



Footprinting Using Nmap

Yuvraj Singh¹, Pawan Singh², Garima Sinha³

^{1,2}Department of Computer Science and Engineering, Amity University Uttar Pradesh, Lucknow Campus, India

³Department of Computer Science and Engineering, Jain University, Bangalore, India

¹yuvraj.1306.singh@gmail.com, ²pawansingh51279@gmail.com, ³mailatgarima@yahoo.co.in

How to cite this paper: Y. Singh, P. Singh and G. Sinha, "Footprinting Using Nmap," *Journal of Informatics Electrical and Electronics Engineering (JIEEE)*, Vol. 03, Iss. 02, S No. 004, pp. 1–15, 2022.

<https://doi.org/10.54060/JIEEE/003.02.004>

Received: 14/10/2022

Accepted: 19/11/2022

Published: 25/11/2022

Copyright © 2022 The Author(s).
This work is licensed under the
Creative Commons Attribution
International License (CC BY 4.0).
<http://creativecommons.org/licenses/by/4.0/>



Open Access

Abstract

Nmap is inbuilt in Kali Linux that is utilized by the organization to identify the weakness and remediate it. There are different sorts of subtleties that Nmap offers in the wake of filtering the objective. The data expressed in the manuscript can be utilized comprehend the idea of what Footprinting is, what hackers search for to Footprint, and how to shield against it. Nmap is a free and open-source utility for network disclosure and security examining. Numerous frameworks and organization heads additionally find it valuable for errands. In this paper, the study is conducted on the utilization of NMAP for the footprinting. The cloudflare server is utilized for the study. The suggestions on are provided to avoid the footprinting. The results of the study will be helpful to avoid the footprinting.

Keywords

Footprinting, Ethical Hacking, Penetration Testing, Vulnerabilities, Bugs, Scanning, Reconnaissance, Ping, Intrusion, Firewall, Risk, Attacker, Security Issues.

1. Introduction

Footprinting is one of the techniques applied to recover the data about the objective framework. Footprinting innovation generally talks about stages at pre-assaults at the organization. The Footprinting ordinarily accumulates network related data, for example, Network ID, space name alongside inside area name, access control instruments, IP address, conventions, VPNs, consents, client and gathering data, directing tables, framework flags, public statements and news stories, distant framework types, web waiter joins and so on. Assuming the aggressor assembles the touchy data, they might involve the information for extortion, making the phony profiles, and so on. The assailant by get-together more comparable kind of data connected with target interests and exercises, the aggressor can join a few other web-based entertainment and gatherings which further leads further Footprinting.



Footprinting alludes to the method involved with gathering however much as data as could reasonably be expected about the objective framework to track down ways of entering into the framework. An Ethical programmer needs to invest most of his energy in profiling an association, gathering data about the host, organization and individuals connected with the association. Data, for example, ip address, Whois records, DNS data, a working framework utilized, worker email id, Phone numbers and so on is gathered. Footprinting serves to:

- **Realize Security Posture**

The information assembled will assist us with getting an outline of the security stance of the organization, for example, insights regarding the presence of a firewall, security designs of utilizations and so on.

- **Lessen Attack Area**

Can recognize a particular scope of frameworks and focus on specific targets in particular. This will incredibly decrease the quantity of frameworks we are focussing on.

- **Recognize weaknesses**

We can construct a data set containing the weaknesses, dangers, provisos accessible in the arrangement of the objective association.

- **Draw Network map**

Assists with drawing an organization guide of the organizations in the objective association covering geography, confided in switches, presence of server and other data.

In this paper, the study of the various hacking styles is discussed. The study on the technique of footprinting is conducted and the cloudflare server is utilized for the case study. The ethical hacking tool NMAP available with kali Linux is utilized to perform the task of the footprinting. The suggestion to avoid the footprinting are suggested and the detailed study is conducted. The organization of the paper is as follows: in the section 2, the background of the hacking and footprinting is discussed. Section 3 explains phases of ethical hacking. In the section 4, the footprinting is explained in detail. The utility and working of NMAP is discussed in the section 5. The result of the study and its detailed discussion is reflected in the section 6. Section 7 shows the efforts required to avoid the footprinting. In the last section 8, the conclusion is provided.

2. Background

2.1. Ethical Hacking

Ethical Hacking some of the time called as Penetration Testing is a demonstration of encroaching/entering into framework or organizations to figure out dangers, weaknesses in those frameworks which a malignant assailant might find and take advantage of causing loss of information, monetary misfortune or other significant harms. The reason for ethical hacking is to work on the security of the organization or frameworks by fixing the weaknesses found during testing. To put it in the most basic terms, a computer system vulnerability is a flaw or weakness in a system or network that could be exploited to cause damage, or al-low an attacker to manipulate the system in some way.[15] Ethical programmers might utilize similar techniques and apparatuses utilized by the malignant programmers yet with the authorization of the approved individual to work on the security and shielding the frameworks from assaults by vindictive clients.

A 'white-hat' hacker, also referred to as an ethical hacker, is someone who has non-malicious intent whenever breaking into security systems.[7] Ethical programmers are supposed to report every one of the weaknesses and shortcoming found during the cycle to the administration.

Ethical hacking includes an approved endeavor to acquire unapproved admittance to a PC framework, application, or information. Cybercrime is characterized as wrongdoing where an IT system is utilized as an instrument to carry out an offense. A cyber-criminal may utilize a gadget to get to a client's very own data, classified business data, government data, or make

device disable.[11] Completing an ethical hack includes copying techniques and activities of vindictive aggressors. This training assists with recognizing security weaknesses which can then be settled before a pernicious assailant has the valuable chance to take advantage of them. Ethical hacking is a technique for securing and defending computer systems. Independent computer security professionals hack into a computer system without causing harm or stealing information.[10]

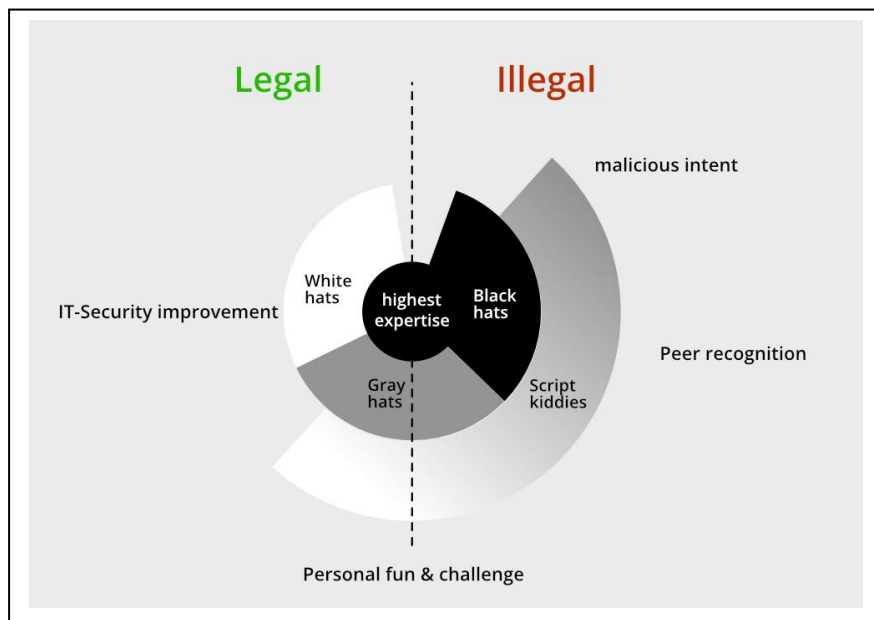


Figure 1. White, Black and Gray Hat Hackers.

An Ethical Hacker is a talented expert who has great specialized information and abilities and knows how to recognize and take advantage of weaknesses in target frameworks. Security threats and challenges in IoT are the biggest concern the corporate coders have to deal with due to innumerable threats, cyber-attacks, risks and vulnerabilities of the system.[18]

Hacking specialists follow four key convention ideas:

- **Remain legitimate** - Get legitimate endorsement prior to getting to and playing out a security evaluation.
- **Characterize the degree** - Decide the extent of the evaluation so the ethical programmer's work stays lawful and inside the association's endorsed limits.
- **Report weaknesses** - Tell the association of all weaknesses found during the appraisal. Give remediation guidance to settling these weaknesses.
- **Regard information responsiveness** - Contingent upon the information responsiveness, ethical programmers might need to consent to a non-exposure understanding, notwithstanding different agreements expected by the evaluated association.

There are a few limits of ethical hacking:

- **Restricted scope** - Ethical programmers can't advance past a characterized extension to make an assault effective. In any case, it's not irrational to examine out of degree assault potential with the association.
- **Asset imperatives** - Vindictive programmers don't have time limitations that ethical programmers frequently face. Figuring power and spending plan are extra requirements of ethical programmers.
- **Limited techniques** - A few associations request that specialists keep away from experiments that lead the servers to crash (e.g., Denial of Service (DoS) assaults)

2.2. Contrast Between Ethical and Malicious Hackers

Ethical programmers utilize their insight to get and work on the innovation of associations. They offer a fundamental support to these associations by searching for weaknesses that can prompt a security break.

An ethical programmer reports the distinguished weaknesses to the association. Furthermore, they give remediation exhortation. By and large, with the association's assent, the ethical programmer plays out a re-test to guarantee the weaknesses are completely settled. the attacker gets control and hold on the personal and private information and data which is stored within the person's smartphone illegally [16].

Malevolent hackers use software package programs like Trojans, associated spyware to realize entry into an organization's network for thievery info.[6] Vindictive programmers plan to acquire unapproved admittance to an asset (the more delicate the better) for monetary benefit or individual acknowledgment. Attackers have been utilizing the internet to get access to users' computers and carry out destructive operations such as data theft [13]. A few malignant programmers ruin sites or crash backend servers for the sake of entertainment, notoriety harm, or to cause monetary misfortune. The techniques utilized and weaknesses found stay unreported. They aren't worried about further developing the associations security pose.

3. Phases of Ethical Hacking

There are principally 5 stages in hacking. Not really a programmer needs to follow these 5 stages in a successive way. It's a stepwise cycle and when followed yields an improved outcome.

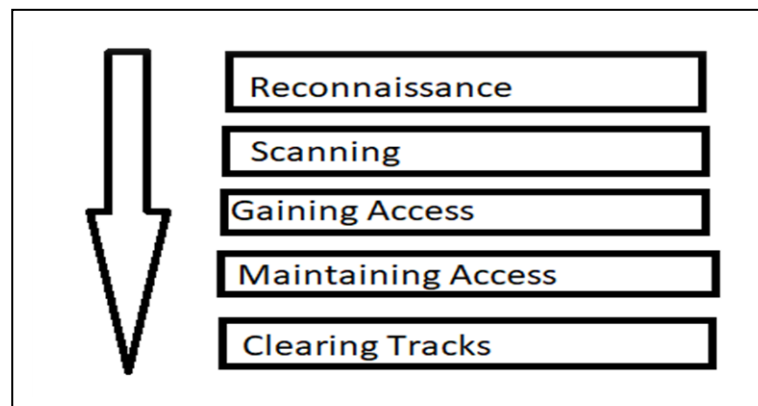


Figure 2. Phases of Ethical Hacking.

3.1. Reconnaissance

This is the initial step of Hacking. It is likewise called as Footprinting and data gathering Phase. Here we gather however much data as could be expected about the objective. Reconnaissance refers to gathering information about the target for the ex-Domain name, IP, Target personal information, Email, Subdomains, Job information, etc. Reconnaissance is also known as Foot-Printing.[12] We normally gather data around three gatherings: Network, Host and Individuals included.

It refers to gather as more information as we can about target in prior to perform an attack. It can be further classified into Active and Passive [8]:

- **Active:** Directly connecting with the objective to accumulate data about the objective. E.g., Using Nmap apparatus to filter the objective.
- **Passive:** Trying to gather the data about the objective without straightforwardly getting to the objective. This includes

gathering data from web-based entertainment, public sites and so on.

3.2. Scanning

Three kinds of checking are involved:

- **Port scanning:** This stage includes checking the objective for the data like open ports, Live frameworks, different administrations running on the host.
- **Vulnerability Scanning:** Checking the objective for shortcomings or weaknesses which can be taken advantage of. Normally finished with assistance of mechanized devices
- **Network Mapping:** Finding the geography of organization, switches, firewalls servers if any, and have data and drawing an organization chart with the accessible data. This guide might act as a significant snippet of data all through the hacking system.

3.3. Gaining Access

This stage is where an aggressor breaks into the framework/network utilizing different instruments or techniques. In the wake of going into a framework, he needs to build his honor to oversee level so he can introduce an application he really wants or change information or conceal information.

3.4. Maintaining Access

Hacker may simply hack the framework to show it was powerless or he can be devilish to the point that he needs to keep up with or persevere the association behind the scenes without the information on the client. This should be possible utilizing Trojans, Rootkits or other malevolent documents. The point is to keep up with the admittance to the objective until he completes the responsibilities he wanted to achieve there.

3.5. Clearing Track

No hoodlum needs to get found out. A canny hacker generally clears all proof so in the later mark of time, nobody will find any follows prompting him. This includes changing/debasing/erasing the upsides of Logs, adjusting vault values and uninstalling all applications he utilized and erasing all organizers he made.

4. Footprinting Methodology

Different strategies used to gather data about the objective association are :

- **Footprinting through Search Engines**

This is a passive data gathering process where we accumulate data about the objective from virtual entertainment, web search tools, different sites and so on. Data assembled incorporates name, individual subtleties, topographical area details, login pages, intranet entryways and so forth. Indeed, even some objective explicit data like Operating framework subtleties, IP subtleties, Netblock data, advancements behind web application and so on can be accumulated via looking through web crawlers. E.g.: gathering data from Google, Bingo and so on

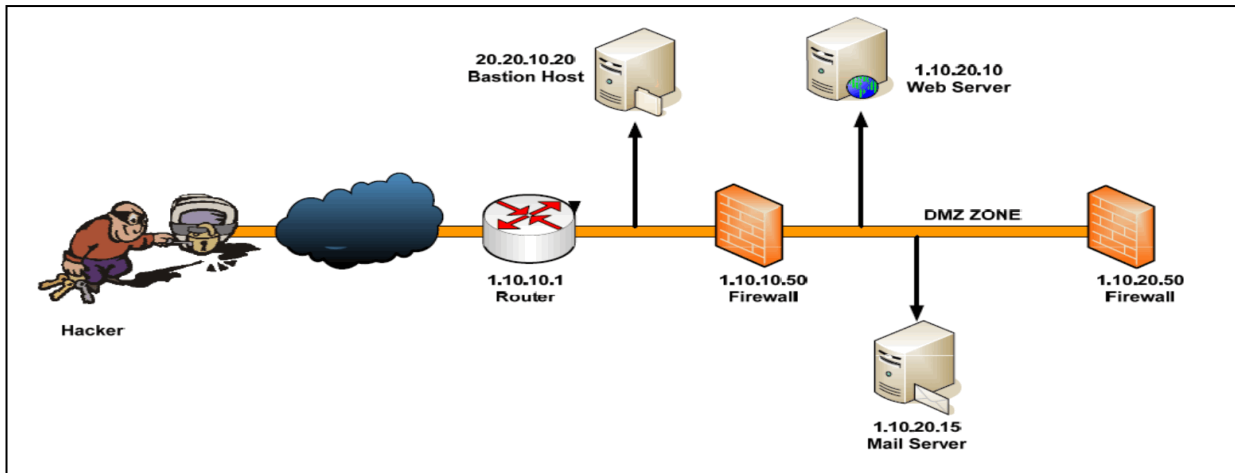


Figure 3. Footprinting in Ethical Hacking

- **Google Hacking**

Google hacking alludes to gathering data utilizing google doofuses (watchwords) by building search questions which bring about finding delicate information. Details gathered incorporate compromised passwords, default certifications, contender data, data connected with a specific point and so on.

E.g.: inurl, site, allintitle and so forth

- **Examining HTML Source and Examining Cookies**

Html source codes of a web application might provide us with a comprehension of the application usefulness, stowed away fields, remarks, variable names and so on. Treats are utilized to recognize a client in his meeting. these treats might be put away in the program or passed in the URL, or in the HTTP header.

The whole site can be reflected utilizing devices like HTTracker to accumulate data at our own stage.

Separate site Archives: more established forms of site can be gotten which might uncover some data connected with the objective.

E.g.: www.archive.org

- **Email Footprinting**

email header uncovers data about the mail server, unique source's email id, inner IP tending to conspire, as well as the conceivable design of the objective organization.

- **Competitive Intelligence**

Competitive intelligence gathering is the method involved with social occasion data about the contenders from assets like the Internet.

E.g.: organization site, web index, web, online data sets, public statements, yearly reports, exchange diaries

- **Google Hacking/Google Dorks**

This is a course of making search questions to remove stowed away data by utilizing Google administrators to look through unambiguous strings of text inside the query items. Some google administrators, site, allinurl, inurl, allintitle .

- **Whois Footprinting**

Whois information is maintained by the district's online registration centers and contains personal details of the domain owner.[9] Whois data sets and the servers are worked by RIR - Regional Internet Registries. These data sets contain the individual data of Domain Owners. Whois is a Query reaction convention utilized for questioning Whois data sets and its convention is reported in RFC 3912. Whois utility grills the Internet space name organization framework and returns the

area proprietorship, address, area, telephone numbers, and different insights concerning a predetermined space name.

- **Footprinting through Social Engineering**

Virtual entertainment like twitter, Facebook are looked to gather data like individual subtleties, client qualifications, other delicate data utilizing different social designing procedures. A portion of the strategies incorporate.

- **Eavesdropping**

It is the process of intercepting unauthorized communication to gather information.

- **Shoulder surfing**

Subtly noticing the objective to accumulate delicate data like passwords, individual distinguishing proof data, account data and so on.

- **Dumpster Diving**

This is a course of gathering touchy data by investigating the garbage can. A considerable lot of the records are not destroyed prior to arranging them into the garbage can. Recovering these archives from garbage may uncover touchy data in regards to contact data, monetary data, delicate data and so forth.

5. Nmap

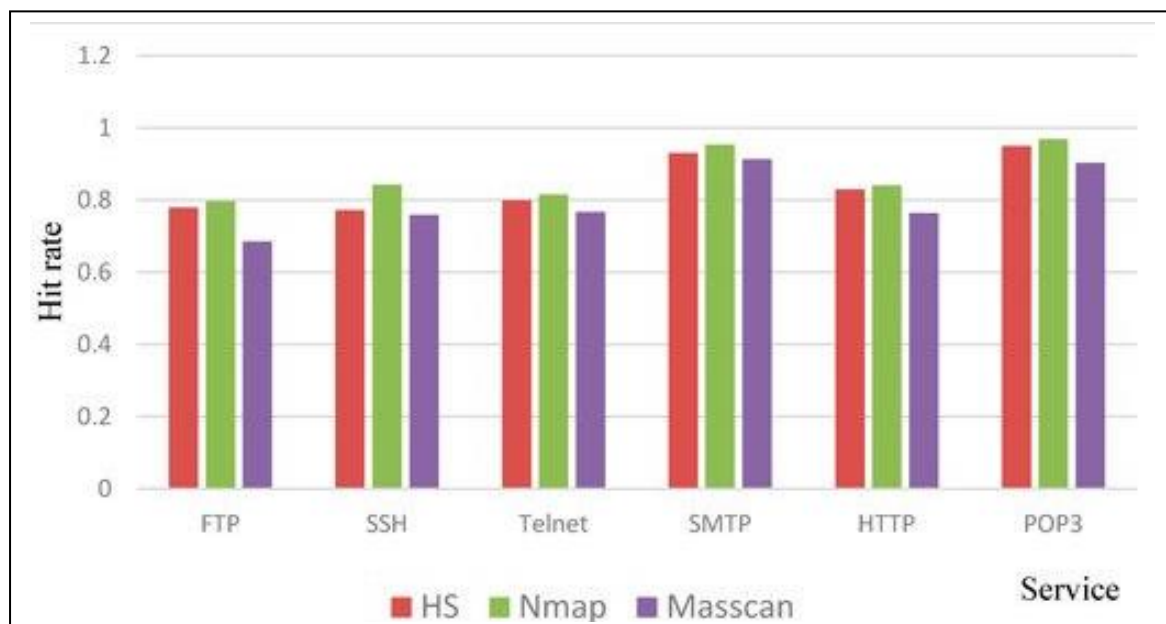


Figure 4. The comparison of Hit rates of different port scanning tools.

Nmap, short for Network Mapper, is a free and open-source instrument utilized for weakness checking, port filtering and, obviously, network planning. Regardless of being made back in 1997, Nmap stays the highest quality level against which any remaining comparative apparatuses, either business or open source, are judged.

Nmap has kept up with its superiority in view of the huge local area of designers and coders who help to keep up with and update it. The Nmap people group reports that the device, which anybody can get free of charge, is downloaded a few thousand times consistently.

In view of its adaptable, open-source code base, working inside most redone or vigorously specific environments can be changed. There are conveyances of Nmap well defined for Windows, Mac and Linux conditions, however Nmap additionally

upholds less famous or more seasoned working frameworks like Solaris, AIX or AmigaOS. The source code is accessible in C, C++, Perl and Python.

Network Mapper, also called "Nmap," is a strong open-source program, ideal for directing surveillance and count. Indeed, Nmap is notable for this reason, and it's remembered for each Whitehat-to-Blackhat's tool kit for that very reason; notwithstanding, I need to bring up that it has numerous different purposes too. For example, an organization head might depend on Nmap to review or confirm frameworks that are right now running on the organization. This makes it a reasonable choice for consistence checking.

In spite of the fact that there are a lot of pragmatic purposes to examine, this post sets its emphasis basically on observation and count. This would be the second and third period of the Certified Ethical Hacker's approach.

5.1. Mechanism

Nmap works by conveying crude IP bundles to an organization or a solitary host. This permits Nmap to distinguish which hosts are presently up and which hosts are as of now down. Furthermore, contingent upon the kind of output being utilized, certain frameworks answer these sweeps in novel ways, in this way distinguishing what these frameworks are.

For instance, Nmap's information base incorporates examines that will recognize an objective framework's working framework (and rendition), administrations (name and variant), and even parcel channels or firewalls. It's challenging to make reference to its superb qualities, yet the primary concern is all that Nmap is strong. It has won various honors, it's very much upheld, and it's additionally proven and factual. Best of all... it's free.

The core of Nmap is port checking. How it functions is that clients assign a rundown of focuses on an organization that they need to learn data about. Clients don't have to distinguish explicit targets, which is great on the grounds that most overseers don't have a total image of all that is utilizing the possibly large number of ports on their organization. All things being equal, they gather a scope of ports to filter. It's likewise conceivable to examine all organization ports, albeit that would possibly require some investment and eat up a considerable amount of accessible data transfer capacity. Furthermore, contingent upon the kind of passive safeguards that are being used on the organization, such an enormous port sweep would probably set off security cautions.

In that capacity, a great many people use Nmap in additional restricted arrangements or split various pieces of their organization for planned to look over time.

As well as setting up a reach focuses to be filtered, clients can likewise control the profundity of each output. For instance, a light or restricted output could return data about which ports are open and which have been shut by firewall settings.

More point-by-point outputs could also catch data about what sort of gadgets are utilizing those ports, the working frameworks they are running and, surprisingly, the administrations that are active on them. Nmap can likewise find further data, similar to the adaptation of those found administrations.

That makes it an ideal device for tracking down weaknesses or helping with fix the board endeavors. Controlling the outputs used to require console orders, which obviously implies that some preparation was required. Yet, the new Zen map graphical point of interaction makes it simple for basically everybody to let Nmap know what they believe it should find, regardless of formal preparation.

In the meantime, experts can keep on utilizing the control center orders they generally have, making it a helpful device for the two specialists and fledglings the same.

5.2. Is Nmap a Security Risk?

While one could suggest the viewpoint that Nmap is an ideal hacking device, a large number of the more deeply examine

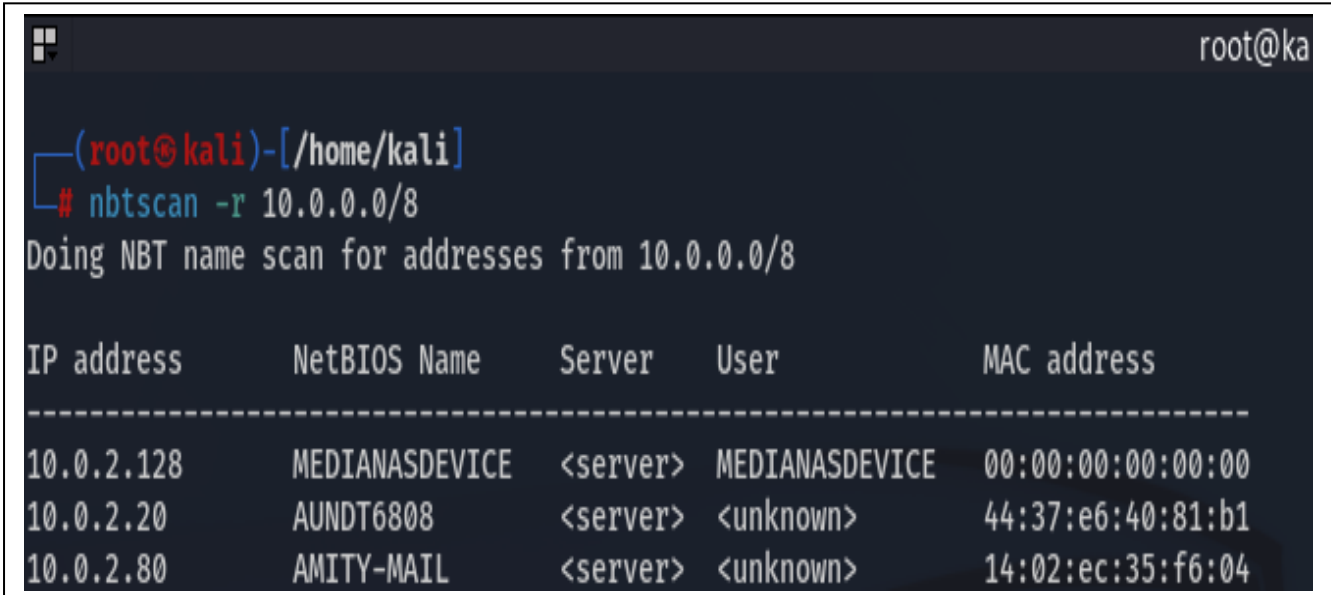
exercises require root access and honors. Somebody from outside can't simply point Nmap at an objective organization they don't have consent to get to and have it mysteriously uncovered weaknesses for them to take advantage of. That, however the endeavor would probably set off a basic security alert by any protective or network checking devices.

This isn't to imply that that Nmap couldn't be risky in some unacceptable hands, particularly on the off chance that conveyed by a turncoat framework director or somebody utilizing taken certifications. This was exhibited in the 2016 Oliver Stone film Snowden (another film that highlighted Nmap) about the blamed backstabber Edward Snowden.

6. Result and Discussion

For this show, we utilize the 10.0.0.0/8 organization. It is protected, legitimate, and quick. The unapproved examining of frameworks we don't possess verges the legalities forced under the United States Code, Title 18, Chapter 47, Sections 1029 and 1030 (Crimes and Criminal Procedure). It's an ill-defined situation with respect to port checking, however there are people who have had charges brought against them for not looking for composed consent from their objective in advance.

We used `nbtscan -r 10.0.0.0/8` command to discover live hosts in the network.



```

root@ka
(root@kali)-[~/home/kali]
└─# nbtscan -r 10.0.0.0/8
Doing NBT name scan for addresses from 10.0.0.0/8

IP address      NetBIOS Name    Server    User          MAC address
-----
10.0.2.128     MEDIANASDEVICE  <server>  MEDIANASDEVICE  00:00:00:00:00:00
10.0.2.20      AUNDT6808       <server>  <unknown>      44:37:e6:40:81:b1
10.0.2.80      AMITY-MAIL      <server>  <unknown>      14:02:ec:35:f6:04

```

Figure 5. list of live hosts in the network.

We checked the whole 10.0.0.0 territory hosts to distinguish open ports, administrations and the working framework executing on them. We checked 10.0.2.128 to distinguish open ports, executing administrations and working framework on it. In this, all ports examined with various port numbers like 49152 and 22.

```

root@kali: /home/kali 169x38
root@kali)~[/home/kali]
# nmap -Pn -sV -O -p1-65535 10.0.2.128
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-12 21:56 IST
Nmap scan report for 10.0.2.128
Host is up (0.059s latency).
Not shown: 65512 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.0 (protocol 2.0)
80/tcp    open  http         Apache httpd
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp   open  ssl/https
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
548/tcp   open  afp          Netatalk 3.1.9.q1 (name: MEDIANASDEVICE; protocol 3.4)
2000/tcp  open  tcpwrapped
2049/tcp  open  nfs          2-3 (RPC #100003)
5000/tcp  open  http         Apache httpd
5001/tcp  open  http         Apache httpd
5060/tcp  open  tcpwrapped
6600/tcp  open  ganglia      Ganglia XML Grid monitor
6621/tcp  open  kftp?
6623/tcp  open  ktelnet?
8008/tcp  open  http
8080/tcp  open  http-proxy
8081/tcp  open  http         Apache httpd
30000/tcp open  mountd       1-3 (RPC #100005)
30001/tcp open  status       1 (RPC #100024)
30002/tcp open  rquotad     1-2 (RPC #100011)
42205/tcp open  nlockmgr    1-4 (RPC #100021)
49152/tcp open  upnp        Portable SDK for UPnP devices 1.6.22 (Linux 5.10.60-qnap; UPnP 1.0)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS: SCAN(V=7.92%E=4%D=9/12%OT=22%CT=1%CU=39185%PV=Y%D5=5%DC=I%G=Y%TM=631F5E9
OS: 1%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10A%TI=Z%II=I%TS=A)SEQ(SP=1
OS: 06%GCD=1%ISR=10A%TI=Z%TS=A)OPS(O1=M43EST11NW9%O2=M43EST11NW9%O3=M43ENNT1
OS: 1NW9%O4=M43EST11NW9%O5=M43EST11NW9%O6=M43EST11)WIN(W1=FFFF%W2=FFFF%W3=FF
OS: FF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M43ENNSNW9%CC=Y%Q=
OS: )T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y
OS: %T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=16
OS: 4%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 5 hops
Service Info: Host: MEDIANASDEVICE; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel:5.10.60-qnap
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 197.06 seconds

```

Figure 6. Scanning of 10.0.2.128.

Next, we filtered 10.0.2.20 to recognize open ports, executing administrations and working framework and found other various ports open on various administrations with establishing windows adaptation.

```

root@kali: /home/kali 169x38
root@kali)~# nmap -Pn -sV -O -p1-65535 10.0.2.20
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-12 22:03 IST
Nmap scan report for 10.0.2.20
Host is up (0.040s latency).
Not shown: 65516 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
2000/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server   Microsoft Terminal Services
5040/tcp  open  unknown
5060/tcp  open  tcpwrapped
5280/tcp  open  flexlm          FlexLM license manager
5357/tcp  open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8008/tcp  open  http
49664/tcp open  msrpc          Microsoft Windows RPC
49665/tcp open  msrpc          Microsoft Windows RPC
49666/tcp open  msrpc          Microsoft Windows RPC
49667/tcp open  msrpc          Microsoft Windows RPC
49668/tcp open  msrpc          Microsoft Windows RPC
49674/tcp open  msrpc          Microsoft Windows RPC
49675/tcp open  msrpc          Microsoft Windows RPC
49677/tcp open  msrpc          Microsoft Windows RPC
49697/tcp open  flexlm          FlexLM license manager
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=9/12%OT=135%CT=1%CU=37524%PV=Y%DS=5%DC=I%G=Y%TM=631F65
OS:99%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10D%TI=RD%TS=U)OPS(O1=M43E
OS:NW8NNS%O2=M43ENW8NNS%O3=M43ENW8%O4=M43ENW8NNS%O5=M43ENW8NNS%O6=M43ENNS)W
OS:IN(W1=FFF%W2=FFF%W3=FFF%W4=FFF%W5=FFF%W6=FF70)ECN(R=Y%DF=Y%T=80%W=F
OS:FFF%O=M43ENW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T
OS:3(R=N)T4(R=N)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N
OS:U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=N)

Network Distance: 5 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

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 1613.51 seconds
zsh: segmentation fault nmap -Pn -sV -O -p1-65535 10.0.2.20

```

Figure 7. Scanning of 10.0.2.20

Then, at that point, we filtered 10.0.2.80 to recognize open ports, executing administrations and working framework on it. In this, all kinds of ports 21, 80, 8443 and different ports viewed as opened with various administrations.

```

root@kali: /home/kali 169x38
root@kali) ~ [~/home/kali]
root@kali) nmap -Pn -sV -O -p1-65535 10.0.2.80
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-12 22:31 IST
Nmap scan report for 10.0.2.80
Host is up (0.024s latency).
Not shown: 65496 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              FileZilla ftpd 0.9.41 beta
26/tcp    open  smtp
80/tcp    open  http             Microsoft IIS httpd 8.5
110/tcp   open  pop3
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
143/tcp   open  imap
366/tcp   open  smtp
443/tcp   open  ssl/http         Microsoft IIS httpd 8.5
445/tcp   open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
465/tcp   open  ssl/smtp
587/tcp   open  smtp
993/tcp   open  ssl/imap
995/tcp   open  ssl/pop3
1000/tcp  open  cadlock?
1801/tcp  open  msmq?
2000/tcp  open  tcpwrapped
2103/tcp  open  msrpc            Microsoft Windows RPC
2105/tcp  open  msrpc            Microsoft Windows RPC
2107/tcp  open  msrpc            Microsoft Windows RPC
3389/tcp  open  ssl/ns-wbt-server?
5000/tcp  open  tcpwrapped
5222/tcp  open  xmpp-client?
5223/tcp  open  ssl/hpvirtgrp?
5985/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7070/tcp  open  realserver?
7443/tcp  open  ssl/oracleas-https?
8006/tcp  open  http
8081/tcp  open  blackice-icecap?
8443/tcp  open  ssl/https-alt
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=9/12%OT=21%CT=1%CU=44496%PV=Y%D5=5%DC=I%G=Y%TM=631F67E
OS:6%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10A%TI=I%TS=7)OPS(O1=M43ENW
OS:8ST11%O2=M43ENW8ST11%O3=M43ENW8NNT11%O4=M43ENW8ST11%O5=M43ENW8ST11%O6=M4
OS:3EST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%
OS:T=80%W=2000%O=M43ENW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)
OS:T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=
OS:N)T7(R=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G
OS: )IE(R=N)
Network Distance: 5 hops
Service Info: Host: webmail.amity.edu; OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft
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 503.64 seconds

```

Figure 8. Scanning of 10.0.2.80

In these scan results, we get the data we are searching for. Then the following stage will be to find the Vulnerabilities in light of the data we got from filter on the active ports and rendition of the framework.

In this work, we utilized NMAP. NMAP is an integral asset accessible in the digital protection space for data assembling or filtering of the organization. In future, we will utilize some other data gathering apparatus to enroll the help accessible on the open port of the machine of the objective organization. In future, we will likewise close the open port to improve the net-

work safety. There is likewise an open degree to do disavowal of administration assaults with the assistance of open ports.

7. Battle Against Footprinting

Guarding our organization against assault requires consistent cautiousness and training. The purpose of testing is quality assurance, verification, and validation or dependableness estimation.[17] Data Security is the protection of these data and privacy, which prevent hackers from unauthorized access to computers, applications, and data servers.[14] In spite of the fact that there is no recipe for ensuring the outright security of your organization, the accompanying ten practices address the best protection for your organization.

Stay up with the latest by introducing week after week or everyday if conceivable. Support flood and honor heightening assaults can ordinarily be forestalled by staying up with the latest. Check your seller's site every day for new fix deliveries and screen the Computer Emergency Response Team's site, <http://www.cert.org>, for data on the most recent weaknesses.

Close down pointless administrations/ports. Audit your establishment necessities by wiping out superfluous administrations and applications.

Change default passwords by picking solid passwords that use capitalized/lowercase/numbers/unique characters. Some data set applications make a data set head account with no secret phrase. To safeguard against this weakness, test the records after introducing, and in the event that no secret phrase is tracked down regardless, impair the record or set areas of strength for a. Powerless passwords are not far superior to no secret key by any means. Instances of feeble passwords incorporate the client's name, birth date, or a word reference word.

Teach your overseers and clients about the significance of solid passwords. A solid secret key ought to contain upper- and lower-case letters, as well as numbers and exceptional characters (! #, \$, and so forth). A solid secret phrase ought to likewise be no less than 7-8 characters long, contingent upon working framework. Many working frameworks give means to requiring complex passwords, when empowered. More outrageous countermeasures incorporate one-time secret key components.

Control actual admittance to frameworks. Safeguarding actual admittance to PC frameworks is all around as significant as safeguarding PC access. Be certain workers secure control center when not being used — an opened work area screen can in a split-second permit a hacker admittance to the organization as a favored client. A hacker may likewise get to the organization through an organization jack in a gathering room or any non-limited region. Alerts, camcorders, raised floors, safety officers, client available enclosures, biometric sweeps, and ID cards might be important to enough protect against network assaults. Reduce surprising info. Some Web pages permit clients to enter usernames and passwords. These Web pages can be utilized malevolently by permitting the client to enter in something other than a username. Username: jdoe; rm - rf/This could permit an assailant to eliminate the root record framework from a UNIX Server. Software engineers ought to restrict input characters, and not acknowledge invalid characters, for example, |; < > as conceivable info.

Perform reinforcements and test them consistently. Teach workers about the dangers of social designing and foster methodologies to approve characters via telephone, through email, or face to face. Scramble and secret phrase safeguard delicate information. Information, for example, Web open email ought to be viewed as delicate information and ought to be scrambled. This will deter any kind of sniffer program or openness of touchy organization information.

Carry out security equipment and programming. Firewalls and interruption recognition frameworks ought to be introduced at all borders of the organization. Infections, Java, and ActiveX might possibly hurt a framework. Against infection programming and content sifting ought to be used to limit this danger. Foster a composed security strategy for the organization.

These strategies will assist with diminishing assaults of footprinting, which lead to your PC or your organization being hacked. So, an organization needs to remain vigil consistently because of new techniques for interruption being grown practically every day.



8. Conclusion

This Paper is to express the idea of how Footprinting is done using the ethical hacking tool Nmap. Here we have taken the example of the Cloudflare server ip address 10.0.0.0 to show the process. The data we get in the process is about the system, its open ports and which port is closed, the time of opening, system version, firewall etc. This data can be used in the next step of the penetration testing which is intrusion. Nmap is popular among pen testers for its simplicity and ability to bypass the firewall which is not present in normal pinging tools. The data expressed above can be utilized comprehend the idea of what Footprinting is, what hackers search for to Footprint, and how to shield against it. I, myself, took in an extraordinary arrangement over the subject while doing the exploration. I feel we should protect against Footprinting for the guard of our organization. The Footprinting instrument assists with keeping away from post delicate and confidential data via web-based entertainment. The apparatus recognizes and stays away from undesirable companion demands and stops obscure solicitations. Footprinting likewise cautions about sort of weaknesses. The assistance in setting legitimate setups and furthermore evades break of target framework designs and document sharing data. There are numerous Footprinting devices and methods for social occasion an objective framework's information. No product is made with zero weakness. So, it is smarter to comprehend how a framework's data is accumulated prior to hacking the objective framework. Along these lines, different measures can be created to forestall framework assaults. Before long extreme changes should be visible in the improvement of Footprinting devices. If a client can figure out the various procedures of Footprinting and furthermore follow counter-measures of Footprinting then the client will actually want to shield the individual information from getting hacked. A client should refresh the framework security consistently. By working on the framework's security, assaults on the framework can be forestalled. The more data the hacker can assemble, the higher are their possibilities of an effective assault. Assuming we increment our security right from the underlying stage, it will lessen the opportunities for an aggressor to get into our framework. By controlling our advanced impression, we can expand your security stance and protect our information from hackers.

Acknowledgements

To start with, I wish to communicate my most earnest and significant appreciation to Dr. Pawan Singh, Dr. Deepak Arora, Wg. Cdr. (Dr.) Anil Kumar, Computer Science and Engineering department, ASET, Amity University Lucknow Campus, for allowing me motivation and offering a chance to feature my capacities. I'm additionally thankful to them for participation in giving every one of the necessary assets. I stretch out unique on account of my loved ones for their consistent help. I thankfully recognize the help of my supervisor Prof. Dr. Pawan Singh. I wouldn't envision finishing this work without all his promotion indecencies. I recognize the time he spent in our week after week gatherings, even with his bustling timetable and different responsibilities. I'm profoundly obliged to him for his understanding. He aided all parts of this work from talking about groundbreaking plans to composing and finishing this undertaking. I might want to say thanks to Amity University, Lucknow Campus for giving me a brilliant stage to this work.

References

- [1]. N. Antunes and M. Vieira, "Enhancing penetration testing with attack signatures and interface monitoring for the detection of injection vulnerabilities in web services," in IEEE International Conference on Services Computing, pp. 104-111, July 2011.
- [2]. P. S. Shinde and S. B. Ardhapurkar, "Cyber security analysis using vulnerability assessment and penetration testing," in World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), pp. 1-5, March 2016.



- [3]. J. Fonseca, M. Vieira, and H. Madeira, "Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks," in 13th Pacific Rim International Symposium on Dependable Computing (PRDC), pp. 365-372, Dec. 2007.
- [4]. Y. Stefinko, A. Piskozub, and R. Banakh, "Manual and automated penetration testing. Benefits and drawbacks. Modern tendency," in 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), pp.488-491, Feb. 2016
- [5]. S. Kumar, R. Mahajan, N. Kumar, et al, "A study on web application security and detecting security vulnerabilities," in 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) pp. 451-455. Sept. 2017.
- [6]. Mukesh. M, S. Venkateshkumar, "Ethical Hacking", International Journal of Trend in Scientific Research and Development (ijtsrd), vol. 3, Iss. 6, pp. 1-2, 2019.
- [7]. V. Chandrika, "Ethical Hacking: Types of Ethical Hackers", International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), vol. 11, Iss. 1, pp. 44-45, 2014.
- [8]. M. Pangaria, V. Shrivastava, "Need of Ethical Hacking in Online World", International Journal of Science and Research (IJSR), vol. 2, Iss. 4, pp. 530-531, 2013.
- [9]. R. Jaiswal, A. Sharma, "Ethical Hacking", Journal of Xi'an University of Architecture & Technology, vol. 12, Iss. 6, pp. 853-854, 2020.
- [10]. K.P. Kumar, K. Pranathi," A Survey on Ethical Hacking, Approaches, Attacks, Procedure & Reliability in case of Cyber Crime", Journal of Composition Theory, vol. 14, Iss. 6, pp. 100-110, 2021.
- [11]. U. Singh and P. Singh, "Managing Cyber Security", J. Manage. Serv. Sci., vol. 2, no. 1, pp. 1–10, 2022. DOI: <https://doi.org/10.54060/JMSS/002.01.002>.
- [12]. S. Kumar Tomar and P. Singh, "Cyber Security Methodologies and Attack Management", J. Manage. Serv. Sci., vol. 1, no. 1, pp. 1–8, 2021. DOI: <https://doi.org/10.54060/JMSS/001.01.002>
- [13]. A. Srivastava and P. Singh, "Security Issues in Cloud Computing", J. Manage. Serv. Sci., vol. 2, no. 1, pp. 1–11, 2022. DOI: <https://doi.org/10.54060/JMSS/002.01.003>.
- [14]. F. Abbasi and P. Singh, "Cryptography: Security and Integrity of Data Management", J. Manage. Serv. Sci., vol. 1, no. 2, pp. 1–9, 2021. DOI: <https://doi.org/10.54060/JMSS/001.02.004>.
- [15]. S. Yadav and P. Singh, "Web Application and Penetration Testing", J. Infor. Electr. Electron. Eng., vol. 1, no. 2, pp. 1–11, 2020. DOI: <https://doi.org/10.54060/JIEEE/001.02.003>.
- [16]. M. Singh Saini and S. Rizvi, "Vulnerabilities in Android OS and Security of Android Devices", J. Infor. Electr. Electron. Eng., vol. 3, no. 1, pp. 1–11, 2022. DOI: <https://doi.org/10.54060/JIEEE/003.01.004>.
- [17]. N. Srivastava, U. Kumar, and P. Singh, "Software and Performance Testing Tools", J. Infor. Electr. Electron. Eng., vol. 2, no. 1, pp. 1–12, 2021. DOI: <https://doi.org/10.54060/JIEEE/002.01.001>.
- [18]. H. Khan and P. Singh, "Issues and Challenges of Internet of Things: A Survey", J. Infor. Electr. Electron. Eng., vol. 2, no. 3, pp. 1–8, 2021. DOI: <https://doi.org/10.54060/JIEEE/002.03.002>.