# INTRUSION DETECTION AND RESPONSE

# TABLE OF CONTENTS

# 1. DETECTING RECONNAISSANCE

❖ Potential intruders can collect and use reconnaissance data by various methods.

- Identifying unusual patterns of network traffic
- Attempting to gain access to a firewall through web or ftp server
- Using recon
- Cloud services
- Spear phishing
- Executing automated scripts on websites

It is possible to identify the organization's flaws using reconnaissance data. For instance, an intruder might find that the company lacks a suitable security mechanism to safeguard the sensitive data kept on its computer network. An attacker might look for network vulnerabilities using strategies like port scanning or website crawling. An attacker might try to access a network, for instance, by trying to penetrate a firewall through one of the services it is running, if the attacker is looking for vulnerable systems and websites on the Internet. To search for open ports, these tools often use a large number of ports in a range. These tools may occasionally additionally include ping commands to check the connectivity of the target hosts.

Intruders must do reconnaissance in order to ascertain their next move. They must look for ports, services, and resources from which they can switch and access customer information, credit card information, source code, and other information. Cybercriminals that engage in active reconnaissance employ techniques like ping, netcat, automated scanning, and manual testing to try and learn more about computer systems. Utilizing the lifecycle rules of cloud services, users can carry out extensive information management duties, such as automatic rebalancing and data filtering in service of compliance issues. packet sniffing, ping sweeps, packet inspection, hacking, social manipulation, and internet information searches are a few typical kinds of reconnaissance assaults. (Thakkar, et al., 2020).

Both passive and active attacks are possible in a network. Passive attack refers to watching network traffic in order to gather sensitive information that is not encrypted, including passwords. Without the user's awareness, information is disclosed as a result. It leads to data exposure, data manipulation, or service denial (DoS). Passive and aggressive attacks, respectively, include sniffing and spoofing. Sniffing is the process of reading data on a system other than the destination. Sniffing can be used to gather low level protocol information such as ip address, hardware address, routing information, financial information, emails, passwords, and private information. In spoofing, one networked system assumes the identity of another system. (mandal, 2016)

- Ultimate goal for an attacker is not the network but the data stored and processes running on the server.

  For collecting as much as information about a target system, there are certain steps

  - Gather preliminary information
  - Identifying active machines
  - Determine open ports and access points
  - OS fingerprinting
  - Reveal all the services on ports
  - Network mapping
  - End point security

  In order to gain information about network, attacker will use file permissions, running network services, OS platforms, trust relationship, user account information etc. (patil & Jangra, 2017)

  Data at the flow level: By analyzing related packets collectively, flow analysis can assist track application health, network performance, host activity, and highlight abnormal network traffic that could indicate an intrusion. The usability, dependability, authenticity, and safety of a network and its data must all be protected. The three Cs—Confidentiality, Integrity, and Availability—are the main focuses of network security. (Kasongo, et al., 2020)

- The tools that are used the most commonly during the reconnaissance phase are those for network mapping, networks, and vulnerability scanning. Cheops, for instance, is a powerful network mapping tool that can generate networking graphs. They could be of great help later on, during the attack phase or while getting a general picture of the network. A network mapping tool is quite helpful when performing an internal ethical hack.

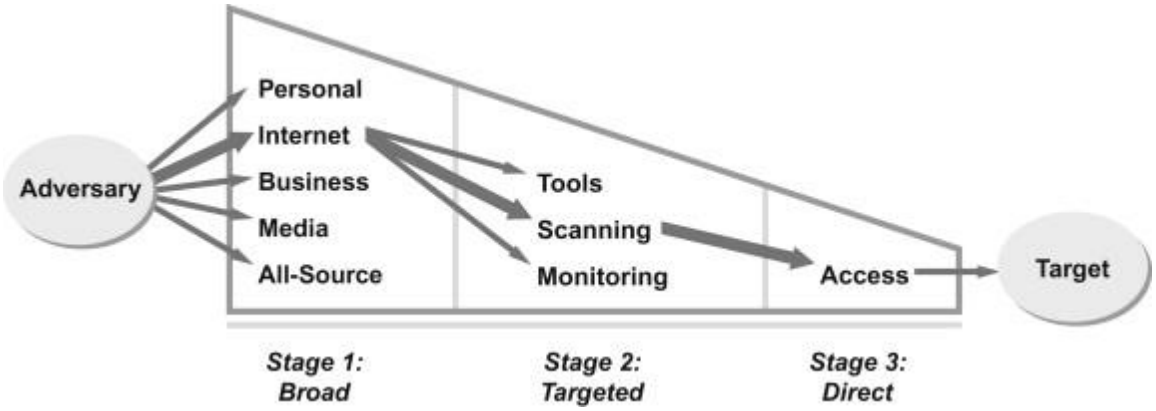



Figure 1:Stages of reconnaissance

Tools like Nmap and Metasploit, wireshark, shodan, google, os finger printing can be used to discover operating system vulnerabilities and identify potentially vulnerable hosts in the network.

A security scanner is called Nmap. It finds hosts and services in a network, creating a "map" of the network. Nmap sends specially constructed packets to the target host and then analyses the responses to those packets. Nmap has a number of features, including host finding, port scanning, version detection, and operating system detection. The following command is used to install nmap:$ sudo apt-get install nmap (mandal, 2016)

Testing tools like Metasploit look for flaws in apps and operating systems. The idea of "exploit" serves as the foundation for this penetration testing tool. It creates a framework for penetration testing by executing a set of commands on the test target. It runs on Microsoft Windows, Apple Mac OS X, and Linux. (Hessa Mohammed Zaher Al Shebli, 2018)

The best packet analyzer with an open source GUI is thought to be Wireshark. Administrators and network security engineers use Wireshark to diagnose network-related issues and look into security issues, respectively. Users use it to study the internals of network protocols. It is utilised by developers to QA protocol implementations. Wireshark can be started from the ubuntu terminal using the following command:- $ sudo wireshark (mandal, 2016)

Shodan is made to crawl the Internet, index services that are found, and find weak points in equipment. As a result, it is frequently utilised by security experts and has significantly raised awareness of the issues facing the IoT ecosystem. (mandal, 2016)

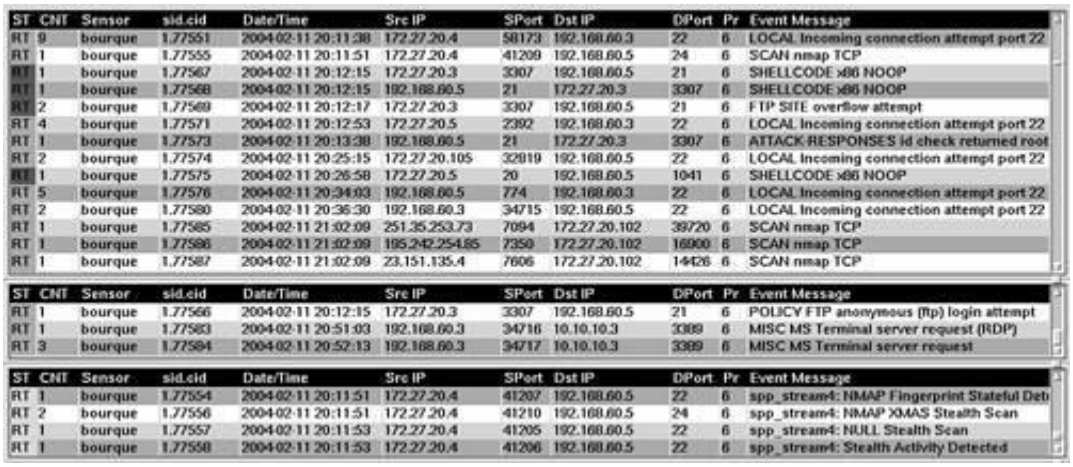
OS fingerprinting identifies the operating system that a distant computer is using. The majority of exploitable flaws are operating system-specific, hence cyber reconnaissance primarily uses OS fingerprinting.

Utilizing search engines like Google is another method for doing reconnaissance. Search engines are the most effective passive reconnaissance techniques available.

- Network performance is drastically decreased by congestion, the number of years that data travels via a network section with latency, which slows down enterprise network performance. The main sources of network congestion, network bottlenecks, should be eliminated. Set up a network analyzer like wireshark to examine network traffic in order to spot and report problems with the network infrastructure. A bottleneck is a network portion that is unable to handle the level of traffic coming out of its adjacent segments. Data transmission needs to be prioritized based on the needs. Once the problem has been located, a suitable solution can be developed to reduce traffic and alter the network as a whole. Troubleshoot the problem if the tracking program determines that a certain segment is generating more traffic than anticipated (Vinayakumar, et al., 2020).

## 2. SESSION DATA COLLECTION

A record of the communication between two network nodes is called session data. Session data contains endpoints and metrics of the interaction, e.g., number of packets or size of data. Based on its analysis of network traffic, an NSM tool like Bro can produce a wide variety of logs. Time stamp, source IP address and port, destination IP address and port, protocol, application bytes delivered by the source and application bytes sent by the destination, among other details, are condensed into these key elements. The summary of communication between two network devices is known as session data. This summary data, which is often referred to as a dialogue or a flow, is one of the most adaptable and practical types of NSM data. Even while session data isn't as detailed as FPC data, it can be stored for a lot longer thanks to its tiny size, which is quite helpful for conducting retrospective analysis. Session data is incredibly minimal in size because it is only a collection of text records and statistics. As a result, developing large-scale flow storage solutions is simple. Although full content data could be used to generate session data, tracking simply session data may be preferable if hard drive capacity is at a premium. To see session data, one can alternatively utilise the free software Sguil, which has historically rendered and collected session data via the SANCP utility. The call-specifics of network activity are typically the main focus of session data. Most of the time, session data does not include the nature of those transactions. We look at transaction data for that. (Sanders & Smith, 2014)



| ST | CNT | Sensor | sid.cid | Date/Time | Src IP | SPort | Dst IP | DPort | Pr | Event Message |
|---|---|---|---|---|---|---|---|---|---|---|
| RT | 9 | bourque | 1.77551 | 2004-02-11 20:11:38 | 172.27.20.4 | 58173 | 192.168.60.3 | 22 | 6 | LOCAL Incoming connection attempt port 22 |
| RT | 1 | bourque | 1.77555 | 2004-02-11 20:11:51 | 172.27.20.4 | 41209 | 192.168.60.5 | 24 | 6 | SCAN nmap TCP |
| RT | 1 | bourque | 1.77567 | 2004-02-11 20:12:15 | 172.27.20.3 | 3307 | 192.168.60.5 | 21 | 6 | SHELLCODE x86 NOOP |
| RT | 1 | bourque | 1.77568 | 2004-02-11 20:12:15 | 192.168.60.5 | 21 | 172.27.20.3 | 3307 | 6 | SHELLCODE x86 NOOP |
| RT | 2 | bourque | 1.77569 | 2004-02-11 20:12:17 | 172.27.20.3 | 3307 | 192.168.60.5 | 21 | 6 | FTP SITE overflow attempt |
| RT | 4 | bourque | 1.77571 | 2004-02-11 20:12:53 | 172.27.20.5 | 2392 | 192.168.60.3 | 22 | 6 | LOCAL Incoming connection attempt port 22 |
| RT | 1 | bourque | 1.77573 | 2004-02-11 20:13:38 | 192.168.60.5 | 21 | 172.27.20.3 | 3307 | 6 | ATTACK-RESPONSES id check returned root |
| RT | 2 | bourque | 1.77574 | 2004-02-11 20:25:15 | 172.27.20.105 | 32819 | 192.168.60.5 | 22 | 6 | LOCAL Incoming connection attempt port 22 |
| RT | 1 | bourque | 1.77575 | 2004-02-11 20:26:58 | 172.27.20.5 | 20 | 192.168.60.5 | 1041 | 6 | SHELLCODE x86 NOOP |
| RT | 5 | bourque | 1.77576 | 2004-02-11 20:34:03 | 192.168.60.5 | 774 | 192.168.60.3 | 22 | 6 | LOCAL Incoming connection attempt port 22 |
| RT | 2 | bourque | 1.77580 | 2004-02-11 20:36:30 | 192.168.60.3 | 34715 | 192.168.60.5 | 22 | 6 | LOCAL Incoming connection attempt port 22 |
| RT | 1 | bourque | 1.77585 | 2004-02-11 21:02:09 | 251.35.253.73 | 7094 | 172.27.20.102 | 39720 | 6 | SCAN nmap TCP |
| RT | 1 | bourque | 1.77586 | 2004-02-11 21:02:09 | 195.242.254.85 | 7350 | 172.27.20.102 | 16900 | 6 | SCAN nmap TCP |
| RT | 1 | bourque | 1.77587 | 2004-02-11 21:02:09 | 23.151.135.4 | 7606 | 172.27.20.102 | 14426 | 6 | SCAN nmap TCP |

| ST | CNT | Sensor | sid.cid | Date/Time | Src IP | SPort | Dst IP | DPort | Pr | Event Message |
|---|---|---|---|---|---|---|---|---|---|---|
| RT | 1 | bourque | 1.77566 | 2004-02-11 20:12:15 | 172.27.20.3 | 3307 | 192.168.60.5 | 21 | 6 | POLICY FTP anonymous (ftp) login attempt |
| RT | 1 | bourque | 1.77583 | 2004-02-11 20:51:03 | 192.168.60.3 | 34716 | 10.10.10.3 | 3389 | 6 | MISC MS Terminal server request (RDP) |
| RT | 3 | bourque | 1.77584 | 2004-02-11 20:52:13 | 192.168.60.3 | 34717 | 10.10.10.3 | 3389 | 6 | MISC MS Terminal server request |

| ST | CNT | Sensor | sid.cid | Date/Time | Src IP | SPort | Dst IP | DPort | Pr | Event Message |
|---|---|---|---|---|---|---|---|---|---|---|
| RT | 1 | bourque | 1.77554 | 2004-02-11 20:11:51 | 172.27.20.4 | 41207 | 192.168.60.5 | 22 | 6 | spp_stream4: NMAP Fingerprint Stateful Det |
| RT | 2 | bourque | 1.77556 | 2004-02-11 20:11:51 | 172.27.20.4 | 41210 | 192.168.60.5 | 24 | 6 | spp_stream4: NMAP XMAS Stealth Scan |
| RT | 1 | bourque | 1.77557 | 2004-02-11 20:11:53 | 172.27.20.4 | 41205 | 192.168.60.5 | 22 | 6 | spp_stream4: NULL Stealth Scan |
| RT | 1 | bourque | 1.77558 | 2004-02-11 20:11:53 | 172.27.20.4 | 41206 | 192.168.60.5 | 22 | 6 | spp_stream4: Stealth Activity Detected |

Figure 2: Interface of sguil

Alert data has been generated by the sensor to warn the users that there‘s event been taking place in the network. Whether traffic prompts an alarm in an NSM tool is reflected in the alert data. The notification that a detection tool generates when it finds an anomaly in any of the data it is set up to look at is referred to as alert data. This information normally includes a description of the alert and a reference to the data that seems out of the ordinary. Since alert data just provides pointers to other data, it is typically incredibly short in size. Typically, the production of alert data serves as the foundation for the study of NSM events.

One source of alert information is an intrusion detection system (IDS). Two well-known open source IDSs are Snort and Suricata. These tools monitor and analyse network traffic, and when they notice anything they are designed to report, they produce a message. (Bejtlich, 2013)

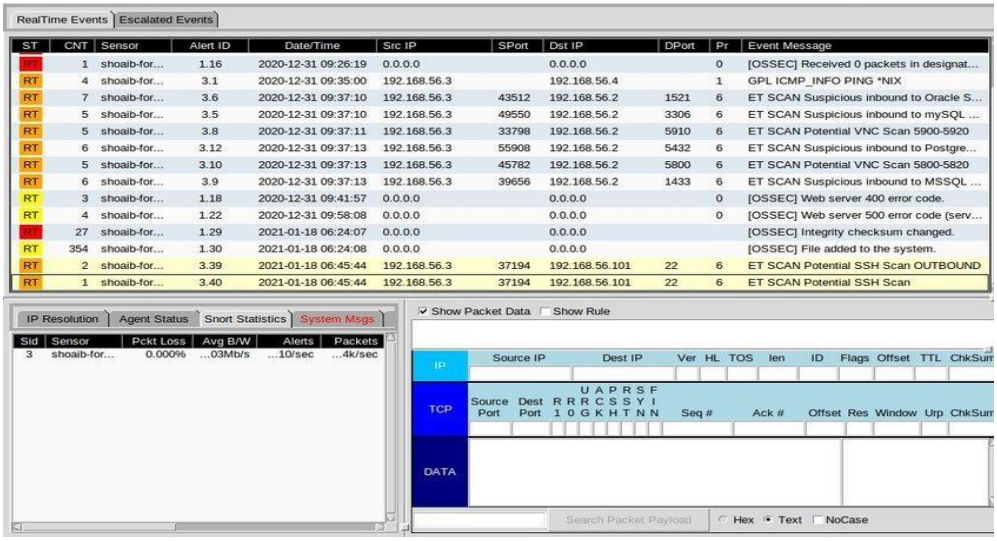



Figure 3: Sguil interface shows the alert for attacks

## 3. SPLUNK OR ELASTIC STACK?

Users can use Splunk to search through the data and find what they need. The three main parts of Splunk are its forwarder, which pushes data to remote indexers, indexer, which has roles for storing and indexing data and handling search requests, and search head, which is the front end of the web interface where these three elements can be combined or distributed across servers. Additionally, Splunk enables the use of SDKs to integrate its features into applications. In typical use cases like operational monitoring, security, and user behaviour analytics, they have proved quite successful. Splunk is a paid service, and indexing volume determines pricing. Splunk accepts data quite easily. The forwarders are used to import data into Splunk after installation and come pre-configured for a variety of data sources including files and directories, network events, windows sources, and application logs. It's important to remember that the Splunk web UI has adaptable features that alter and add new dashboard elements. The management and user controls are excellent and may be set up individually for different users, each with their own dashboard. With application and visualisation components that are simple to customise using XML, Splunk offers visualisations on mobile devices as well. (Verma, 2020)

The Elasticsearch, Logstash, and Kibana (ELK) Stack is a collection of three open-source tools created and maintained by Elastic. Lucene is the search engine used by the NoSQL database Elasticsearch. Elasticsearch receives data from Logstash via a pipeline for data processing and delivery . Kibana is a dashboard built on top of Elasticsearch that enables data analysis using dashboards and visualisations. The entire Elastic Stack's central

authentication hub is Elasticsearch. Role-based access control, single sign-on and authentication, field-level, attribute-level, and document-level security, as well as encryption-at-rest and audit logging, are among the security features. The Elastic Stack's user interface is called Kibana. Through venues for code sharing like GitHub and Elastic docs, the community has distributed dozens of Kibana plug-ins. Data ingestion tools like Beats and Logstash allow users to gather and enhance any type of data from any source for storage in Elasticsearch. The architecture of Beats and Logstash is extendable and modular. Beats are little agents designed specifically to gather information from computers, servers, and containers. (Verma, 2020)

Users of Logstash can develop data stream capture and transformation logic without writing code because to its robust and versatile configuration language. This significantly broadens and speeds up the possibility for a range of businesses and people to build data management pipelines. This seems to be where Splunk falls short.

As an open source platform, the ELK stack, which consists of Elasticsearch for search, Logstash for data input and processing, and Kibana for reporting and visualisation, offers a reduced entry barrier. Logstash serves as the log workhorse in the ELK stack, building a centralised pipeline for archiving, searching, and analysing log data. Strong functionality is delivered to logs via a variety of plugins as well as built-in filters, inputs, and outputs. Because it's open source, it's simple to add plugins for unique data sources like SMF or modify it to support specific log formats. Teams may better understand mainframe settings by using Elasticsearch to process and analyse data from mainframe machines. Therefore effectiveness of the Elastic stack is slightly better. (Verma, 2020)

## 4. INCIDENT RESPONSE

The core of security activities is recognising and responding to data security problems. The team designated to security operations is tasked with keeping an eye on the organization's internal benefits and responding to security issues and occurrences, including the detection and analysis of any indicators of compromise (IOC).

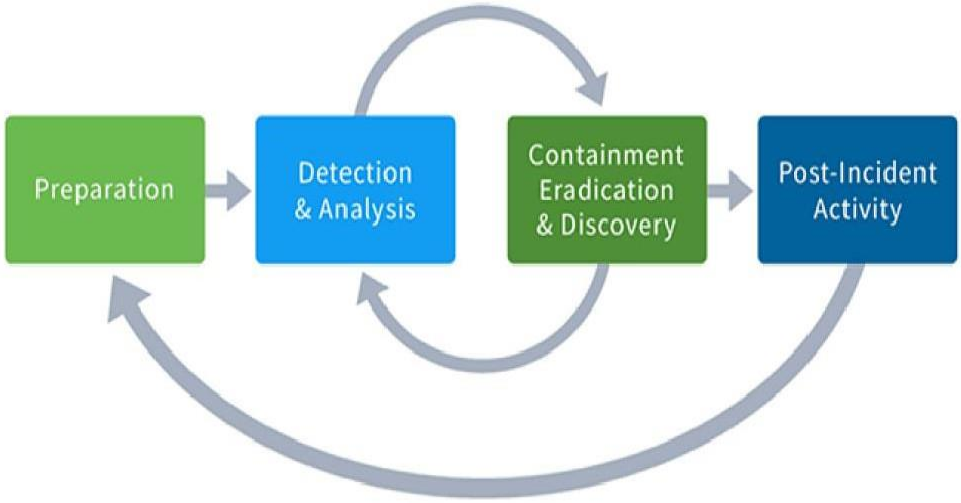



Figure 4 shows the basic process of incident response team

The four basic steps of the NIST Incident Handling Process serve as a guidebook for event operators. The organisation accumulates the necessary personnel, plans, knowledge, and tools during the preparation stage in order to quickly and effectively address an incident. The method's second stage entails the detection and analysis of security events from the organization's network perimeter, a target perimeter, system-level activity, application-level activity, or user activity. Additionally, reporting an occurrence is part of it. Upon learning of an occurrence, the organisation will begin the stages of confinement, eradication, and restoration. During this phase, the threat may continue on its route of intervention. As fresh information about the danger becomes available during an incident response, incident controllers frequently alternate between the second and third stages. The incident response team also develops options to improve the procedure for the subsequent incident during the post-incident operation stage. (Djufri & Lim, 2021)

The containment step of the IR process is crucial because it enables to determine whether or not any changes—such as those that affect registry keys, file locations, or computer system manipulation—have been made. Knowing the attacker's behaviour will help with forensic and incident response analyses (IR). Computer systems must take proactive measures to prevent intrusion. Events should be recorded in entire event logs that are not isolated. To acquire an IOC, failed login is not sufficient; event should be related with some other to determine compromised system events

**IOC**

In every organisation where an incident is compromised, there has been a security violation. One should learn how the present Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) might claim that a cyber activity is an effort at an assault by the adversaries in order to better comprehend Indicator of Compromise (IOC). One should be aware of how current Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) can justify a cyber activity to be an attempt of attack launched by the

adversaries. IDS and IPS share the same methods on how they can detect an activity. Their detection mechanism is by parsing through previously collected data so that in the end they can generate alert based on currently flowing data compared to the collected data. (Chauhan, 2021)

IoCs can also be used to assess how much a compromise damaged a company or to compile knowledge gained to better protect the environment from future assaults. However, various artificial IoC cybersecurity solutions can be used to gather and organise indicators during incident response. Indicators are often gathered through software, including antimalware and antivirus systems.

Data collected with the use of different tools which are used in detecting reconnaissance are relevant to incident response handling case. These are gathered in initial stage.

## 5. APT(ADVANCED PERSISTENT THREATS)

- Testing recommendation.

A penetration test is performed to identify the risks that might exist if an attacker got access to the company's computing systems and networks. A PEN test will estimate the mitigation strategy to fix security holes before the real attack. Conducting PEN tests assists an organization's ability to reduce monetary and information loss that may have occurred from security breaches and eroded customer trust. A PEN test aids an organisation in assessing the degree of security awareness among its personnel, the efficacy of the current security policy and procedure, as well as the effectiveness of its goods. In order to plan for security investments and IT strategies, it is helpful to evaluate the security of the organization.

Ethical hackers should conduct the testing. System for detecting intrusions IDS penetration refers to attempts to break in from the outside as well as from within to discover security gaps caused by lax security measures. Many hackers and security consultants are aware of the standard IDS rule set, including typical threshold values, despite it being doubtful that they have complete knowledge of the rule set of the current IDS. They build their penetration technique around getting around the standard IDS setup. The test should aid in locating weaknesses in IDS thresholds, signatures, or rules. (Hessa Mohammed Zaher Al Shebli, 2018)

Various types of testing are:

- External and Internal testing
- Blind and double blind testing
- Router penetration
- Firewall penetration
- Application penetration
- Password cracking

Tools used for penetration testing:

- Nmap
- Metasploit
- BeEF(Browser exploitation frame work)
- Nessus
- John the Ripper

❖ When there is a professional team doing the penetration test, everyone is aware of their roles and responsibilities as well as what needs to be done and how. A person engaging in a penetration test may run into a number of ethical and competency problems when working on the system or protocol. A large omission or explicit inclusion could be hazardous to the organisation. To satisfy the needs of the customer and thereby guarantee that the tests do not produce false or deceptive issues, tester staff always adhere to ethical and regulatory requirements. Although professional groups have established codes of conduct and best practises, it is frequently necessary for test takers to make decisions on their own, thus they should have the requisite procedural, ethical, and technical training such as

• IEEE, 2010
• IEEE Computer Society IEEE CS
• BCS British Computer Society
• BCS - The Chartered Institute for IT, 2010
• BCS Information Security Specialist Group
BCS-ISSG
• Institute of Information Security Professionals
(iisp)

The common codes of conducts for technical competency are:

✓ EC Council or EC Council, 2010
✓ ISC2 code of ethics of The ISC 2 code of Ethics (Hessa Mohammed Zaher Al Shebli, 2018)

❖ An advanced perpetual threat the (APT) is the form of cyber attack which uses to continuing, stealthy, & advanced cyber tactics to enter the system and remain there for a long time while potentially doing harm. APT is the kind of attack that needs to be on every company's mind. This doesn't though, imply that small and medium-sized businesses can ignore such a barrage APT attackers frequently leverage smaller businesses that add to the supplies of their final objective to get access to large corporations. Due to the fact that they are frequently less well-defended, they exploit these companies as stepping stones. Cybercriminals commonly get access through spam emails, networks, files that are attached, and application vulnerabilities to install malware onto a target system, just like a thief would do with a crowbar to pry open a door. Cybercriminals use malware to create a collection of tunnels or backdoors that they could use to covertly access computers. Malware commonly employs strategies like code rewriting to help hackers disguise their

tracks. However, the attackers may have left multiple security holes open, allowing them to return anytime they choose, when APT activities are discovered and the immediate risk appears to have subsided. Other targets might be organizations involved in the transmission of power and telecommunications services, and other crucial infrastructures, social networks, media outlets, and election and other political objectives. Threats may be funded by criminal organizations in order to gather information they can use to commit crimes for financial gain. Even though APT assaults are difficult to detect, data leak is never completely untraceable. Another characteristic of sophisticated determined to overcome is their emphasis on creating numerous sources of entry. To sustain access, APTs usually try to establish multiple points of entry into targeted networks. Advanced persistent agents are motivated by a variety of factors. . For instance, attackers supported by nation-states can target copyrights to obtain an advantage in a select few industries.

## 6. COST EFFECTIVENESS

The security objectives of intrusion detection systems (IDSs) must be maximised while expenses are kept to a minimum.While intrusion detection and prevention systems monitor network traffic, anti-malware software examines files. They are able to identify malware, violations of policy, and other threats. It could take the shape of hardware or software. IPS & IDS are each responsible for a variety of duties. IDS are a reliable method that discreetly scans the network, identifies, and categorizes potential threats. Malware commonly employs strategies like code rewriting to help hackers disguise their tracks. With IPS, those duties can be completed, but they can also be utilized to thwart attacks. Suspects could be followed by certain intrusion detection systems (IPS).

Since the tools used in reconnaissance are open source. So it is free of cost. Cost for tools used for monitoring, encryption, vulnerability testing, training given among employess ,attaining certifications is approximately $2500. Also there is cost for giving training among employees and to attain certifications. As opposed to typical operations, which will use more expensive equipment at optimal efficiency, disruption activities must require certain high grade types of equipment. The equipment, which includes hardware, software, and training resources needed to secure networks, is intended for the defense and security to offer justification based on the equipment.

It is difficult and crucial to study cost-sensitive modelling for intrusion detection. The creation of a framework for examining cost factors and creating cost-sensitive models is one of our study's main contributions. (Lee et al., 2002)

# REFERENCES


Bejtlich, R. (2013). *The practice of network security monitoring : understanding incident detection and response*. No Starch Press.

Chauhan, P. (2021). *Assessment of Forensics Investigation Methods*.

Djufri, F. I., & Lim, C. (2021). Revealing and Sharing Malware Profile Using Malware Threat Intelligence Platform. *ACMIT Proceedings*, *6*(1), 72–82. https://doi.org/10.33555/acmit.v6i1.100

Hessa Mohammed Zaher Al Shebli. (2018). *A Study on Penetration Testing Process and Tools*.

Lee, W., Fan, W., Miller, M., Stolfo, S. J., & Zadok, E. (2002). Toward cost-sensitive modeling for intrusion detection and response. *Journal of Computer Security*, *10*(1-2), 5–22. https://doi.org/10.3233/jcs-2002-101-202

mandal. (2016). *A Survey on Network Security Tools for Open Source*.

patil, & Jangra, A. (2017). *Ethical Hacking: The Need for Cyber Security*.

Sanders, C., & Smith, J. (2014). *Applied network security monitoring : collection, detection, and analysis*. Syngress, An Imprint Of Elsevier.

Verma, G. (2020). *Splunk vs ELK : Security, Scale and High Availability Perspectives*.