Red Team Engagement: Penetration Testing Methodology, Routine Assessments, and Keylogger

Dr. Parkavi K [1], Mohamed Ibrahim[2]

[1]*Assistant Professor Senior, School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India*

[2]*Student, School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India*

Abstract

This research talks about the three teams, the red team, the blue team, and the purple team in brief. The red team blueprint is discussed in detail highlighting penetration testing methodology, scope identification, metrics, routine assessments, PE Files & DLLs, and the red team sample report. A red team runs a vulnerability scan, identifies the services that are vulnerable, and reports them. The red team exploits the actual issue to determine whether the vulnerability is genuine, how it impacts an organization, check new exploits, and if they can fit into an organization. There are a wide variety of types of assessments like phishing, password cracking, external penetration testing, internal testing, network segmentation testing, etc. Red team simulates internal external threats, such as employees hacking into the system or hacking from a faraway nation, and attempts to simulate both sides. The blue team's role is to identify, detect, and respond to any threat that the organization faces from insider and outsider-based attacks. The blue team addresses security concerns such as breaches and compromises, access control failures, and all other events that could generate a security-based alert that has to be examined. In most cases, they operate 24 hours a day, seven days a week by having multiple groups in different time zones cover an hour-by-hour basis. The research created multiple dimensions of red team effectiveness from the perspectives of the client, management, and team members.

Keywords: *Penetration Testing Methodology, Routine assessment, Metrics, Keylogger, Red Team.*

I. INTRODUCTION

This module will focus on the three teams, how effectively they work together, and what their goals are. The three teams are the red team, the blue team, and the purple team. The red team and blue team will highlight a broad overview of what the team does on a high level and how they interact with each other. The purple team is an exception in that it is not a physical team with a manager, director, and so on. The three teams are critical when analyzing a company's security posture from both an engineering and an attacker's perspective.

1.1 Red Team

In a nutshell, the role of the red team is to find and exploit flaws in an organization's environment. The red team conducts a vulnerability scan, identifies vulnerable services, and reports them. They proceed to test the actual issue to check whether it is real. The red team mimics external and internal threats, such as staff hacking into the system or hacking from another nation, and attempts to simulate both sides.

In certain circumstances, phishing is handled by the red team, which handles awareness training, what one can and cannot do, what went wrong, how to fix it, and so on. Additionally, testing the organization's response to active threats, whether in an engagement or not, may result in blowing off alarms in the blue team. In some cases, the red team would want to test something without informing the blue team. A good red team must understand the defensive side as well as the offensive. The problem arises when many people come up with the offensive side. However, to be well around it need to be able to understand what could exploit the issue. It is important to be well-grounded in terms of offensive and defensive strategies. The intuition detection system and alerting software will alert the blue team and they must be aware of the situation ahead of time.

There are a lot of reasons why a red team is needed. In most events, assaults, data penetration, and exploitation might occur to an organization that is able to intervene and determine if it is a threat or not. Realistically test the scope of an attacker's effectiveness. If permitted through, and assuming the development team does not consider it a major concern, it must be verified. There are several methods for obtaining authenticated access to a web app. Relying on something behind the authentication is not necessarily a good spot end. Just because have access to that, exploiting it will be able to get an execution on the machine from that machine will get access to the network. As they have access to it, they will be able to achieve an execution on the system from which they will get network access.

Table 1: The team structure of a red team

Level	Size of Employees
Director	1
Senior Manager	2
VP	2
Manager	2-3
Lead	3
Mid-Level	3-4
Entry-Level	1-2

Is the red team required? In a larger organization most definitely yes. There are just too many moving components, developers piled on top of each other, and far too much that can go wrong in an organization. A red team may not be necessary for smaller firms of 50-100 employees since a single person may manage software development, network administration, and security. Table 1 shows a more generic structure for an ideal red team in general; the size of the team may vary based on the organization's size. This is a suitable team structure for a large-scale corporation with a team of 10000-15000 employees. Most entry-level red team members have worked as system administrators, IT service desk personnel, and so on before joining the red team.

1.2 Blue team

In a nutshell, the blue team's job is to identify, detect, and respond to any threat that the firm confronts from an insider or outsider-based attack. They manage all security concerns involving breaches and compromises, access control failures, and anything else that might generate a security-based alert that has to be investigated. In most situations, they function 24 hours a day, seven days a week by having numerous groups in different time zones cover an hour-by-hour basis. Alternate names are Security Incident Response Team (SIRT) and Security Operations Center (SOC). Generally, the blue team covers SIRT and SOC core names. A blue team provides an organization with real-time protection. They serve as the first line of defense against both internal and external threats. They contain, analyze, and mitigate threats to an organization whether there is new malware that comes up, present malware, or harmful executables being rated. They are also in charge of antivirus, static analysis, and so forth. Depending on the compliance requirements, the customers sign Service Level Agreements (SLA) for notification of breaches or issues with patches, and it is critical for a blue team to be present.

Table 2: The Team Structure of a Blue Team

Level	Size of Employees
Director	1
Senior Manager	1-2
Manager	1
VP	1-2
Lead	2-3
Mid-Level	4-8
Entry-Level	5-15

Are they required? There may not be many complaints or requirements in smaller firms; 1-2 individuals on the security team can address them. For larger organizations, there is too much work in response that the red team and the system administrator cannot handle and they are essential. Often the depth of the blue team is a special skill set as compared to a red team. The team structure again depends on the size of the organization. A lot of big organizations tend to use rotation on contractors, they may have 5-10 different contractors that need to be on rotation, so they start a year, and when a contractor is over, they either renew it or give them a full-time offer or let them go. This enables the cycle of talent that comes through. This is significant because a lot of individuals tend to move up fast within the business with that skill set, and perhaps may even be able to shift to the red team because they work so closely. The blue team is substantially larger, with many more security analysts on standby to handle day-to-day data activities.

1.3 Purple Team

The red team and blue team work together in an organization to form a purple team. This is a growing term in the industry right now. People are trying to learn about the purple team inside the organization, which is a good combination between the red and the blue team. The organizations will use an email distribution list that one can contact the purple team directly. There is something called a detection feedback loop, which is extremely important, not just for detection, but the feedback loop in general. In a sense is the ability to take an action, respond, and reaction. The detection feedback loops the blue team has put the protection for logging in to any malicious software and notify them about a specific command. The red team then comes in, makes an adjustment to the commands, and reports that back to the blue team, takes the response and tries to fix the problem, then goes back and forth. This is called detection feedback, which also feeds into system improvements.

A blue team does not include any red team members. There may be a few individuals in the team that will experiment on their own, but in general, blue team members do not prioritize team participation or activities. The factors that the red team members will look out for, much like the blue team, are to create a specific command, because the command process of elevating from a standard user to an administrator is dependent on it. Consider the red team going on an engagement and identify a specific technique to elevate privileges, such as a certain command or password file that was alerted. That is a good reason for the feedback loop and that's kind of why both teams are needed. The detections are live and real, as far as concerned an internal person, an external or the red team will monitor throughout the process. There is also something called replay where the red team will sit down with the blue team and start a purple team aspect and run through the entire engagement from start to finish. They go through everything that was done, every command or tool that was used, step by step. Till they complete the entire engagement in which everything should be detected during the form. This process happens on a monthly or semi-monthly basis. In some cases, there is a simulation of phishing engagement where testing a specific point is taking place, and the blue team is aware of this. The final step is training this is the blood, sweat, and tears of the purple team along with the feedback loops it is the training aspect. The purple team teaches a specific job, such as static analysis, building roles, executing service, or handling phishing engagements. There is a lot of training that happens here.

II. METHODOLOGY

2.1 Penetration Testing Methodology

Penetration testing methodology is a set of procedures or steps that are performed when doing an assessment or engagement. A red teaming assessment must first confirm that all tests completed during a month and the same test conducted the next month fall under the same parameters. It is critical to follow the methodology and practices for red team engagements to go well. As a result, auditors should be able to determine whether a framework was put in place in response to a high-level executive. A framework is another approach to talking about technique since it prevents missing important details such as the reporting, and scanning of a particular target. The methodology illustrated in figure - 1 is a proven and tested model. There are a thousand different ways to use different methodologies. But in a general sense, it will cover all the aspects at some point throughout the test.

Figure 1. Methodology of Penetration testing

What is a goal?

The first stage involves determining the scope and goals of the actual assessment or engagement. In this scenario, the goal is to identify the outcome of the test or interaction as well as the sub-goals. For example, consider segmentation testing and firewall rules on the reverse side of it. Within the primary evaluation, which is checking segmentation, there may be sub-goals. Followed by corporate testing it is important to identify what one is aiming to look for in a particular test. The goal is to portray to a larger audience. In some cases, might be working on a network segment and Docker containers as well. Entirely depends on the situation and reporting style of the company work for whether it is a consultant or an agency.

2.1.1 Scope Identification

Scope identification in a nutshell is being able to understand a wide variety of options that could go into a place with an engagement. To get to know what the end goal happens to be, one needs to get notified that the test is about to occur. If any stability or service considerations must be taken into place, such as a Java service being taken specifically finicky about receiving traffic, that would be something one would want to take into consideration in the scope identification phase. Scope identification is more of the paperwork side of things, there needs to be a paper trail around the assessments for a freelancer or consultant.

2.1.2 Reconnaissance

Reconnaissance is used to gather information about a specific target, also known as recon. When going through the penetration testing process, being able to understand what information is relevant and what is not. Is important to gather as much information as possible and never know what is

needed to make an attack work [6]. And could be something just as small as an employee posting on a different form about a specific topic using their corporate address to lay down fishing attempts or whether it is gaining information about a particular service that might be running in its version through the banner. There are two types of reconnaissance passive and active. Passive reconnaissance is not touching the target such as not doing port scans, or trying to not manipulate the site in any way when using Google, Netflix, or any other third-party elements. The key is not to leave a footprint that can be seen as an attacker. One may not want to throw off any flags, should just look like a normal user around the world trying to use the service and should not be poking at the system directly.

Active reconnaissance is where interfacing with the target directly by running a port scan, banner grabbing, and connecting the services. One must make sure from being detected by the blue team. In some engagements or assessments, one might need to do this but, in some cases, one need not do it, depending on the requirement based on the scoping. One needs to make sure to pull it back just a little bit and keep it into consideration. Throwing a giant port scan across the whole network segment is a good way to give routine notice. Physically touching the site and browsing the site is a grey line. If one is just browsing the site and reading some text around it and not going to the directories. That could be labeled as passive or active. But it is important to understand the difference between the two. Because one must remember to do the passive reconnaissance first, which helps narrow down the active reconnaissance. Active reconnaissance can get deep, quickly, and have as much information about where one can start targeting as possible.

2.1.3 Exploitation

Exploitation is attacking the host and gaining access of some kind, validating the findings that as found in the reconnaissance space, exploiting the target, and then ensuring the stability of the exploits as well. There is also a scope identification phase, one should know what services they are attacking or an attack. That will have a better effect on the stability of the system.

2.1.4 Post Exploitation

Post exploitation in a nutshell is around the task of gaining full access to the machine. Starting from low-level user access to full admin or route access. The post-exploitation is considered the privilege escalation phase. One wants to get into persistence on the machine, to make sure they do not have to re-explain a service that may have crashed and be able to get onto the box again quickly without any issues. Moving laterally is part of this as well, and might gain access to a host. But from an attacking perspective must have a foothold in the network being able to scan different machines. Depending on the engagement where a user wants to have the logs, reporting tools can alert the management to what a user is doing. Must hide the persistence whether that is through a rootkit or OS level. It is important to clean up depending on the engagement, and not leave a foothold for somebody else.

2.1.5 Reporting

The audience reporting to, whether that’s executives or another red teamer, one must understand to create reports for different audiences, the feedback loop depends on it. Prioritizing business risk based on the report is necessary to decide what systems to construct, detection, patching systems, etc. Depending on where the system was located, remote code execution may be more common in organizational situations but not in others.

III. PROPOSED MODEL

3.1 Sample Red Team Report

One can always acquire a template if they are just starting off on a red team. There are quite a few companies, like Offensive Security, Packetlabs, Framework Security, etc. that all have a nice template, illustrate what and can always take that adjustment if it is necessary and construct it from scratch, depending on what users want to achieve. The crucial point is that when a business pays a contractor or even an internal red team they are paying for its expertise and the assessment's final conclusion. At that moment, the consumer is merely handed the report. It is necessary to ensure that the report contains all that the customer need, but it should not be so extensive that everyone becomes disoriented. There is no reason to create a report of 60-100 pages unless absolutely necessary. The report should be user-friendly to read, summarise the interaction in several different ways, and assess the risk.

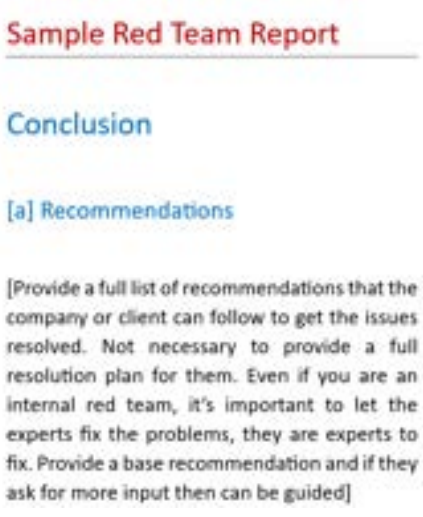
[a]

[b]

[c]

[d]

[e]



[f]

[g]

Figure 6. The sample section on [a] Title report [b] Table of Content [c] Executive summary [d] Summary of Results [e] Attack details [f] Recommendations to the Company or Client [g] Risk associated with the Test.

Consider the red team sample template shown in figure 6 [a] the firm logo, what kind of report it is, and when the report was prepared must all be included on the first page. Then following this in figure 6 [b] table of contents contains an executive summary, the summary results, and then attack details, which goes over the actual attack. The conclusion should therefore include both the risk and the recommendations. The executive summary in figure 6 [c] is where the report will be reviewed at the executive level. The executive may not be the technical officer, but rather from a management perspective. May attempt to avoid using as many technical terms, phrases, or sentences as possible.

It must be easily consumable from any position of leadership, regardless of technical competence. A brief overview of the extent of what was discovered and the conclusion, as well as some fundamental hazards, should be provided. Following this summary of results in figure 6 [d] must contain a higher-level overview of the report. Chief Executives may be the ones who ask for the report, but the true beneficiary is the one who fixes the problem. The overview should encompass the entire scope from top to bottom without delving into detail about each command, as well as a slew of screenshots. The reconnaissance portion follows, including details on how the system was attacked, what was compromised, and whether there was lateral movement.

Figure 6 [e] contains the real details about what commands were run, screenshots, and all the steps and details needed for the admins on the technical team to retrace the steps to replicate the attack. This is where red team engineers will spend 90% of their time working. The report could be 60 to 70 pages lengthy, with a 1-page executive overview, a 2-page summary of observations, and the rest dedicated to attacking details. The conclusion and recommendation are then presented in figure 6 [f] and figure 6 [g]. In most cases, the red team, or the consultant, is not going to be the expert in the particular service or system. There are professionals on the teams responsible for running such services within the business who must be able to perform the necessary repairs. Can direct what the problem is and the standard recommended fix, after which they will figure it out. In a standard situation, there are two types of audience technical and non-technical. On the technical side, there are engineers, service owners, and individuals who will fix the issues discovered. On the non-technical side, there are executives, managers, program managers, and executive summary readers.

Completely relies on whom the report is going to be presented to once it has been completed. Explaining a technological problem to a non-technical person is a valuable ability. This ability cannot be acquired by online research and browsing on the internet; one must really get out and present to people. For example, one can choose analogies that behave similarly in the actual world and that everybody can connect to, and then try to describe them based on that. This is more of a social skill than a technical skill, one must be able to convert technical to non-technical based on the audience, to resolve the issue.

3.2 Keylogger

A key logger is spyware or surveillance software, which is used to track all the activities of a particular user. It can record a keystroke if a user is typing on his keyboard, and with the help of a key Logger, can also take a screenshot of that system. Key loggers are very advanced and are capable of recording internet history. In the targeted system install the key logger, which can monitor all the activity of a particular user. Keyloggers are helpful for parents to monitor their children on the internet platform. Key loggers are available for Windows, Linux, Mac, and Android.

Figure 7. Main menu of a keylogger

This is the primary menu of the keylogger from which one can capture keystrokes by just selecting that user. There is currently only one user on the system.

```
root@kali: /var/www/html

┌──(root㉿kali)-[/var/www/html]
└─# ls
shell1.php

┌──(root㉿kali)-[/var/www/html]
└─# cat shell1.php

<?php
eval(base64_decode(Lyo8P3BocCAvKiovIGVycm9yX3JlcG9ydGluZygwKTsgJGlwID0gJzE5Mi4xNjguMC4xMDgnOyA
kcG9ydCA9IDQ0NDQ7IGlmICgoJGYgPSAnc3RyZWFtX3NvY2tldF9jbGllbnQnKSAmJiBpc19jYWxsYWJsZSgkZikpIHsgJ
HMgPSAkZigidGNwOi8veyRpcH06eyRwb3J0fSIpOyAkc190eXBlID0gJ3N0cmVhbSc7IH0gaWYgKCEkcyAmJiAoJGYgPSA
nZnNvY2tvcGVuJykgJiYgaXNfY2FsbGFibGUoJGYpKSB7ICRzID0gJGYoJGlwLCAkcG9ydCk7ICRzX3R5cGUgPSAnc3RyZ
WFtJzsgfSBpZiAoISRzICYmICgkZiA9ICdzb2NrZXRfY3JlYXRlJykgJiYgaXNfY2FsbGFibGUoJGYpKSB7ICRzID0gJGY
oQUZfSU5FVCwgU09DS19TVFJFQU0sIFNPTF9UQ1ApOyAkcmVzID0gQHNvY2tldF9jb25uZWN0KCRzLCAkaXAsICRwb3J0K
TsgaWYgKCEkcmVzKSB7IGRpZSgpOyB9ICRzX3R5cGUgPSAnc29ja2V0JzsgfSBpZiAoISRzX3R5cGUpIHsgZGllKCdubyB
zb2NrZXQgZnVuY3MnKTsgfSBpZiAoISRzKSB7IGRpZSgnbm8gc29ja2V0Jyk7IH0gc3dpdGNoICgkc190eXBlKSB7IGNhc
2UgJ3N0cmVhbSc6ICRsZW4gPSBmcmVhZCgkcywgNCk7IGJyZWFrOyBjYXNlICdzb2NrZXQnOiAkbGVuID0gc29ja2V0X3J
lYWQoJHMsIDQpOyBicmVhazsgfSBpZiAoISRsZW4pIHsgZGllKCk7IH0gJGEgPSB1bnBhY2so.Ik5sZW4iLCAkbGVuKTsg
JGxlbiA9ICRhWydsZW4nXTsgJGIgPSAnJzsgd2hpbGUgKHN0cmxlbigkYikgPCAkbGVuKSB7IHN3aXRjaCAoJHNfdHlwZS
kgeyBjYXNlICdzdHJlYW0nOiAkYiAuPSBmcmVhZCgkcywgJGxlbi1zdHJsZW4oJGIpKTsgYnJlYWs7IGNhc2UgJ3NvY2tl
dCc6ICRiIC49IHNvY2tldF9yZWFkKCRzLCAkbGVuLXN0cmxlbigkYikpOyBicmVhazsgfSB9ICRHTE9CQUxTWydtc2dzb2
NrJ10gPSAkczsgJEdMT0JBTFNbJ21zZ3NvY2tfdHlwZSddID0gJHNfdHlwZTsgaWYgKGV4dGVuc2lvbl9sb2FkZWQoJ3N1
aG9zaW4nKSAmJiBpbmlfZ2V0KCdzdWhvc2luLmV4ZWN1dG9yLmRpc2FibGVfZXZhbCcpKSB7ICRzdWhvc2luX2J5cGFzcz
1jcmVhdGVfZnVuY3Rpb24oJycsICRiKTsgJHN1aG9zaW5fYnlwYXNzKCk7IH0gZWxzZSB7IGV2YWwoJGIpOyB9IGRpZSgp
Ow));
?>
```

Figure 8. PHP code of the Keylogger

```
root@kali: ~/Test

┌──(root㉿kali)-[~/Test]
└─# cat index.html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /</title>
 </head>
 <body>
<h1>Index of /</h1>
  <table>
   <tr><th valign="top"><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Na
me</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><t
h><a href="?C=D;O=A">Description</a></th></tr>
   <tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="shell1.php">s
hell1.php</a></td><td align="right">2023-03-02 12:40  </td><td align="right">1.5K</td><td>&nbs
p;</td></tr>
   <tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.55 (Debian) Server at 192.168.0.108 Port 80</address>
</body></html>
```

Figure 9. The HTML code of the Keylogger

Figure 10. General properties of a keylogger

If inputted anything on the keyboard, it will record keystrokes and store them on a USB device. It can also record Skype conversations and texts. A snapshot also saves the browser's history and search terms. If a user wishes to ensure that no one can access the key logger, he or she can protect the key logger by setting a password. The file will be saved on the local desktop by the key logger. After 15 days all files will be deleted.

Figure 11. The properties of a keylogger on screen capture

The screen capture option will snap a screenshot of a user's PC after a certain interval.

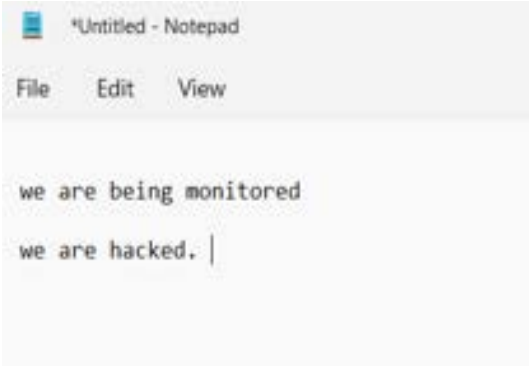


Figure 12. Notepad with random text

Now in order to verify, let us open notepad. Write here, “we are being monitored” and “we are hacked” and close the notepad file in order to check whether the keylogger is storing the data. There are two options here: either stop the keylogger and check or move directly to the local directory where the keylogger is stored. The key logger stores all the data in an HTML file.

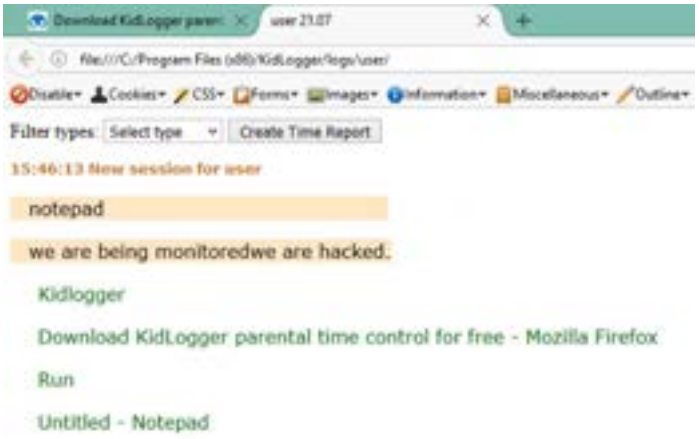


Figure 13. Keylogger default option

During the procedure, the notepad was used, data was written on the notepad, and Mozilla Firefox was utilized, which is displayed on the screen. The keylogger takes a record of all the applications which are being run. This is the default option can select the type.

Figure 14. Keylogger filter-type application

The type of filters may be seen at the top. There are multiple filters, if clicked on the applications it will show all the applications that the person has launched. If used Skype chat, then can take the record messages, but currently, there are no messages. This is how a standard key logger works.

IV. CONCLUSION

This research presents a brief idea about the red team, blue team, and purple team. Red teams are “ethical hackers” who help test an organization's defenses by identifying vulnerabilities and launching attacks in a controlled environment. Red teams are opposed by defenders called blue teams, and both parties work together to provide a comprehensive picture of organizational security readiness. Red team tests are designed to expose vulnerabilities associated not only with security infrastructure (networks, routers, switches, etc.) but also with people and even physical locations. During red team testing, the security environment is defended by a “blue team,” which is generally comprised of the security professionals who are normally tasked with the protection of the organization’s infrastructure and assets. Because they are intimately familiar with organizational defenses and security objectives, their goal is to raise the level of defense and avert unfolding attacks. Then have proposed a model for a keylogger, a keylogger is a spyware, which is used to track all the activities of a particular user. Key loggers are very advanced and are capable of recording internet history. In the targeted system install the key logger, which can monitor all the activity of a particular user. The proposed model can be useful for parents to monitor their children in a cyber environment.

V. REFERENCES

1. M. A. Vatis, “NIPC Cyber Threat Assessment”, National Infrastructure Protection Center (NIPC), 2021.
2. B. Wood and R. Duggan, “Survivability Information Systems Red Teaming Analysis Results”, October 2019.
3. Sally Adee, “The Hunt for the Kill Switch”, IEEE Spectrum Magazine 2021.
4. Swanson Marianne, Nadya Bartol, and Rama Moorthy, “Piloting Supply Chain Risk Management Practices for Federal Information Systems”, National Institute of Standards and Technology, 2020.
5. Adam Waksman and Simha Sethumadhavan, "Silencing Hardware Backdoors", IEEE Symposium on Security and Privacy, pp. 49-63, 2019.