provide correct XML filename

We can easily see that by scanning nmap.scanme.org and exporting an XML file, we can easily import it to Ncrack. Although this is just one host, you can imagine how much time we would save if we used this for a large network! It's also worth noting that services that either don't support login, or that Ncrack doesn't know how to use, are by default excluded from the scan. In this case, nping-echo was excluded due to not having a login prompt.

There are a few flags that are absolutely necessary to run Ncrack effectively, in addition to specifying target files. The two most important flags for Ncrack are -U and -P flags, which each point to a text file containing usernames and passwords.

There are a plethora of other flags, configuration settings, and uses for Ncrack—all of which can be found on the very useful main page.

# Nping

Although you might not expect it from its name, Nping does much more than ICMP echo requests (what we typically call a ping)—primarily, it can also execute ARP probes and TCP or UDP requests to given ports, in order to find out if those hosts are online based on the response. For example, if we want to debug certain network connections, we can easily use Nping to determine what's happening on the wire. The following screenshot shows a basic Nping command:

### Task

nping –c2 scanme.nmap.org –p80 –tcp

In the preceding output, we ran Nping with two checks per port (-c 2, where "c" stands for "count"), and scanned ports on scanme.nmap.org—80. In this case, 80 is an open port, and we can clearly see the responses we are expecting.

Find information on TCP Handshake and check how the part of the output listed below is related to TCP handshake. Notice the word echo in output.

SENT (0.1696s) ICMP [172.31.42.57 > 45.33.32.156 Echo request (type=8/code=0) id=51844 seq=1] IP [ttl=64 id=52845 iplen=28 ]

RCVD (0.2326s) ICMP [45.33.32.156 > 172.31.42.57 Echo reply (type=0/code=0) id=51844 seq=1] IP [ttl=41 id=49025 iplen=28 ]

Hackers love the output of Nping. One of the most unique features of Nping is its built-in echo mode. The echo mode allows Nping to work as both a server and a client, and sends packets back and forth. By showing the entirety of a network connection (the packets that the client is sending, in their original state, and the packets as they are received by a server), it is extremely easy to detect network address translation, interfering intrusion prevention systems, packet shaping, and so on.

### Task

Run the same nping command with –v. Check if the information about packet is more or less.

# Ncat

Ncat has SSL support (natively), great connection redirection reliability, and several other built-in features that make it a great tool in a security administrator's toolbox.

Ncat has two modes: the "listen" mode, which listens on a provided port for incoming connections, and the "connect" mode, through which commands are sent and feedback is received. In the connect mode, we can use Ncat to connect to a variety of services, including HTTP-based web servers.

Ncat is also very useful when conducting a penetration test or security assessment, as it can be used as both a method for data exfiltration, and as a way to have a persistent backdoor into a compromised system.

The ability to send a file through Ncat uses both the "listen" and "connect" functionalities of the tool.

### Task

If Ncat does not work because it is not installed, then you will need to install it first. The package name is ncat with apt-get install.

### Task

Run the following command and check its output. What scripting language can be noticed in the output? Notice the version number in DTD line (Document Type Definition).

Ncat nmap.org 80

In one word, it invokes a GET /HTTP/1.0 REQUEST. This same functionality of Ncat can also be used to connect to many different types of services, including SMTP, FTP, POP3, and so on. When trying to send different inputs to different protocols, Ncat can be invaluable!

### Task See the power of Ncat – as a Chat tool

Open two terminals

On one terminal enter ncat –l 8080

On second terminal enter ncat localhost 8080

Enter a text like Hello Imran and hit enter. Now check the first terminal. The text appears there.

Ctrl + C to get out of chat mode.

### Task Sending files

NC can also be used to copy the files from one system to another, though it is not recommended & mostly all systems have ssh/scp installed by default. But none the less if you have come across a system with no ssh/scp, you can also use nc as last ditch effort.

Start with machine on which data is to be received & start nc is listener mode,

ncat -l  8080 > file.txt

Now on the machine from where data is to be copied, run the following command,

ncat 192.168.1.100 8080 --send-only < data.txt

Here, data.txt is the file that has to be sent. –send-only option will close the connection once the file has been copied. If not using this option, than we will have press ctrl+c to close the connection manually.

We can also copy entire disk partitions using this method, but it should be done with caution.