

# **A Thesis/Project/Dissertation Report**

on

## **Detection and Analysis of Web Application Threats through Monitoring Tool**

*Submitted in partial fulfilment of the  
requirement for the award of the degree of*

**B.Tech CSE**



(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

**Under The Supervision of**

**Name of Supervisor: Ms. Lalita Verma**

**Assistant professor**

**Submitted By**

**Name of Student/s**

**Sagar Agrawal-(19SCSE1010656)**

**Shikhar Mittal-(19SCSE1010695)**

**SCHOOL OF COMPUTING SCIENCE AND ENGINEERING DEPARTMENT OF  
COMPUTER SCIENCE AND ENGINEERING**

**GALGOTIAS UNIVERSITY, GREATER NOIDA**

**INDIA**



**SCHOOL OF COMPUTING SCIENCE AND  
ENGINEERING  
GALGOTIAS UNIVERSITY, GREATER  
NOIDA**

**CANDIDATE'S DECLARATION**

I/We hereby certify that the work which is being presented in the thesis/project/dissertation, entitled “**Threats through Monitoring Tool**” in partial fulfilment of the requirements for the award of the School of Computer Science and Engineering submitted in the School of Computing Science and Engineering of Galgotias University, Greater Noida, is an original work carried out during the period of month, Year to Month and Year, under the supervision of Name- **Ms. Lalita Verma** Designation, Department of Computer Science and Engineering/Computer Application and Information and Science, of School of Computing Science and Engineering , Galgotias University, Greater Noida

The matter presented in the thesis/project/dissertation has not been submitted by me/us for the award of any other degree of this or any other places.

Sagar Agrawal(19SCSE1010656)

Shikhar Mittal-(19SCSE1010695)

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

Supervisor Name

Ms. Lalita Verma

Assistant professor

**CERTIFICATE**

The Final Thesis/Project/ Dissertation Viva-Voce examination of Sagar Agrawal : 19SCSE1010656,  
Shikhar Mittal: 19SCSE1010695 has been held on \_\_\_\_\_ and his work is recommended  
for the award of B-tech.

**Signature of Examiner(s)**

**Signature of Supervisor(s)**

**Signature of Project Coordinator**

**Signature of Dean**

Date:

## **ACKNOWLEDGEMENT**

---

I would like to express my gratitude to my premier supervisor Lalita Verma ,who guided me through out this project I would also like to thanks my friends who supported me and offered deep insight into the study.

I am grateful to Dr Munish Sabharwal, Dean Academics, for his unfailing encouragement and suggestions, given to me in the course of my project work.

I would also like to thank Dr.S.P.S Chauhan, Professor and Head, Department of Computer Science and Engineering, for her constant support.

I express my gratitude to Lalita Verma, Assistant Professor, my project guide, for constantly monitoring the development of the project and setting up precise deadlines. Her valuable suggestions were the motivating factors in completing the work.

Finally a note of thanks to the teaching and non-teaching staff of Dept of Computer Science and Engineering, for their cooperation extended to me, and my friends, who helped me directly or indirectly in the course of the project work.

## INDEX

---

Sections	TITLE	PAGE NO.
o	Abstract	7
1	Introduction	7
2	Literature review	8
3	<b>CYBER CRIMES</b>	10
4	Cyber security	12
5	<b>ATTACK PHASES</b>	13
	- 5.1- Reconnaissance Phase	13
	- 5.2 - Infiltration Phase	16
	- 5.3 – Conclusion phase	17
6	<b>TRENDS CHANGING CYBER SECURITY</b>	17
	- 6.1 – Web servers	17
	- 6.2 – Mobile networks	18
	- 6.3 – Cloud computing	18
	- 6.4 – Encryption of the code	19
	- 6.5- IPv6 New internet protocol	20
7	Role of social media in cyber security and applications	20

---

8	CYBER SECURITY TECHNIQUES	21
	- 8.1 – Access control and password security in devices	21
	- 8.2 – Authentication data	22
	- 8.3 – Firewalls	22
	- 8.4 – Antivirus software	22
	6.5- Honeypots	22
<hr/>		
8	Results of the project	23
9	Conclusion	27
<hr/>		
o	References	20
<hr/>		

## **ABSTRACT**

Network protection plays out a urgent capacity inside side the subject of realities innovation .Securing the realities have end up one in every one of the biggest requesting circumstances inside side the blessing day. At whatever point we consider the digital assurance the essential issue that includes our musings is 'digital wrongdoings' which may be developing hugely day through day. Different Governments and gatherings are taking numerous actions so one can save you those digital violations. Other than different measures digital security stays a totally huge circumstance to many. This paper explicitly has some expertise in requesting circumstances went up against through digital assurance at the cutting edge innovations .It also works in current roughly the digital insurance strategies, morals and the improvements changing over the substance of digital security.

## **1. Introduction**

Network protection or digital danger is a malignant conduct pointed toward annihilating information, taking information, or disturbing the overall computerized life. Digital dangers incorporate PC infections, information spills, disavowal of administration (DoS) assaults, and other assault counteractions. The prospects of a princely digital assault against IT resources, PC organizations, or other delicate information for unapproved access, harm, annihilation or burglary. Reliant organizations with broadcast communications organizations, incorporated frameworks, and basic foundation.

Indeed, even the last hardly any new innovations like distributed computing, portable processing, E-trade, web banking and so on conjointly wants significant degree of safety. Since these advancements hold some vital data about an individual their security has become something prerequisite. Upgrading network safety and defensive pivotal data foundations are fundamental for each country' security and financial prosperity. making the web more secure (and ensuring net clients) has gotten fundamental to the occasion of most recent administrations likewise as legislative arrangement. The battle against digital wrongdoing needs a serious and an innovative methodology. on condition that particular measures alone can't forestall any bad behavior, it's significant that prerequisite workplaces are allowed to explore and arraign computerized bad behavior satisfactorily. nowadays a couple of nations and governments are driving demanding laws on advanced securities to upset the inadequacy of some essential information. each individual should attempt to be ready on this organization security and save themselves from these expanding digital violations The segments of digital assault normally follow same example as a conventional wrongdoing. the essential period of assault is observation mission of the person in question. By attentive the customary activities of an objective

supportive data are frequently gathered identical to equipment and programming framework utilized, correspondence design and different things Hackers see and analyze networks before they assault to initiate information concerning the objective.

Malignant assaults on basic framework have become a genuine danger to business and government activities. Fast and simple admittance to the organization makes the business effective and makes delicate data more powerless against digital criminals. Programmers are capable and outfitted with different hacking apparatuses, which can without much of a stretch endeavor all the proviso. The expression "secret help" is gotten from its tactical use and is utilized to portray insight gathering undertakings. Mindfulness is the main phase of a digital assault, and they will explore this stage to decide viable counter measures. This organization knowledge record centers around port examining and working framework finger impression assaults, and gives some simple to-utilize arrangements. Inactive observation is an endeavor to get data about the objective PC and organization without effectively associating with the framework. , The assailant associates with the objective framework, ordinarily by filtering ports to check whether there are any open ports.

The periods of digital assaults by and large follow the example of customary wrongdoing. The primary period of the assault is the ID of the person in question. By filtering and analyzing the typical activity of an objective, helpful data can be assembled, for example, the equipment and programming utilized, the correspondence design, and so on They assault to get data about the set objective.

## **2. LITERATURE REVIEW**

This short evaluation suggests the effect of cyber protection within the current global. Security all through ITC global is vital each to guard legal use of statistics from attackers and to offer self belief and agree with within the ICT this is vital for its use.

On the elective side, digital hoodlums accepting this stage as a little something extra and abusing designs to hold onto tricky data. This peril of misuse might be safeguarded digital wellbeing experts in IT areas. The time span digital wellbeing arrived into ways of life in Seventies with an examinations task known as ARPANET. Subsequent to watching discernible impressions close by the local area course the utilization of a product progressed through the scientist named Bob, he started out calling it CREEPER. Later Ray Tomlinson who's the essayist of email administration, updated the indistinguishable programming with self-replication capacity. That developed first pc deception and to watch that he progressed a product known as REAPER. Today there are various methodologies progressed in digital security to monitor countrywide and worldwide digital wrongdoings. As this virtual environmental factors is just a triangle of interaction, people and time, the threat of being a sufferer is high. According to the facts accrued from big scale commercial enterprise sectors



budget has been elevating with 63% in 2018 and 67% in 2019 and small scale corporations with 50% in 2018 and 66% in 2019 competitively to hold safety. Protecting from cyber threats, figuring out threats in much less time, convalescing facts loss, stopping device from similarly hazardous are the primary capabilities of cybersecurity which might be additionally taken into consideration as most important issues in corporations and personal lives. The vital infrastructures are getting increasingly more prone to cyber assaults, which has emerged as a sport changer for corporations of their respective industries. twenty years in the past infrastructures had been now no longer prone to cyber assaults due to the fact the structure became separated as these days we see structures being integrated. The Achilles heel of those infrastructures is their business management structures (ICS) along with supervisory manage and facts acquisition (SCADA) structures and allotted management structures (DCS). ICS had been to begin with designed with proprietary era and had been cut loose different current company networks, along with nearby region networks and extensive region networks. Because of this separation of structure the structures had been now no longer uncovered to outside assaults.

Malicious cyber activities are becoming more complex and easier to execute. Individuals or groups interested in organizing cyberattacks do not need any knowledge of computer programming, as they can access online crime tools on YouTube or buy off-the-shelf crime tools. Tracking criminals or cybercriminals is not easy because there are programs that can help them complete their work without being tracked. An example of such a program is the Zeus CrimeKit, whose malicious code can be adapted, and the source code version of the banking Trojan can be found on the Internet. Zeus series prices range from \$700 to free online routes. A report published by the World Economic Forum in January 2014 examined the need for new methods to establish resilience to cyber attacks, and indicated that the lack of effective cyber defense measures may result in a cumulative impact of approximately US\$3 trillion by 2020 (Hyper-Cyber World, 2014). Information threats in cyberspace are rapidly increasing and evolving, and have recently spread to platforms such as social media and mobile technology. With technological innovation, the ever-changing technological world poses a threat to your data, and a large amount of data is exposed to vulnerabilities.

The quality of connected atmosphere is constant to evolve in Net, as a totally electronic world created by interconnected networks in just like the physical world, is characterized by an enormous amount of {information}. The necessities of data are frequently being combined, connected, compared and connected to alternative information as organizations try and make the most of its worth and to supply new and improved services to their users. the amount of data is getting down to increase drastically because the net of things is changing into a reality. The cyberspace has become inherently advanced to manage and difficult to secure. The threats of Net can still target the weakest links in any advanced internet business or any government processes, organizations and stakeholders have a job in cyber security and in protective the infrastructure and also the info that flows through it. It ought to be each stakeholder's priority to safeguard the interest of their business in protecting their customers from cybercrimes.

Cyber threats may be invisible, but the effects are real, and connected systems that are globally connected are the most vulnerable systems. As the size of the flow of information in cyberspace increases, so does the value to collaboration, government, and people around the world. plays a role in creating a footprint in cyberspace and exposes us to cyber threats. Cyberspace offers opportunities for organizations looking to make a profit in the online marketplace, but they are unaware that these opportunities are typically a market for criminal activity. Data protection is becoming more and more important. Organizations, developers, and the government have a greater responsibility to ensure the security of online platforms and back-end systems that are used to collect, manipulate, and store so much personal data.

In the present worldwide computerized world, information is the main resource for organizations. "Ensuring your organization's licensed innovation, monetary data, and notoriety is a necessary piece of business system. Nonetheless, with the increment in dangers and the complexity of assaults, this is an overwhelming test "(Loveland and Mark Lobel 2012. Endeavors should now retaliate against the pervasive cyberattacks, the danger of digital crooks or even disappointed representatives who uncover private data, bring mental ones Ownership of contenders or participating in online misrepresentation (James Kaplan, Shantnu Sharma, and Allen Weinberg 2011). Organizations must comply with various laws and regulations to operate in one or more jurisdictions. When it comes to security, cyberspace means However, the mechanical compliance approach does not mean that individuals and organizations are safe. Cybersecurity is complex and changes political issues; Cybersecurity is more than just a technology. Technical problem because it plays the security of the entire communications network legislator and legislator a role in ensuring that regulations protect and protect information at rest and in transit. They play a role in strengthening data protection values to ensure that cybersecurity policies respect data protection rights and give priority to the protection of personal data.

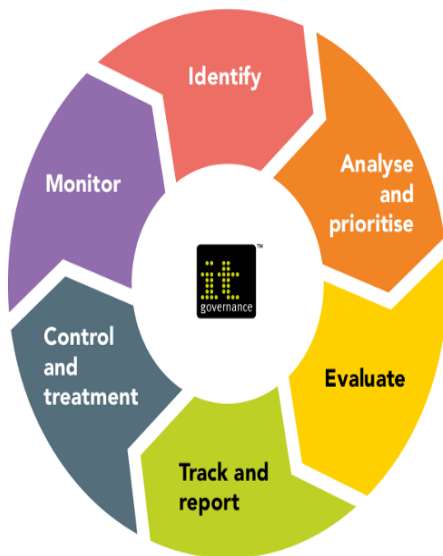
### **3. CYBER CRIMES**

The time-frame digital wrongdoing is depicted as any unlawful interest completed utilized pc or web. The definition is drawn out to local area interruption, scattering noxious records into frameworks, tormenting and burglaries comprising of equipment carport apparatus and recognizable proof robberies.

The U.S. Branch of Justice grows the meaning of digital wrongdoing to envelop any unlawful interest that utilizes a pc for the carport of evidence. Privacy and security will be the top worry of any organization or association as most sensitive information is constantly introduced in computerized structure. In organization data, yet in addition in getting to day by day correspondence through friendly sites utilizing hacking

methods like Eve Drop or social designing. Eventually, they lead to passionate cheating and cheating.

Not most effective on laptop or server threats there may behugevariety of assaultshappening on android telephones as well. As clevertelephones and IoT gadgets are related with differentpresent IoT gadgets, gaining access to any week secured tool lead to finishcommunity compromise. As the generation and net convincing humans with its handy and speedytechniques of processing a task, groups and clientshaven't anydesire to refuse the automatic environment.



Generally in not unusualplace man's language digital wrongdoing can be portrayed as wrongdoing committed the utilization of a PC and the net to metallic an individual's ID or advance stash or tail victims or disturb tasks with vindictive projects. As day by day age is betting age and medical services chiefs in chief capacity in an individual's presence the digital wrongdoings cross country, Silicon Valley Bank verified that actually will development related to the mechanical gatherings concur with digital attacks are an extreme advances. opportunity to each their records and their business.

How about we consider an illustration of the UK's most infamous digital assault, the 2017 WannaCry ransomware assault. The WannaCry episode, which started on May 12, 2017, contaminated around 200,000 frameworks in around 150 nations worldwide with a total assets of £ 6 billion. a malevolent email that is consequently downloaded and executed on the framework when the email is opened. This bolts the PC and the private information on it. The assailant then, at that point requests a payment as cryptographic money. In the UK, this influenced the National Health Service requesting £ 230 to open the PC and this brought about the scratch-off of around 19,000 medical checkups, medical procedures and patient crises.

#### **4. CYBER SECURITY**

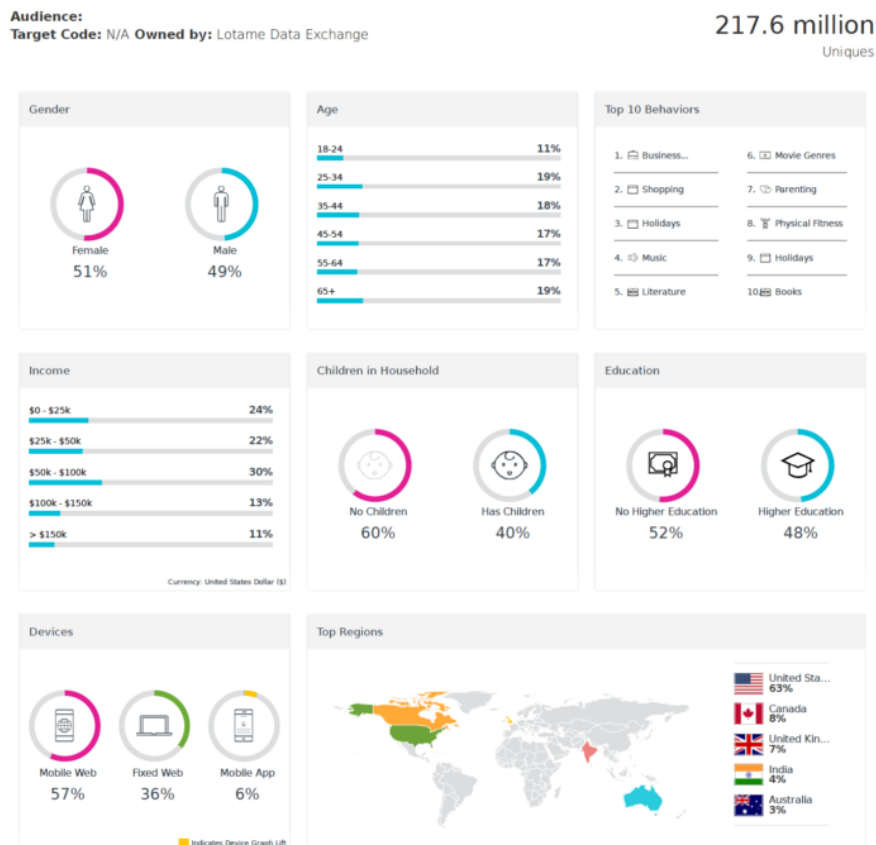
Protection and security are consistently the primary safety efforts that each organization thinks often about. We right now face a daily reality such that all data is put away carefully or on the web. Interpersonal interaction destinations give a space to clients to have a sense of security while talking with companions. with family. All things considered, cybercriminals will keep on assaulting interpersonal organizations to take their characters.

Not only on socialmedia, but also in banking, one must take all necessary security measures. Even after complyingwith security rules and guidelines,organizationsstill facecybercrime threats suchas insider threats, storage device theft,and social engineering. Cybercriminals are now targetingeconomic interests allover the world. WannaCry and NotPetya ransomware attacks are useful examples of global cyber threats. Theft ofpersonal bank accounts and Bitcoin mining techniques arenew methods that lead to widespread financial fraud.

Brilliant methodologies of getting an enterprise is through sorting out and forestalling dangers withinside the starter degree and characterizing own personal assurance guidelines for safeguarding information. This might be performed through digital subject matter experts. In every area, malware are the most extreme not unusualplace dangers noticeable in PC frameworks and organizations which fuses pc infection, worms, trojans, adware, garbage mail, ransomware and that's only the tip of the iceberg. These are intended to harm PC frameworks both intentionally or coincidentally. As malware bundles might be progressed with novel styles to pass firewalls, receiving innovation like gadget acquiring information on systems to consistent sites and garbage mail channels like interruption recognition and interruption avoidance structures are helpful for sorting out and barricading suspected documents. As protracted as the wellbeing design and activities are related with the association's business undertaking model, privacy and honesty can't be upset.

There will be new assaults on gadgets dependent on the Android working framework, however not altogether. Since tablets utilize a similar working framework as cell phones, they will before long be assaulted by the equivalent malware as these stages. Tests for Mac would keep on developing, yet much not exactly for PCs. Windows 10 will permit clients to foster applications for essentially any gadget (PC, tablets, and cell phones) running Windows 8, so it will be feasible to foster vindictive applications like Android, so these are a portion of the patterns anticipated to incorporate norms and the executives structures in of an association, the PPT system is the principal part.

This system is the construction of individuals, cycles and innovation that is additionally helpful in light of episodes. For instance, a DDOS assault on the workers will bring about the inaccessibility of the assistance The activity can be separated into the individual who carried out the wrongdoing, the method they utilized, and the hardware they utilized. With the three segments, the system is likewise called the 3 mainstays of network safety



## 5 ATTACK PHASES

There are three main attack phases

1. Reconnaissance
2. Infiltration
3. Conclusion of a cyber-attack.

### 5.1 Reconnaissance Phase

In this stage, flimsy parts in the objective framework are distinguished. Adequate assets should be utilized for this stage to

discover flimsy parts in the casualty's safeguards or to get to the casualty's capacities. Any data about the designated casualty can be basic to Critical Defense. Weaknesses Uncovered Critical data can likewise be acquired during this stage is recorded in the table underneath

**Table 1 Information gathered in reconnaissance phase [6]**

<b>Network Information</b>	<ul style="list-style-type: none"> <li>• IP addresses</li> <li>• subnet mask</li> <li>• network topology</li> <li>• domain names</li> </ul>
<b>Host Information</b>	<ul style="list-style-type: none"> <li>• user names</li> <li>• group names</li> <li>• architecture type (e.g. x86 v/s SPARC)</li> <li>• operating system family and version</li> <li>• TCP and UDP services running with versions</li> </ul>
<b>Human Information</b>	<ul style="list-style-type: none"> <li>• home address</li> <li>• home telephone number</li> <li>• frequent hangouts</li> <li>• computer knowledge</li> <li>• dark secrets</li> </ul>
<b>Security Policies</b>	<ul style="list-style-type: none"> <li>• password complexity requirements</li> <li>• password change frequency</li> <li>• expired/disabled account retention</li> <li>• physical security (e.g. locks, ID badges, etc.)</li> <li>• firewalls</li> <li>• intrusion detection systems</li> </ul>

In the surveillance stage, assailants behave like criminal investigators, collecting records to in actuality perceive their objective. The component is everything! From investigating electronic mail records to open inventory records, they will probably understand the local area higher than the people who run and safeguard it. They focus on the security thing of the innovation, inspect the shortcomings, and utilize any weakness for their potential benefit.

Reconnaissance can be divided into two phases:

1. Passive reconnaissance.
2. Active reconnaissance.

## **Passive reconnaissance**

In this fragment a pentester endeavors to gather information roughly the objective, by means of freely to be had reassets, one such stock is Open-supply insight moreover perceive as (OSINT). There are a wide range of reassets like Shodan which can be exceptionally powerful hardware according to inactive observation.

## **Active reconnaissance**

In this cycle, you'll on the double draw in with the PC contraption to profit records. This records might be pertinent and precise. In any case, there's a danger of having identified on the off chance that you are making arrangements exuberant surveillance with out authorization. On the off chance that you're distinguished, the contraption administrator can take exceptional movement towards you and way your next exercises.

### **Port Scanning-**

Port Scanning could be a reliably examining PC ports as entire information goes in and out is through port and port checking distinguishes open ports to a PC. Through port checking transgressor derive that administrations are apparent and any place assault is conceivable. Fundamental head of port checking is that to recover information from the opened port and examine it. There are numerous techniques to perform port checking. each procedure has its experts and cons. A few techniques are convention Null, TCP SYN, TCP Xmas, TCP FIN and UDP port output. There are a few techniques for findion and impedance of port sweep assault. Any assistance or fringe that recognize filter parcel and drop it's anything but, a viable approach for obstructing examine. nonetheless normally we find that totally various outputs have their particular mark. A NULL, Christmas Day, or FIN sweep would be identified and impeded by a stateful gadget. As a matter of course grunt is placed in with stateful IDS dynamic that' why grunt will recognize FIN, NULL, and XMAS checks. convention SYN and UDP examines appear to be real association makes an endeavor to the objective however their lone unmistakable trademark is that they hit numerous ports. this could not the slightest bit happen multiple times in less than a second from a similar stock. By corresponding alliance makes an endeavor it is finished that the source data science was action a sweep on target machine, on the grounds that the source made five association endeavors to totally various ports in under a second.

### **OS Fingerprinting-**

Operating system cycle could be a method for unequivocal that product will the far off pc runs. It is typically utilized for digital knowledge as exploitable weaknesses are working framework explicit. Like making an attempt to seek out vulnerability of IIS server on UNIX system machine is results in a failure. If an aggressor succeed to urge remote software name then it'll be simple for him to abuse the weakness of an objective framework and necessities to focus exclusively on the prominent weakness that outcomes in pleasant likelihood of accomplishment in somewhat less time and less danger of getting distinguished.. Operating system measure also has numerous strategy like port examining technique to with progress finger impression the usable framework. Essential technique behind operating system fingerprinting is to distinguish each operating system trademark which might be nonheritable from the remote system. These method is examining default communications protocol window size in an exceedingly} packet, activity knowledge in ICMP packets, estimate TCP initial sequence range etc.. TCP Standard is one in everything about procedure for operating system measure. Namp and Ring are the device wide utilized for operating system fingerprinting. Operating system fingerprinting relies upon information accumulated from conventional IP address traffic along these lines it's extremely difficult to dam operating system fingerprinting. a procedure to attempt to is that square immediate admittance to touchy pc frameworks. this might be finished by Organization Address Translation (NAT) that leaves just one machine vulnerable to most external OS process

## **5.2 Infiltration Phase**

In this section attacker's intention is to take manage of the goal by gaining far off get admission toto shell or terminal because the administrator at the host. Knowing vulnerability isn't sufficient for attacker, he must realize the way to make the most it. For an attacker it isn't vital to realize advanced know-how of programming however having it enhance the success I chance. Anyone can wager a susceptible password however growing a custom application to make the most vulnerability calls for ability and programming know-how. There are plenty of gear to be had on net for exploitation certainly considered one among them is metasploit.

## **5.3 Conclusion Phase**



This stage is to ensure that the goal is achieved and to delete the 654,987 traces that led to the attacker. Generally speaking, this step is the most difficult, because the computer keeps a log for every logins, logouts, startups, shutdowns, network connections, program execution and errors received. The attacker deletes all traces of intrusion from the target computer

## **6. TRENDS CHANGING CYBER SECURITY**

Purchasing cutting edge shrewd gadgets to ensure the framework or an association is just effective if the innovation is appropriately executed with the necessary arrangements. The following are the most mainstream advancements that mirror the network safety sway.

### **6.1 Web servers:**

The threat of attacks on web applications to eliminate data or to scatter vindictive code proceeds. Advanced hooligans scatter their malicious code through genuine web workers they've compromised. In any case information taking assaults, a few of that get the eye of media, are a monster threat. Now, we need a bigger weight on defensive web workers and web applications. Web workers are especially the least difficult stage for these digital lawbreakers to take the information. Thus one should utilize a more secure program particularly all through crucial exchanges in order to not fall as a prey for these violations. Digital hoodlums are utilizing web as an open stage to unfurl noxious documents through frail got web workers. Along these lines, getting web getting and application was a genuine concern. Exploitation virtual non-public organization work in programs will stop digital assaults

### **6.2 Mobile networks**

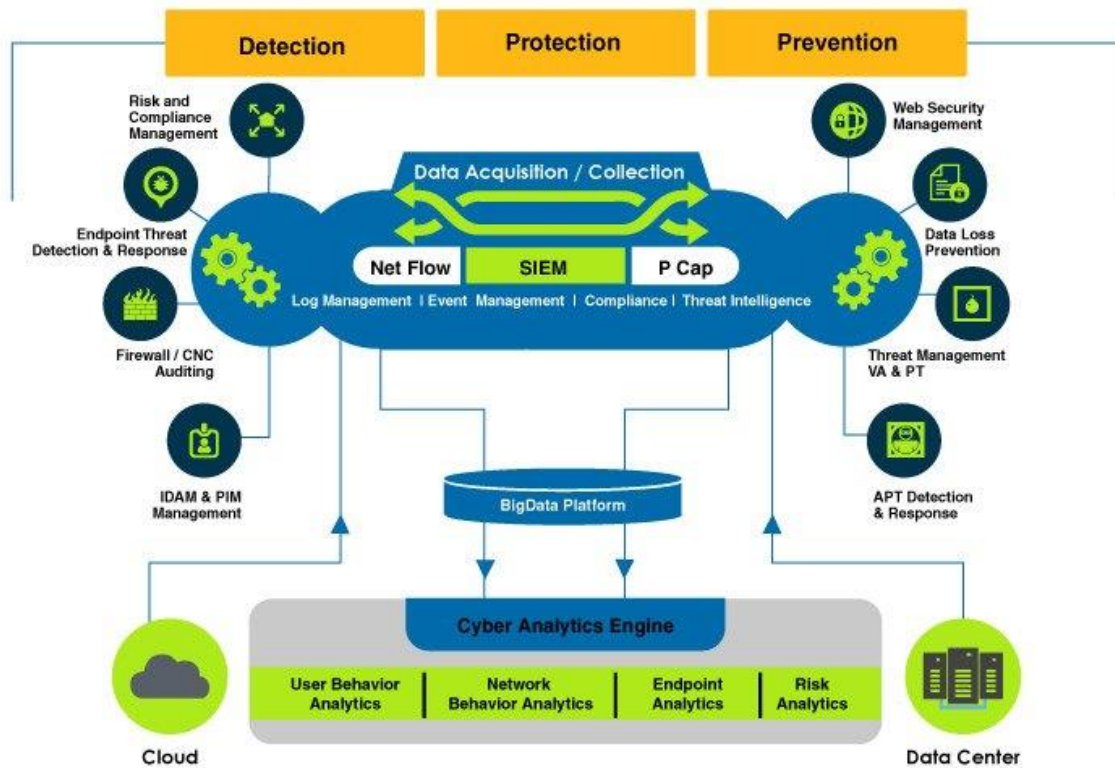
The peril of attacks on net applications to remove information or to scatter vindictive code perseveres. Advanced hooligans suitable their vindictive code through genuine web workers they've compromised. In any case information taking assaults, a few of that get the eye of media, additionally are a gigantic threat. Now, we need a bigger weight on defensive web laborers and web applications. Net laborers are particularly the best stage for these computerized evildoers to take the data. Accordingly one ought to use a safer program especially all through fundamental trades to not fall as a prey for these wrongdoings. Digital hoodlums are utilizing net as an open stage to unfurl noxious records by means of frail got web workers. Along these lines, getting web getting and application turned into a huge concern. Exploitation virtual non-public organization work in programs will stop digital assaults. Nowadays firewalls and diverse wellbeing highlights have gotten permeable as people are the utilization of devices along with tablets, telephones, PC's, etc all of which again require more protections beside the ones present withinside the projects utilized. We need to as a rule consider the wellbeing issues of those cell organizations. Further cell networks are hugely helpless against those digital wrongdoings a ton of care should be taken on the off chance that in their security issues.

### **6.3 Cloud computing**

Nowadays all little, medium and tremendous enterprises are gradually receiving cloud administrations. In various words the globe is gradually moving towards the mists. This most recent pattern presents a colossal test for network protection, as traffic will circumvent old marks of review. With the issue, distributed storage clad to be the adequate goal to stop SQL infuse assaults. Along these lines, the majority of the small and enormous scope ventures round the world are embracing cloud administrations. With expansion in data, distributed storage capacity changes that makes security imperfections. Administrations also epitomize code as an assistance, stage as a help, foundation as a help. This likewise work with clients to get and save assets. Additionally, on the grounds that the assortment of utilizations out there inside the cloud develops, strategy controls for web applications and cloud organizations will ought to create to stop the insufficiency of critical information. tho' cloud organizations are encouraging their own models still huge loads of issues are being referred to concerning their security. Cloud could offer immense chances nonetheless it ought to be noticed that

as the cloud is develops so as its security issues increment.

### Visualization into Context, Content, Behaviour - Integrated Cyber Risk Posture



### 6.4 Encryption of the code

Encryption is the way toward encoding messages (or data) so they can't be perused by gatecrashers or programmers. In an encryption plot, the message or data is encoded utilizing an encryption calculation, which changes over it into ambiguous ciphertext. utilizing an encryption key that indicates how the message will be scrambled. Encryption at an underlying level secures protection and honesty. Be that as it may, the expanded utilization of encryption represents extra network safety challenges. In the encryption cycle, hardly any specialized encryption calculations are utilized to change over information with a key that depicts the kind of encryption. While not another method, scrambling information by various pieces decides its solidarity. Salt is the procedure utilized in encryption that makes breaking troublesome. This implies that the information stays secret. albeit open encryption is additionally used to secure information on the way, for instance information communicated over networks (for example web, internet business), cells, remote mouthpieces, remote radios. Subsequently, by scrambling the code, it can assist with deciding if there has been a data spill.

## 6.5 IPv6: New internet protocol

IPv6 is another Internet convention that replaces IPv4 (old adaptation), which is the foundation of our overall organization and the Internet. IPv6 security is something other than porting IPv4 capacities; IPv6 is a finished substitute. By giving more IP addresses, some key changes to the convention should be considered in the security strategy. Presently Internet Protocol rendition 6 is changing this pattern, supplanting IPV4 with IPV6, which upholds more pluggable gadgets with better security highlights. The presentation of IPV6 innovation can not just lessen the quantity of assaults in private life, yet in addition diminish the quantity of assaults in the enormous IT industry.

Consequently, it is ideal to move to IPv6 straightaway to lessen the dangers related with cybercrime.

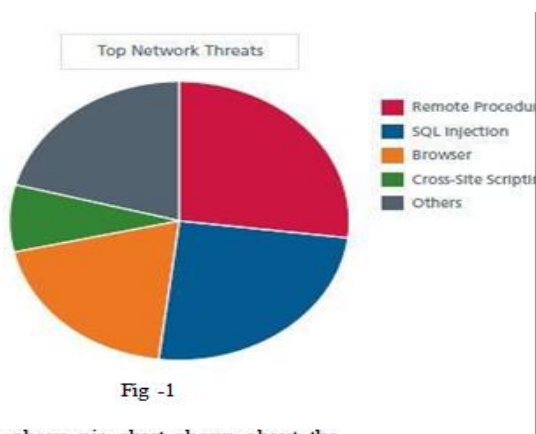


Fig -1  
The above pie chart shows about the major threats for networks and cyber security.

## 7.ROLE OF SOCIAL MEDIA IN CYBER SECURITY AND APPLICATIONS

As we become all the more cordial in an evidently related world, associations ought to find better ways to deal with guarantee singular data. Electronic media accepts a gigantic part in network security and will transform into an enormous advocate to individual organization dangers. The quantity of interpersonal organizations among workers is developing quickly. Since most representatives utilize interpersonal organizations or interpersonal organizations consistently, it's anything but an astounding stage for cybercriminals to take private data and take significant information.

In reality as we know it where we are delivering our own information rapidly, associations need to convey sure that they distinguish intimidations similarly as fast, act in-your-face time and forestall any kind of safety penetrate. The media are utilized by programmers as lure to get the data and information they need. In this manner, particularly while overseeing interpersonal organizations, individuals need to take proper measures to try not to lose their data. Millions is at the center of the specific test that online media models for organizations. Not exclusively does web-based media enable anybody to disseminate industrially delicate data, yet it likewise gives the very ability to circulate bogus data that can be comparably destructive. The fast spread of deception by means of web-based media is one of the new dangers distinguished in the 2013 Global Risks Report.

In any case online media are regularly used for advanced bad behaviors these associations can't tolerate forestalling abuse electronic media considering the way that it's anything but's a critical occupation in packaging of an association. Taking everything into account, they should have courses of action that may pull out them of the risk to fix it before any certified naughtiness is done. however, associations should see this and see the meaning of looking at the data particularly in friendly discussions and supply adequate security arrangements to stay eliminated from hazards. Everybody should deal with online media by utilizing sure arrangements and right advancements.

## **7.CYBER SECURITY TECHNIQUES**

The reasonable innovations used to keep up with security framework more grounded are as per the following.

### **7.1 Access control and password security in devices**

The username and secret phrase idea was an essential methods for ensuring our data and one of the initial steps we took when it came to network safety. Keeping up with ACL(Access oversee posting) for gaining admittance to archives depending upon their affectability is moving with the creating digital dangers. Upper leg tendon is makes a chose posting of individuals with advantages to get admission to records or catalogs or to dam exact association of people. This is fundamentally used in big business to consistent particularly close to home reports from insiders. Rundown ordinarily depends upon on capacity and guidelines at the representative

## **7.2 Authentication of data**

The reports that we will overall persuade should be genuine be preceding downloading that is it should be checked if it's anything but's a trusty and a strong stock which they're not changed. Approving of those records is to a great extent done by the counter disease PC code favoring inside the devices. so a certifiable foe of disease writing computer programs is likewise basic for screen the devices from contaminations

## **7.3 Firewalls**

A firewall could be a bundle program or piece of equipment that arranges programmers, infections, and worms that endeavor to arrive at your pc over the Internet. All messages getting into or going the web go through the firewall present, that inspects each message and squares the individuals who don't meet the specified security criteria. albeit the perform of a firewall is investigating and sifting bundles, fixing with suitable setups matter. Firewall with erroneous arrangements is bi-passed by unique the document pattern. Hence firewalls assume a critical part in identification the malware.

## **7.4 Anti-virus software**

Antivirus programming is a PC program that recognizes and forestalls malevolent programming programs, for example, infections and worms, and finds a way ways to incapacitate or eliminate them. Most antivirus programs incorporate a programmed update highlight that permits the program to download new infection profiles for you for new infections when they are recognized . These incorporate infections, trojans, worms, ransomware, spyware, and that's just the beginning. This malware can be distinguished by malware scanners prominently known as antivirus programming. Antivirus programming is an unquestionable requirement and an essential for everybody.

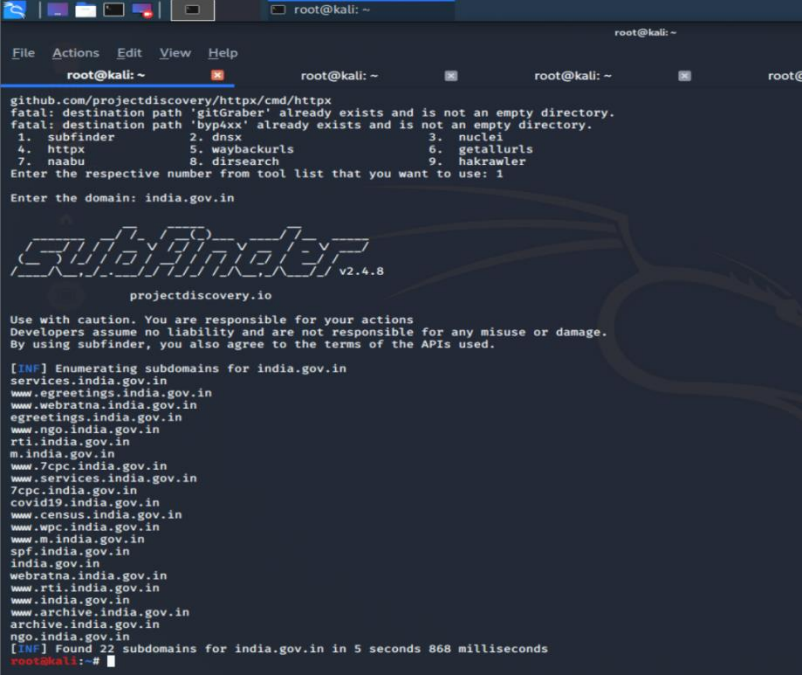
## **7.5 Honeypots**

In the new years honeypots are created to as a security alert that helps the administrator or security expert discover the interloper. These are wont to redirect the programmer to very surprising way and stop the data. tho' abuse this innovation assault is forestalled inside the underlying stage, bogus cautions will happen with inappropriate designs.

## 8.Results of project

### 8.1 Testing india.gov.in

When you spot a website like example.org and you then definitely see in some other region drugs.example.org you're seeing a subdomain. In extrarealistic words, subdomains are like having a organisation and their dependencies wherein the organisation is the area and the dependencies are the subdomains. A extra technical clarification may be located here. Most domain names have at the least more than one subdomains, they're used to arrange topics, as an example having a weblog as an example.org with inside the weblog.example.org subdomain, a discussion board in discussion board.example.org or for some other duties like a subdomain referred to as mail.example.org to path mail traffic, etc. Having a huge wide variety of subdomains can cause protection issues if they're not longer controlled properly sufficient and that's what normally occurs with companies (however now no longer confined to) which have tens, hundreds, or heaps of subdomains. It isn't clean to song them one at a time and that they come to bestroling previous software, having miss-configurations, and awful protection policies. With subdomain enumeration you may discover the best amount of subdomains for a goal area both for protection testing, crawling, subdomain takeover checks, or some other task. Subdomain enumeration is one of the maximum vital steps at the same time as doing protection checks to a goal area.



```
root@kali: ~
File Actions Edit View Help
root@kali: ~ root@kali: ~ root@kali: ~ root@kali: ~
github.com/projectdiscovery/httpx/cmd/httpx
fatal: destination path 'gitGraber' already exists and is not an empty directory.
fatal: destination path 'byp4xx' already exists and is not an empty directory.
1. subfinder 2. dnsx 3. nuclei
4. httpx 5. waybackurls 6. getallurls
7. nmap 8. dirsearch 9. hakrawler
Enter the respective number from tool list that you want to use: 1
Enter the domain: india.gov.in

Subfinder v2.4.8
projectdiscovery.io

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

[INF] Enumerating subdomains for india.gov.in
services.india.gov.in
www.egreetings.india.gov.in
www.webratna.india.gov.in
egreetings.india.gov.in
www.ngo.india.gov.in
rti.india.gov.in
m.india.gov.in
www.7cpc.india.gov.in
www.services.india.gov.in
7cpc.india.gov.in
covid19.india.gov.in
www.census.india.gov.in
www.wpc.india.gov.in
www.m.india.gov.in
spf.india.gov.in
india.gov.in
webratna.india.gov.in
www.rti.india.gov.in
www.india.gov.in
www.archive.india.gov.in
archive.india.gov.in
ngo.india.gov.in
[INF] Found 22 subdomains for india.gov.in in 5 seconds 868 milliseconds
root@kali: ~#
```

```

root@kali: ~
go: github.com/modern-go/reflect2 upgrade => v1.0.1
go: github.com/projectdiscovery/stringsutil upgrade => v0.0.0-20210617141317-00728870f68d
go: github.com/golang/snappy upgrade => v0.0.3
go: golang.org/x/text upgrade => v0.3.6
go: github.com/projectdiscovery/mapcidr upgrade => v0.0.7
go: github.com/miekg/dns upgrade => v1.1.43
go: github.com/projectdiscovery/iptutil upgrade => v0.0.0-20210429152401-c18a5408ca46
go: github.com/projectdiscovery/gologger upgrade => v1.1.4
go: go.uber.org/atomic upgrade => v1.8.0
go: github.com/logrusorgru/aurora upgrade => v2.0.3+incompatible
fatal: destination path 'gitGraber' already exists and is not an empty directory.
fatal: destination path 'byp4xx' already exists and is not an empty directory.
 1. subfinder      2. dnsx          3. nuclei
 4. httpx          5. waybackurls  6. getallurls
 7. naabu          8. dirsearch    9. hakrawler
Enter the respective number from tool list that you want to use: 2
Enter the domain: india.gov.in

Subfinder v2.4.8
projectdiscovery.io

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

[INF] Enumerating subdomains for india.gov.in
www.india.gov.in [www.india.gov.in.akamaized.net]
covid19.india.gov.in [s3850af92f8d9903e7a4e0559a98ecc857.s3waas.gov.in]
root@kali: ~#

```

```

root@kali: ~
go: github.com/logrusorgru/aurora upgrade => v2.0.3+incompatible
go: github.com/projectdiscovery/iptutil upgrade => v0.0.0-20210429152401-c18a5408ca46
fatal: destination path 'gitGraber' already exists and is not an empty directory.
fatal: destination path 'byp4xx' already exists and is not an empty directory.
 1. subfinder      2. dnsx          3. nuclei
 4. httpx          5. waybackurls  6. getallurls
 7. naabu          8. dirsearch    9. hakrawler
Enter the respective number from tool list that you want to use: 3
Enter the domain: india.gov.in

nuclei v2.2.1-dev
projectdiscovery.io

[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] nuclei-templates are not installed, use update-templates flag.
[INF] Loading templates...
[INF] [php-backup-files] PHP source disclosure through backup files (@StreetOfHackerR007 (Rohit Soni)) [medium]
[INF] [exposed-mysql-initial] Exposed mysql.initial (@ELSA7110) [info]
[INF] [settings-php-files] settings.php information disclosure (@Sheikhrishad) [medium]
[INF] [default-sql-dump] MySQL Dump Files (@geeknik,dwisiswant0) [medium]
[INF] [zip-backup-files] Compressed Web File (@Toufik Airane,dwisiswant0) [medium]
[INF] [error-logs] common error log files (@geeknik,daffainfo) [low]
[INF] [pyramid-debug-toolbar] Pyramid Debug Toolbar (@geeknik) [medium]
[INF] [oracle-ebs-sqllog-disclosure] Oracle EBS SQL Log Disclosure (@adhiyanshdk) [medium]
[INF] [trace-axd-detect] ASP.NET Trace.AXD Information Leak (@adhiyanshdk) [low]
[INF] [squid-analysis-report-generator] Squid Analysis Report Generator (@geeknik) [high]
[INF] [rails-debug-mode] Rails Debug Mode Enabled (@apdteam) [medium]
[INF] [npm-log-file] Publicly accessible NPM Log file (@Sheikhrishad) [low]
[INF] [laravel-log-file] Laravel log file publicly accessible (@Sheikhrishad,geeknik) [high]
[INF] [elmah-log-file] elmah.axd Disclosure (@shine) [medium]
[INF] [laravel-telescope] Laravel Telescope Disclosure (@geeknik) [medium]
[INF] [struts-debug-mode] Apache Struts setup in Debug-Mode (@pdteam) [low]
[INF] [php-debug-bar] PHP Debug bar (@adhiyanshdk) [high]
[INF] [access-log-file] Publicly accessible access-log file (@Sheikhrishad) [low]
[INF] [darkstat-detect] Detect Darkstat Reports (@geeknik) [high]
[INF] [newrelic-rest-api-key] REST API Key Disclosure (@Ice3man) [info]
[INF] [newrelic-synthetics-location-key] Synthetics Location Key Disclosure (@Ice3man) [info]
[INF] [newrelic-admin-api-key] Admin API Key Disclosure (@Ice3man) [info]
[INF] [newrelic-insights-key] Insights Keys Disclosure (@Ice3man) [info]
[INF] [zapier-webhook-token] Zapier Webhook Disclosure (@Ice3man) [info]

```



```
File Actions Edit View Help
root@kali: ~ root@kali: ~ root@kali: ~
go: golang.org/x/sys upgrade => v0.0.0-20210629170331-7dc0b73dc9fb
go: golang.org/x/text upgrade => v0.3.6
go: golang.org/x/net upgrade => v0.0.0-20210614182718-04defd469f4e
go: github.com/json-iterator/go upgrade => v1.1.11
go: github.com/modern-go/concurrent upgrade => v0.0.0-20180306012644-bacd9c7ef1dd
go: github.com/projectdiscovery/mapcidr upgrade => v0.0.7
go: go.uber.org/atomic upgrade => v1.8.0
go: github.com/modern-go/reflect2 upgrade => v1.0.1
go: github.com/miekg/dns upgrade => v1.1.43
go: github.com/projectdiscovery/retryabledns upgrade => v1.0.12
go: github.com/golang/snappy upgrade => v0.0.3
go: github.com/logrusorgru/aurora upgrade => v2.0.3+incompatible
go: github.com/projectdiscovery/gologger upgrade => v1.1.4
go: github.com/microcosm-cc/bluemonday upgrade => v1.0.14
go: github.com/projectdiscovery/stringsutil upgrade => v0.0.0-20210617141317-00728870f68d
go: github.com/projectdiscovery/iputil upgrade => v0.0.0-20210429152401-c18a5408ca46
fatal: destination path 'gitGraber' already exists and is not an empty directory.
fatal: destination path 'byp4xx' already exists and is not an empty directory.
 1. subfinder      2. dnsx          3. nuclei
 4. httpx          5. waybackurls  6. getallurls
 7. naabu          8. dirsearch    9. hakrawler
Enter the respective number from tool list that you want to use: 4

Enter the domain: india.gov.in

Subfinder v2.4.8
projectdiscovery.io

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

[INF] Enumerating subdomains for india.gov.in
[INF] Found 22 subdomains for india.gov.in in 5 seconds 384 milliseconds
https://covid19.india.gov.in
https://www.services.india.gov.in
https://www.india.gov.in
https://webratna.india.gov.in
https://www.webratna.india.gov.in
https://services.india.gov.in
https://india.gov.in
root@kali:~#
```

```
https://www.india.gov.in/constitution-site-allotment-advisory-board-saab-committee-thingsai-village?page=4
https://www.india.gov.in/constitution-site-allotment-advisory-board-saab-committee-thingsai-village?page=5
https://www.india.gov.in/constitution-site-allotment-advisory-board-saab-committee-thingsai-village?page=6
https://www.india.gov.in/constitution-site-allotment-advisory-board-saab-committee-thingsai-village?page=7
https://www.india.gov.in/constitution-site-allotment-advisory-board-saab-committee-thingsai-village?page=8
https://www.india.gov.in/constitution-site-allotment-advisory-board-saab-committee-thingsai-village?page=9
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=1
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=10
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=11
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=12
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=13
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=14
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=15
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=16
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=17
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=18
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=2
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=3
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=4
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=5
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=6
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=7
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=8
https://www.india.gov.in/constitution-skill-development-initiative-sdi-cell?page=9
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=1
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=10
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=11
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=12
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=13
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=14
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=15
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=16
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=17
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=18
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=19
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=2
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=20
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=21
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=22
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=23
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=24
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=25
https://www.india.gov.in/constitution-society-prevention-cruelty-animals-8-eight-administrative-district-hqrs-mlzoram?page=2
[2]+ Stopped cat india.gov.in.txt
root@kali:~#
```

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ root@kali: ~ root@kali: ~/dirsearch root@kali: ~  
4. httpx 5. waybackurls 6. getallurls  
7. naabu 8. dirsearch 9. hakrawler  
Enter the respective number from tool list that you want to use: 9  
Enter the domain: india.gov.in  
HAKRAWLER  
Crafted with <3 by hakluke  
[url] https://www.india.gov.in/user/login  
[subdomain] www.india.gov.in  
[url] https://www.india.gov.in/user/register  
[url] https://www.india.gov.in/hi/  
[url] https://www.india.gov.in/  
[url] https://www.india.gov.in/topics  
[url] https://www.india.gov.in/topics/agriculture  
[url] https://www.india.gov.in/topics/art-culture  
[url] https://www.india.gov.in/topics/commerce  
[url] https://www.india.gov.in/topics/communication  
[url] https://www.india.gov.in/topics/defence  
[url] https://www.india.gov.in/topics/education  
[url] https://www.india.gov.in/topics/environment-forest  
[url] https://www.india.gov.in/topics/finance-taxes  
[url] https://www.india.gov.in/topics/food-public-distribution  
[url] https://www.india.gov.in/topics/foreign-affairs  
[url] https://www.india.gov.in/topics/governance-administration  
[url] https://www.india.gov.in/topics/health-family-welfare  
[url] https://www.india.gov.in/topics/home-affairs-enforcement  
[url] https://www.india.gov.in/topics/housing  
[url] https://www.india.gov.in/topics/industries  
[url] https://www.india.gov.in/topics/infrastructure  
[url] https://www.india.gov.in/topics/information-broadcasting  
[url] https://www.india.gov.in/topics/labour-employment  
[url] https://www.india.gov.in/topics/law-justice  
[url] https://www.india.gov.in/topics/power-energy  
[url] https://www.india.gov.in/topics/rural  
[url] https://www.india.gov.in/topics/science-technology  
[url] https://www.india.gov.in/topics/social-development  
[url] https://www.india.gov.in/topics/transport  
[url] https://www.india.gov.in/topics/travel-tourism  
[url] https://www.india.gov.in/topics/youth-sports  
[url] http://services.india.gov.in/  
[subdomain] services.india.gov.in
```

## Conclusion

PC security could be a huge theme that is transforming into a ton of important because of the globe is getting incredibly interconnected, with networks being utilized to hold out crucial exchanges. Digital wrongdoing keeps on wandering down totally various ways with each twelvemonth that passes and afterward will the wellbeing of the information. The most recent and pained advances, close by the new digital instruments and dangers that return to lightweight every day, are troublesome associations with not exclusively notwithstanding they secure their framework, in any case how they need new stages and knowledge to attempt to so. Indeed, even goliath scaled security associations were the casualties on these digital assaults.

Associations tending to delicate information and having low online protection information like clinical and banking areas have massive danger digital dangers. Recruiting something important to perform network safety tasks for the association to protect digital violations. along with that enterprises includes a respectability to mentor their laborers with right network safety information. This assist representatives with detecting the assault at the underlying stage which can not be valuable in guarded the assault in any case can help in limiting the misfortune. albeit this in a roundabout way prepares representatives to perform corporate chief assault with none follows, this may decreased by carrying out consistent police work and security approaches. There is nothing but bad response for digital wrongdoings nonetheless we should consistently endeavor our breaking point to diminish them to have a protected and secure future in the internet.

## References

1. S. Shin and T. Kwon, "A Privacy-Preserving Authentication, Authorization, and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things," in *IEEE Access*, vol. 8, pp. 67555-67571, 2020, doi: 10.1109/ACCESS.2020.2985719. Link- <https://ieeexplore.ieee.org/document/9057455>
2. S. Z. Sajal, I. Jahan and K. E. Nygard, "A Survey on Cyber Security Threats and Challenges in Modern Society," 2019 IEEE International Conference on Electro Information Technology (EIT), 2019, pp. 525-528, doi: 10.1109/EIT.2019.8833829. Link- <https://ieeexplore.ieee.org/document/8833829>
3. K. Gradon, "Crime Science and the Internet Battlefield: Securing the Analog World from Digital Crime," in *IEEE Security & Privacy*, vol. 11, no. 5, pp. 93-95, Sept.-Oct. 2013, doi: 10.1109/MSP.2013.112. Link- <https://ieeexplore.ieee.org/document/6630019>
4. A. Razaque, D. Kejun, Z. Xueqi, L. Wanyue, Q. B. Hani and M. J. Khan, "Survey: Wildlife trade and related criminal activities over the internet," 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2018, pp. 1-6, doi: 10.1109/LISAT.2018.8378037. Link- <https://ieeexplore.ieee.org/document/8378037>
5. Munich, Germany, 10-12 September 2012, Pre-conference Program WS2— *Future Risks in Cybercrime and Cyberwar: Long-term Trends and Consequences*, on Roessing, 8 September, [www.isaca.org/Education/Conferences/Pages/European-CACS-ISRMEurope-2012.aspx](http://www.isaca.org/Education/Conferences/Pages/European-CACS-ISRMEurope-2012.aspx). An in-depth analysis of the many types of security, cybercrime and cyberwar surveys and the underlying trends, benchmarks and studies that have been made available to the marketplace over the past several years.[accessed 29 January 2015]
6. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy
7. A. Damodaran, F. Di Troia, C. A. Visaggio, T. H. Austin, and M. Stamp, "A comparison of static, dynamic, and hybrid analysis for malware detection," *Journal of Computer Virology and Hacking Techniques*, vol. 13, no. 1, pp. 1-12,2017.