111/TCP/UDP - Pentesting Portmapper

Basic Information

Provides information between Unix based systems. Port is often probed, it can be used to fingerprint the Nix OS, and to obtain information about available services. Port used with NFS, NIS, or any rpc-based service.

Default port: 111/TCP/UDP, 32771 in Oracle Solaris

```
PORT    STATE SERVICE
111/tcp open  rpcbind
```

Enumeration

```
rpcinfo irked.htb
nmap -sSUC -p111 192.168.10.1
```

Sometimes it doesn't give you any information, in other occasions you will get something like this:

program	version	netid	address	service	owner
100000	2	tcp	0.0.0.0.0.111	portmapper	unknown
100000	2	udp	0.0.0.0.0.111	portmapper	unknown
100008	1	udp	0.0.0.0.4.1	walld	unknown
100002	1	udp	0.0.0.0.4.2	rusersd	unknown
100002	2	udp	0.0.0.0.4.2	rusersd	unknown
100024	1	udp	0.0.0.0.4.11	status	unknown
100024	1	tcp	0.0.0.0.4.2	status	unknown
100021	2	tcp	0.0.0.0.4.3	nlockmgr	unknown
100021	1	udp	0.0.0.0.2.175	nlockmgr	unknown
100021	3	udp	0.0.0.0.2.175	nlockmgr	unknown
100021	1	tcp	0.0.0.0.2.175	nlockmgr	unknown
100021	3	tcp	0.0.0.0.2.175	nlockmgr	unknown

Shodan

- `port:111 portmap`

RPCBind + NFS

If you find the service NFS then probably you will be able to list and download(and maybe upload) files:

100003	3	tcp	0.0.0.0.8.1	nfs
100003	4	tcp	0.0.0.0.8.1	nfs
100227	3	tcp	0.0.0.0.8.1	-
100003	3	udp	0.0.0.0.8.1	nfs
100003	4	udp	0.0.0.0.8.1	nfs

Read 2049 - Pentesting NFS service to learn more about how to test this protocol.

NIS

If you find the service `ypbind` running:

100007	2	udp	0.0.0.0.3.210	ypbind	superuser
100007	1	udp	0.0.0.0.3.210	ypbind	superuser
100007	2	tcp	0.0.0.0.3.213	ypbind	superuser
100007	1	tcp	0.0.0.0.3.213	ypbind	superuser

You can try to exploit it. Anyway, first of all you will **need to guess the NIS "domain name"** of the machine (when NIS is installed it's configured a "domain name") and **without knowing this domain name you cannot do anything**.

Upon obtaining the NIS domain name for the environment (example.org in this case), use the ypwhich command to ping the NIS server and ypcat to obtain sensitive material. You should feed encrypted password hashes into John the Ripper, and once cracked, you can use it t

```
root@kali:~# apt-get install nis
root@kali:~# ypwhich -d example.org 192.168.10.1
potatohead.example.org
root@kali:~# ypcat -d example.org -h 192.168.10.1 passwd.byname
tiff:noR7Bk6FdgcZg:218:101::/export/home/tiff:/bin/bash
katykat:d.K5tGUWCJfQM:2099:102::/export/home/katykat:/bin/bash
james:i0na7pfgtxi42:332:100::/export/home/james:/bin/tcsh
florent:nUNzkxYF0Hbmk:199:100::/export/home/florent:/bin/csh
dave:pzg1026SzQlwc:182:100::/export/home/dave:/bin/bash
yumi:ZEadZ3ZaW4v9.:1377:160::/export/home/yumi:/bin/bash
```

Master file	Map(s)	Notes
/etc/hosts	hosts.byname, hosts.byaddr	Contains hostnames and IP details
/etc/passwd	passwd.byname, passwd.byuid	NIS user password file
/etc/group	group.byname, group.bygid	NIS group file
/usr/lib/aliases	mail.aliases	Details mail aliases

RPC Users

If you find the **rusersd** service listed like this:

```
100002    1    udp       0.0.0.0.4.2           rusersd    unknown
100002    2    udp       0.0.0.0.4.2           rusersd    unknown
```

You could enumerate users of the box. To learn how read 1026 - Pentesting Rsusersd.

Bypass Filtered Portmapper port

If during a nmap scan you see open ports like NFS but the port 111 is filtered, you won't be able to exploit those ports. But, if you can simulate a locally a portmapper service and you tunnel the NFS port from your machine to the victim one, you will be able to use regular tools to exploit those services.
More information in https://medium.com/@sebnemK/how-to-bypass-filtered-portmapper-port-111-27cee52416bc

Shodan

- Portmap

HackTricks Automatic Commands

```
Protocol_Name: Portmapper    #Protocol Abbreviation if there is one.
Port_Number:  43     #Comma separated if there is more than one.
Protocol_Description: PM or RPCBind        #Protocol Abbreviation Spelled out

Entry_1:
  Name: Notes
  Description: Notes for PortMapper
  Note: |
    Provides information between Unix based systems. Port is often probed, it can be used to fingerpr

    https://book.hacktricks.xyz/pentesting/pentesting-rpcbind

Entry_2:
  Name: rpc info
  Description: May give netstat-type info
  Command: whois -h {IP} -p 43 {Domain_Name} && echo {Domain_Name} | nc -vn {IP} 43

Entry_3:
  Name: nmap
  Description: May give netstat-type info
  Command: nmap -sSUC -p 111 {IP}
```

← Network Services Pentesting - Previous
110,995 - Pentesting POP

Next - Network Services Pentesting
113 - Pentesting Ident

Last modified 2mo ago