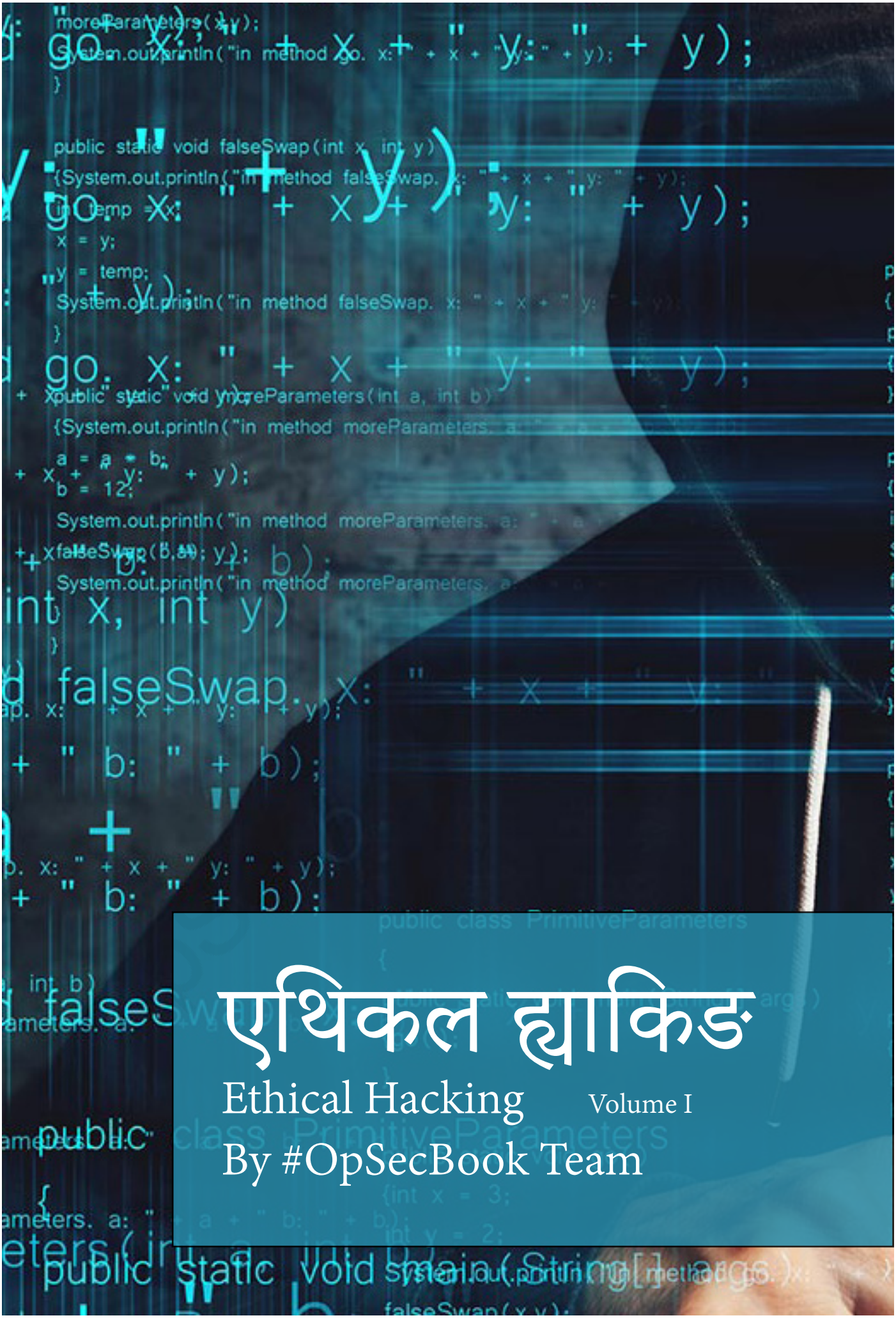


एथिकल ह्याकिङ

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

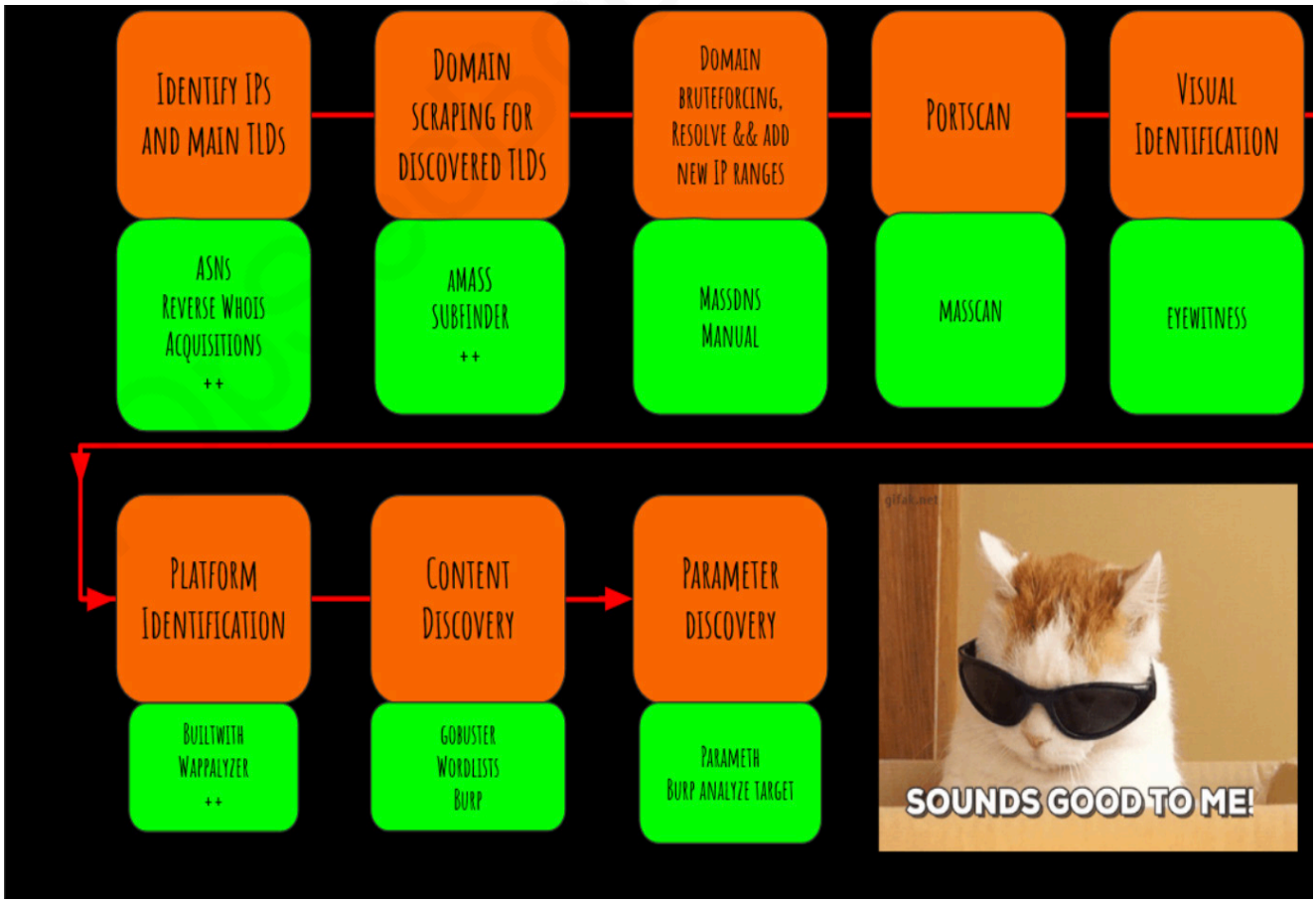
Table of Content :

Reconnaissance

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

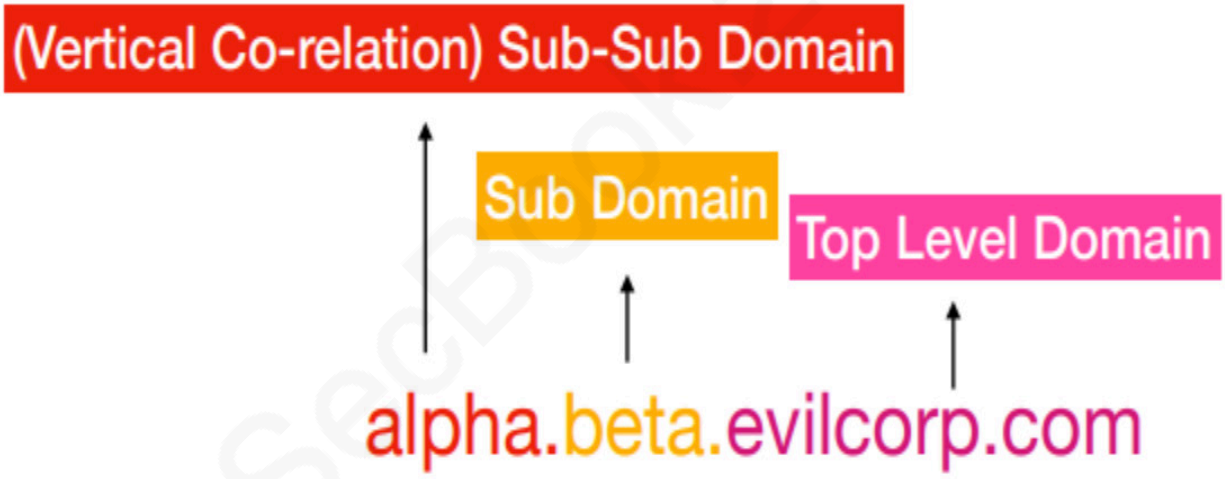
Reconnaissance phase मा attacker, जासूसहरू जस्तो व्यवहार गर्दछन्, संकलन गरिएको जानकारीलाई analysis गरेर उनीहरू आफ्नो target लाई जतिसक्दो बुझ्ने प्रयास गर्दछन्। यसको मुख्य लक्ष्य भनेको target नेटवर्क चलाउने व्यवस्थापक भन्दा राम्रोसँग आफूले त्यस network को बारेमा जान्नु हो। प्रविधिको कमजोरीहरू अध्ययन गर्दै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

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



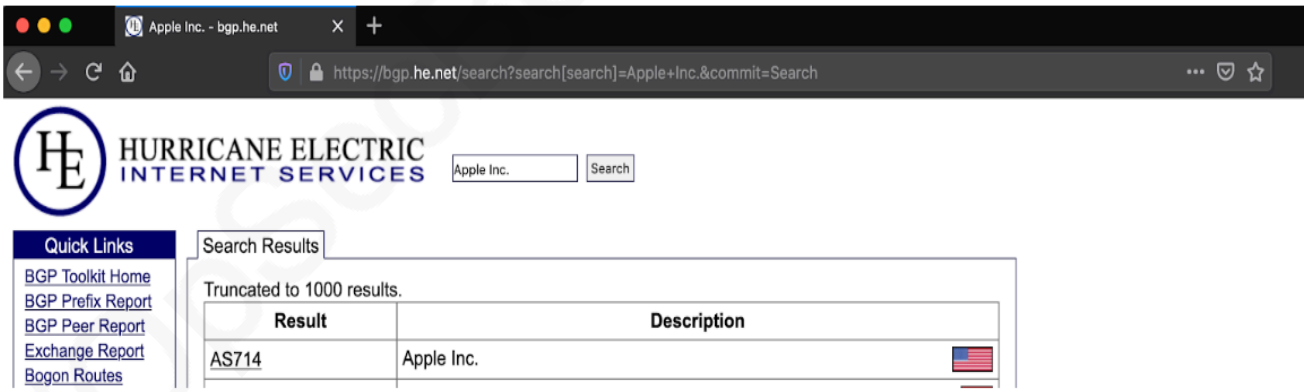
१. १ ASN Enumeration :

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

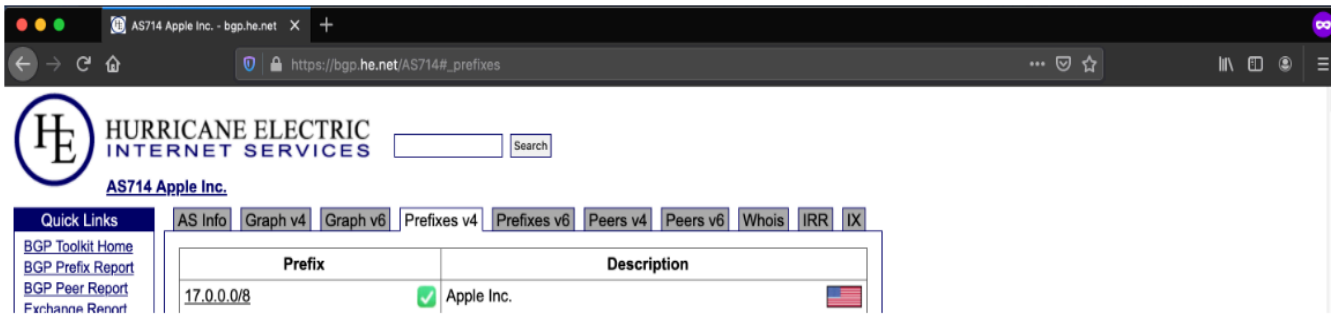
यदि तपाईंसँग भएको domain द्वारा ASN नम्बर फेला पार्न सक्नुभयो भने, तपाईं त्यहाँ भएको सबै publicly faced ip ब्लकहरूको enumeration सजिलैसँग गर्न सक्नुहुन्छ। यो सरल अभ्यास हो, किनकि धेरै संस्थाहरूसँग स्वचालित (automated) संयन्त्र हुदैन जुन publicly face गरिरहेका पूर्वाधारहरूमा constantly मोनिटर गरिरहन्छ।

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



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 ।

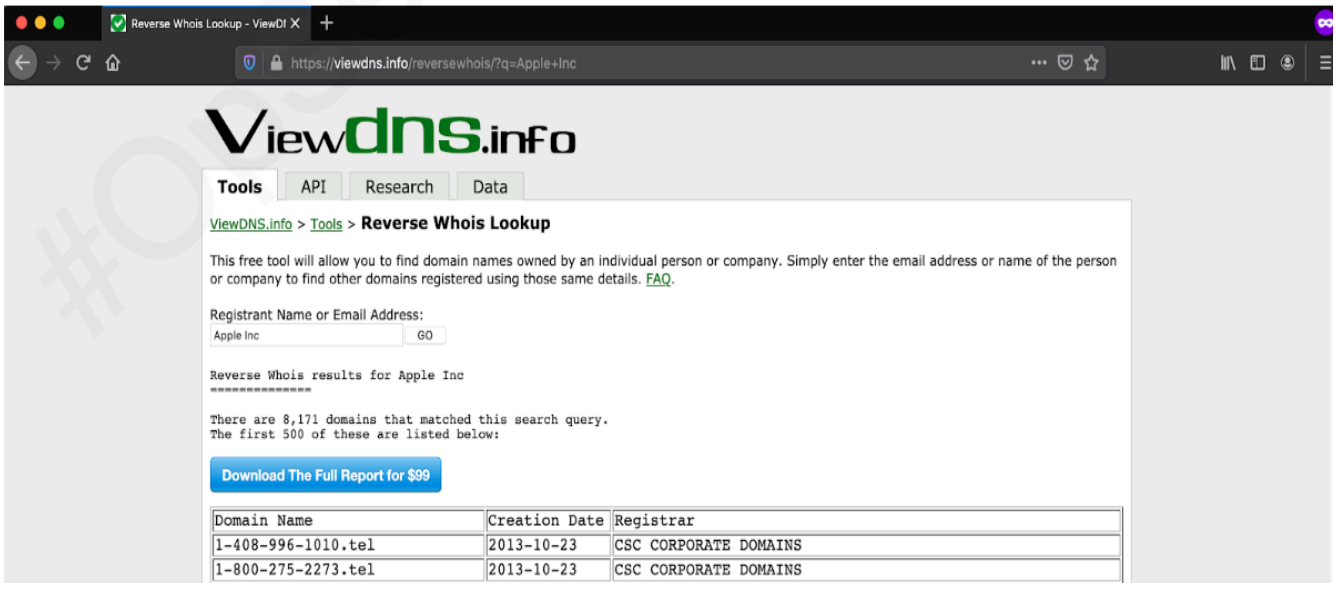


हामी Prefix v4 ट्याबमा देख्न सक्छौं, Apple Inc को 17.0.0.0/8 को subnet range रहेको छ तसर्थ यसले security परीक्षण (test) को लागि हाम्रो दायरा (scope) मा बृद्धि गराएको छ।

१.२ Reverse Whois Lookup:

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

यस https://viewdns.info/ साइटबाट Apple Inc. को जानकारी लिने प्रयास हजुरहरुले तल साभार गरिएको चित्रमा देख्न सक्नु हुन्छ :



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।

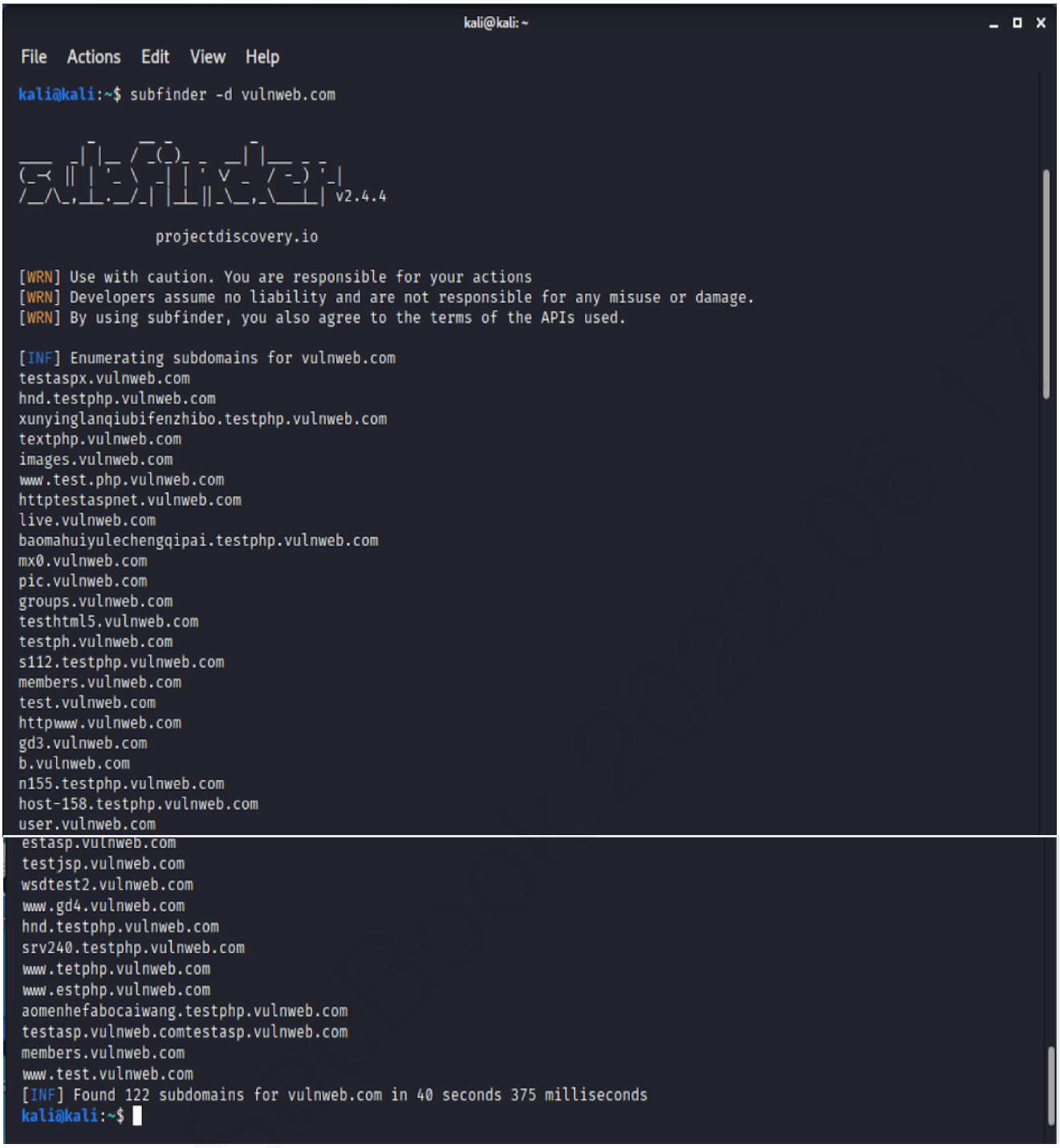
२ . पत्ता लगाईएको TLD को domain scraping गर्ने

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 सहजरुपले 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 ।

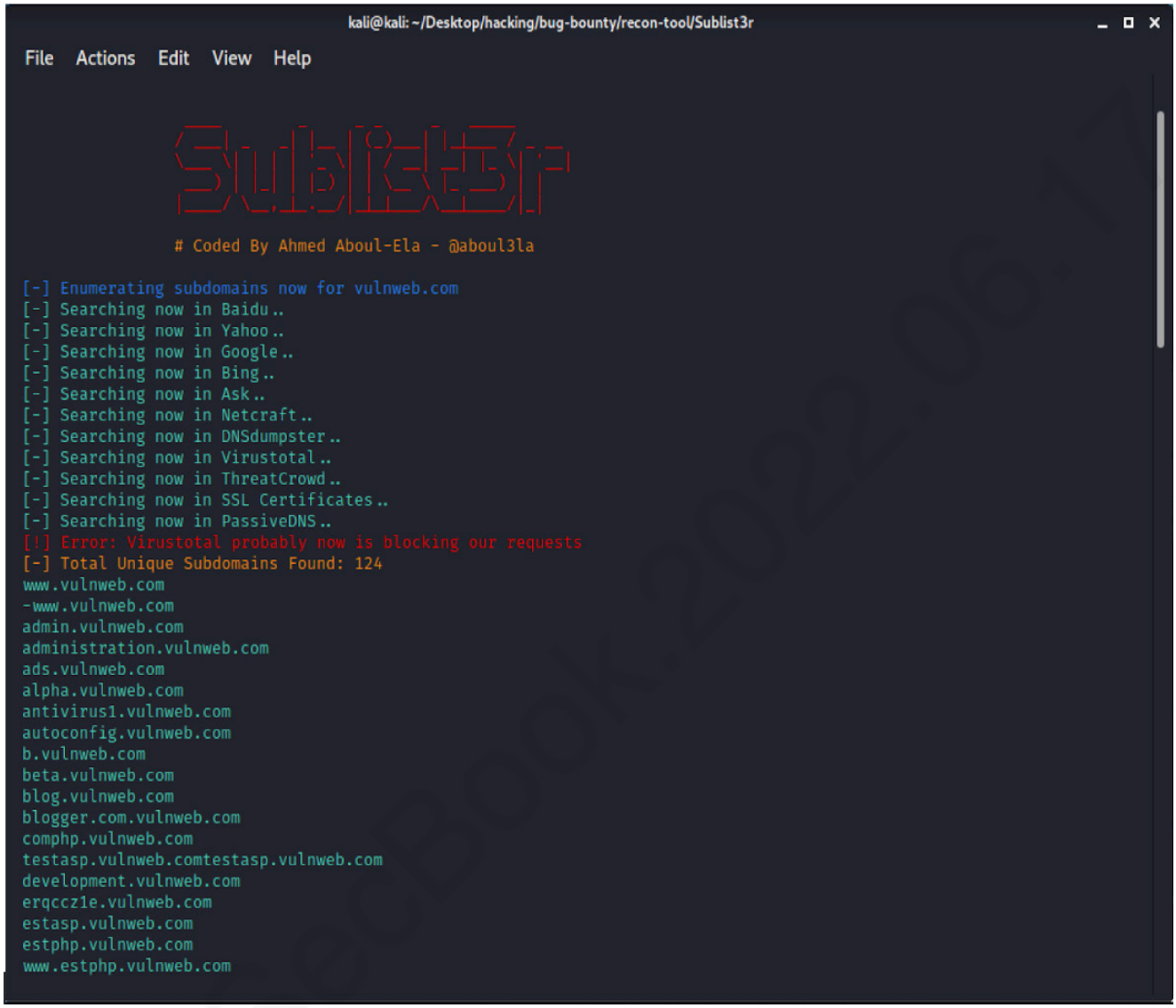


माथि चित्रमा हामीले हाम्रो target को सबडोमेन , Subfinder प्रयोग गरेर पत्ता लगायौं र करीव १२२ सबडोमेन पत्ता लगाउन सफल भएका छौं।

२.२ 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।

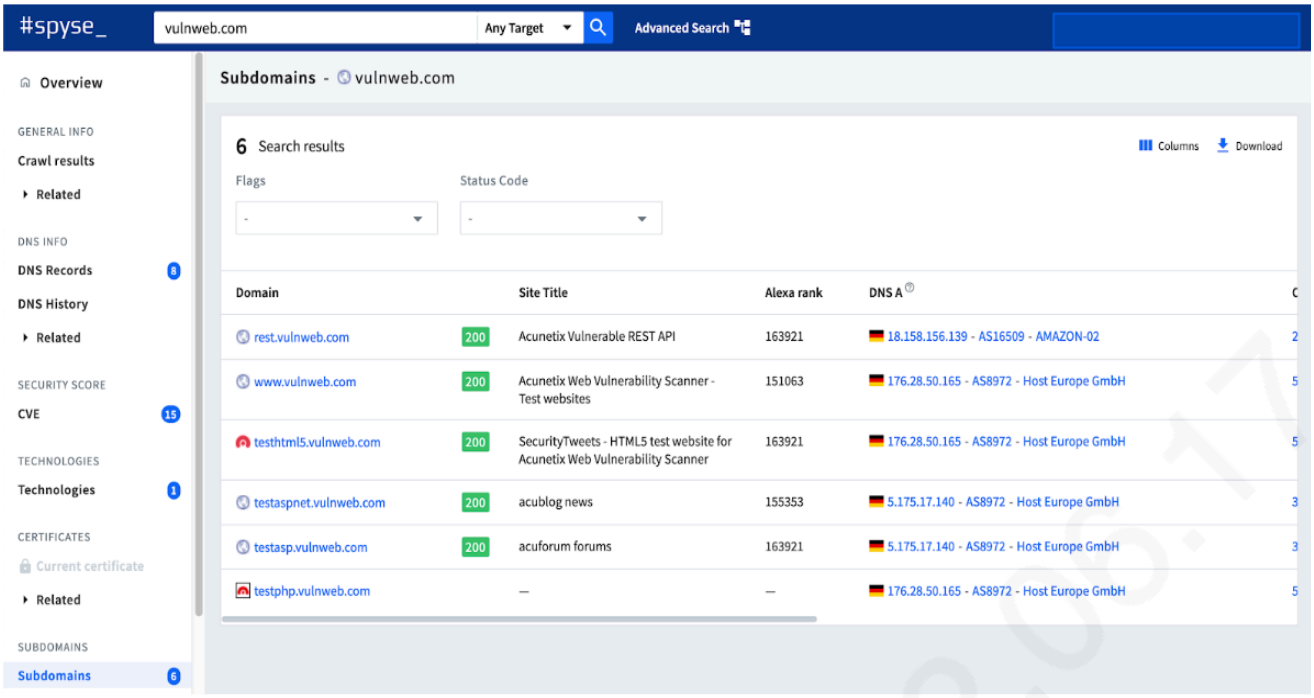
Sublist3r ले Google, Yahoo, Bing, Baidu जस्ता धेरै search engine हरूको प्रयोग गरेर subdomain संकलन गर्दछ।



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

२.३ Spyse :

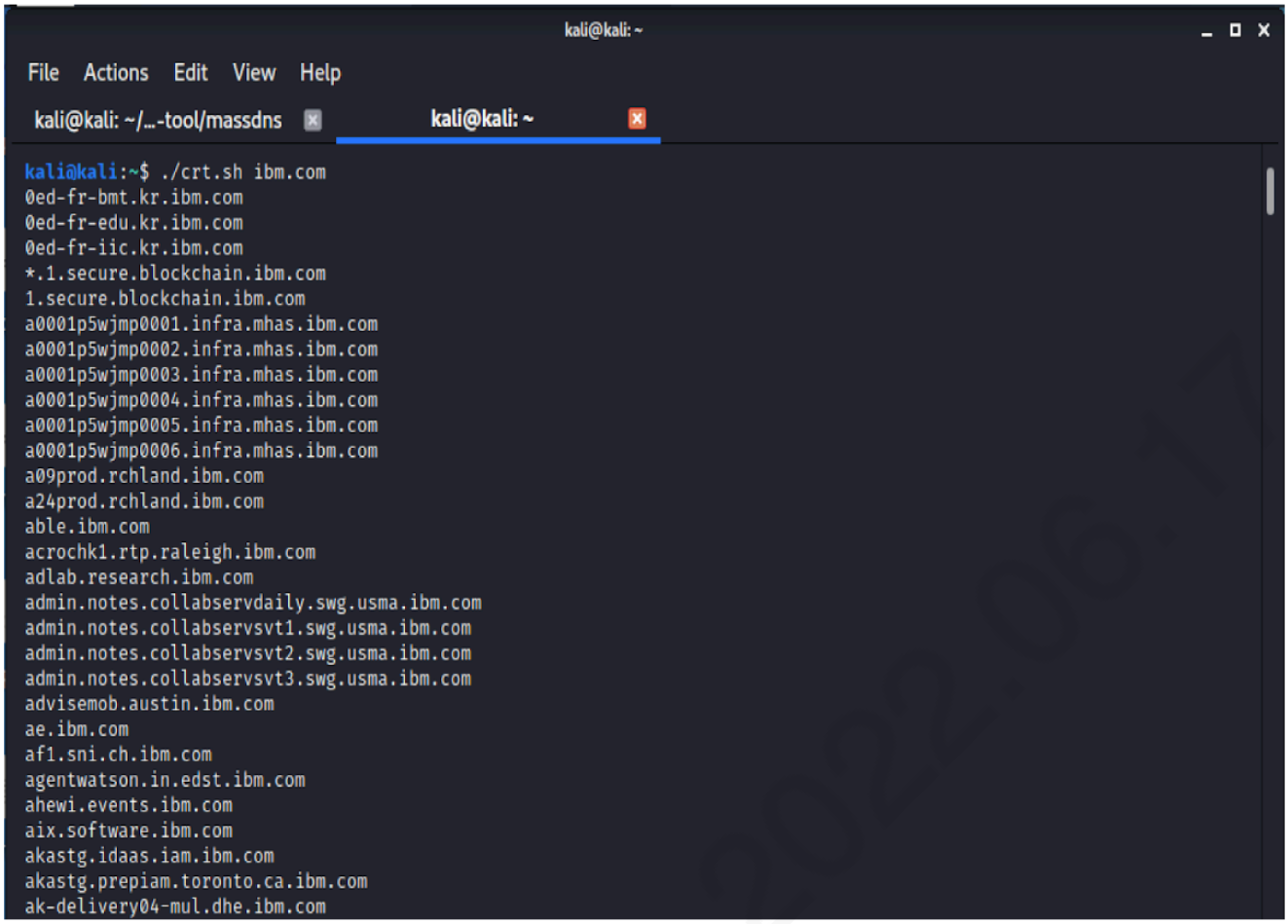
यो एक Cybersecurity Search Engine tool हो जसले इन्टरनेटमा छरिएर रहेको सूचनालाई एकत्रित गरी हाम्रो अनुकूलताअनुसार प्रयोग गर्न मद्दत पुर्याउँदछ ।



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

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 लगहरू फेला पार्न र हामीलाई subdomain गणना गर्नमा मद्दत पुर्याउँदछ।



३. Domain Brute forcing

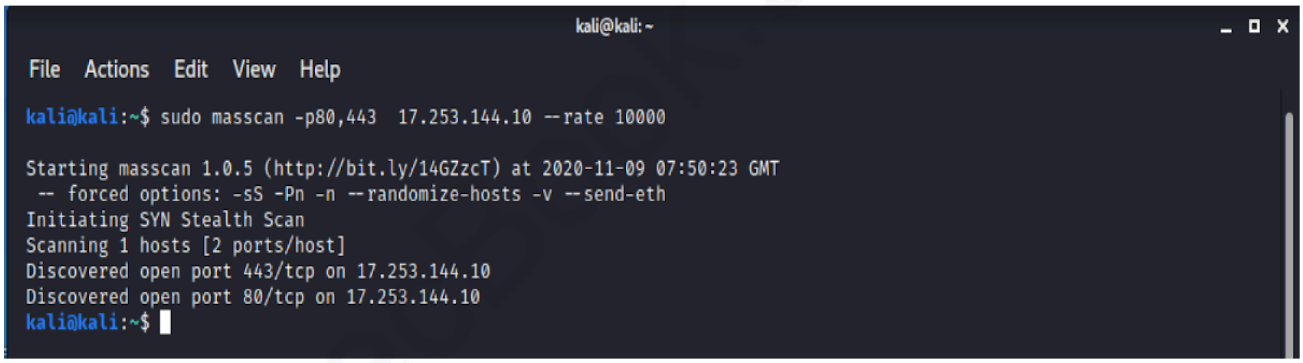
Dictionary based enumeration subdomainहरू खोजी गर्ने अर्को प्रविधि हो। यदि कुनै एक subdomain को नाम अनुमान गर्न अप्ठेरो भएको खण्डमा bruteforcing को प्रयोग गरेर त्यस subdomain को नाम पत्ता लगाउन सकिन्छ ।

३.१ Subbrute :

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

४. पोर्ट स्क्यान (Port scan)

Port Scanning एक महत्वपूर्ण कुरा हो जसबाट हामीले target मा चलिर-हेका 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 ।



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 गाह्रो पर्नसक्छ। उदाहरणको लागि दशवटा

subdomain हुँदा हामीलाई सबै link check गर्न कठिन पर्न जान्छ । यसको लागि हामी tomnomnom द्वारा सिर्जना गरिएको httprobe 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 ।

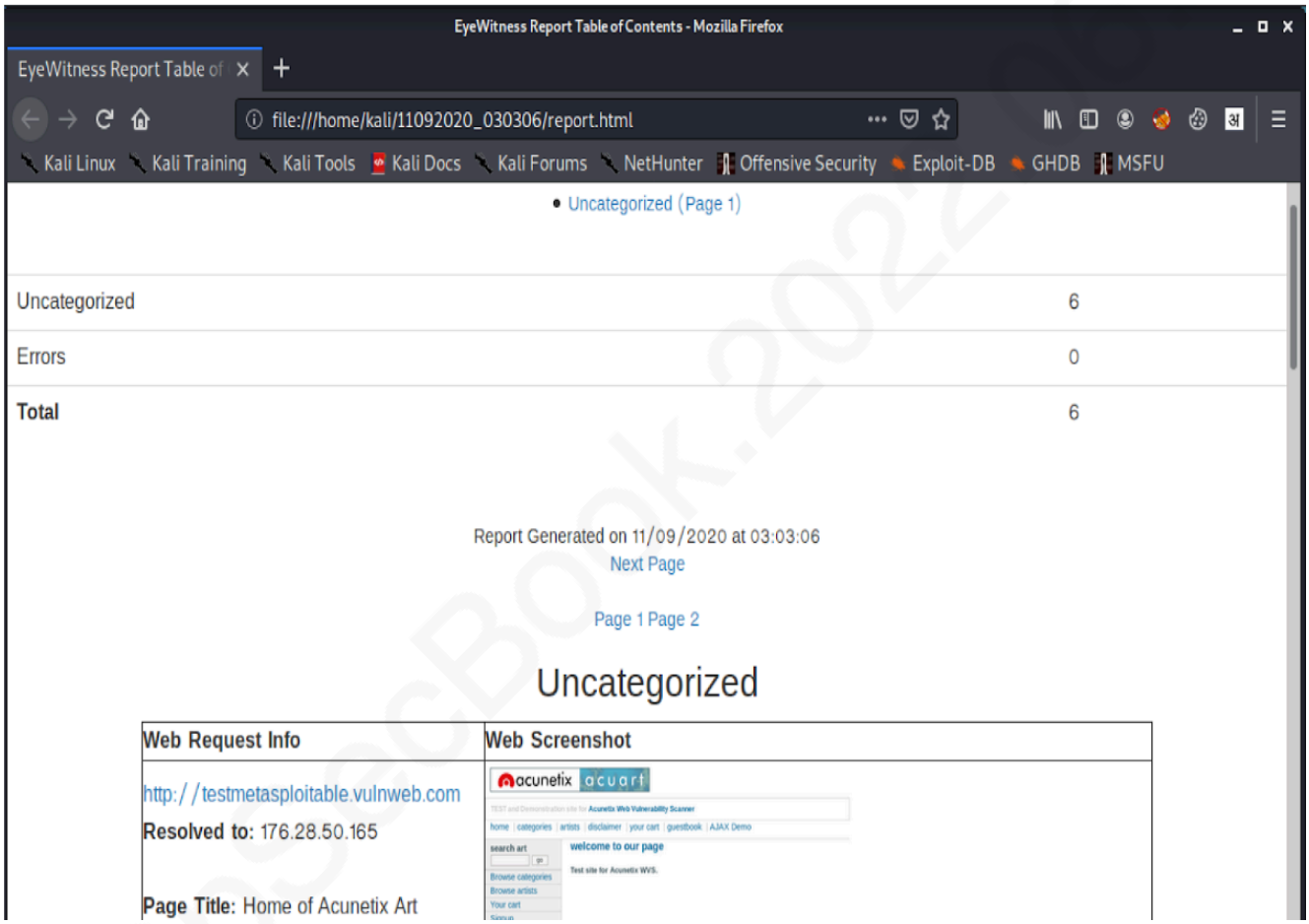
पहिले हामी httprobe मा सबडोमेनहरू पास गरेर alive-domain.txtमा save गर्नेछौं ।

अब alive सबडोमेनलाई तल दिएझै eyewitness मा पास गर्नेछौं ।

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

$ eyewitness alive-domain.txt

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



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

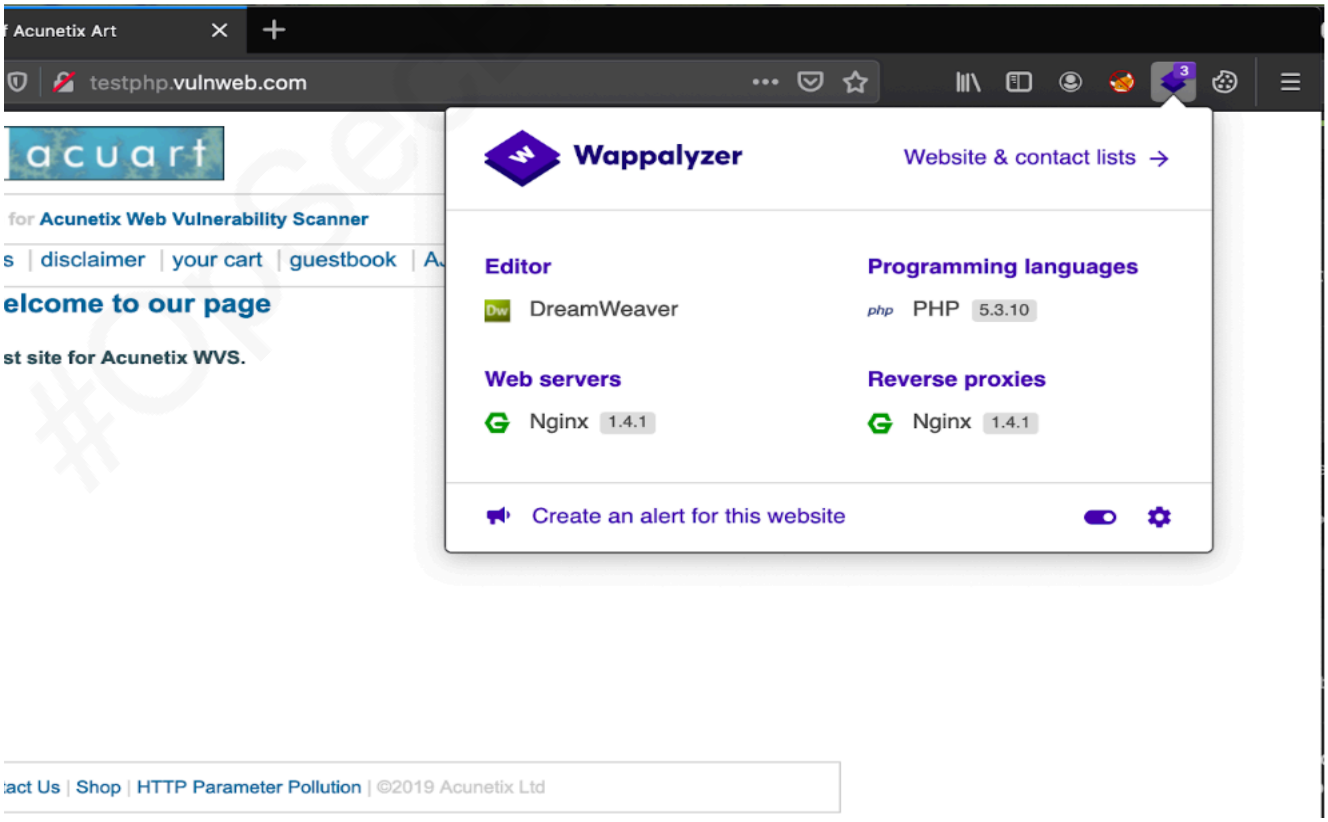
६. Platform पहिचान (identification)

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 सक्दछौ ।

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 सर्भ-रहरू, जाभास्क्रिप्ट फ्रेमवर्क जस्ता कुराहरूको सजिलैसँग जानकारी दिन सक्दछ ।

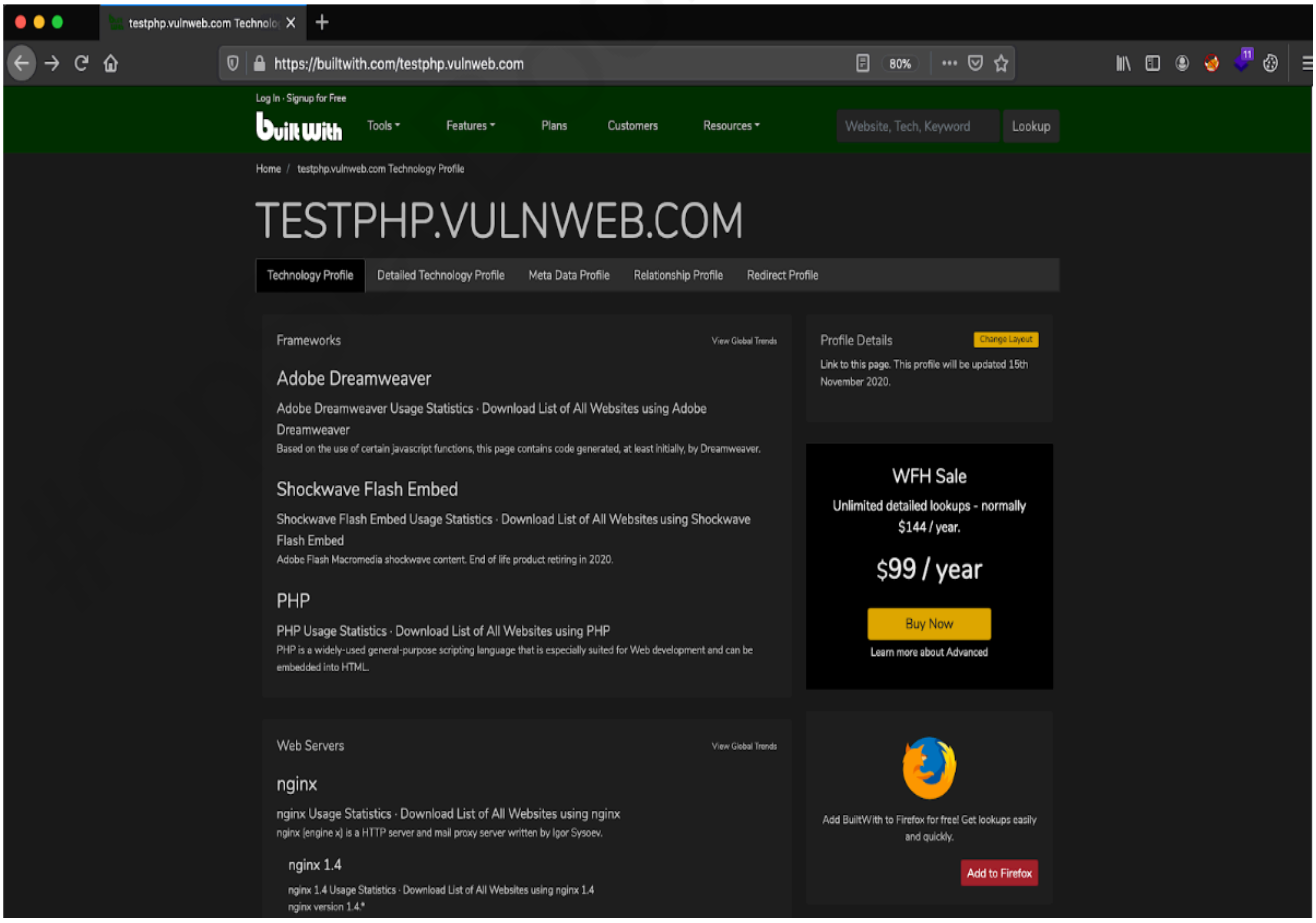


माथिको चित्रमा हामीले testphp.vulnweb.com मा प्रयोग भएको टेक्नोलोजी पत्ता लगाएका छौं ।

६.२ Whatweb :

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

६.३ Builtwith

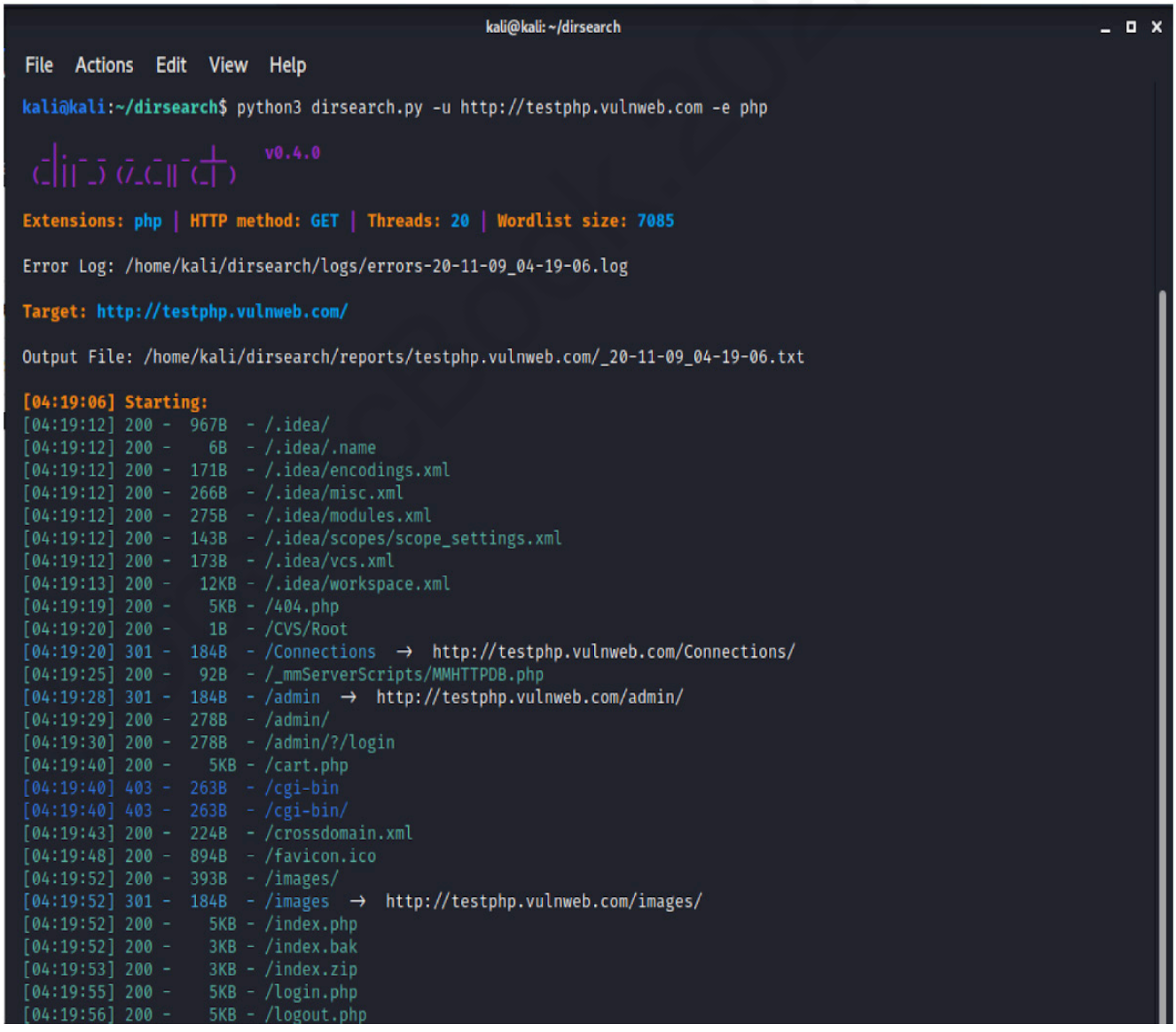


Builtwith पनि आफ्नै addons संग आउँदछ । हामी यसको माध्यमले साइट-हरूमा प्रयोग भएको टेक्नोलोजी सजिलैसँग जान्न सक्दछौं ।

७. Content डिस्कवरी (Discovery)

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

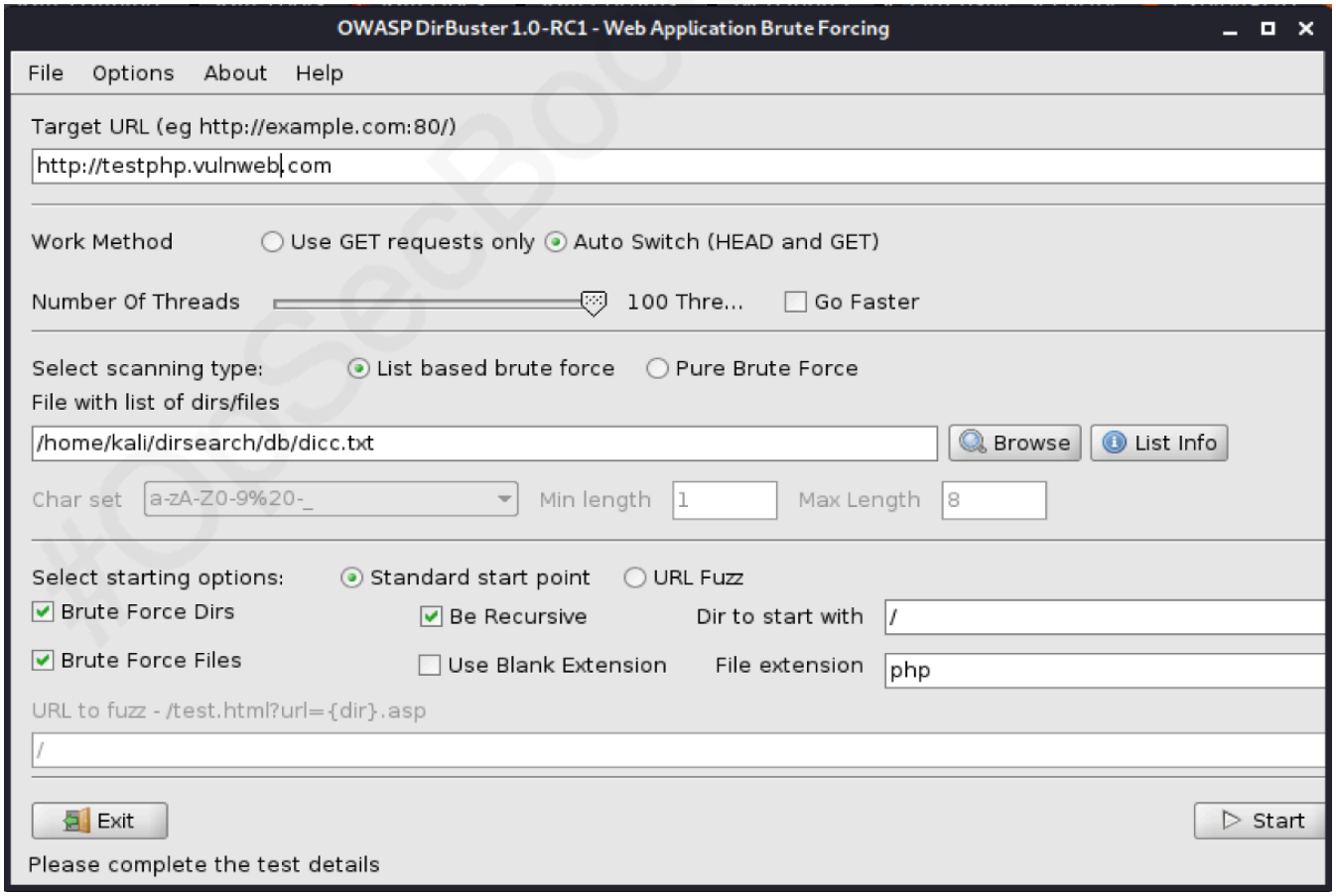
७.१ Content Discovery using Dirsearch :



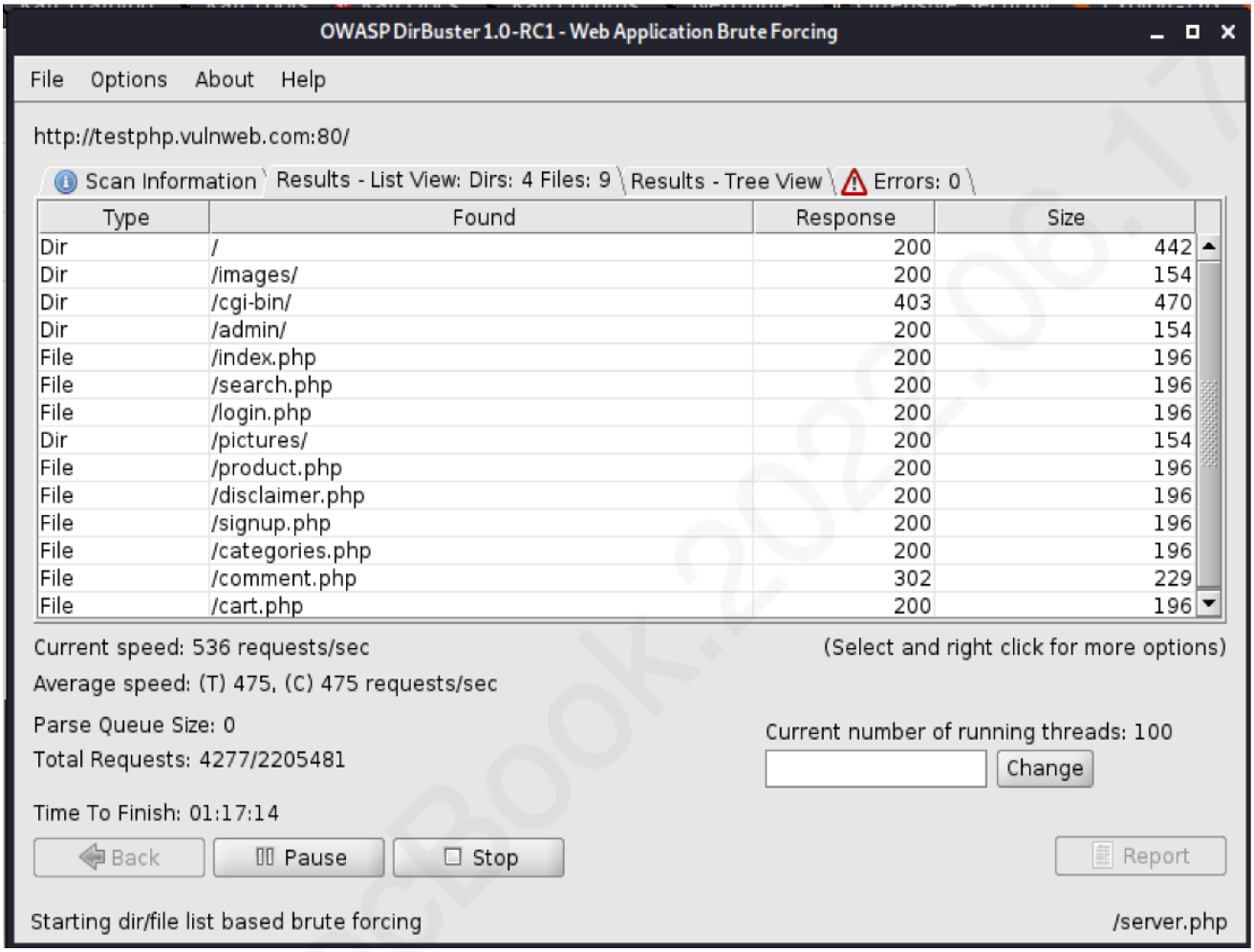
माथिको चित्रमा दिएको result साइट testphp.vulnhub.com को रहेको छ जसमा Dirsearch प्रयोग गरेर content Discovery गरिएको छ ।

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। वेबसाईटहरु हेर्दा सुरक्षित देखिएपनि developer-हरुले कुनै न कुनै ठाउँमा गल्ती गरिरहेको हुन्छ । जस्तै कुनै test purpose मा प्रयोग गरिएको फाइलहरू production server मै भुलेर छोडिदिने जस्ता कार्यले webserver vulnerable हुन्छ । Dirbuster ले त्यस्ता file हरु खोज्न मदत गर्दछ ।



हामीले हाम्रो dicc.txt फाइल Dirbuster मा लोड गर्‍यौं र url पनि बारमा राख्यौं। Start Button मा क्लिक गर्दा तल चित्रमा 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 ।

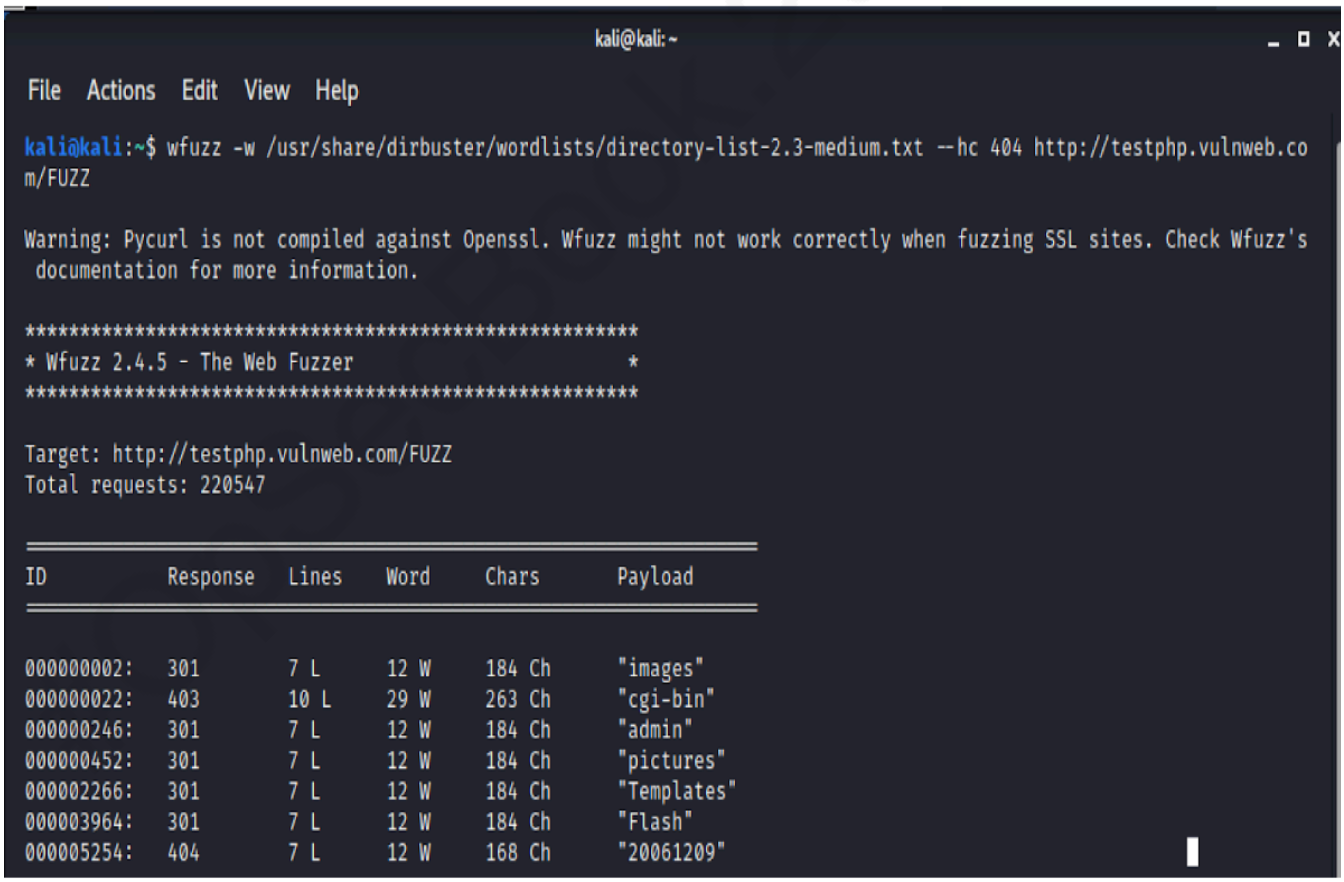
List हरु निम्नलिखित छन् :

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

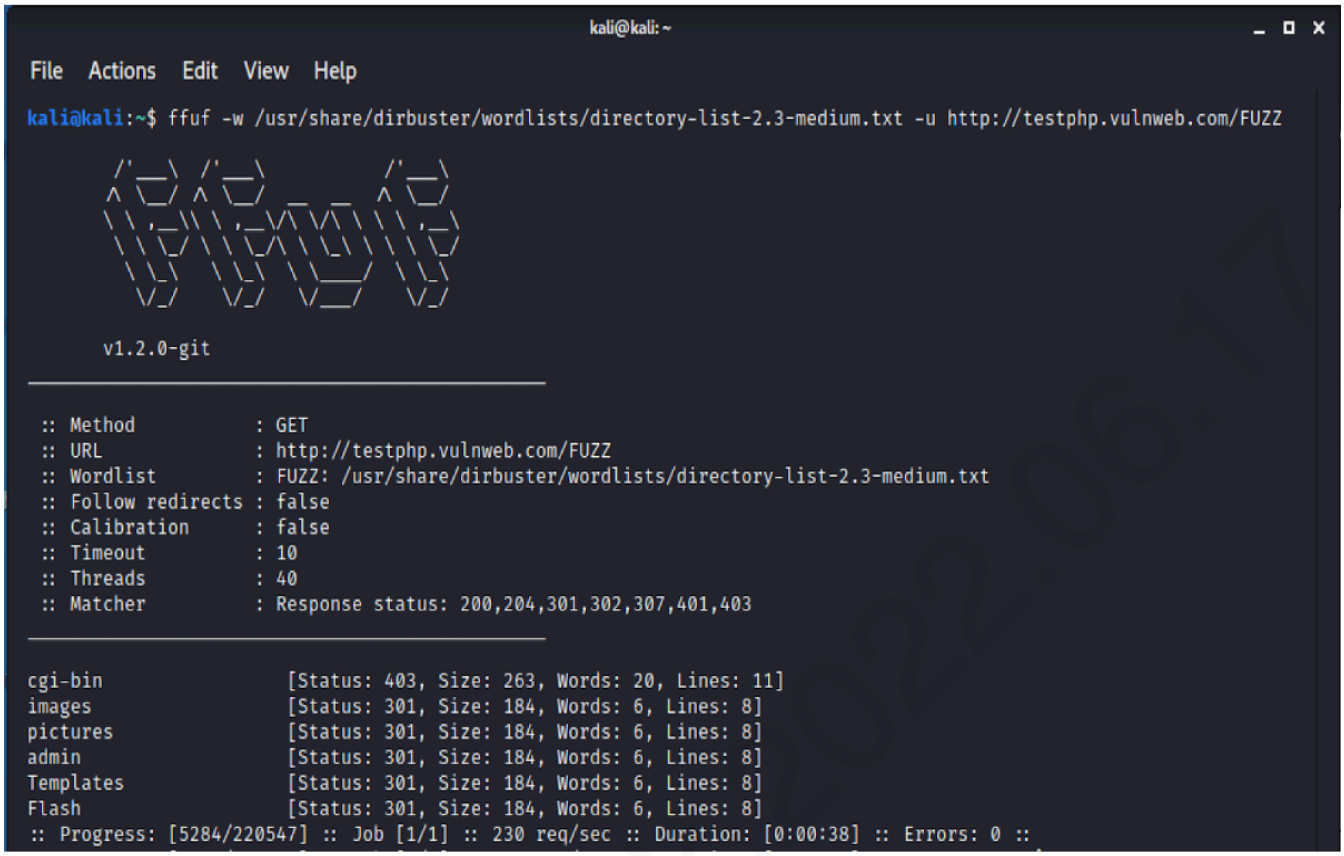
- directory-list-lowercase-2.3-small.txt - (81629 words)
- directory-list-lowercase-2.3-medium.txt - (207629 words)
- directory-list-lowercase-2.3-big.txt - (1185240 words)
- directory-list-1.0.txt - (141694 words)
- apache-user-enum-1.0.txt - (8916 usernames)
- apache-user-enum-2.0.txt - (10341 usernames)

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

७.३ Directory search using wfuzz:



७.४ Content Discovery using FFuF:

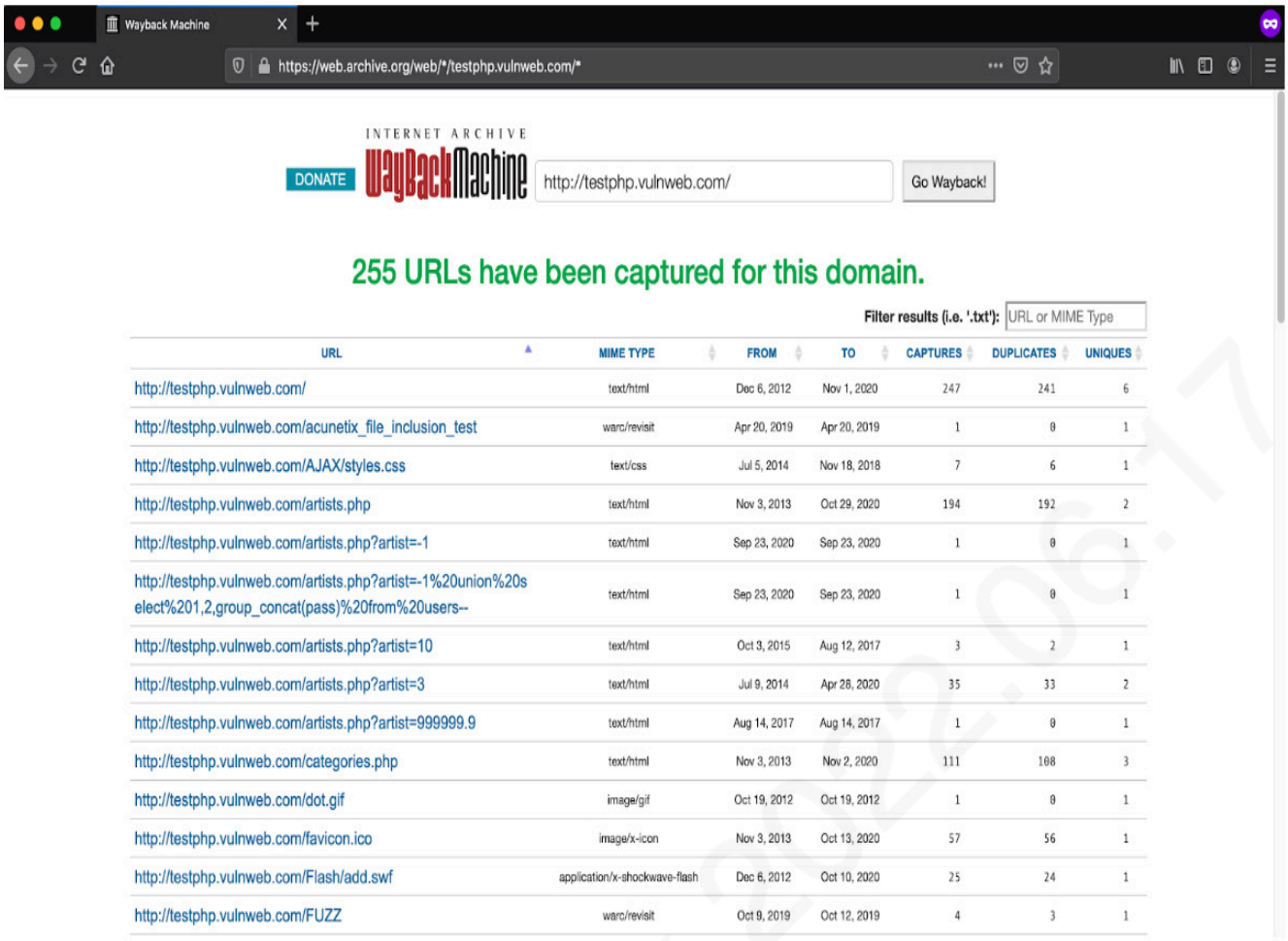


८. Parameter Discovery

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

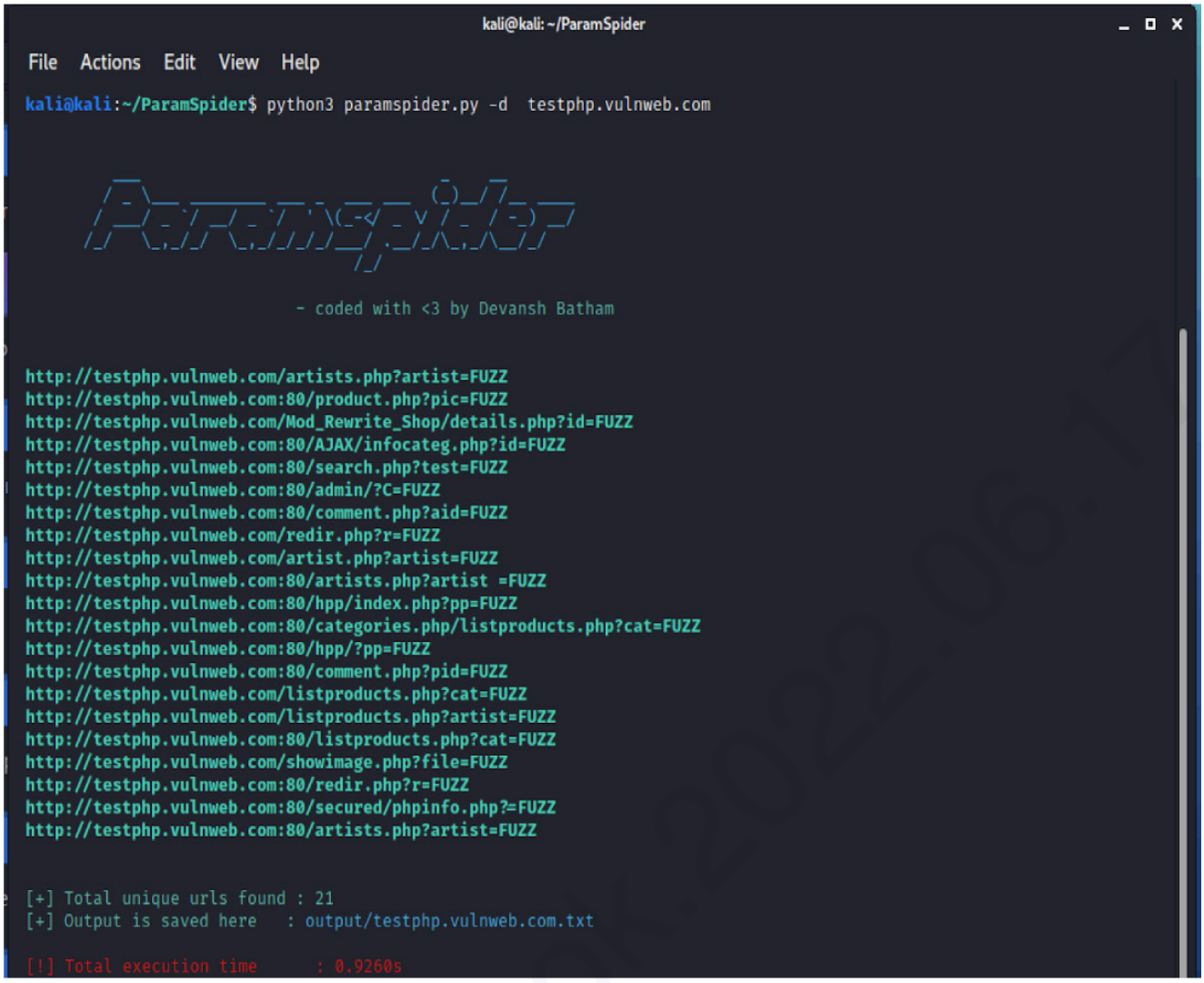
८.१ Waybackurls:

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



८.२ Paramspider:

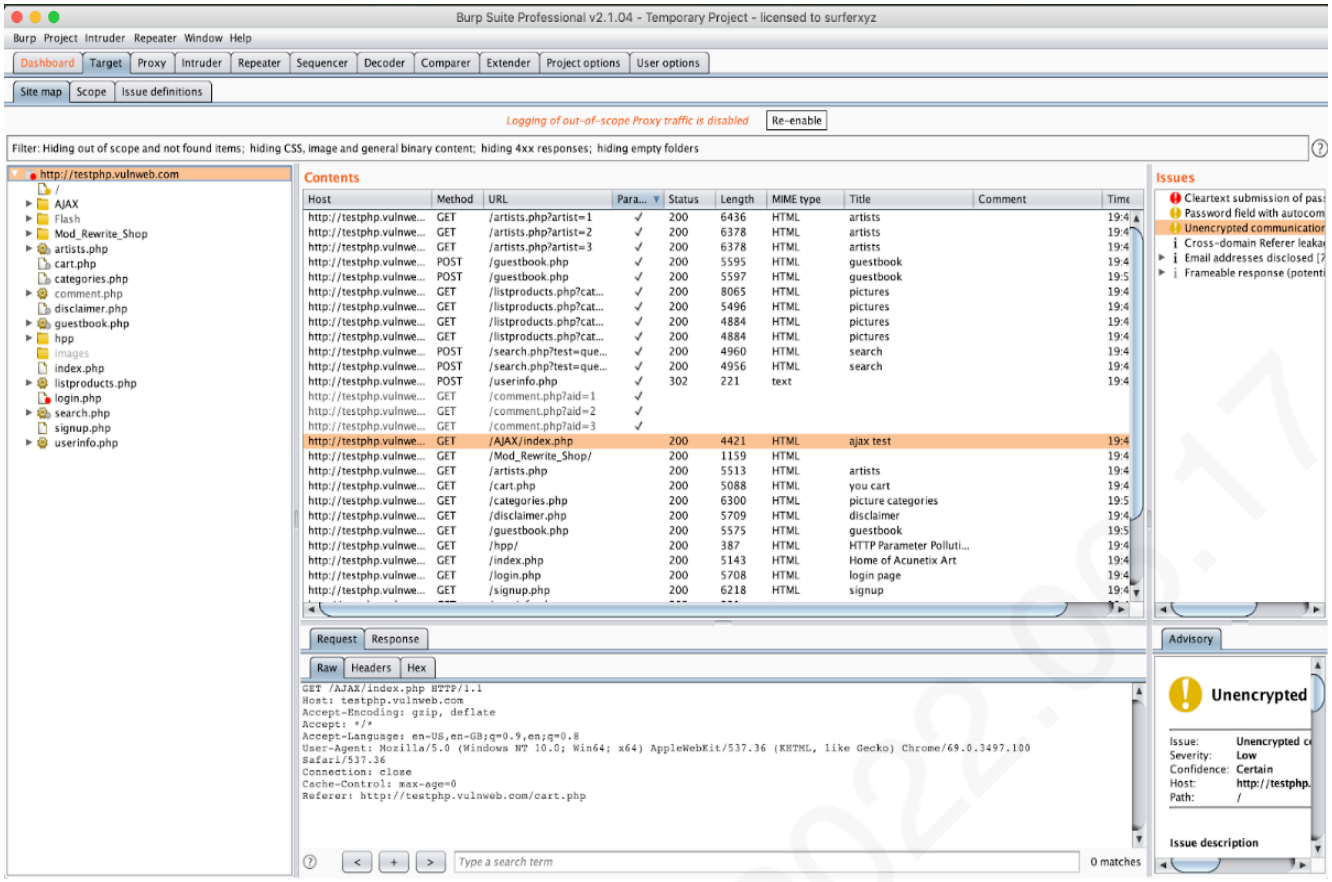
यसले database मा सुरक्षित गरी राखिएको डोमेन र सब-डोमेनको वेब archive बाट प्यारामिटरहरू फेला पार्दछ। यसले output result लाई पनि राम्रो र सफा तरीकाले terminal मा प्रस्तुत गर्दछ (target host सँग अन्तर्क्रिया नगरी)।



८.३ Burp:

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

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



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, संवेदन-शील (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.

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

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
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

Logical Operator	Description	Examples
AND or +	Used to include keywords. All the keywords need to be found.	• web **AND** application **AND** security • web **+**application **+**security
NOT or –	Used to exclude keywords. All the keywords need to be found.	• 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.	• web application **OR** security • web application **|**security
Tilde (~)	Used to include synonyms and similar words.	• web application ~security
Double quote (“)	Used to include exact matches.	• “web application security”
Period (.)	Used to include single-character wildcards.	• .eb application security
Asterisk (*)	Used to include single-word wildcards.	• web * security
Parenthesis (())	Used to group queries	• (“web security” | websecurity)

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

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 हरुले API key, पासवर्डहरू, ग्राहक डेटा आदि समावेश गरिराखेको हुन्छ। मूलतः Github ले संवेदनशील जानकारीहरु 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 ह्याकरहरुको दुनियाँमा लोकप्रीय रहँदै आएको छ।

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

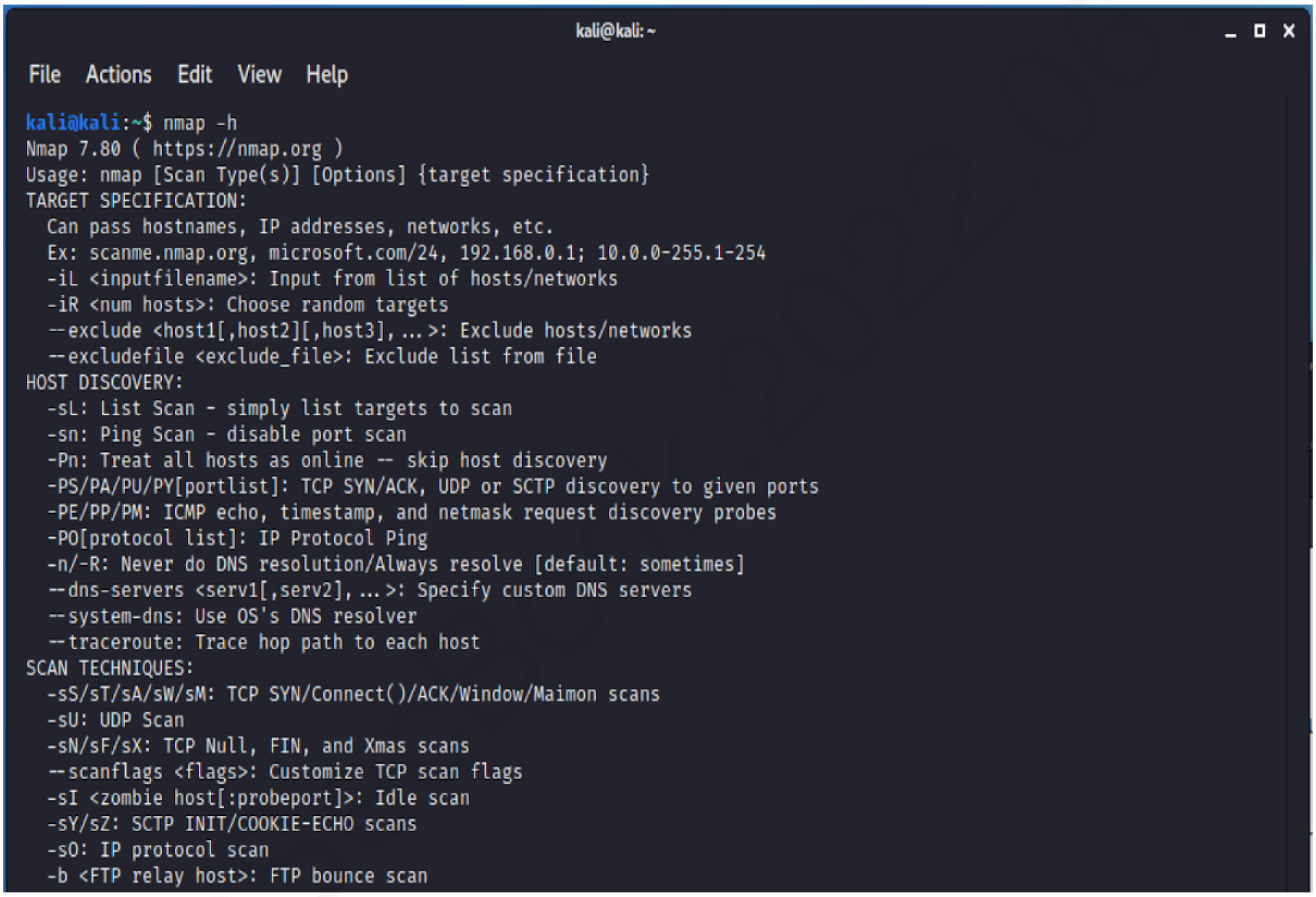
- खुला पोर्ट (open ports) र सेवाहरू (services) खोज्न
- तिनीहरूको संस्करणको (version) साथ सेवाहरू (services) खोज्न
- अनुमानित कस्तो खालको Operating system target मशीनमा चलिरहेको छ जान्न को लागि
- निगरानी गर्नको लागि

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 उपब्ध गराईदिन्छ । उदाहरणको लागि Firewall bypass , Port मा 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 ।

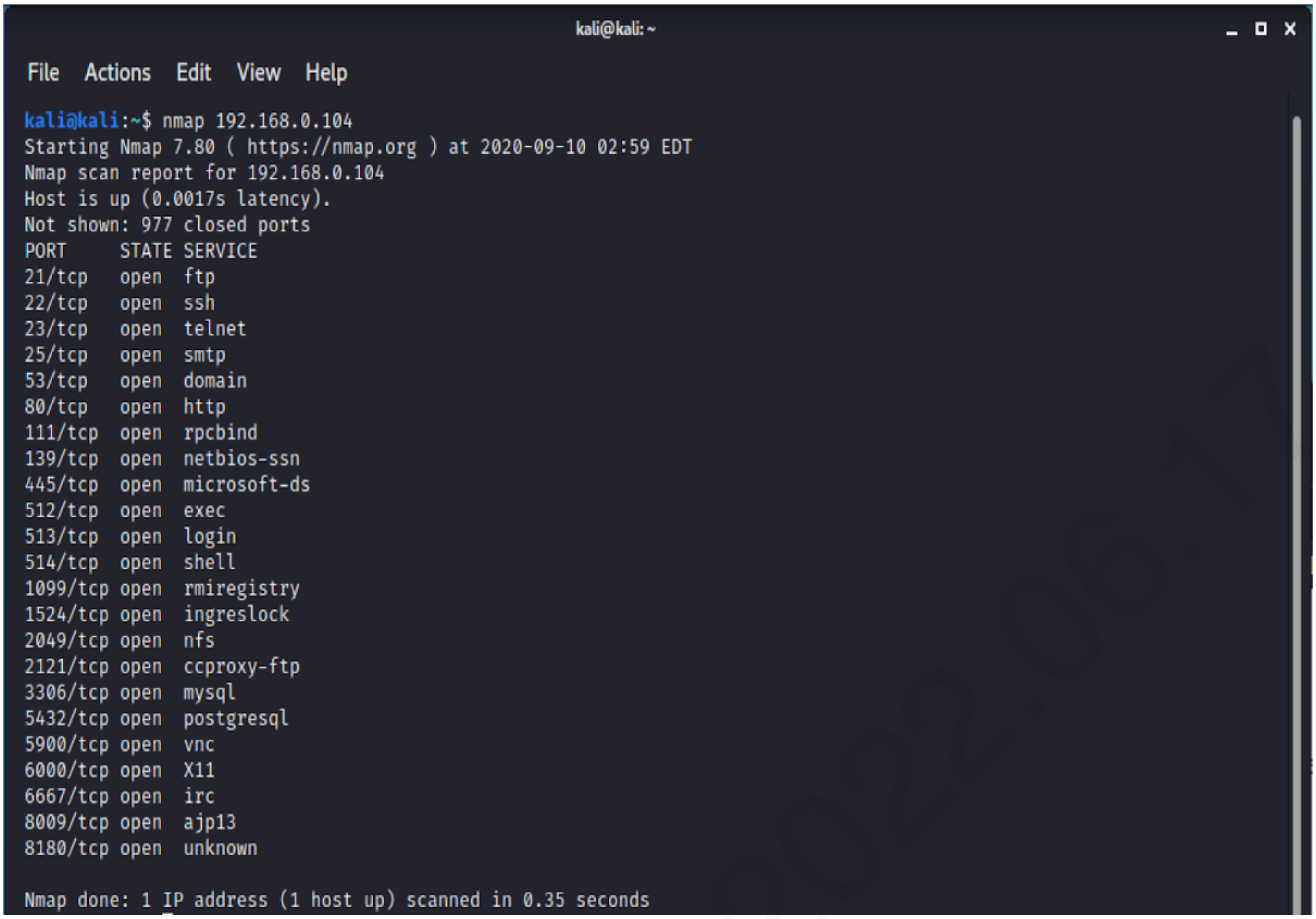
Target IP : 192.168.0.104/24
Attacker IP: 192.168.0.103/24

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



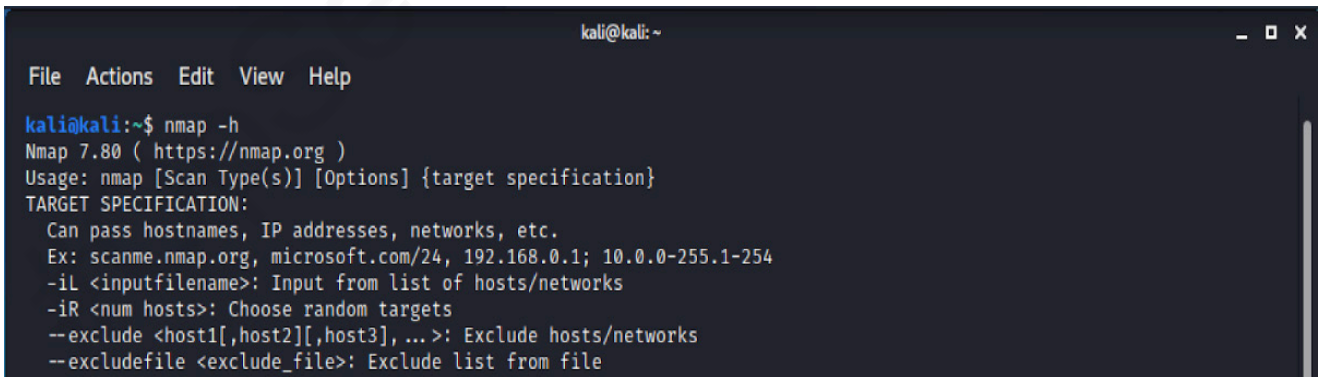
उदाहरणको लागि Nmap को एउटा simple command निम्नानुसार चलाउन सकिन्छ ।

kali@kali:~$ nmap 192.168.0.104



१. Nmap Target specification:

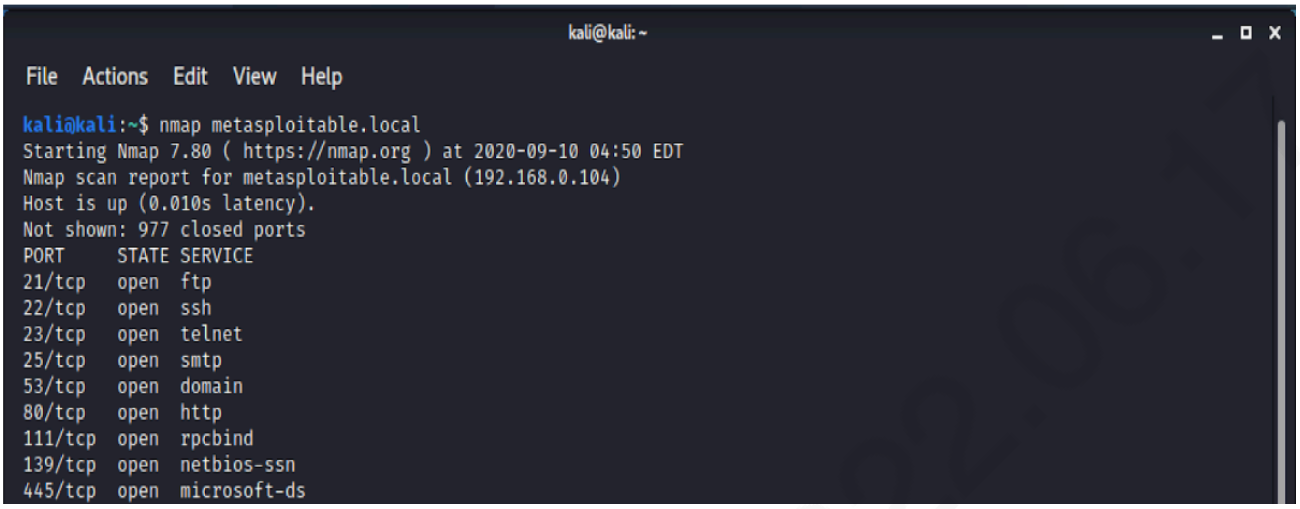
kali@kali:~$ nmap -h



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

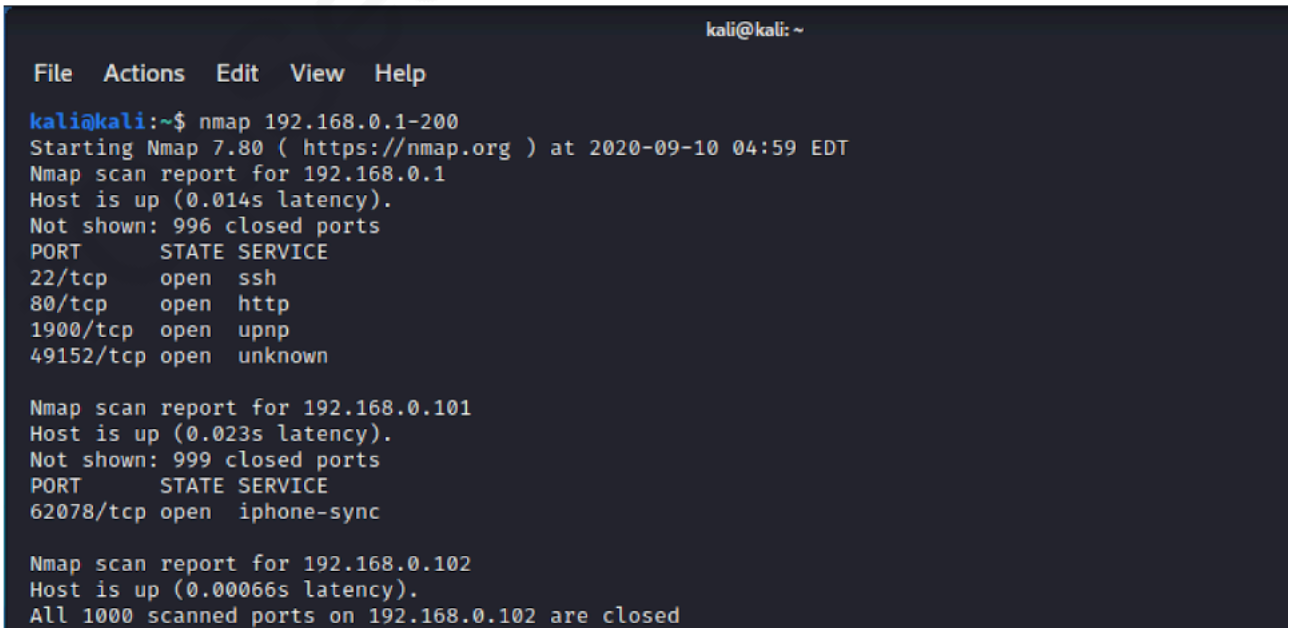
kali@kali:~$ nmap metasploitable.local



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

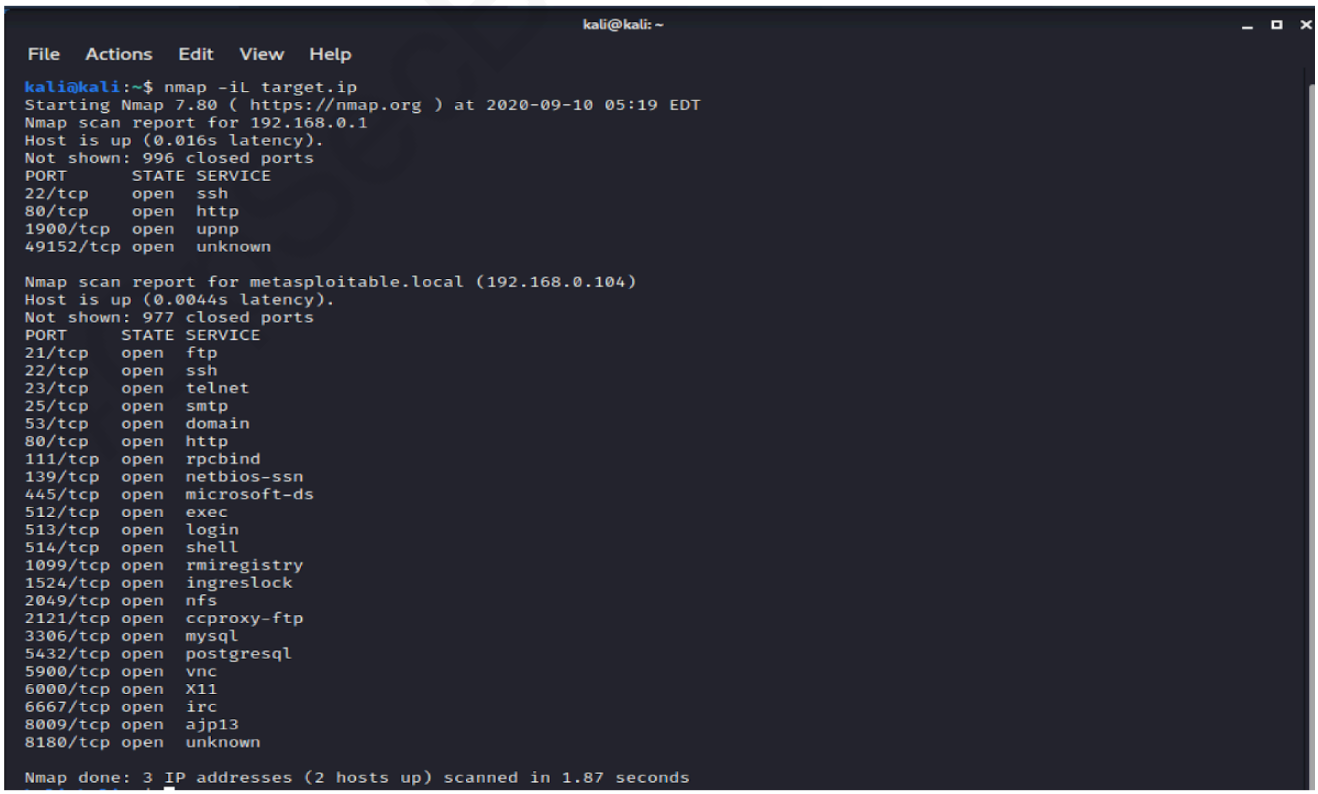


माथिको चित्रमा हामीले ip range 192.168.0.0.1 देखि 192.168.0.200 सम्म Nmapमा specify गरेका छौं।
स्क्यान पछि, ती Host हरू जो नेटवर्कमा जोडिएको (अनलाइन) छ त्यसलाई "Host is up" भनेर Terminal मा रिपोर्टिङ गरिन्छ र ती host हरुमा सम्भावित open पोर्टहरू देखिएको खण्डमा त्यसको स्क्यान result पनि उल्लेख गराइन्छ।

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

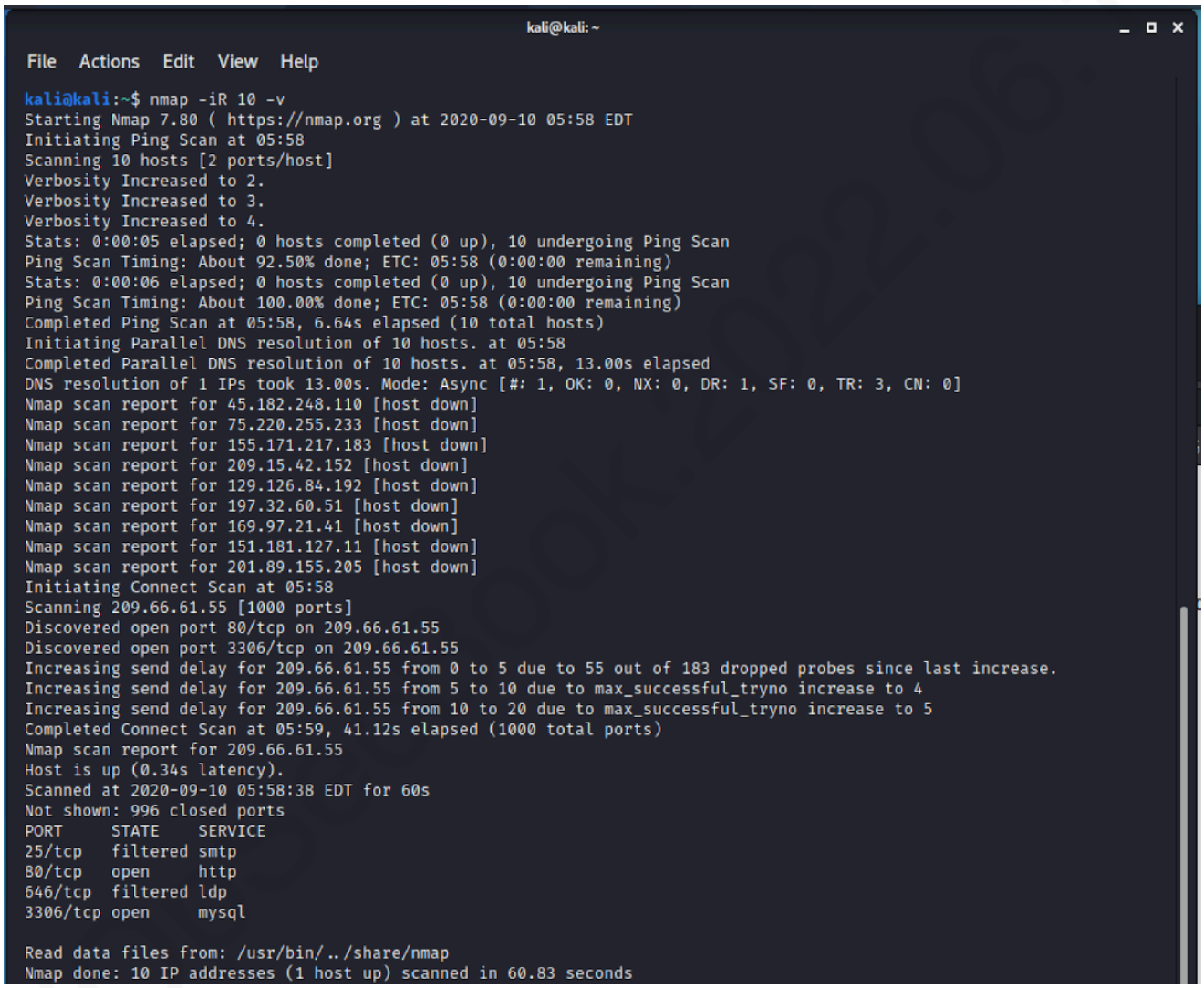
१.३ Input from list of Host

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



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

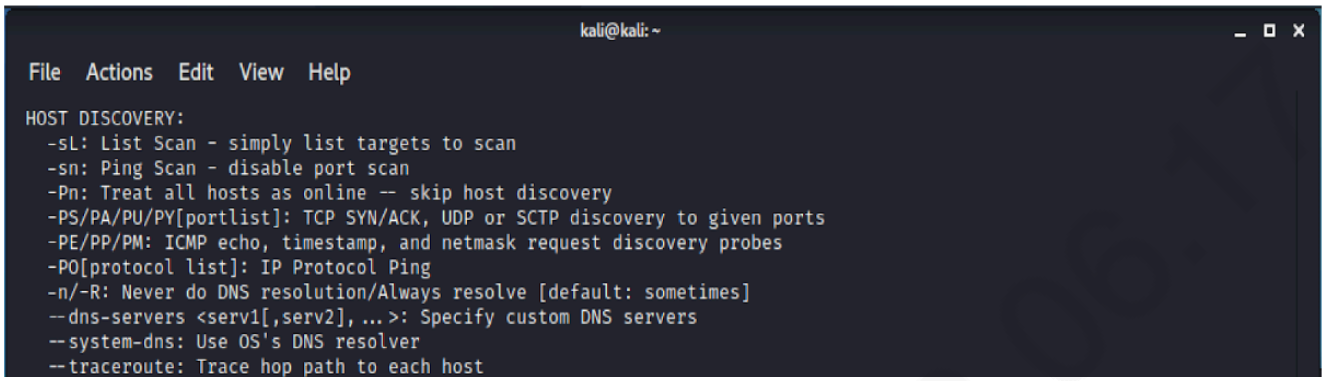


माथिको चित्रमा हामीले कुनै पनि १० वटा ip स्क्यान गर्ने प्रयास गरेका छौं जुन Nmap को -iR switch ले नै randomly generate गर्दछ।

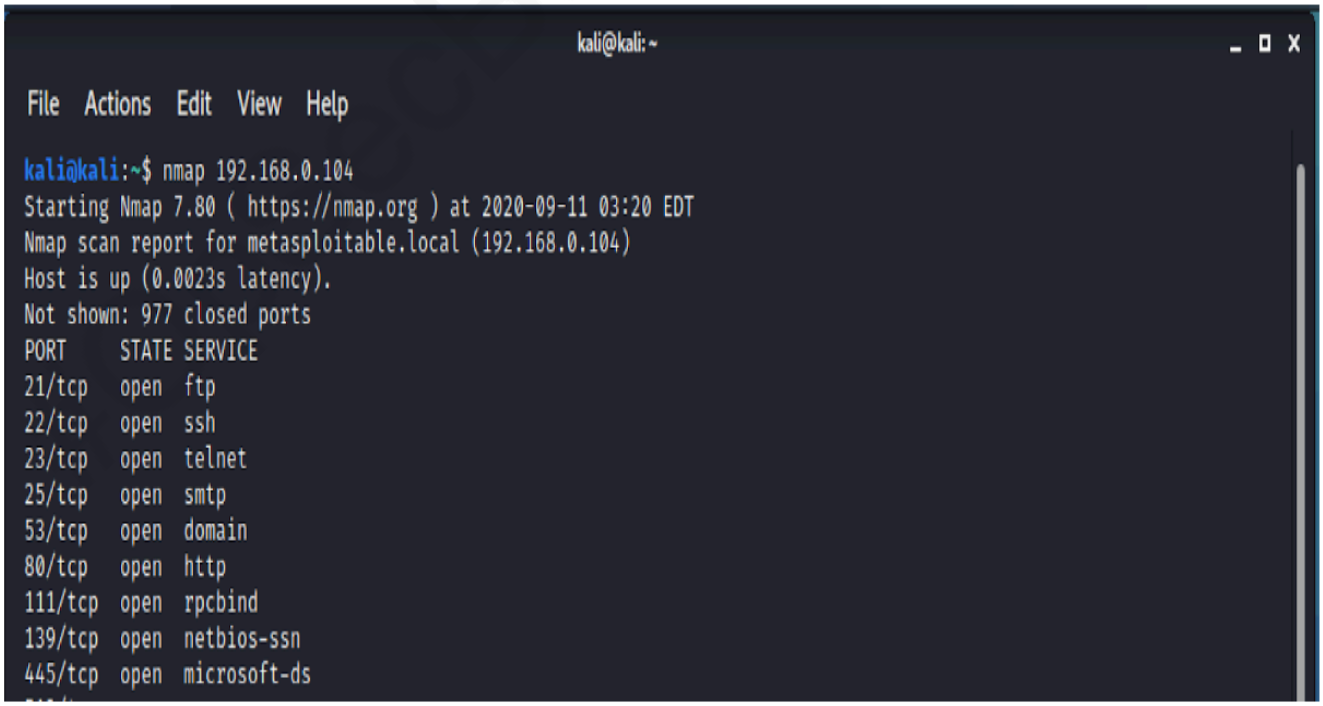
kali@kali:~$ nmap -iR 10 -v

२. Nmap Host Discovery

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



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।



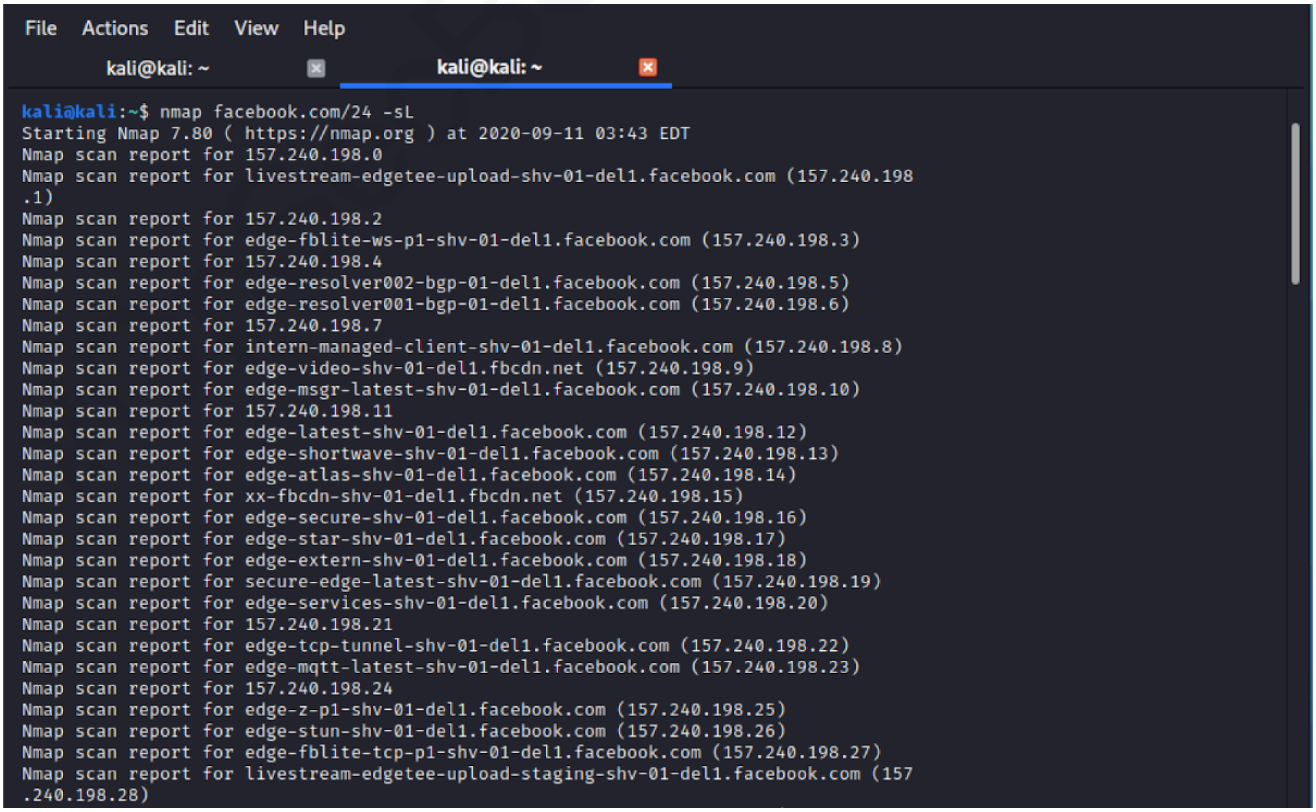
जब Nmap मा कुनै होस्ट डिस्कवरी options हरु जस्तै -sL/-sn/-Pn उल्लेख गरिएको हुँदैन त्यसबखत, NMAP ले पृष्ठभूमि (background) मा निम्न चीजहरू गर्दछ :

- 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 ।

२.१ List Scan (-sL)

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

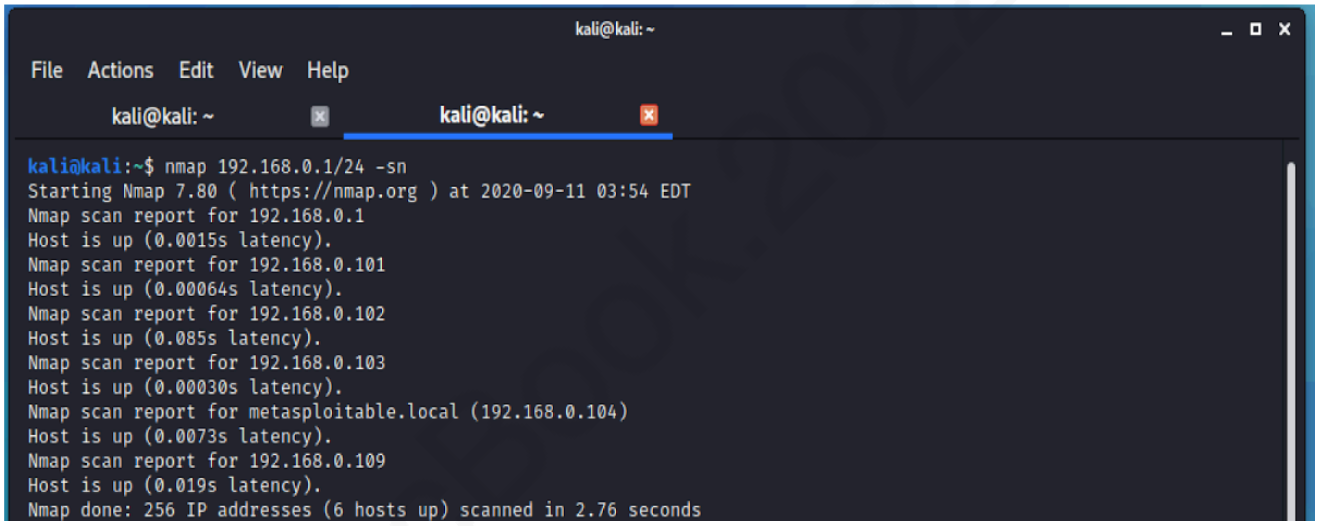


फिगरमा देखाइए जस्तै, -sL ले reverse DNS lookup गर्छ र हामीलाई dns name बताउँछ।

२.२ Ping Scan (-sn)

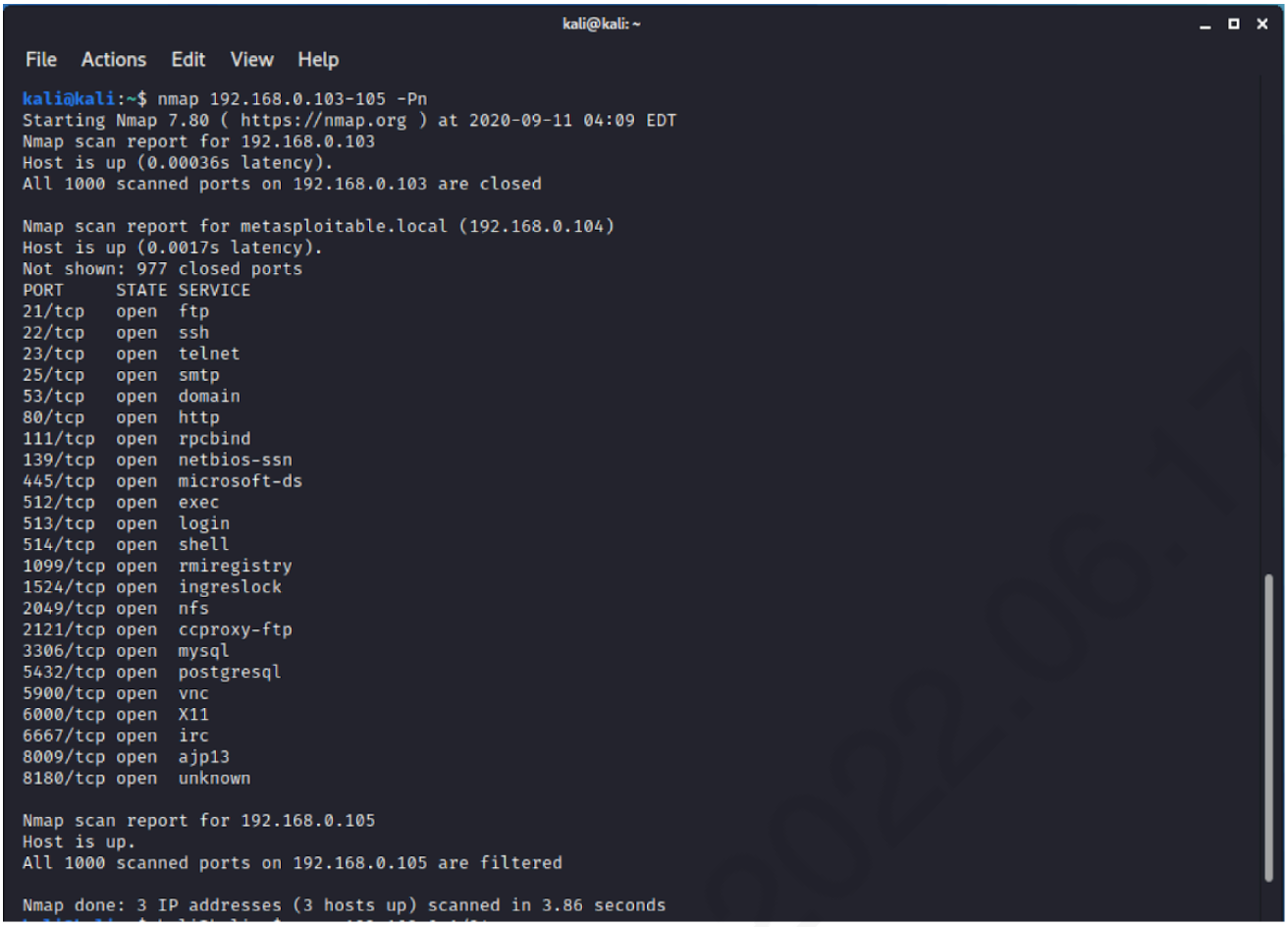
यस "-sn" switchलाई no port स्क्यान (scan)को रूपमा पनि चिनिन्छ। यसले Nmap लाई Alive होस्ट (host) पत्ता लागेपछि पोर्ट स्क्यान अगाडि नबढाउन आदेश दिन्छ।

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



२.३ Skip host discovery (-Pn)

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



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 स्क्यानिंग गरिदिन्छ।

३ NMAP Scan Technique

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

Scan technique हरु तल उल्लेख गरिएको छ:

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

३.१.१ TCP SYN scan

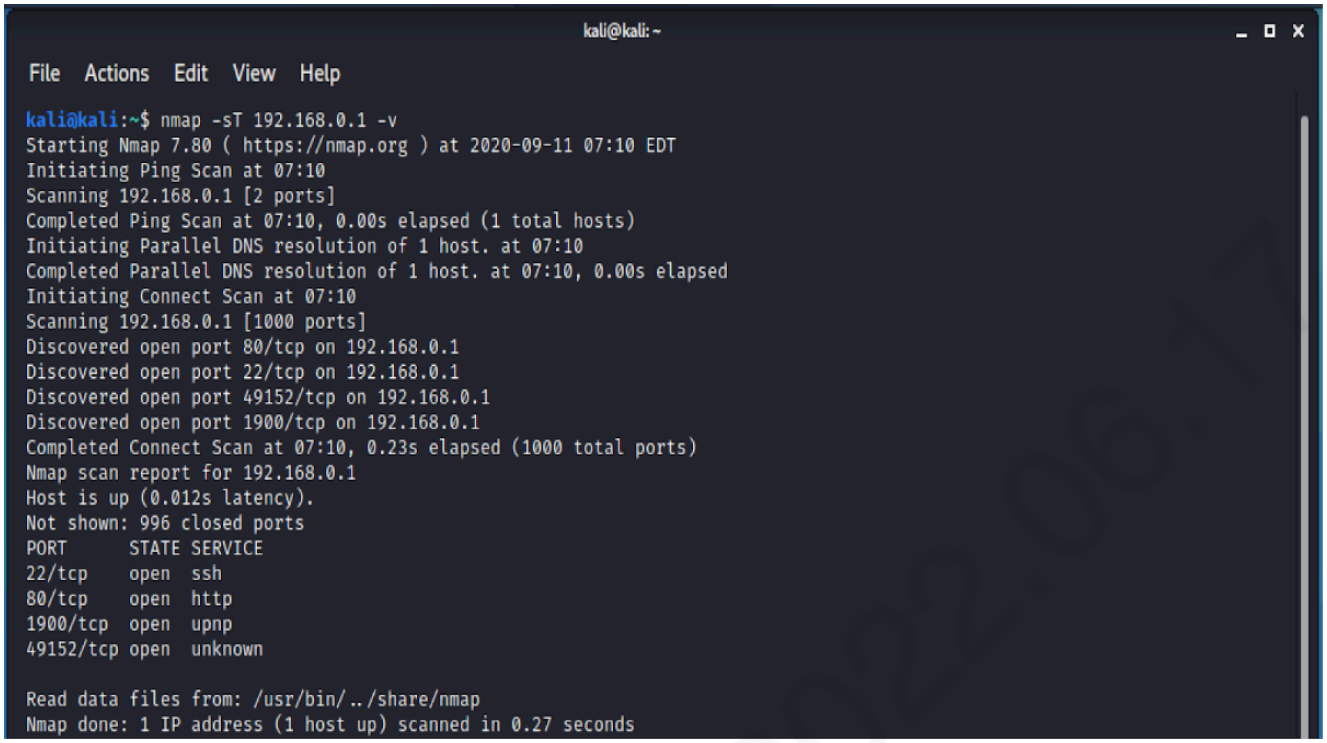
यो स्क्यान Technique, Half Open स्क्यानको रूपमा पनि चिनिन्छ किनकी हामी host सँग Full TCP connection गर्दैनौ। हामी target मा connection open गराउन को लागी SYN प्याकेट(packet) पठाउँछौं तर complete connection भने गर्दैनौ। SYN प्याकेटबाट आएको response लाई निम्न तरिकाले Analysis गर्छौं :

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

यदि हामी "-sS" प्रयोग गर्दैनौं भने पनि, Nmap ले यो switch default प्रयोग गर्दछ ।

$ nmap -sS 192.168.0.1

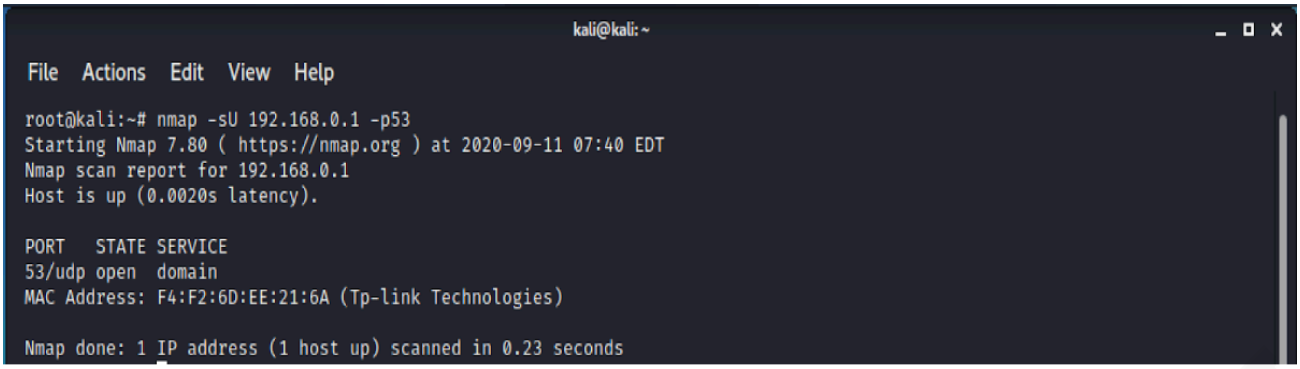
३.१.२ TCP Connect() Scan



Connect() scan गर्नको लागि syn स्क्यान भन्दा बढी समय लाग्दछ एवं बढी noise generate गर्दछ , त्यसकारण Target Host मेशिनमा हाम्रो fingerprint पनि बस्ने 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 सेवाहरु (services) udp मा भन्दा tcp मा हुन्छ। UDP scaningले TCP scanning भन्दा धेरै समय लिन्छ र यसको scanning technique जटिल पनि छ।



$ nmap -sU 192.168.0.1 -p53

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

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

nmap -sU -sT <target_ip>

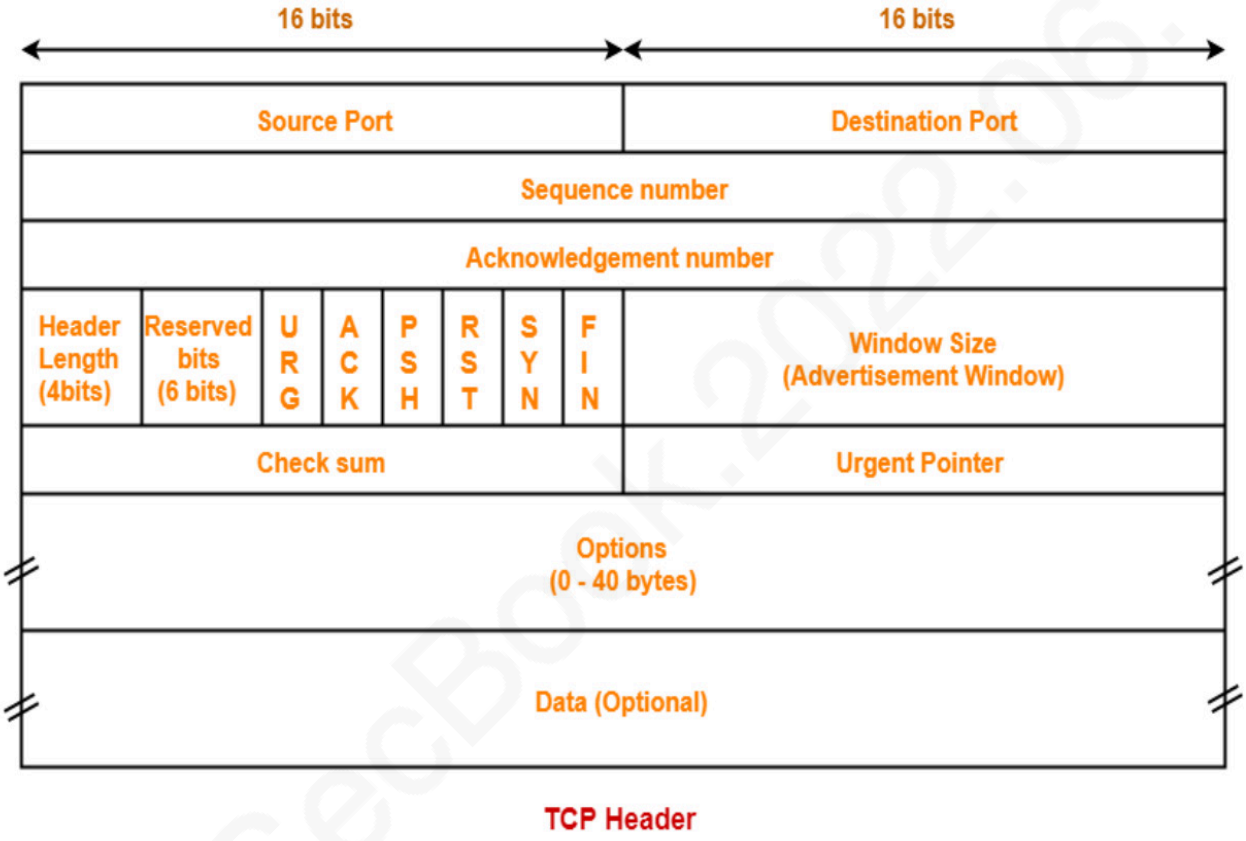
```
Host is up (0.0074s latency).
Not shown: 978 closed ports
PORT      STATE         SERVICE
53/udp    open          domain
67/udp    open|filtered dhcps
158/udp   open|filtered pcmail-srv
786/udp   open|filtered concert
1900/udp  open|filtered upnp
1901/udp  open|filtered fjicl-tep-a
8000/udp  open|filtered 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 बिर्सनु हुँदैन ।

३.३ TCP Null, FIN, and Xmas scans



TCP Header

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 प्रणालीहरू सरल रुपमा अभ्यास गर्नकोलागि TCP/IP को RFC 793 implementation हुन जरुरी पर्दछ ।

३.३.२ FIN Scan

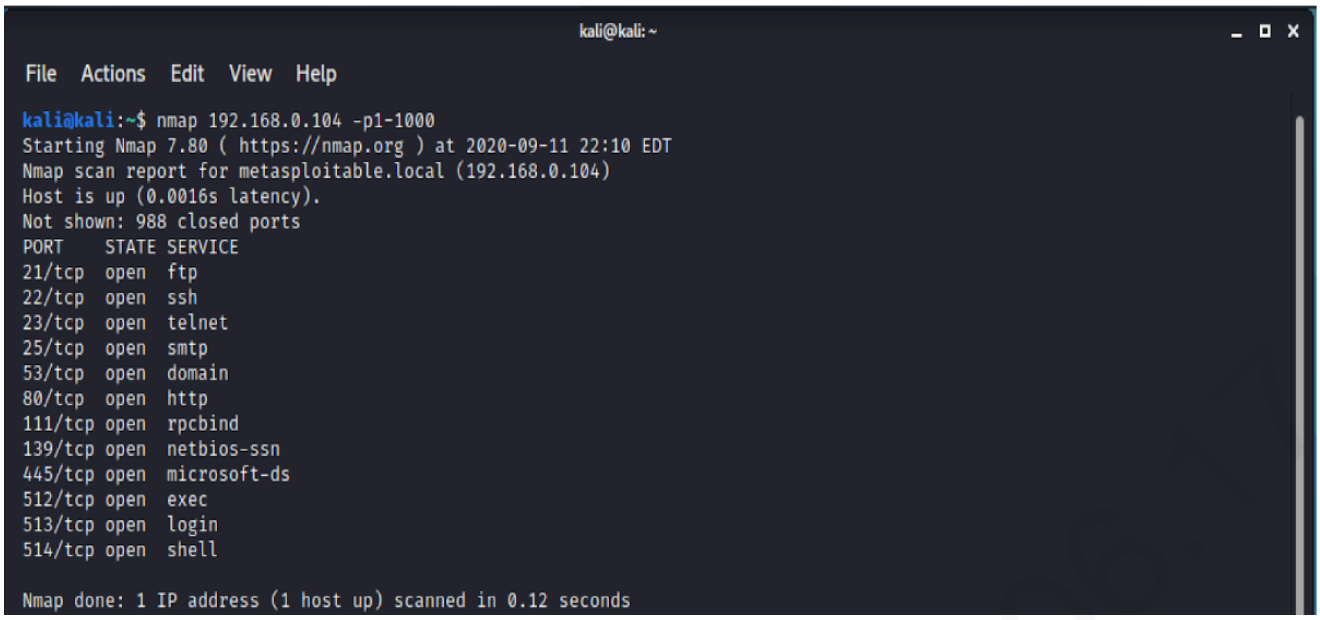
FIN स्क्यान XMAS स्क्यान जस्तै हुन्छ तर FIN Flag set मात्रै पठाउँद-छ ।Port Open वा Closed कुन अवस्थामा छ भन्ने बुझ्नको लागि XMAX Scan को जस्तो response आउँदछ ।

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 ।

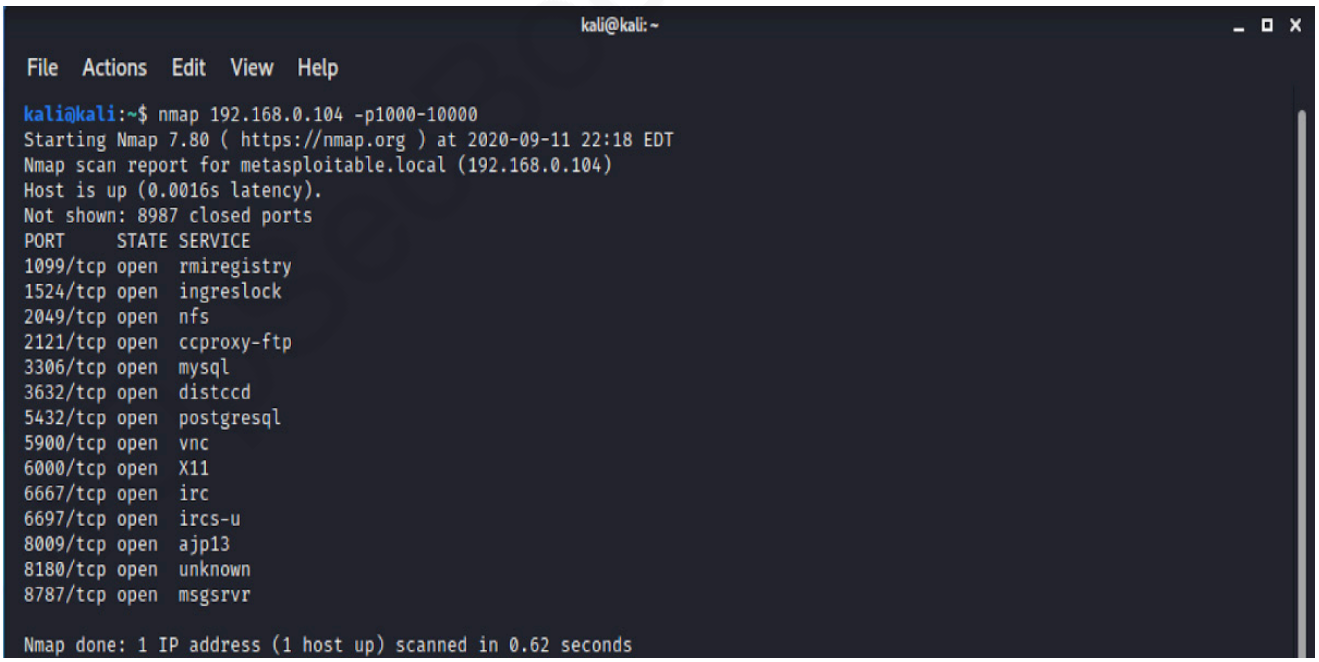
४ Port Specification and Scan Order

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



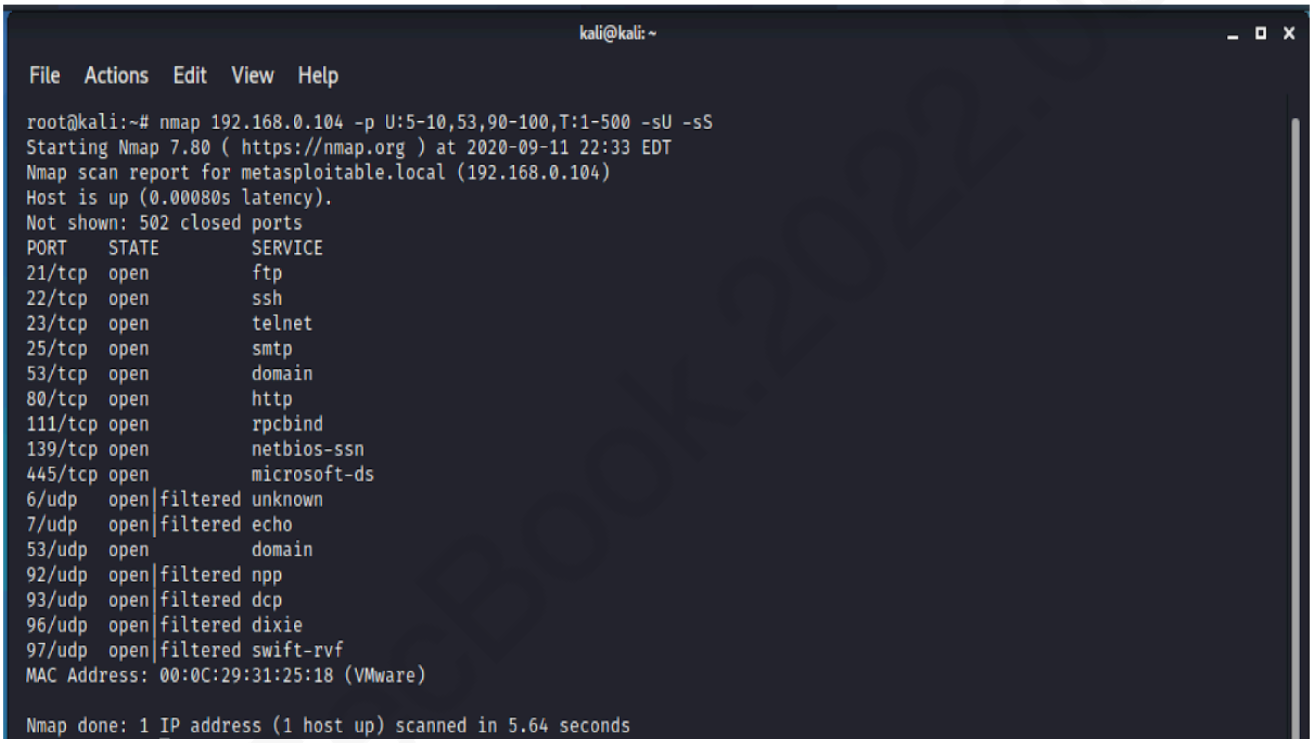
$ nmap 192.168.0.104 -p1-1000

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



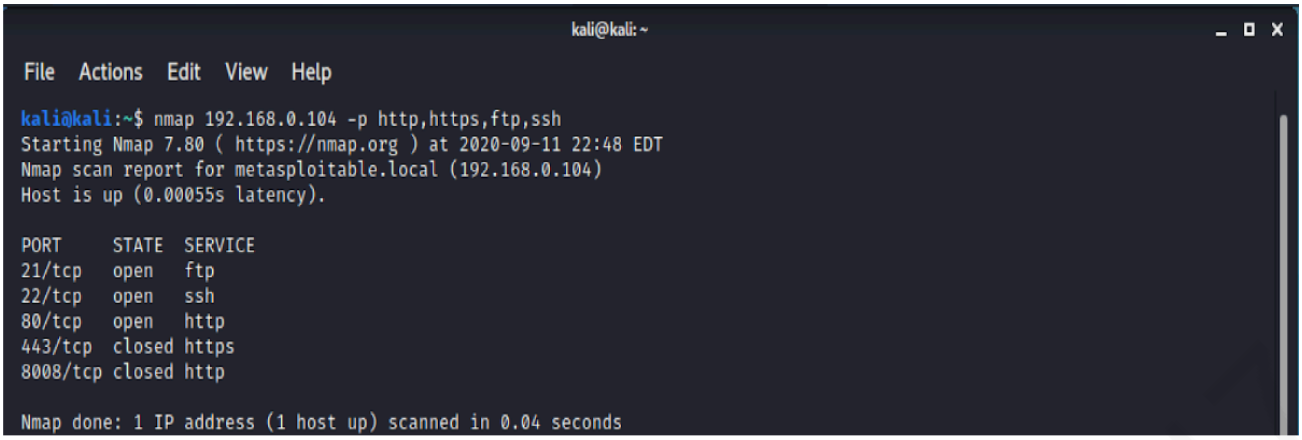
$ nmap 192.168.0.104 -p1000-10000

हामीले होस्टको पोर्ट (Default TCP) १००० देखि १००००० range सम्म स्क्यान गऱ्यौं 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।



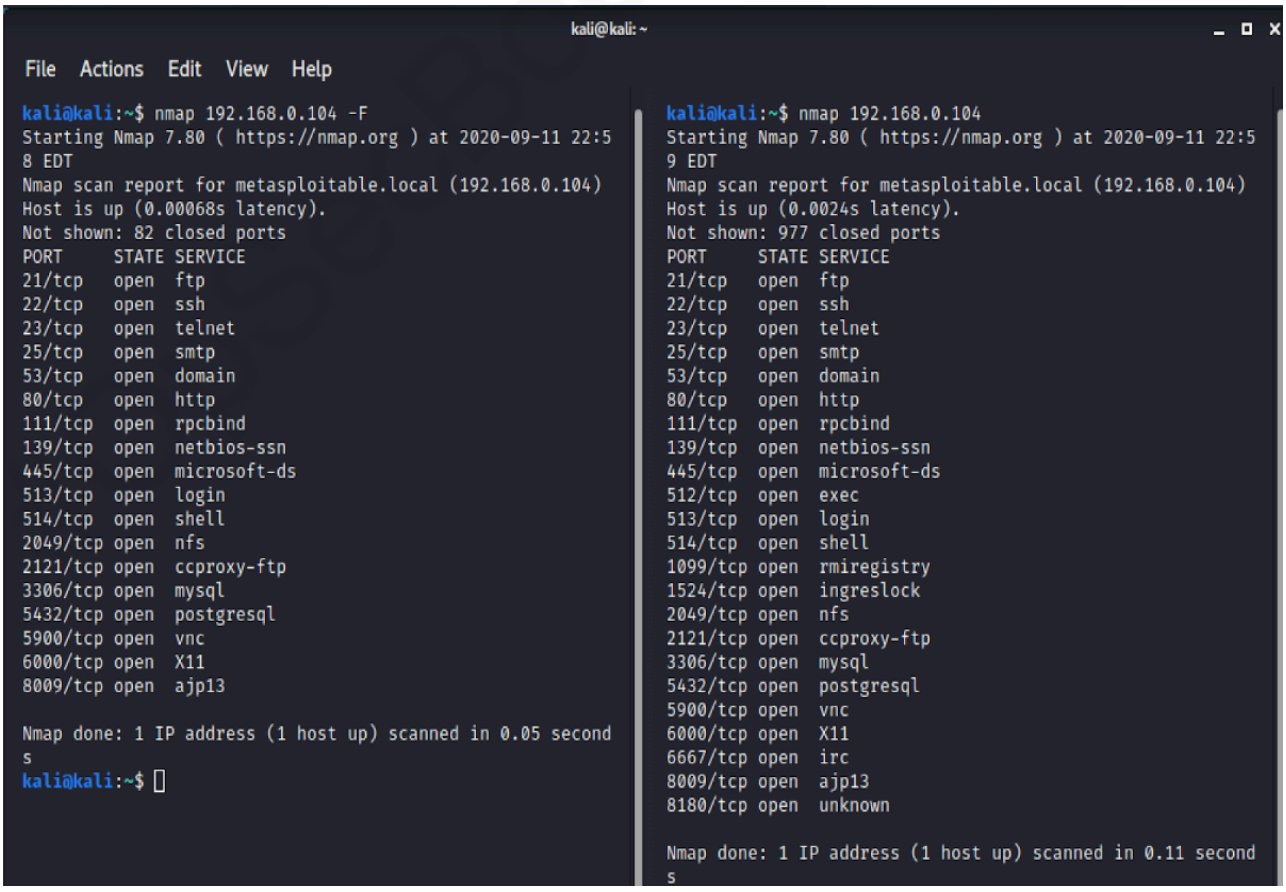
जस्तोकि हामीलाई थाहा छ port को दायरा ० देखि ६५५३५ सम्म हुन्छ ।
 दुबै TCP र UDP port मा यदि हामीले पोर्टहरू स्क्यान गर्नु पर्छ भने हामीले निम्न कुराको ख्याल गर्नुपर्छ:

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



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

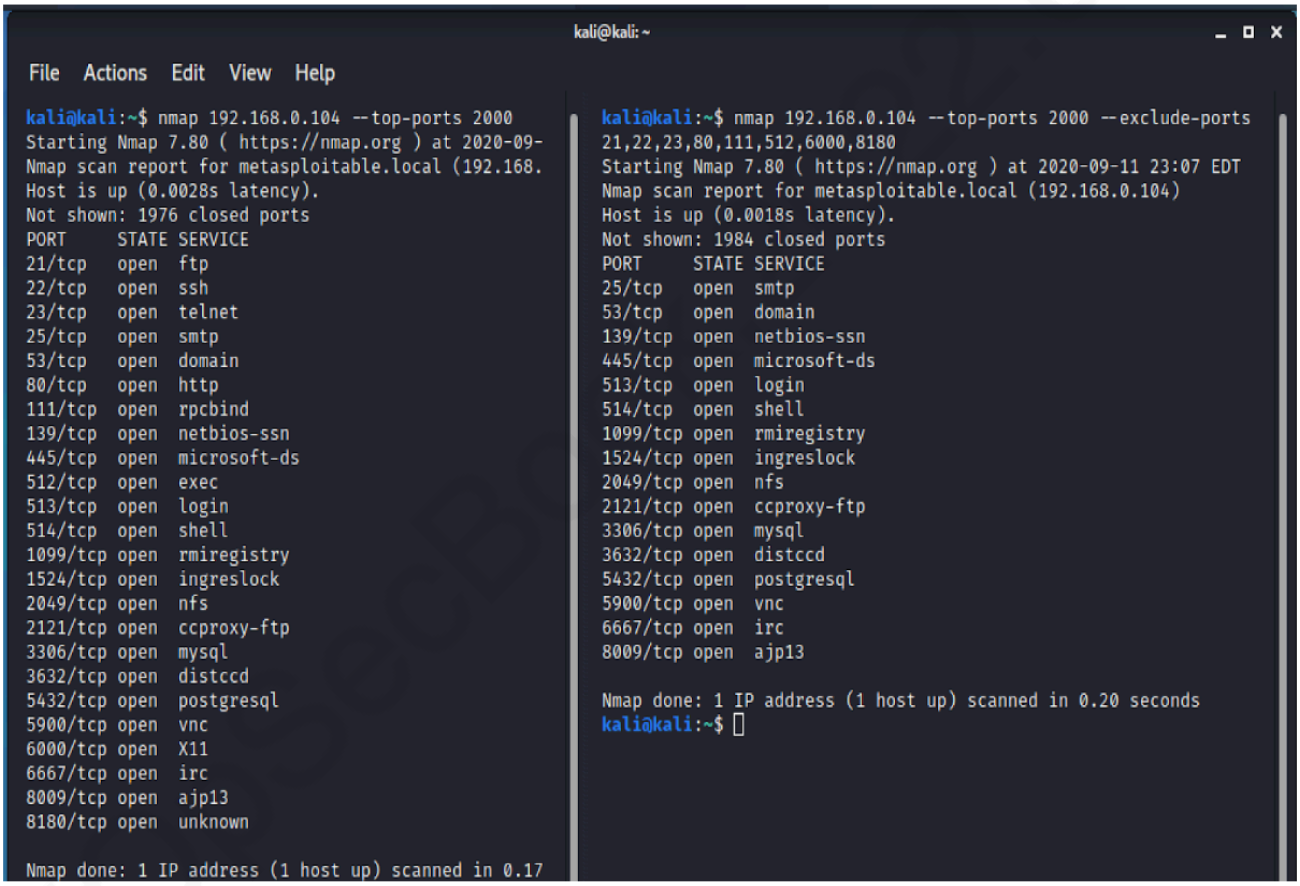
हामी nmap मा services हरूको नाम पनि direct specify गर्न सक्छौं। यसले पोर्ट 80 लाई मात्र http को लागी स्क्यान गर्दैन तर सम्पूर्ण पोर्ट जसले http सेवा host गर्दछ ति सबै जाँच गर्दछ ।



$ nmap 192.168.0.104 -F

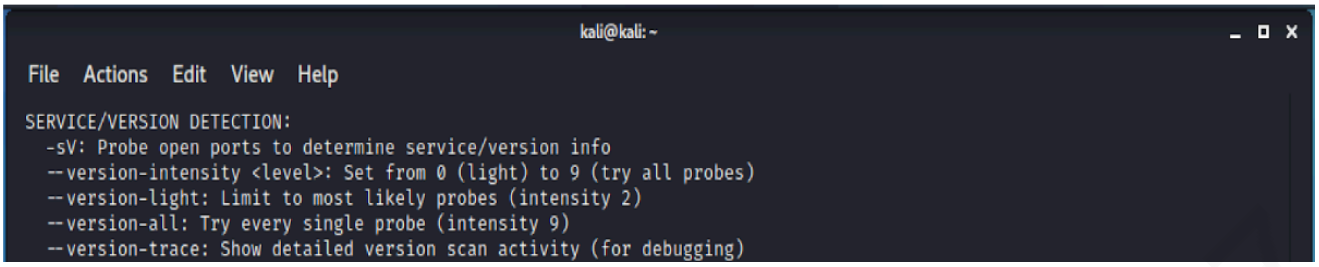
-F स्विचले पूर्वनिर्धारित (default) स्क्यान भन्दा कम पोर्टहरू स्क्यान गर्दछ । हामी -F स्विच र default स्विचको परिणाम तलको चित्रबाट तुलना गर्न सक्छौं ।

Default nmap स्क्यानले १००० Top ports हरू मात्र scan गर्दछ , तर हामी Top ports को दायरा बढाउन सक्दछौं र कुनै समावेश गर्नु नपर्ने पोर्टलाई हामीले exclude गर्नसक्छौं। यसलाई तल चित्र प्रयोग गरेर तुलना गर्न सकिन्छ।

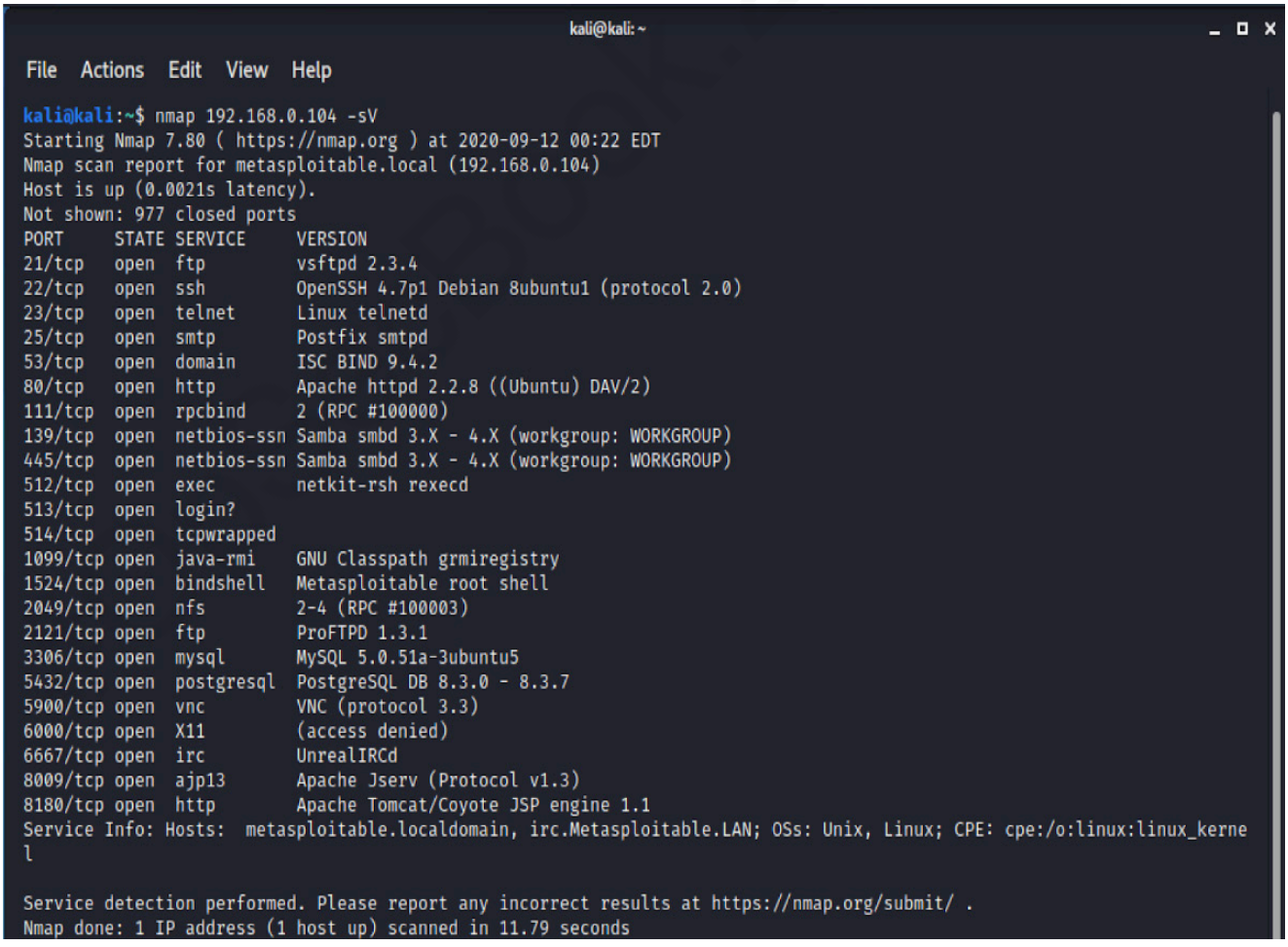


(बाँया)nmap 192.168.0.104 --top-ports 2000
(दायाँ)nmap 192.168.0.104 --top-ports 2000 --exclude-ports 21,22,23,80,111,512,6000,8180

५. Service / Version Detection :



Nmap को Service / Version Detectionले target host मा कस्तो service हरू चलिरहेको छ, ति service हरूमा कुन संस्करण(version) प्रयोग भएको छ आदि कुराहरु 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।



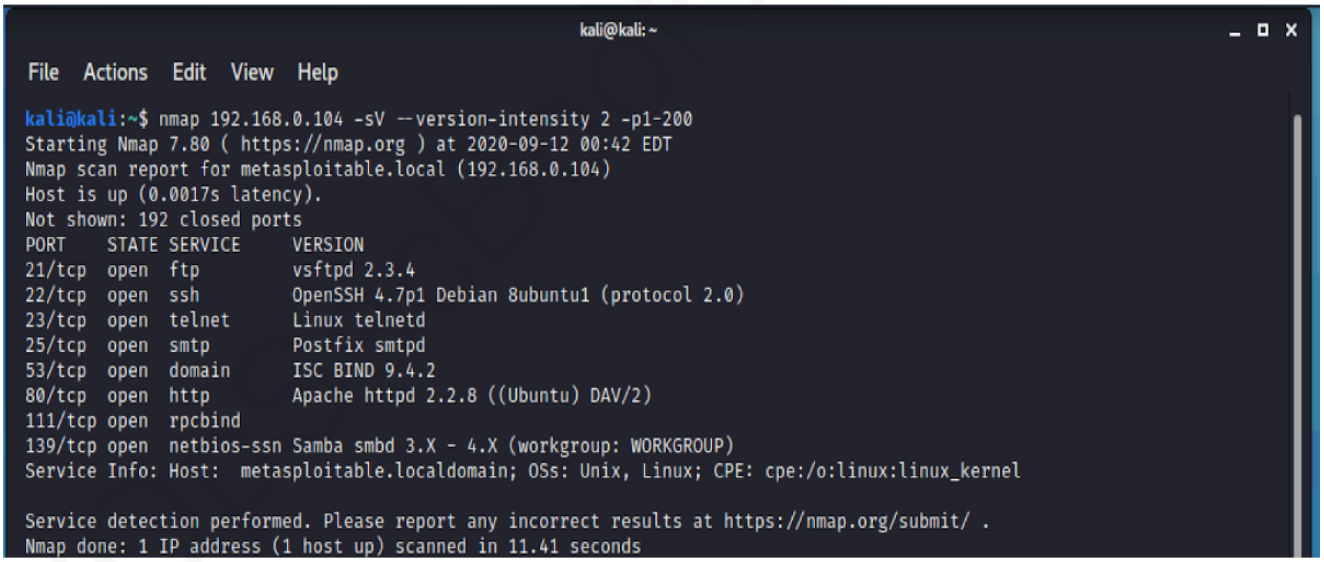
$ nmap 192.168.0.104 -sV

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

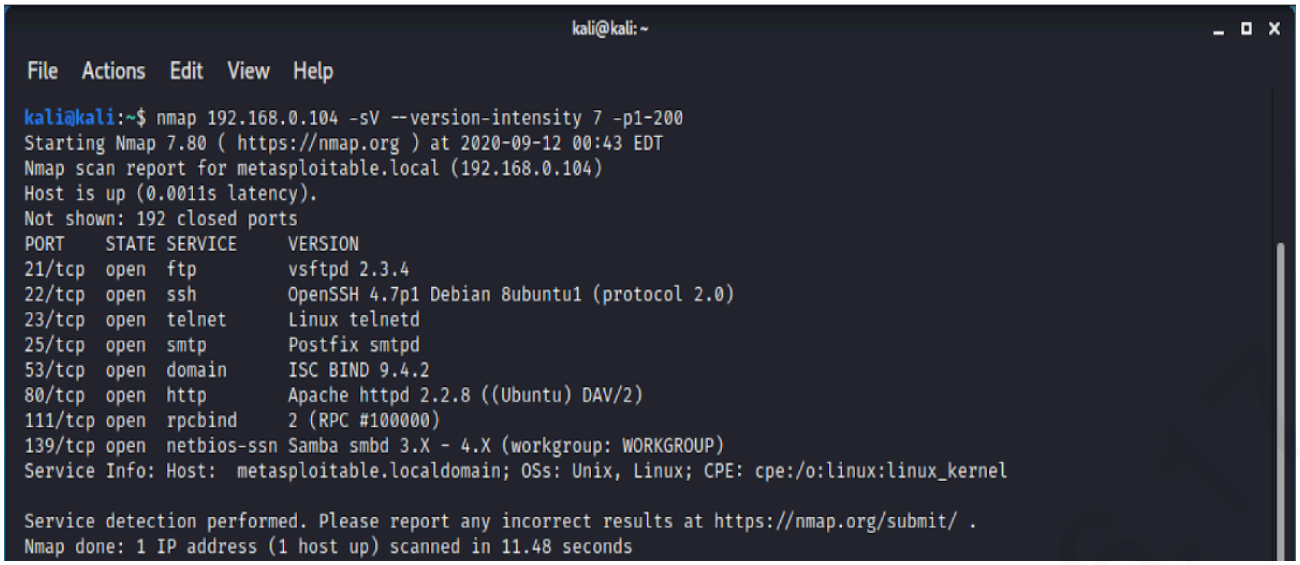
हामीले version intensityको level पनि specify गर्न सक्छौं र यो level 0 देखि 9 सम्मको range मा हुन्छ, जसमा 7 लाई default मानिन्छ।

हामीले यो याद राख्नु पर्छ:

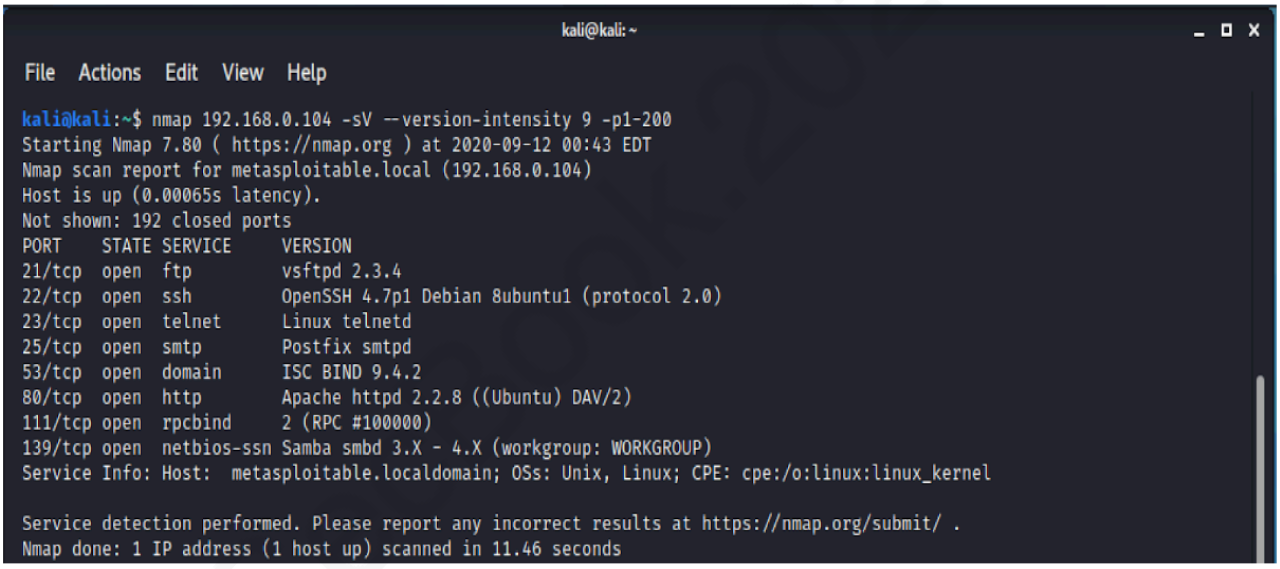
“--version-intensity 2” संक्षेप मा “ --version-light ” पनि भनिन्छ
“--version-intensity 9” संक्षेप मा “ --version-all” पनि भनिन्छ



$ nmap 192.168.0.104 -sV --version-intensity 2 -p1-200
Or
$ nmap 192.168.0.104 -sV --version-light -p1-200



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

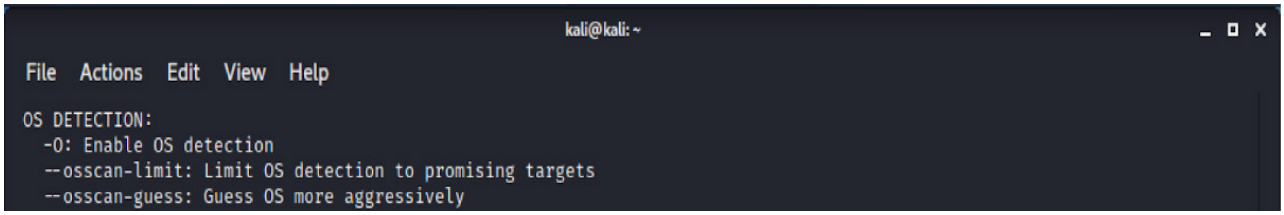


$ nmap 192.168.0.104 -sV --version-intensity 9 -p1-200

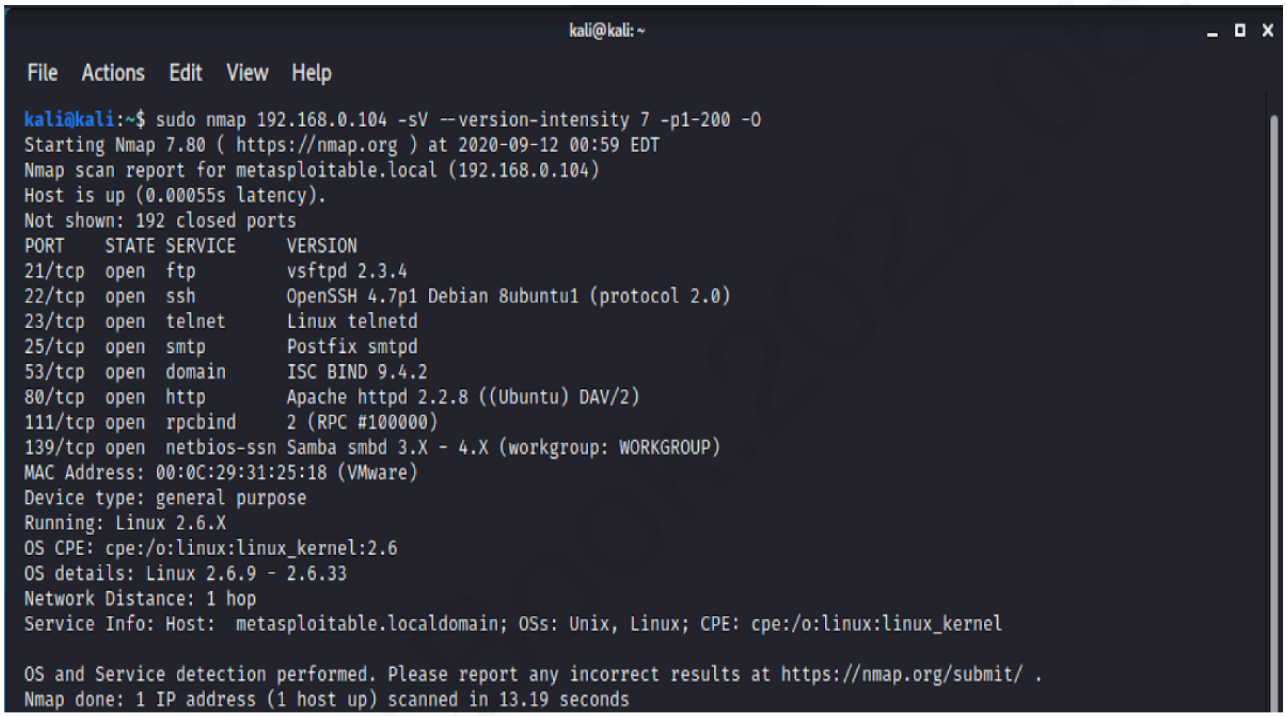
Or

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

६. Nmap OS Detection



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

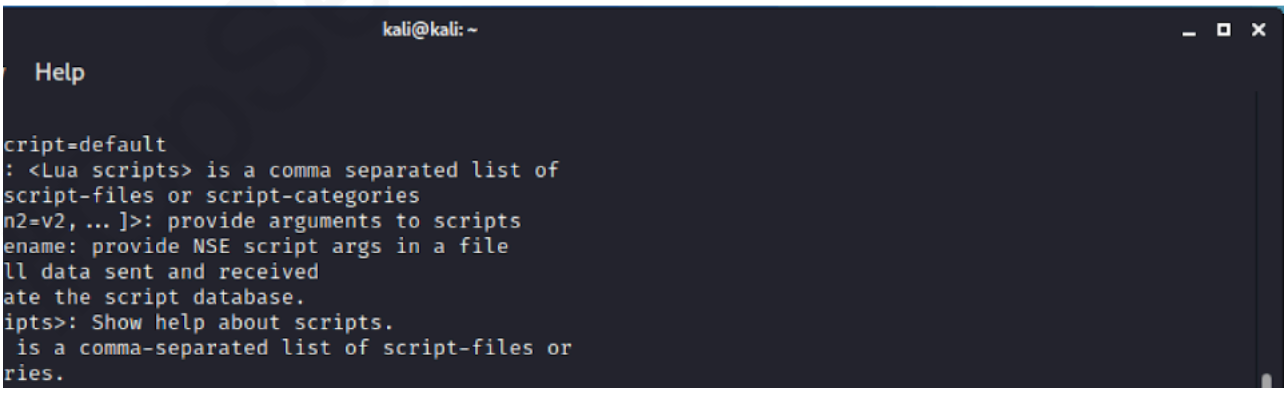


sudo nmap 192.168.0.104 -sV --version-intensity 7 -p1-200 -O

“-O” स्विचले target hostमा चलिरहेको सम्भावित OS को बारेमा जानकारी जम्मा गर्न मद्दत गरेको माथि चित्रबाट 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 छ र OS Fingerprinting signature निम्न तरिकाले राखिएको हुन्छ ।

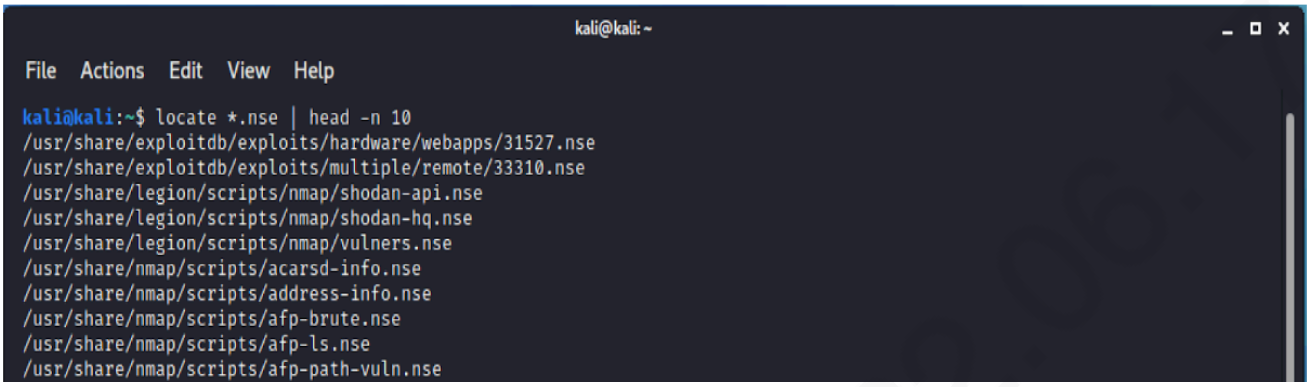
७. Script Scan:



Nmap Scripting Engine(NSE) Nmap को सबभन्दा शक्तिशाली service हरु मध्ये एक हो। यसले प्रयोगकर्ताहरूलाई 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 सक्छौं:

$ locate *.nse



Nse scripts का category निम्न प्रकारका छन;

- 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 बिभिन्न 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 स्क्रिप्टहरु हुन्छ। जब हामी एउटा cateogry मानौं "safe" रोज्यो भने त्यहाँभित्रको सबै script run गराइदिन्छ । तल चित्रमा उदाहरण हेर्न सकिन्छ ।

NSEDoc

Index
NSE Documentation

Categories

auth
broadcast
brute
default
discovery
dos
exploit
external
fuzzer
intrusive
malware
safe
version
vuln

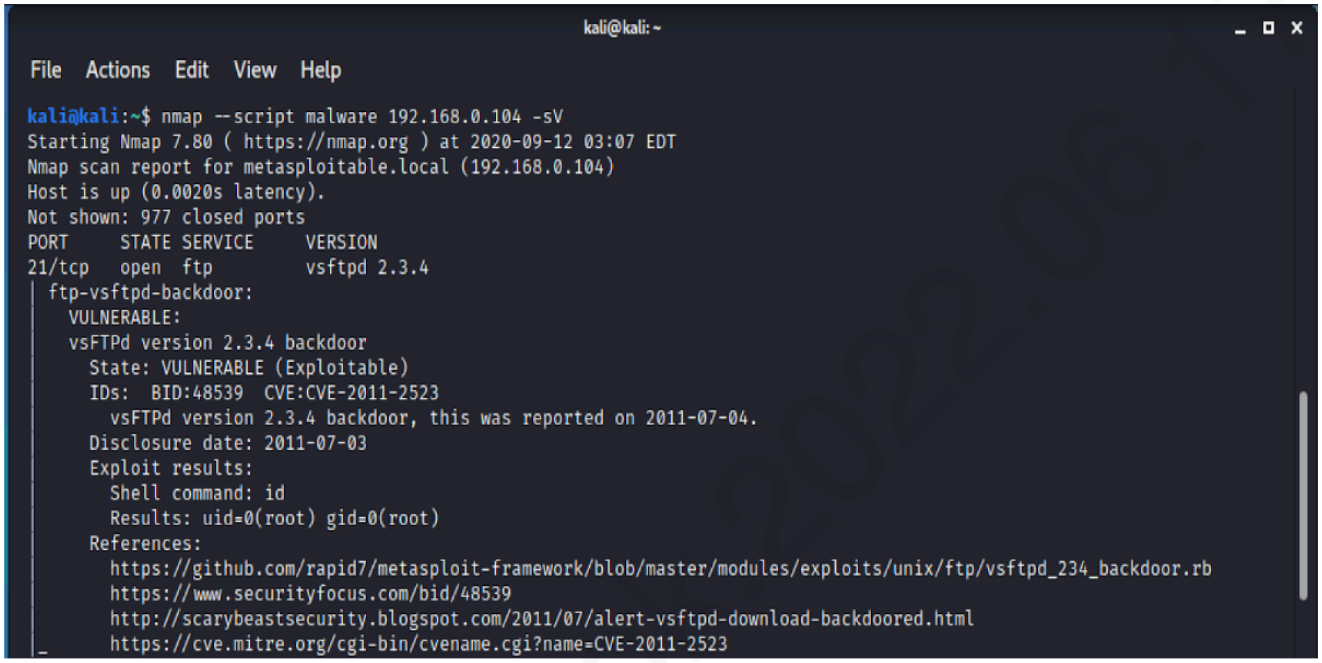
Scripts (show 601)

Libraries (show 139)

Scripts

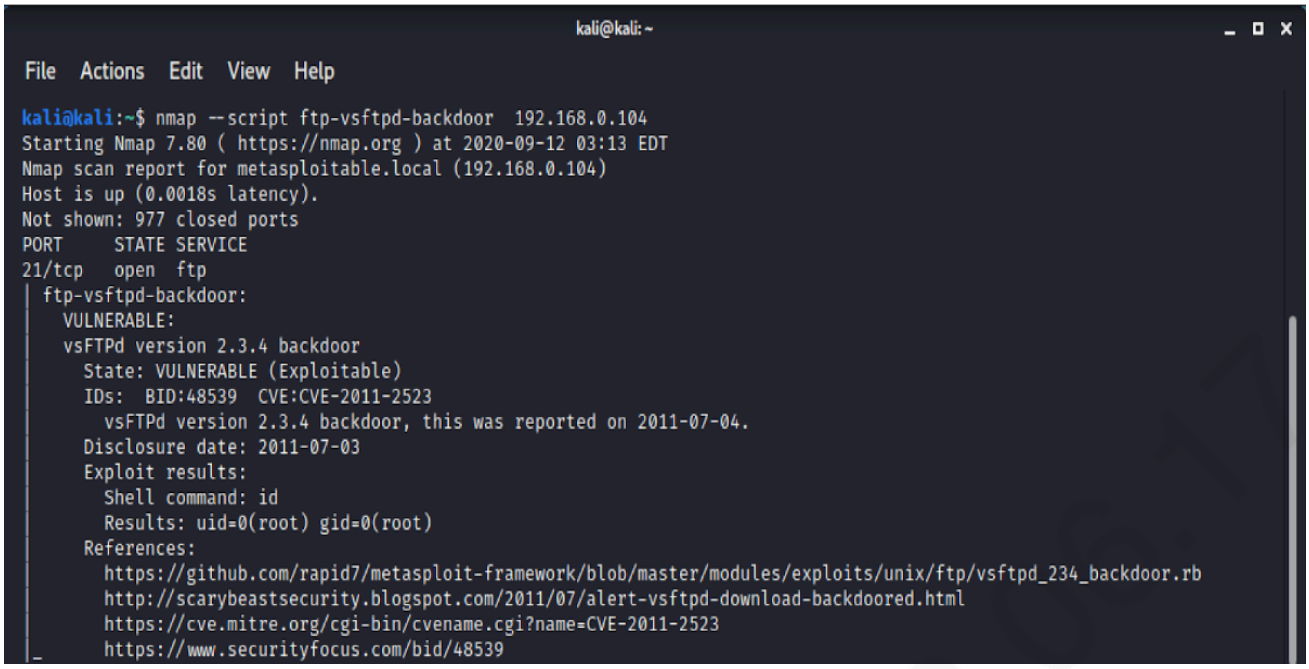
auth-spoof	Checks for an identd (auth) server which is spoofing its replies.
dns-zeustracker	Checks if the target IP range is part of a Zeus botnet by querying ZTDNS @ abuse.ch. Please review the following information before you start to scan: • https://zeustracker.abuse.ch/ztdns.php
ftp-proftpd-backdoor	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.
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.
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.
http-malware-host	Looks for signature of known server compromises.
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: • http://www.virustotal.com
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.
smb-double-pulsar-backdoor	Checks if the target machine is running the Double Pulsar SMB backdoor.
smtp-strangeport	Checks if SMTP is running on a non-standard port.

माथि दिईएको चित्रमा 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।



$ nmap --script malware 192.168.0.104 -sV

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



$ 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।

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

८. 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 छ:

-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)

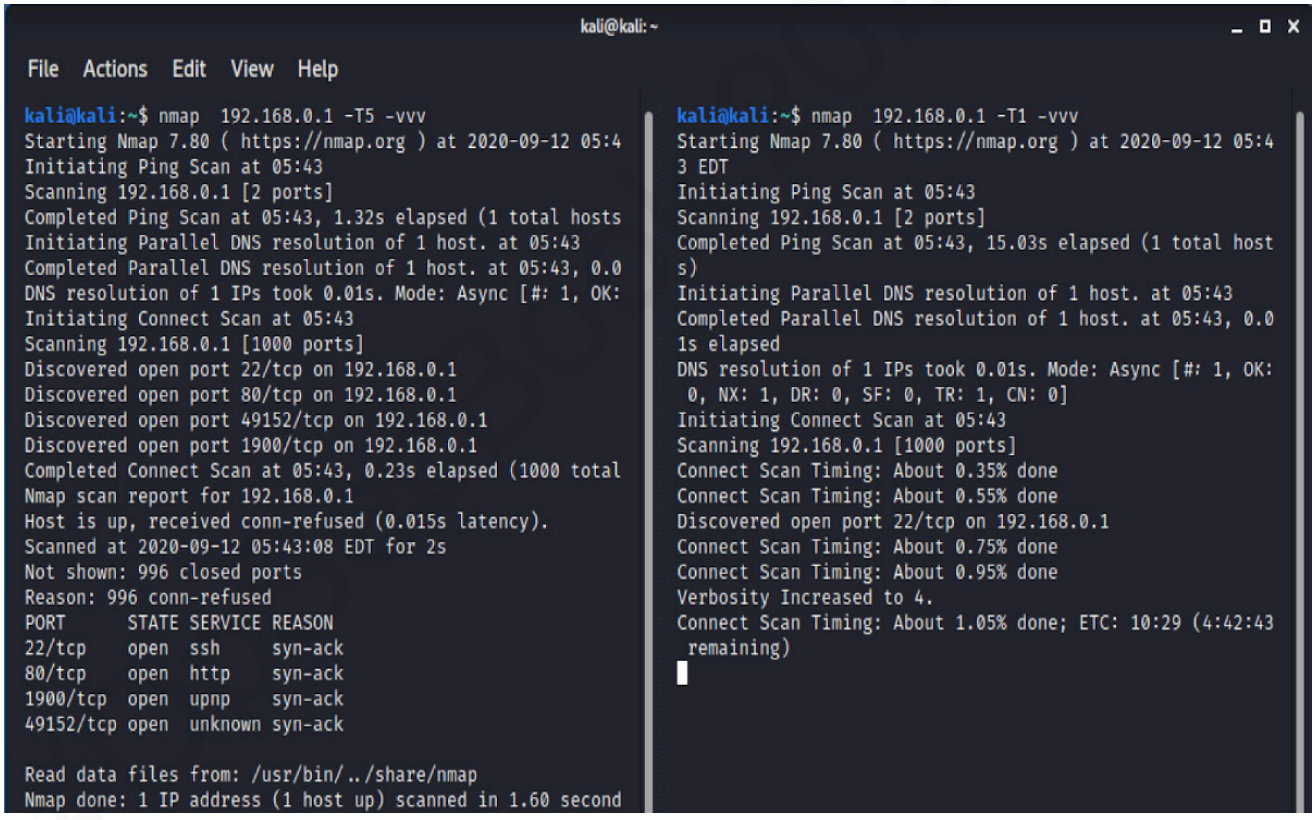
प्रयोग: यस modeले स्क्यानहरु छिटो बनाउँदछ एवं तपाई एक fast र reliable नेटवर्क मा हुनुहुन्छ भन्ने अनुमान गर्दछ।

Command : Nmap -T4 <TARGET_IP>

-T5(insane)

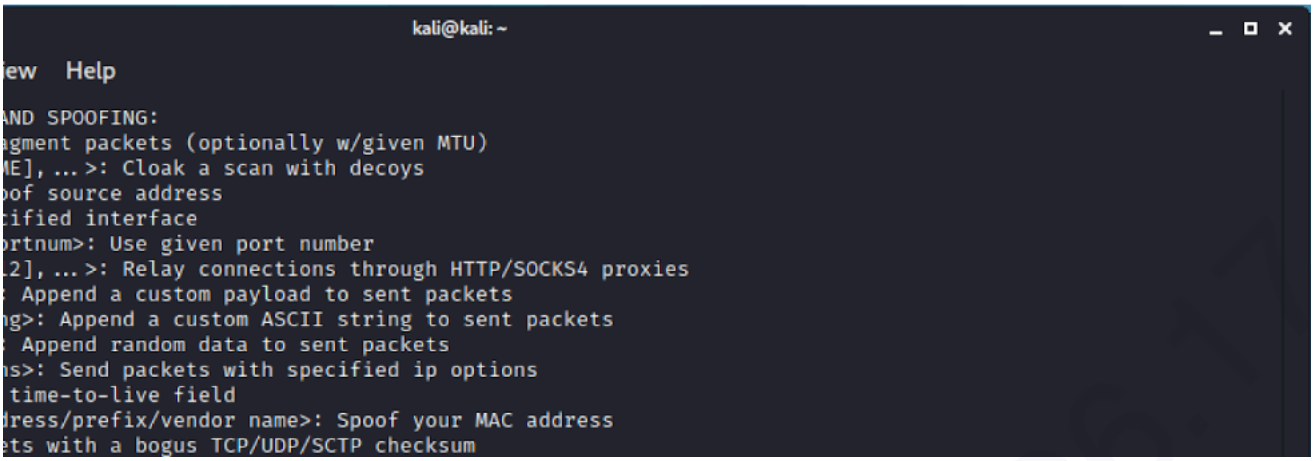
प्रयोग: यहाँ Assumptionके लिइन्छ भन्दा तपाईं एउटा फास्ट नेटवर्कमा हुनुहुन्छ वा तपाईं गतिको(speed) लागि सटीकता(accuracy) त्याग्न इच्छुक हुनुहुन्छ भने यो mode प्रयोग गर्न सक्नुहुन्छ।

Command : nmap -T5 <Target_ip>



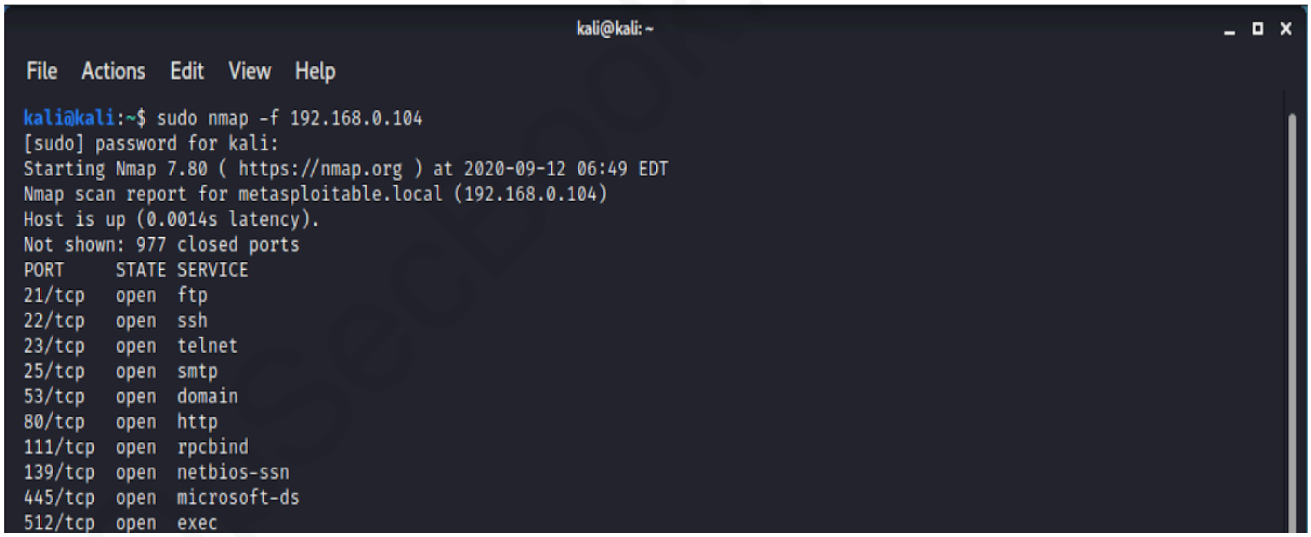
माथि चित्रमा "-T5" प्रयोग गर्दा केवल 1.6 सेकेन्ड लाग्यो भने "-T1" द्वारा अन्दाजी 4:42 घण्टामा scanning सकिन्छ भनेर दायाँ screen मा देख्न सकिन्छ र यो नै "-T1" र "-T5" टेम्पलेट (Template)को मुख्य भिन्नता रहेको छ।

९. Firewall / IDS Evasion And Spoofing:



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

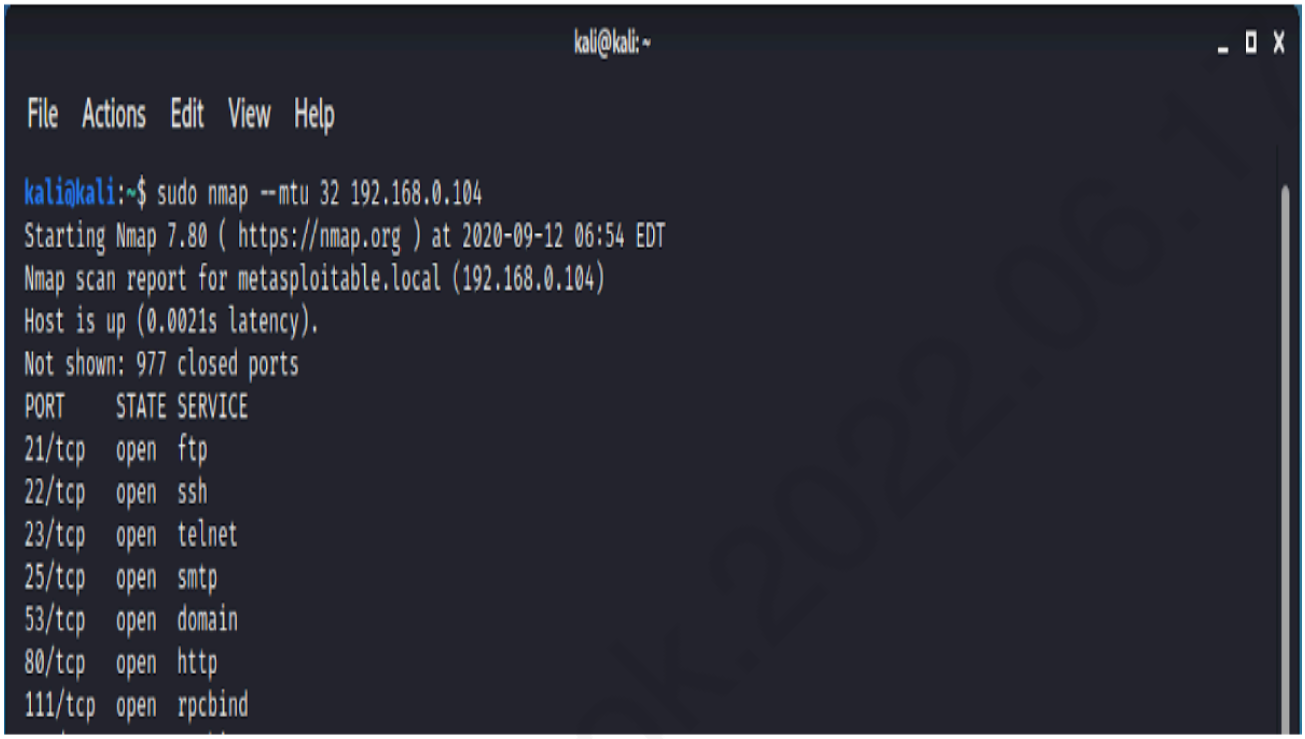
९.१ Packet Fragmentation:



$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 गाह्रो बनाउँदछ।

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

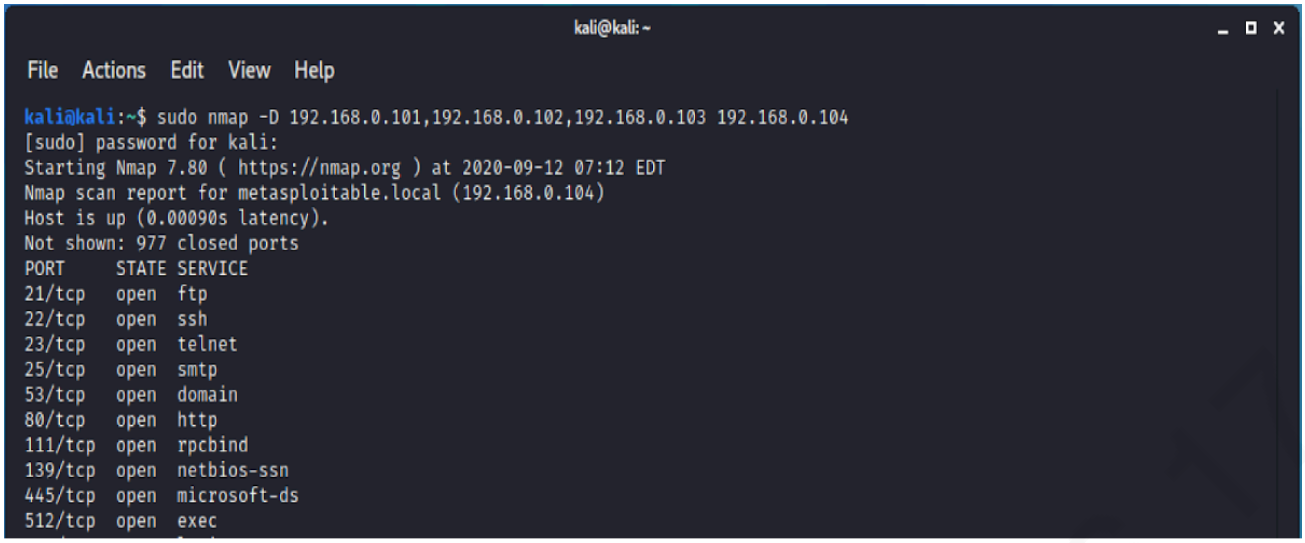


$ sudo nmap --mtu 32 192.168.0.104

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।

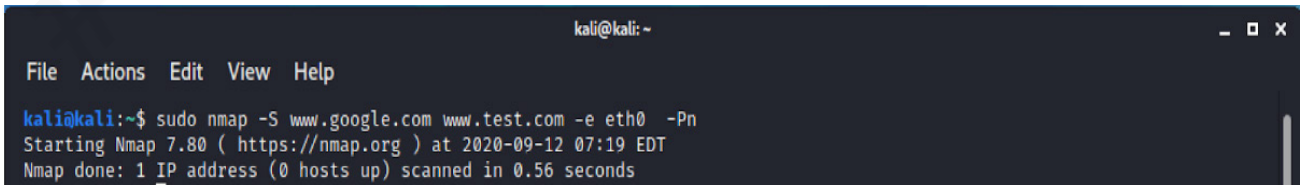


$ nmap -D 192.168.0.101,192.168.0.102,192.168.0.103 192.168.0.104

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

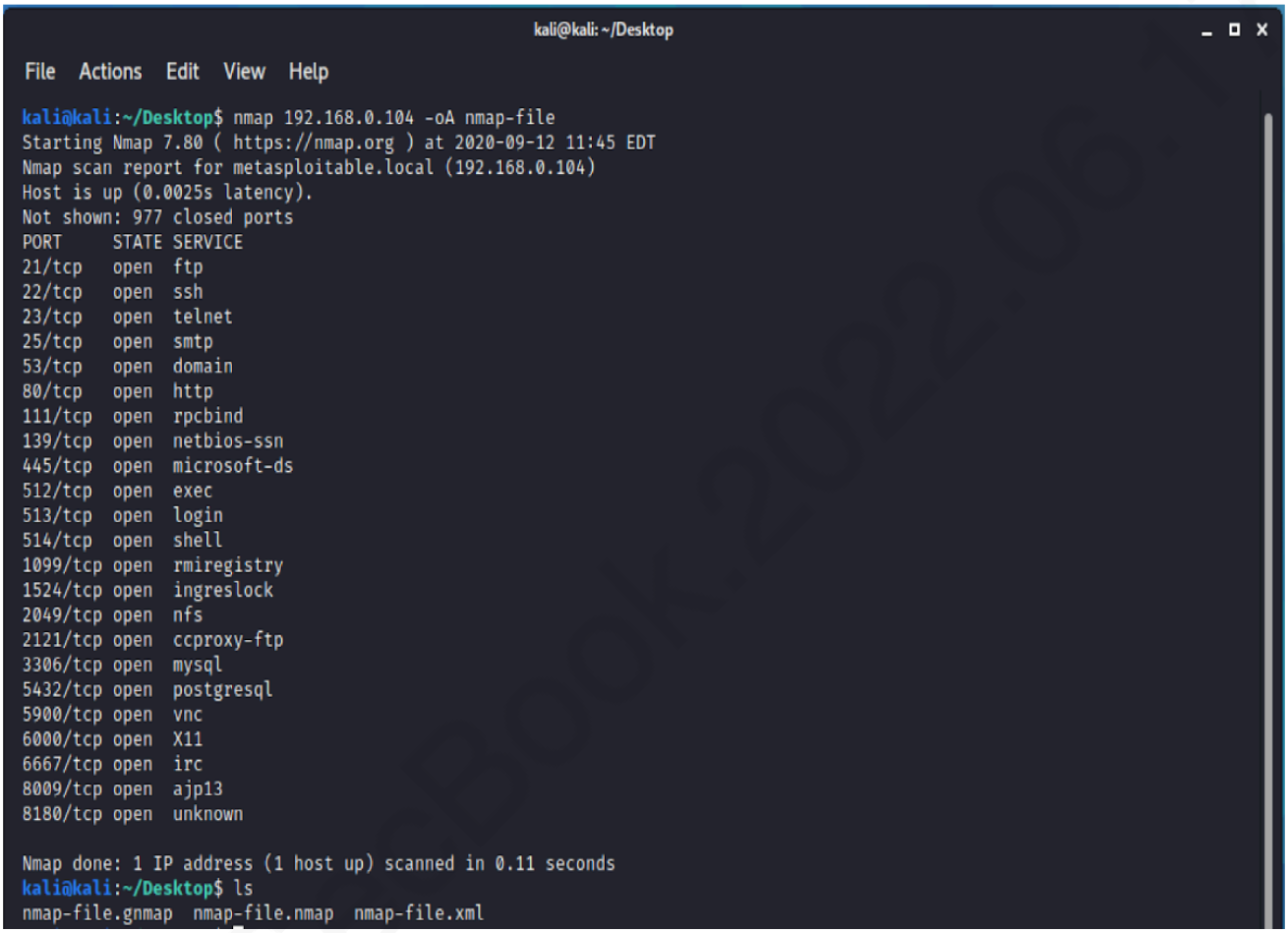
Nmap मा Attacker ले source IP लुकाउन "-S" switch को प्रयोग गर्न मिल्छ । यसोगर्दा Attacker को IP Target system को IDS / Firewall मा legitimate प्रयोगकर्ता हो भनेर पुष्टि गर्न सजिलो हुन्छ ।
Command: nmap -S <spoofed ip> <other optins>



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

१०. Output

हामी nmap search resultको outputलाई बिभिन्न स्विच प्रयोग गरेर पुनःनि-र्देशित गर्न सक्दछौं। धेरै जसो हामी "-oA" प्रयोग गर्न सक्दछौं। यसले फाईललाई 3 वटा बिभिन्न File extensionमा एकैपटक पटक save गरेर राखिदिन्छ।



$ 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 ।

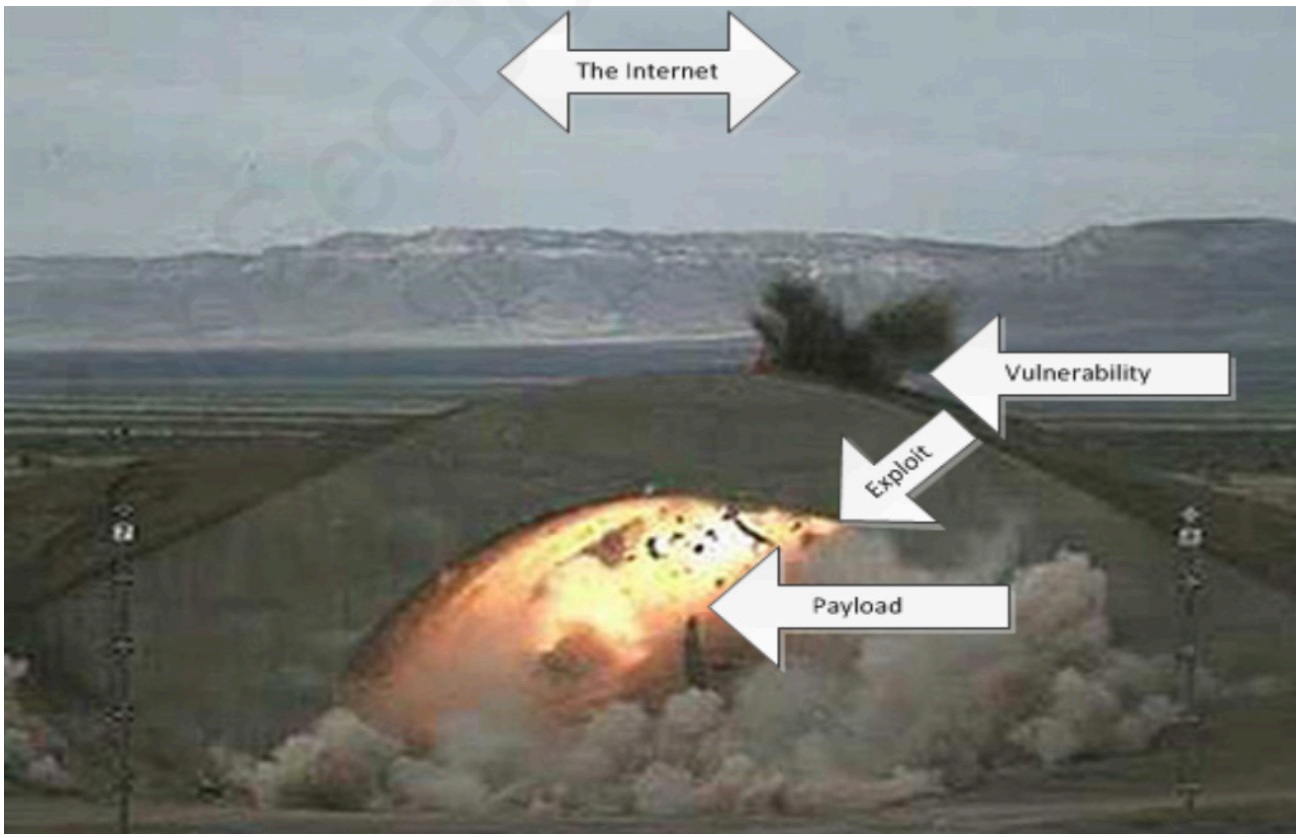
$ nmap -A 192.168.0.104 -p1-100

Gaining access via Password Cracking

System / Network मा access प्राप्त गर्नु कुनै पनि-ह्याकिङको प्रमुख उद्देश्य हुनेगर्दछ। मूलतः ह्याकिङ 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 मद्दत गर्ने अस्त्र 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 रुपले प्रवेश गर्ने प्रयास गर्दछौं । यसले हामीलाई थप शक्तिशाली आक्रमणहरू सुरुवात गर्न मद्दत गर्दछ । यदि network ले इन्क्रिप्सन (Encryption) प्रयोग गर्दैन भने, हामी त्यसमा Sniffing tool जडान गर्न सक्छौं र एन्क्रिप्ट (Encrypt) नगरिएको डाटा सजिलै सुन्न सक्छौं।

Hydra (हाइड्रा) : Authentication Cracker

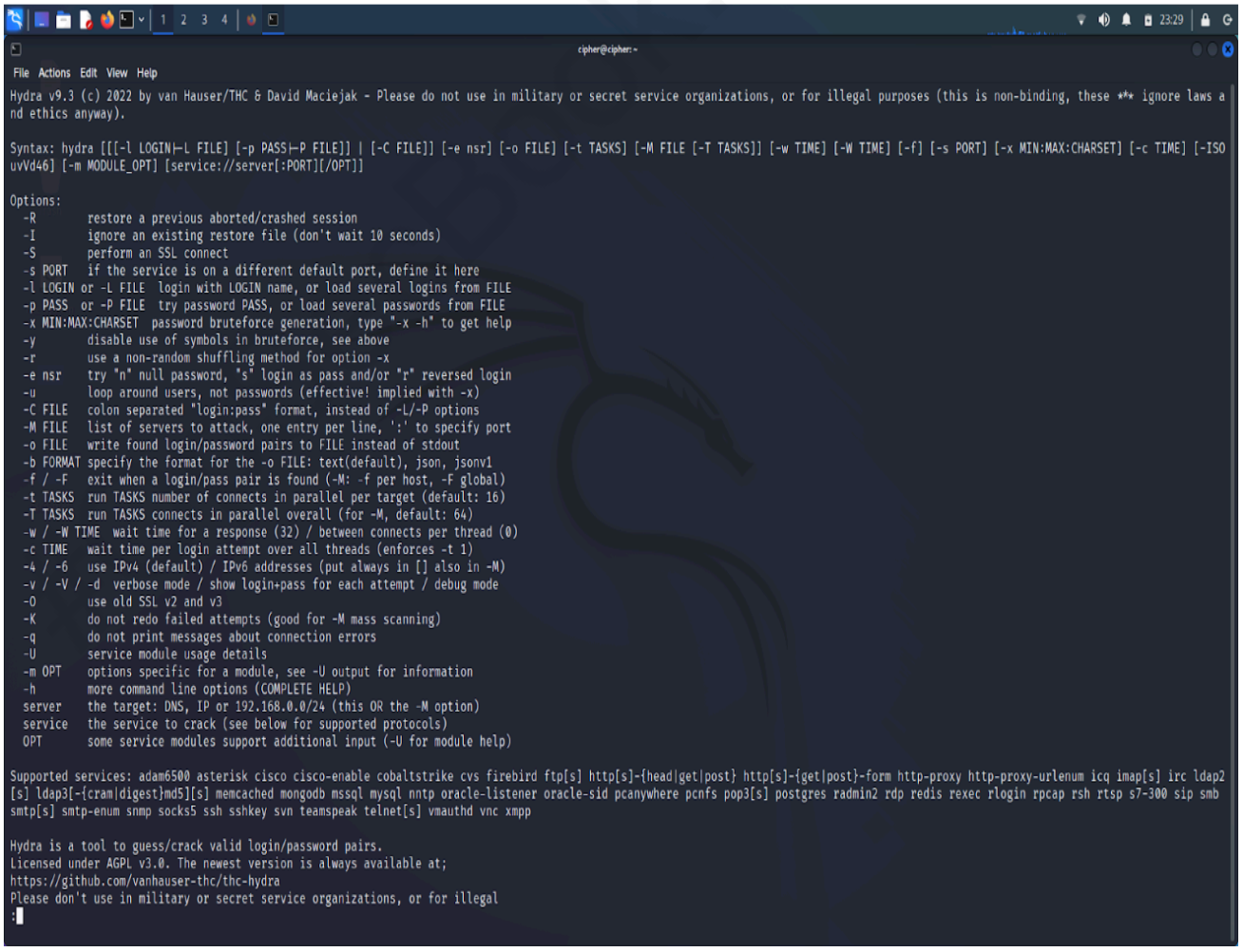
हाइड्रा एक parallel पासवर्ड क्र्याकर हो जसले धेरै प्रोटोकलहरू माथि सजिलोसँग attack गर्ने क्षमता राख्दछ। यो धेरै छिटो र लचिलो छ । हाइड्राको syntax हरु सरल र अन्य पासवर्ड cracking उपकरणहरू जस्तै छ।

हाइड्राले निम्न प्रोटोकलहरूलाई accept गर्दछ:

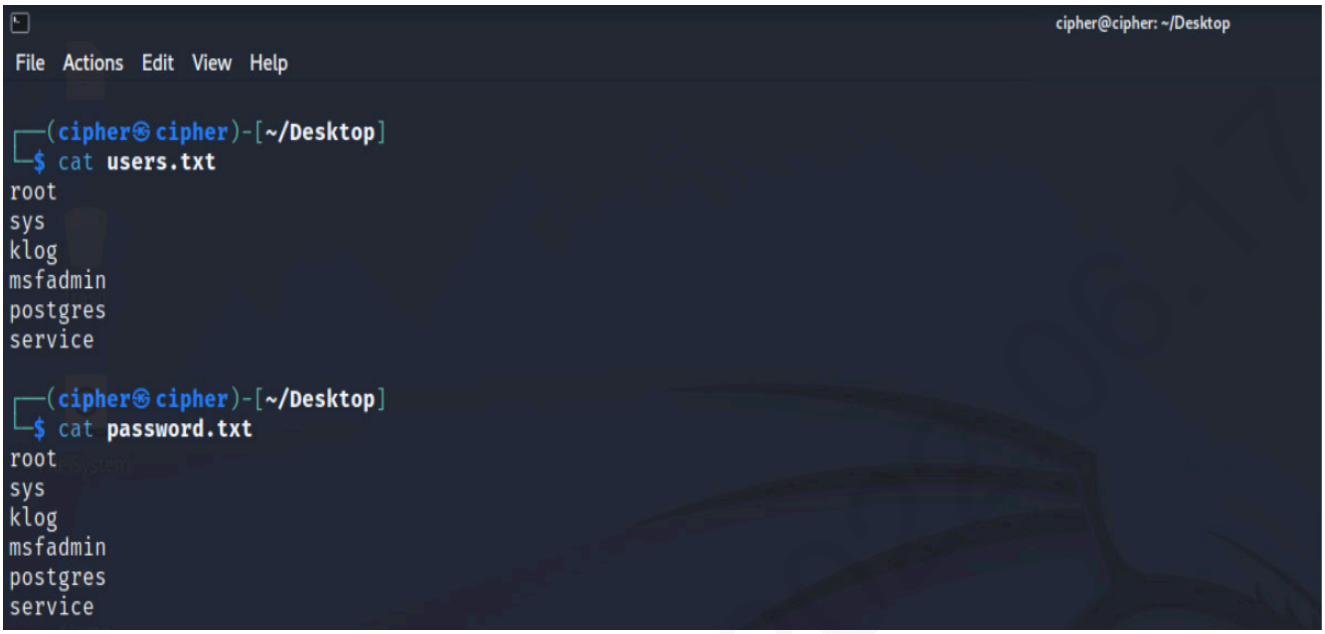
- Ftp
- Http-Form-Get, Http-Form-Post, HTTP-Get,Http-Head, Http-Post
- Imap, Irc, Ldap, Ms-sql, Mysql
- Rlogin, Rsh, SMB, SMTP, SMTP Enum
- SSH (v1 and v2), SSHKEY, Telnet, VMware-Auth, VNC,
- XMPP

THC Hydra को कमाण्डहरु:

$ hydra -h



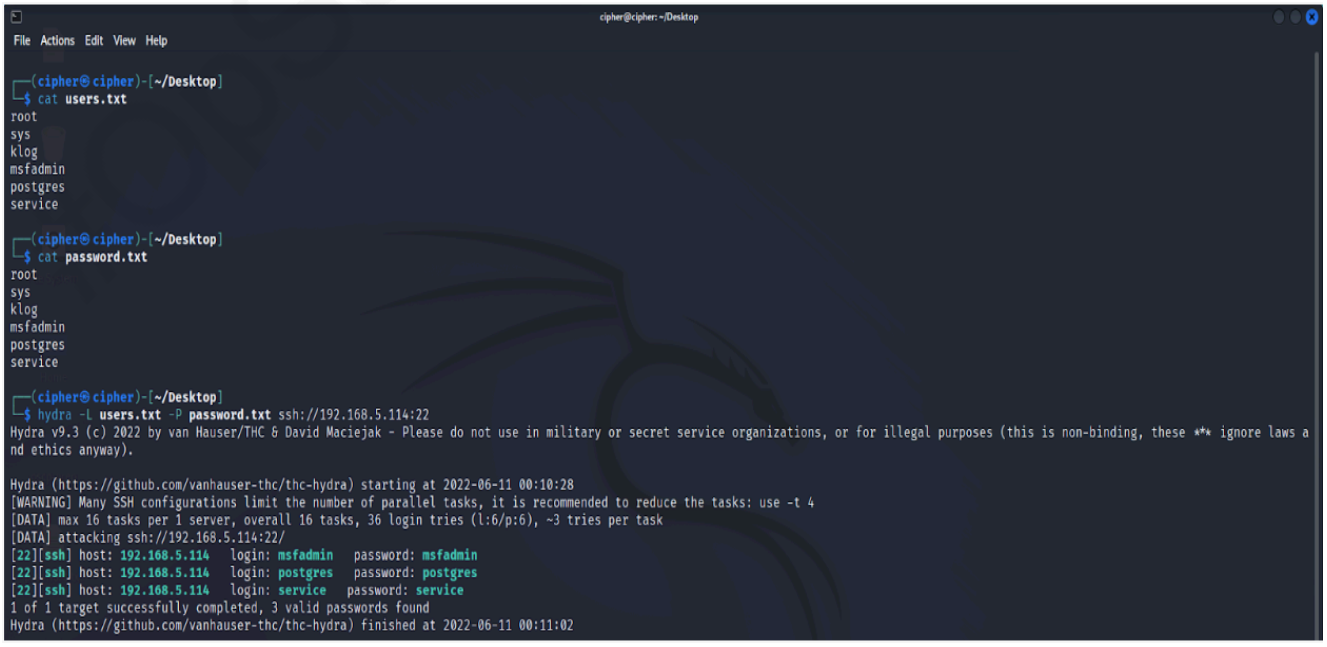
हामीले केही प्रयोगकर्ता र उनीहरुले प्रयोग गर्नसक्ने अनुमानित पासवर्डका सूचीहरू सिर्जना गरेका छौं र metasploitable-2 को ssh प्रोटोकलमा आक्रमण गर्ने प्रयास गर्दैछौं ।



हाइड्रा पासवर्ड Cracking का उदाहरणहरू :

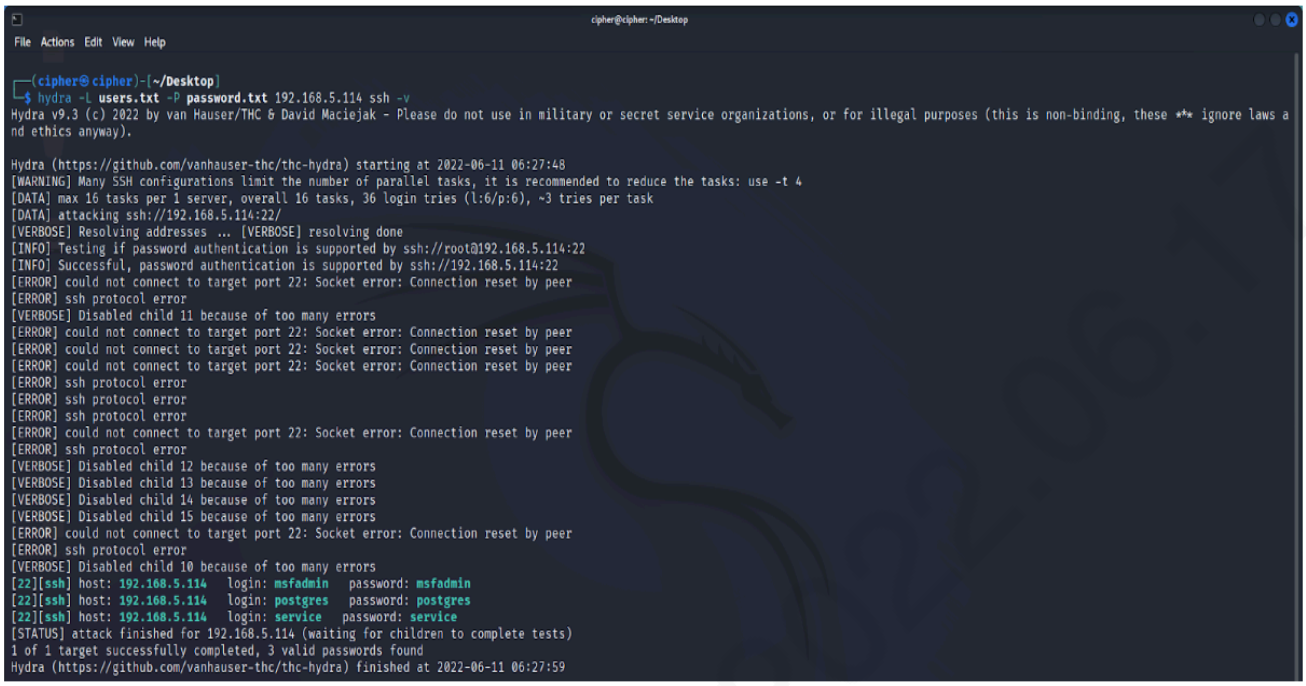
SSH protocol मा गरिएको attack :

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



FTP protocol मा गरिएको attack :

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



John the ripper : Offline Password Cracker

जोनदरिपरपासवर्डक्र्याकरtoolकोनामहोजुनOpenwallद्वाराविकसितगरिएकोहो। यसले automatic रूपमा पासवर्ड ह्यासका प्रकारहरू पत्ता लगाउँ-दछ । यो .zip, .rar, .pdf आदि जस्ता पासवर्ड प्रयोग गरि सुर-क्षित 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 तरिकाहरु प्रयोग गरेर हामीलाई चाहिएको परिणाम प्राप्त गर्न सकिन्छ तर यो मुख्य रूपमा Dictionary attack को लागि परिचित रहेको पाइन्छ।

Dictionary attack:

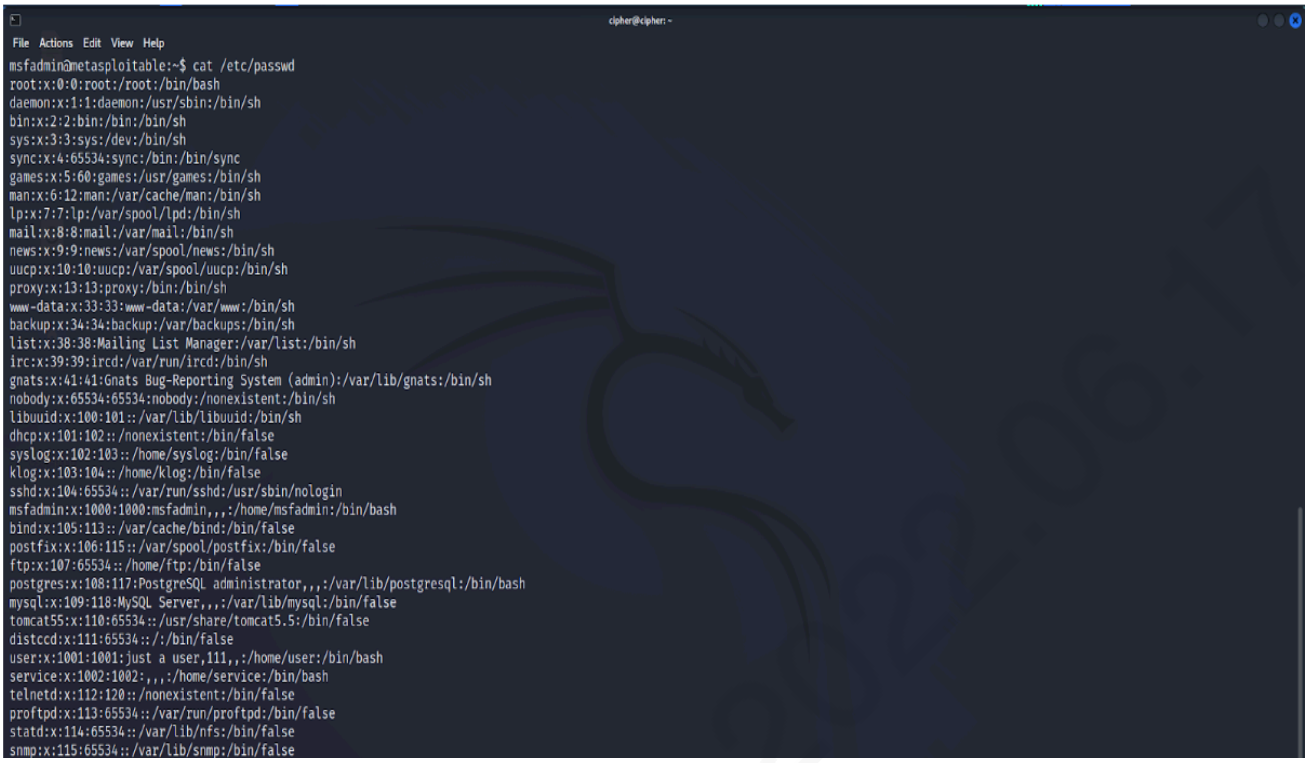
यो JTR (जोन द रिपर) पासवर्ड क्र्याकर tool मा लोकप्रिय एवं सबैभन्दा प्रयोग योग्य attack हो जहाँ हामीले पूर्व-परिभाषित शब्दहरू क्र्याक गर्नको निम्ति प्रयोग गर्दछौं।

Brute-force attack:

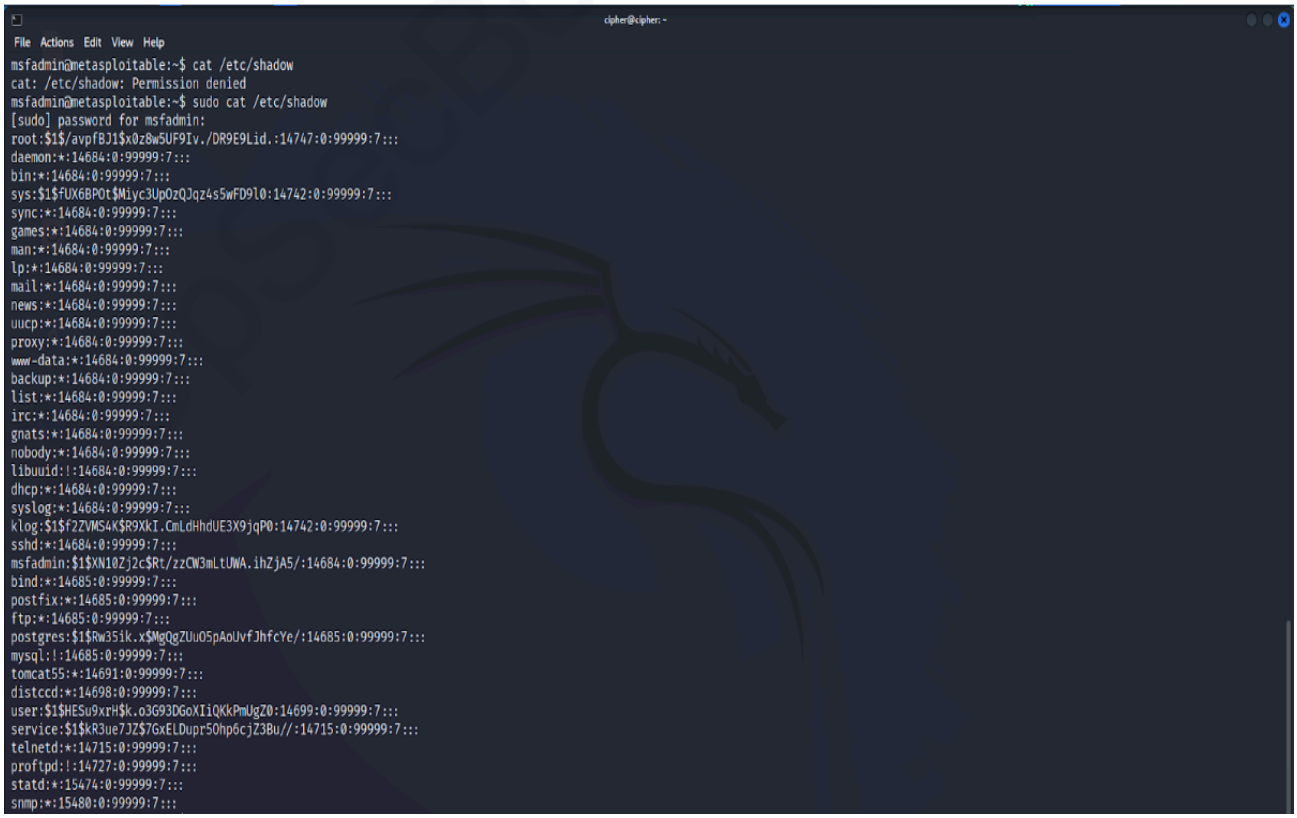
यदि तपाइँ यो attack method प्रयोग गर्दै हुनुहुन्छ भने यसको प्रयोग गर्नु अघि केहि चीजहरूको configuration गर्न जरुरी पर्दछ। जस्तै पासवर्डको न्यूनतम र अधिकतम लम्बाइ परिभाषित गर्ने, क्र्याकिंग प्रक्रियाको क्रममा परीक्षण गर्न चाहनुहुने सम्भावित क्यारेक्टरहरू define गर्ने । जस्तै (विशेष वर्णहरू, अक्षरहरू र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

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

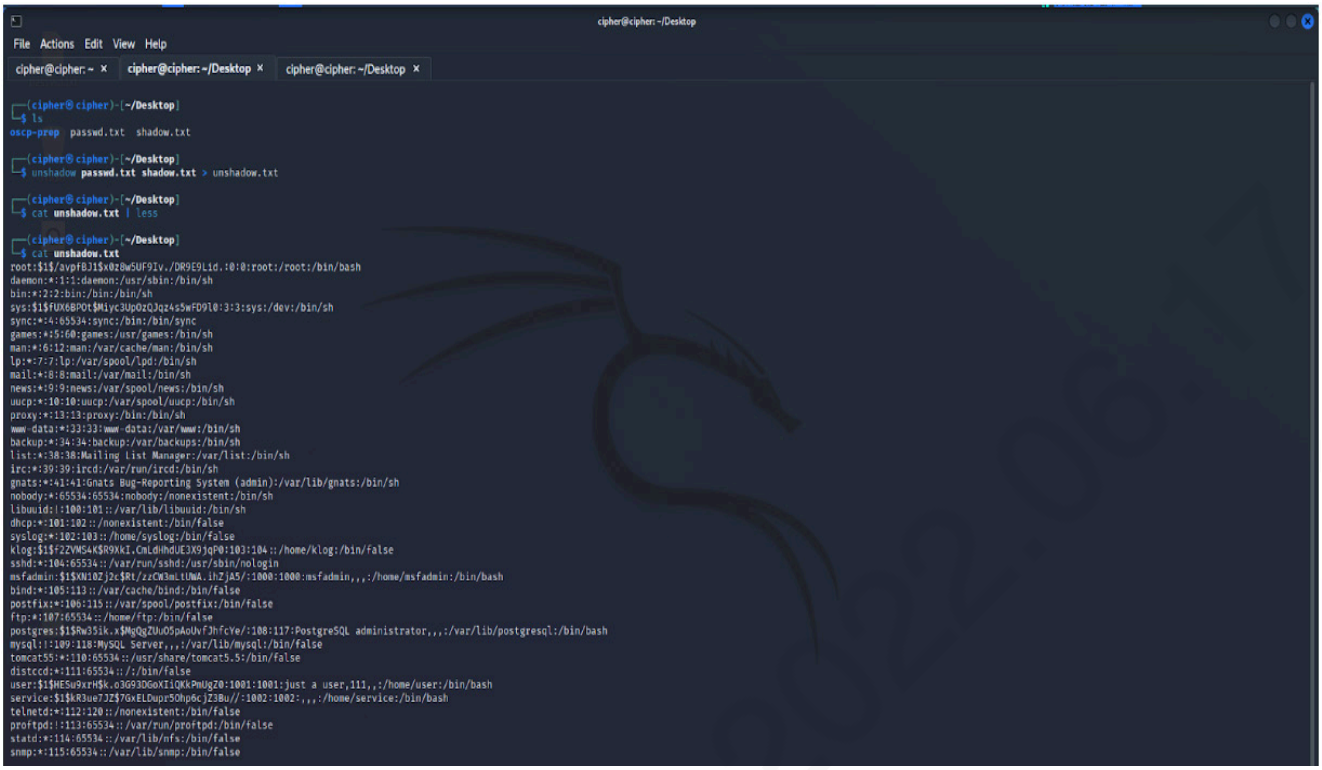
metasploitable-2 को /etc/passwd फाइल



metasploitable-2 को /etc/shadow फाइल :



unshadow को आउटपुट :



john the ripper द्वारा क्र्याकिंग:

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

Maintaining Access

Penetration Test को समयमा, एक पटक target system मा access प्राप्त गरिसकेपछि, Tester हरुले त्यो system मा access कायम राखिराख्न आवश्यक पर्छ। यस chapter ले system /network मा निरन्तर पहुँच कायम राख्न प्रयोग गर्ने विधिहरू (methods) र उपकरणहरू (tools) बारे छलफल गर्नुका साथै target को सूचना सङ्कलन (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 रुपमा 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 हरु 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 स्क्यानिङ :

$ nmap -A -sV -p 21 192.168.5.114

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

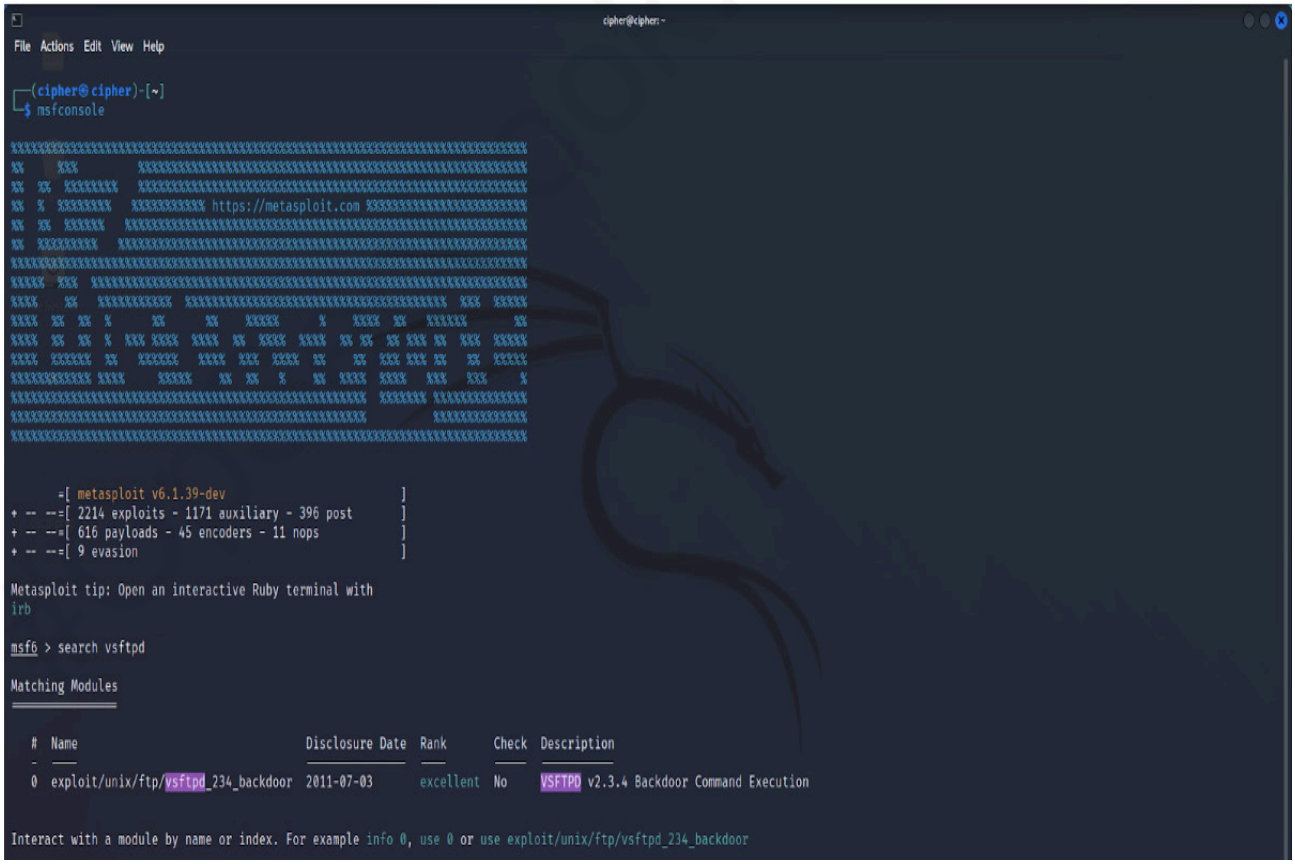
Exploit Identification :

$ searchsploit -s vsftpd 2.3.4

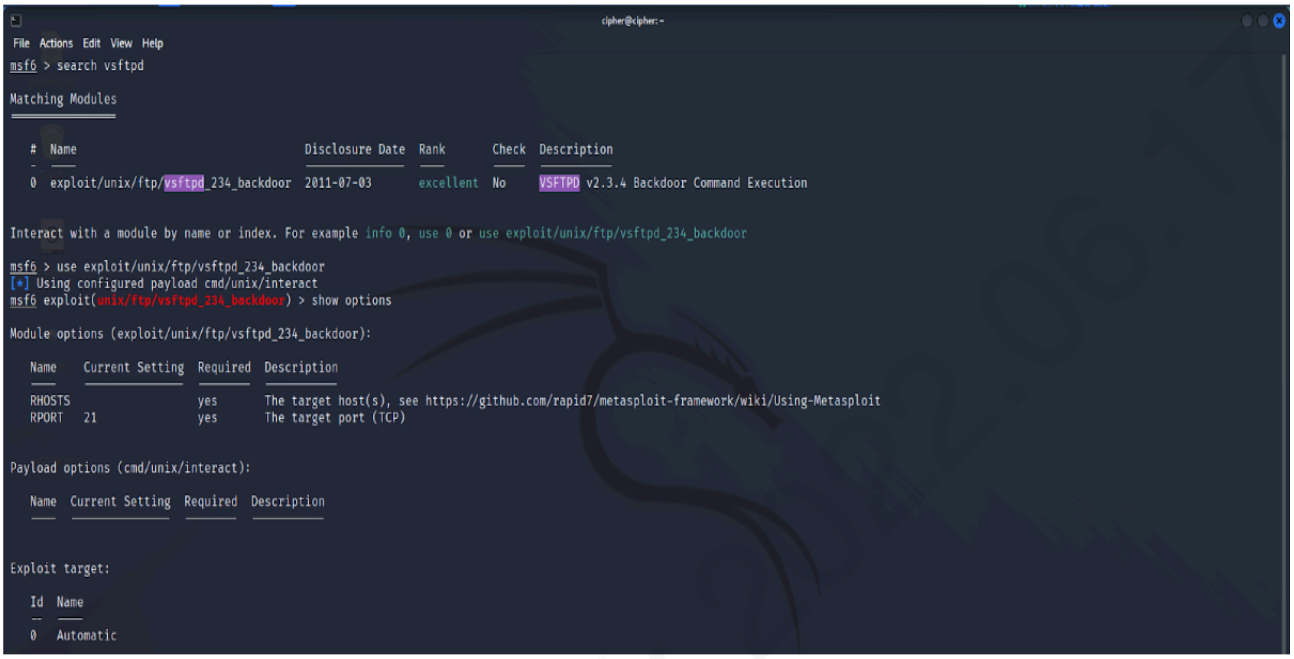
vsftpd 2.3.4 को exploit हरु केही छ कि भनि searchsploit को मध्य-मबाट search गर्दा हामीले RCE (Remote Code Execution) रहेको पत्ता लगाउन सक्दछौं ।

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 ।

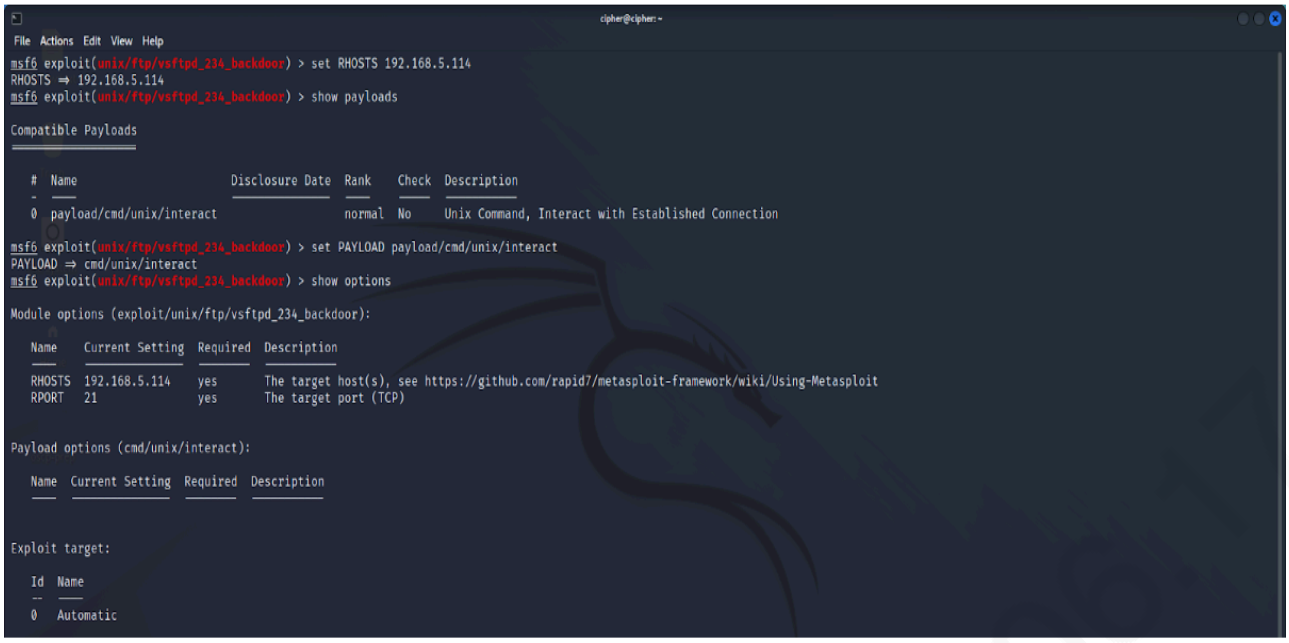


माथि दिएको चित्रमा हामीले vsftpd को exploit खोज्ने प्रयास गरेका छौं जसबाट exploit/unix/ftp/vsftpd_234_backdoor नामको परीणाम हामीले search को output मार्फत पाएका छौं ।

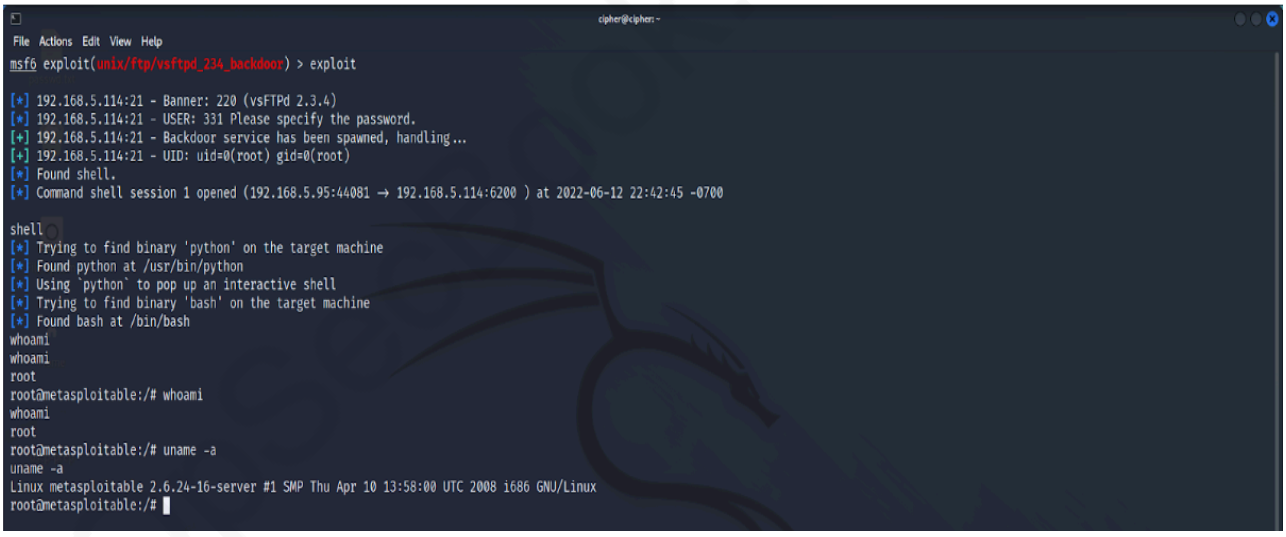


माथि देखाइएको चित्रमा "use exploit/unix/ftp/vsftpd_234_backdoor " command ले vsftpd_234_backdoor नामको exploit प्रयोग गर्नको लागि निर्देशन दिएको हामी पाउन सक्दछौं ।

" 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।



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 छौ ।



सबै चाहिएको 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 जसबाट metasploitable-2 सर्भरमा हामीले illegal root access जुन माथि चित्रमा देखाई जसरी पाउन सक्छौं ।

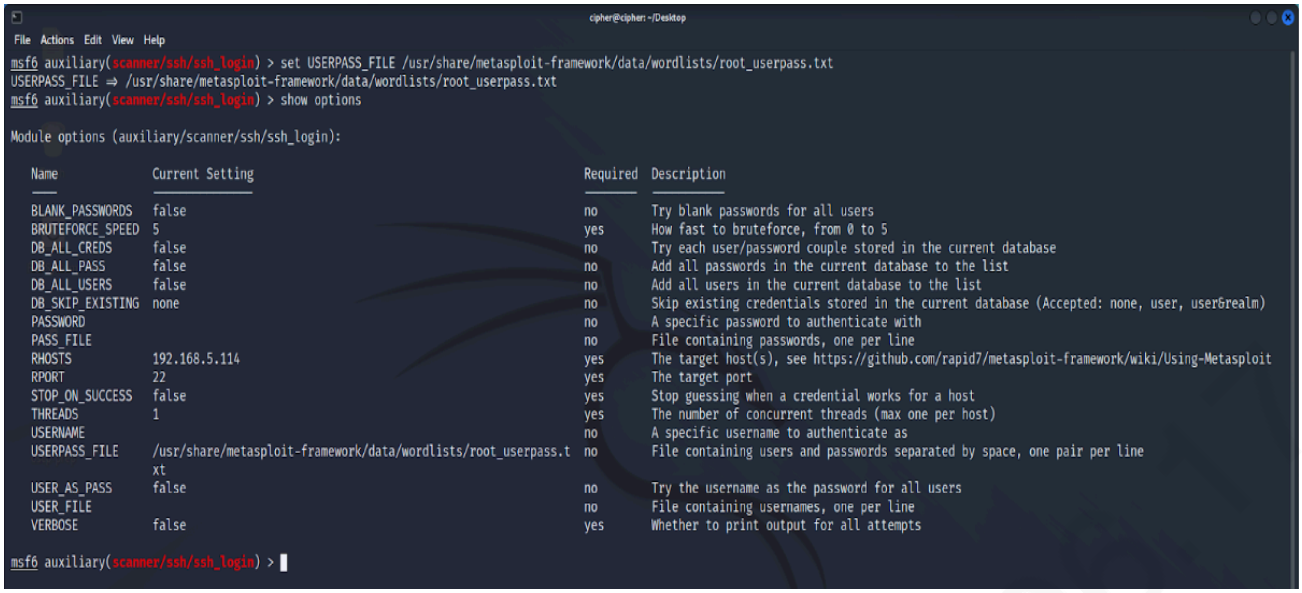
Attacking via Port 22 (ssh) in metasploitable - 2 :

System scanning :

$ nmap -A -sV -p 22 192.168.5.114

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

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



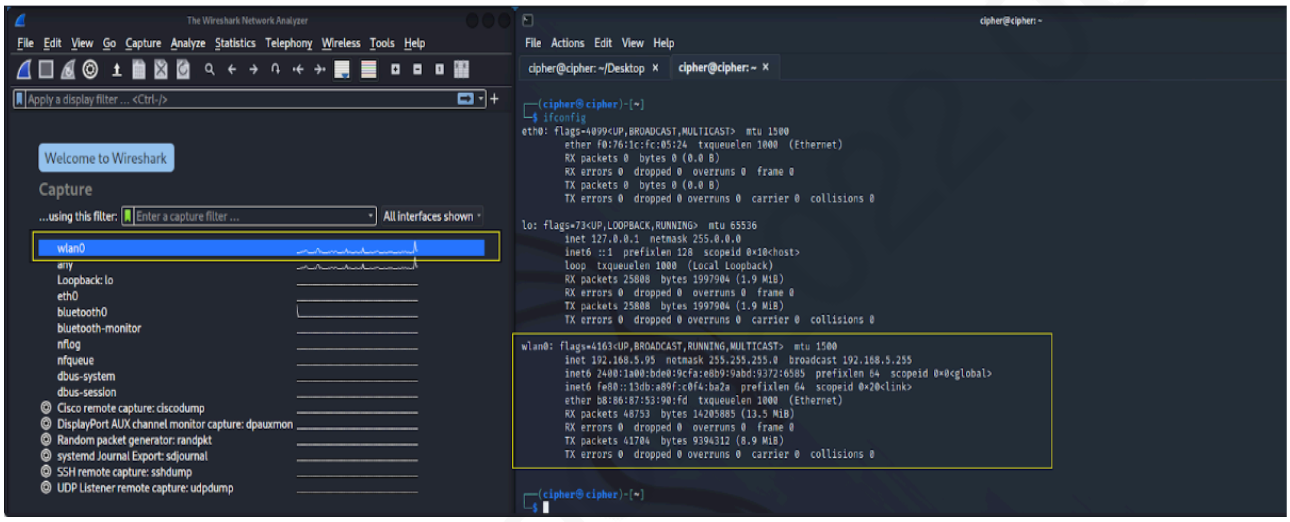
Metasploit मार्फत bruteforce गर्दा file को पुरै location सहित प्रयोग गर्न लागेको text file को नाम माथि चित्रमा झै उल्लेख गर्नुपर्दछ।

"run" कमाण्डले ssh (port number 22) मा रहेको सर्भिसलाई माथि चित्रमा दिए झैँ 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 गरिदिएको हामी “session -i” command मार्फत पत्ता लगाउन सक्दछौं ।

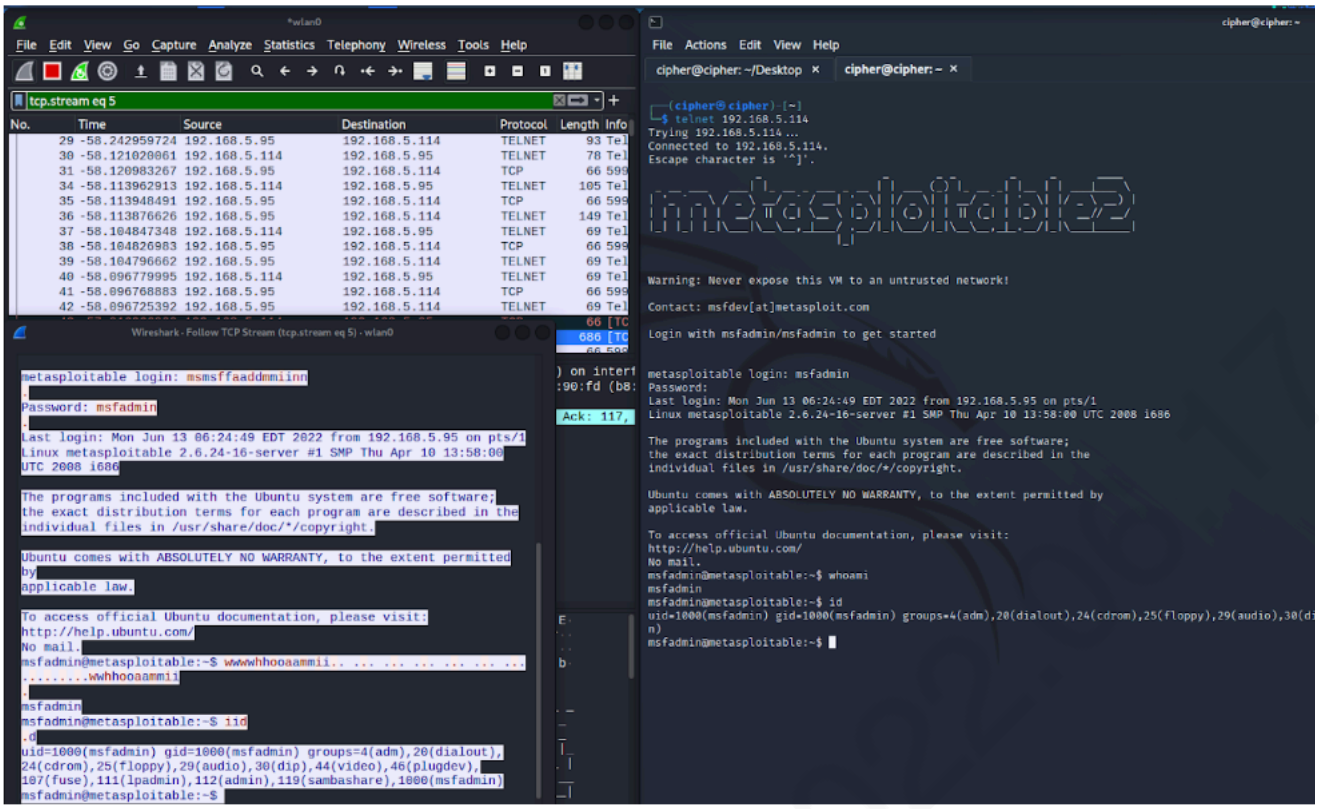
Session login गर्दा metasploitable -2 को server मा direct access चित्रमा दिएझै पाउन सक्छौं ।

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 ।



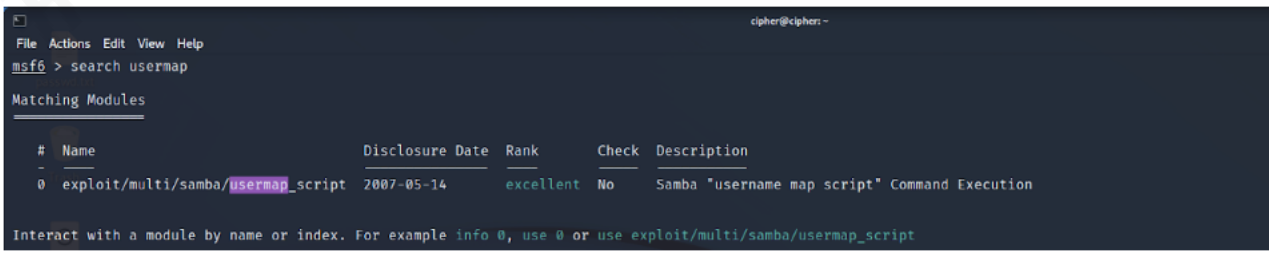
Wireshark मा Follow TCP Stream गर्दा हामीले telnet login गर्नेबेला प्रयोग गरिएको credentials हरु सजिलैसँग Clear text मा नै माथि चित्रमा दिए जसरी भेट्न सक्छौं जसले गर्दा illegal users अरुले सजिलै यस protocol लाई माध्यम बनाएर root access लिन सक्दछ ।

Attacking via Port 445 (samba) in metasploitable2:

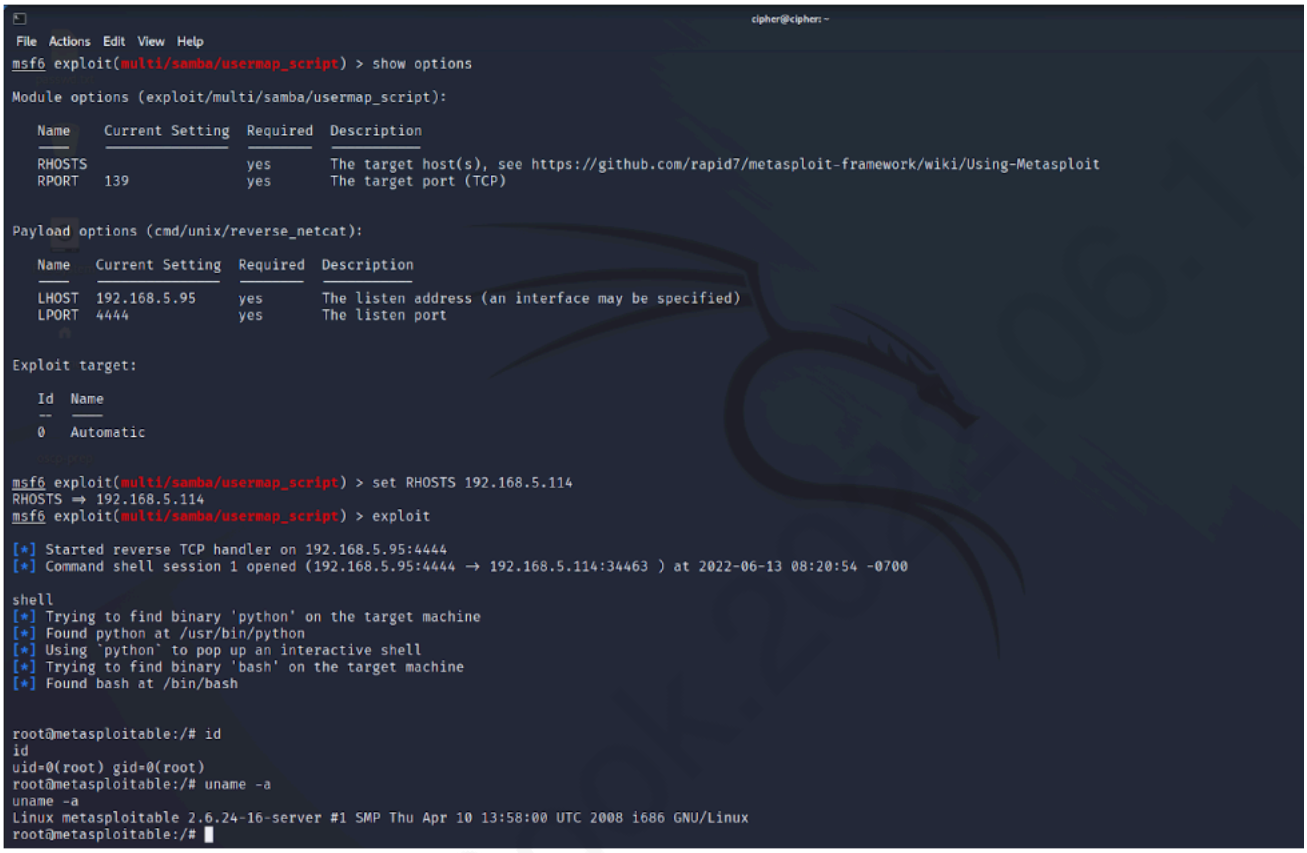
System scanning :

$ nmap -A -sV -p 445 192.168.5.114

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 ।



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



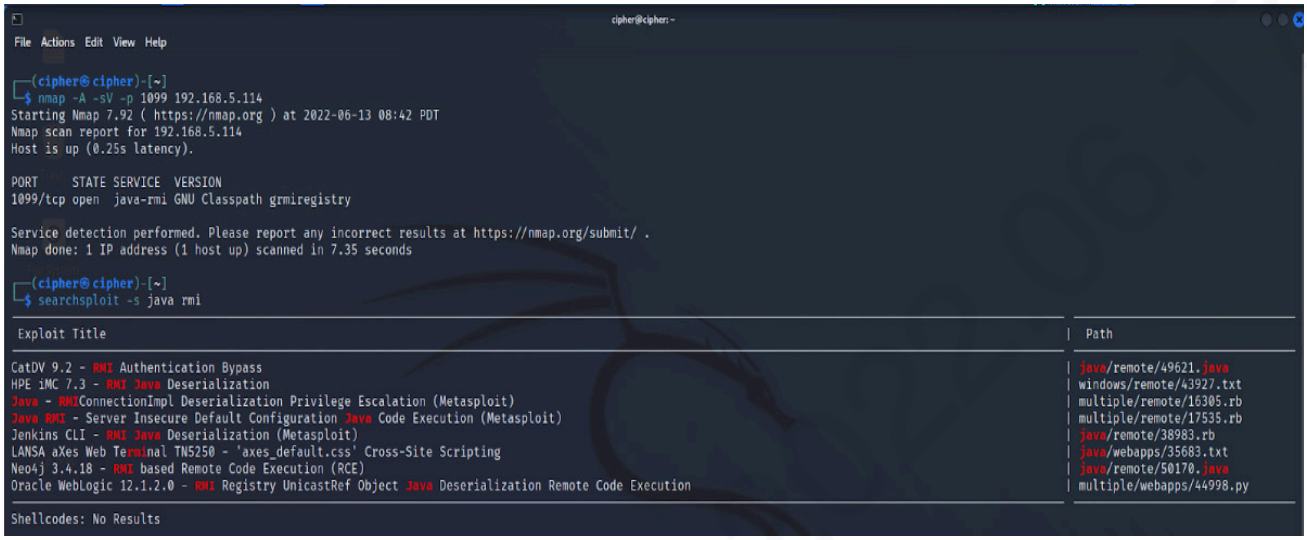
"show options " मार्फत त्यस exploit मा उल्लेख गर्नपर्ने कुरा जस्तै RHOST (Remote Host) को IP , RPORT (Remote Port) को port number , LHOST (Local Host) को IP, LPORT (Local Port) को port number , साथै Payload को selection हरु उल्लेख गरे नगरेको re-check गर्न सक्दछौं ।

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 ।

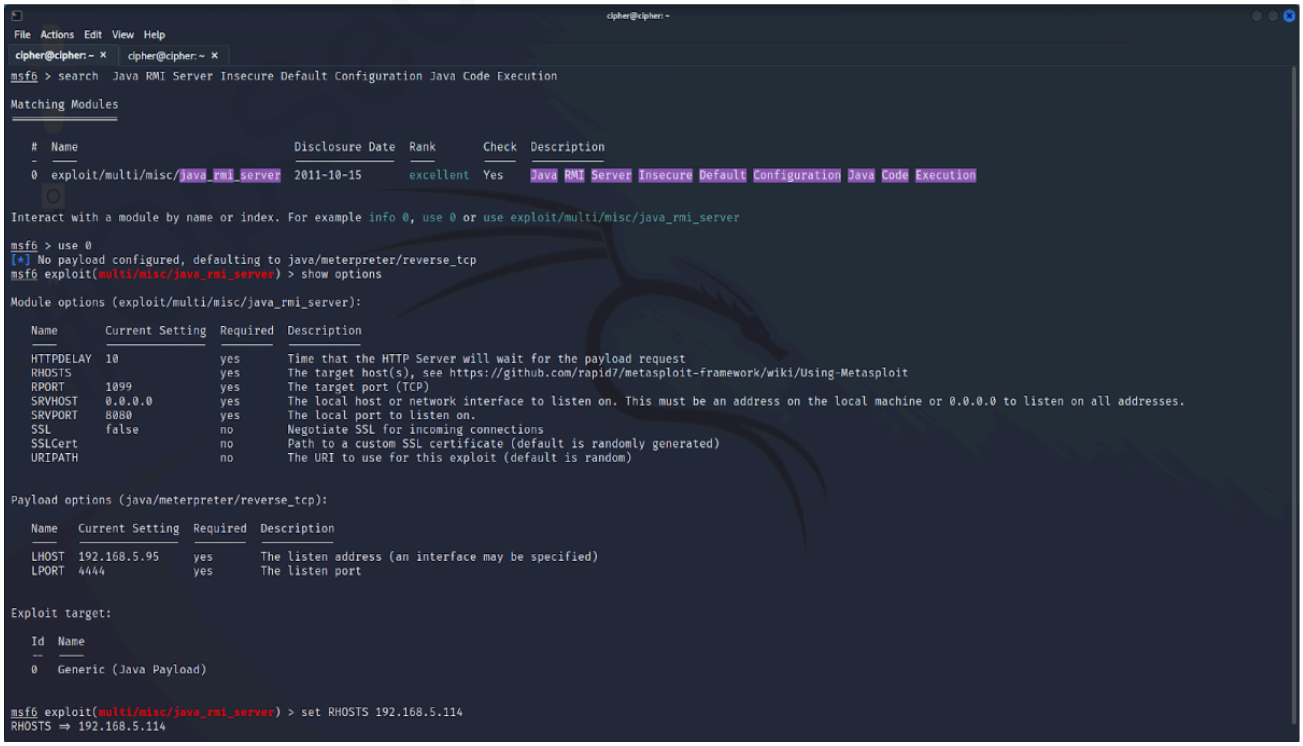
Attacking via port 1099 :

System scanning :

$ nmap -A -sV -p 1099 192.168.5.114



माथि दिईएको चित्रमा 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 ।



"show options " बाट 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 ।

End Of Volume I

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