A New Deceptive Tactic aims better Cyber-Solutions for organizations during Global Pandemic

Vatsal D. Raychura[1], Chandesh D. Parekh[2]

[1]*M. Tech, School of Information Technology & Cyber Security, Raksha Shakti University*

[2]*Dean, School of Information Technology and Cyber Security, Raksha Shakti University, Lavad, Gandhinagar, India*

Abstract- **The use of data Technology (IT) resources are the regular approach for many organizations in order that they assets and belongings are properly managed. This strategic decision implies its exposure to the surface world through the info infrastructure. Nowadays when the whole world is trying to being strong against this pandemic, The Organizations wants to shield themselves against these expanding attacks risk by implementing security strategies, but in point of fact, the network's first & main defense lines are pervious, and therefore the security architectures don't seem to be dynamic enough to face existing or future threats. NOC, SOC etc. type of services may help you to find cure after the system is affected, but the real threats are always innovative with time, so that the threat detection system may be quite accurate against future threats with the assistance of deceptive model. A Deception-based technology could enable the organizations to quick & easy detection, in order that is easy for analyzing and defend networks & whole system against real-time attacks. Deception technology may provide more accurate information on malware and malicious activity not detected by the other styles of cyber defense. The research intends to look at whether that Deception Technology is required to sustain a good response to attacks by taking a proactive approach. It can instantly detect the presence of an intruder, identify the intruder's intent, and supply feasible intelligence to prevent current & future attacks against organization. Therefore the intent is to elaborate an anatomy where the industries can understand The Deception Technology its effectiveness, and strategic value so eventually, they will use this system to feature value to a settlement regarding information security strategy..**

Index terms- **Pandemic, Information Security, Deception, Deceptive Tactic, Data infrastructure, Cyber-threat, Intruder.**

I.INTRODUCTION

Security is the most crucial part of IT sector's progress. The security parameters like Network security, Cloud security, System security. But additionally the cyber-crime trend is increasing, the number of "zero-day" vulnerabilities reported exposes how vulnerable the network perimeter is even with an aggressive patching policy. All the available information lead to the assumption that the organization's first line of defence is not performing as expected, allowing the attackers continuous access to assets and intellectual property impacting the organizations at a brand and financial levels.

Today when the main problem for any organization's security is that cyberspace attacker's techniques are dynamic as they have large community of experts in support and can attack from anywhere from the world, so that how to build a defending system which cannot only help to detect the threats again system but also can give enough time to be prepared against attacks possibility by having prior information about the attack's type as well as attacker's prior information and basic technicality knowledge of the attacker might want to get into the system. The lead time between an attack and the detection of that attack, by the security team of organization, are immense, if ever. The disruption provoked by the cyber-incidents affects everyone from life support devices to financial organizations especially when every single person is trying to work from home this time how to make network system strong to infiltrate by an attacker.

Hackers are already knocking on virtual gateways, trying to find new entry points to be exploited even in this global crisis, resulting in more cybersecurity challenges for both organizations as well as individuals. Focusing on the first one the main Objective of this paper is to identify an organization’s Security against the current (& also future) threats even when working from home is the mandatory.

Also this new era offers increased third-party risks, especially when everything we do becomes web-based and validates higher online dependency. These are troubling security encounters, but there are effective solutions that already protect against these risks and focusing on that, this paper proposed the new and easy approaches to find solutions using new deceptive models which could make the organization’s network architecture more powerful.

II. LITERATURE REVIEW

By reviewing various literature about the identical concept of Deception technology it's a great deal clear that the deception allows you to form an illusion for attackers that they need found something of interest in your environment. [1]When you deploy intruder traps on your network, they act as a virtual trip wire. Once an attacker is tricked into accessing the trap, alert is generated for the suspicious activity.

While using Deception for real time in your system [2]high-fidelity alerts are raised based upon attacker decoy engagement or deception credential reuse. Each alert is substantiated with rich threat intelligence and is actionable, removing false positive and noisy alerts that distract from the prompt incident response of real threats.

There are some kinds of stealthy behaviour which might be difficult to discern from normal activity, these may allow the attacker to sneak past the safety tools into organization undetected. So as the simplest way to distract attackers placing intruder traps can often help to search out attackers earlier and take action to dam them before they access something they must not.

An assumption exist that [3]Deception Technology mechanisms may improve deception and mitigate the results of Advanced Persistent Threats. Decoys and Honeypots are accustomed divert the attackers removed from actual system information. Some key methods utilized by Deception Technology are immediate detection of malware, real-time alert of an attacker, identifies hacker techniques, and tracks the hacker’s every move.

III. DECEPTION TECHNOLOGY

Deception technology may be an important integral of cybersecurity services. It’s helpful for the organization in preventing any cybercriminal activity that has successfully managed to infiltrate a network. Wondering how deception technology will work? Well, the technology work by generating traps and deception decoys that imitates authentic technology assets and/or lures which are mixed among and within existing IT resources to produce a layer of protection to prevent attackers that have penetrated the network. [4]Traps (decoys) are IT assets that either use real licensed OS software, or are emulations of those devices.

Goal of Deception:

Goal of deception captures the most purpose a particular deception technique is trying to attain. [5]This could be either to boost and complement attack detection, to reinforce prevention, or to mitigate successful attacks. the primary category includes those solutions designed to detect an attack, typically because it interacts with active traps or because it uses passive decoy information that are intentionally left accessible to be discovered by the attacker . The second category covers instead those mechanisms that aim at confusing or distracting attackers from the important targets before an attack occurs. Finally, the last category targets on-going attacks and tries to scale back their damage, for example by replying in an exceedingly delayed manner or by redirecting attackers to a secure copy of the target system.

Deception technology [6] is categorized into three basic classes of capability.

- Legacy Deception technology has been around for years and utilizes the notion of hand deployed and individually implemented traps.
- Basic Deception technology added some automation and reporting around honeypots. During this case, the operating systems and vendor applications must still install manually; this feature isn't practical for wide scale or widespread deployment.
- Advanced Deception technology utilizes automation deploy a broad network of emulated

computers, servers and in some cases devices (Supervisory Control and Data Acquisition (SCADA) industrial control systems, medical devices, then forth) and places these throughout your network.

About the infrastructure, the deception decoys can run in an exceedingly real operating environment or a virtual space. It'll bring the cybercriminal into a confidence that they need actually hit the target of stealing the credentials or info. The deception technology, when successfully registers a trap, it notifies the centralized system and therefore the affected decoy is put to record.

Why Deception Technology?

- Early detection of the cybercriminal activities
- No damage to the particular data or server
- Flawless scale and automation
- Suitable for all variety of organizations
- Helps with one step prior security level

IV. NEW DECEPTIVE TACTIC

This new Deceptive tactic is specially designed for the organizations better future even during the hard time of global pandemic, for the better cyber solutions and secured system there are so many methodologies to follow but all of them have to be redesign due unknown threats coming to the system even when the people are not present at the organizations itself, even the attacks could be more serious with least of preventing approaches during work from home time.

That's why the new deceptive tactic helps the organizations directly by detecting threats in advance by big alerts and notifications with basic idea of attacking, which could give the prior conditional idea for the defence team of organizations to prevent the system against these threats.

Using Deceptive Approach These are Immediate Tips to Protecting Your System against Threats:

- Keep the Code on Your Servers - So that you can get straight alert when any threat giver tries to attack on your server where your deceptive mode is connected. And because of that attack might automatically mitigate even before the attacker can get the idea of fraud success. (Mainly Using Honeypot)
- Penetration Testing - This makes sure for your system to be prepare more even if the attacker won't be approaching, by Pen Testing your system side by having deceptive model in your system you can get the possible attacks information agaisnts your system.
- Behavioral Analysis - Now this is something organizations security team should check for every perticular time duration, even with alerts on from the deceptive model, one can infiltrate the system using any innovative method, so the Behavioral Analysis might help to find the outsiders fraude approaches on deceptive model(Mainly Using Honeyusers).

Why New Deceptive Tactic During Global Pandemic:-

- Easy To Generate
- Easy To Deploy
- Easy To Operate
- Early Cautionary System
- Actionable Alerts
- Low Upkeep
- Fortifies Defences

V. WORKING DECEPTIVE MODEL FOR VIRTUAL MACHINE

.

There so many ways to setup the new deceptive tactic, from them the basic and most reliable during this hard time are listed here:-

1 Honeypots: Deploy these to hide the maximum amount network as possible (for instance, one for every subnet)

2 Honey Users: Add a user to the Active Directory that matches how you sometimes configure usernames but also conveys it should be a website admin

3 Honey Files: Deploy files that appear to be valuable, like a financial report or something with personally identifiable information (PII)

Various intruder traps can attracts hackers to attack on the system, for Demo of working model here Rapid7's Honey Items are used which could directly access by the authorized person using InsightIDR portal, so that even when organizations security team is working from home they can get easy access for the positive alerts & can take obligatory steps to secure the system. The foremost common form of intruder trap may be a honeypot, [7] which are decoy systems designed to assemble information about attackers on your network and to permit you to find out how attackers are accessing your systems.

Criterion for Rapid7’s Honeypot:-
A honeypot uses the following resources:

a. Required 2Ghz Processor
b. Required the 1 GB Ram
c. Required the 10Gb or More than 10GB disk space

Service Accounts Permission Requirements:
InsightIDR requires that you just configure a minimum of one account in each
Windows domain that has permissions to gather event logs within the domain. Looking on your environment, this account are going to be accustomed collect: It manages all the devices (computers and Laptops) simultaneously.

- Domain Controller Security Logs with the Active Directory event source.
- User and group information from the Windows domain using the LDAP event source.
- Microsoft DHCP logs using the Microsoft DHCP event source.
- Microsoft DNS logs using the Microsoft DNS event source.
- Microsoft OWA/ActiveSync logs using the Microsoft Outlook Web Access/ActiveSync event source.

Software Requirement:

a. Install InsightIDR (By RAPID7).
b. Download the Honeypot OVA from InsightIDR Homepage.
c. Create a new Virtual Machine (VM) from the OVA.

Deception Using Honeypot Working Process:
Honeypots consist watch for "attacker" events to happen, like a port scan or attempted user authentication, which immediately activates an alarm. [8]If you deploy the Rapid7 Honeypot and enable the associated alerts in Insight IDR, you'll be notified if such activity occurs. Once attackers find an initial foothold in a very network, their next step is often a network scan to spot all the opposite assets within the network.

1 “Figure 1”Power on the VM.
2 “Figure 2”Provide a reputation that matches your network naming convention and makes the machine look real & important.
3 “Figure 3”Configure a dynamic or static IP, and/or web proxy for communication purposes.
4 “Figure 4”Take note of the Agent key that's displayed
5 “Figure 5”To activate the honeypot within the InsightIDR interface, navigate to Data Collection > Setup Honeypot > Activate Honeypot.
6 “Figure 6”Fill out the shape and click on Activate
7 “Figure 7”After clicking Activate, you'll see a loading page while the honeypot completes the activation process.
8 “Figure 8”When you see a “last active” message on the honeypot, the configuration process is complete.

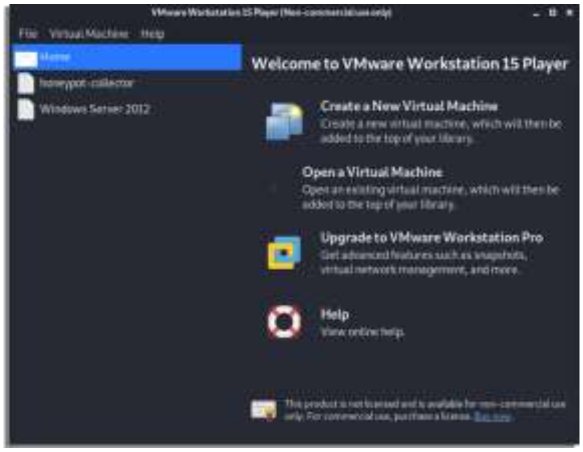
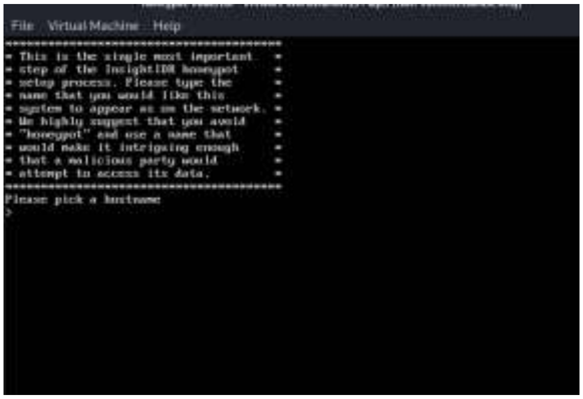
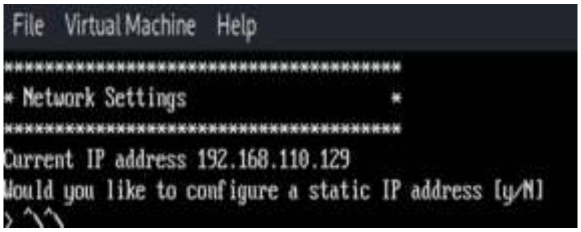

VMware Workstation 15 Player (Non-commercial use only)
File Virtual Machine Help
Home
honeypot-collector
Windows Server 2012
Welcome to VMware Workstation 15 Player
Create a New Virtual Machine
Create a new virtual machine, which will then be added to the top of your library.
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.
Upgrade to VMware Workstation Pro
Get advanced features such as snapshots, virtual network management, and more.
Help
View online help.
This product is not licensed and is available for non-commercial use only. For commercial use, purchase a license. Buy now

Figure 1



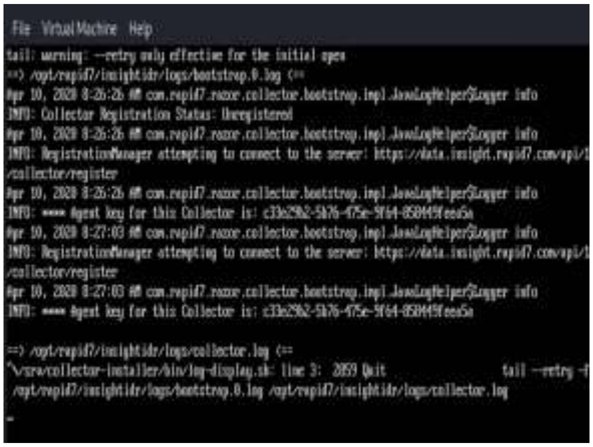
```
****************************************
* This is the single most important    *
* step of the InsightIDR honeypot      *
* setup process. Please type the       *
* name that you would like this        *
* system to appear as on the network.  *
* We highly suggest that you avoid     *
* "honeypot" and use a name that       *
* would make it intriguing enough      *
* that a malicious party would         *
* attempt to access its data.          *
****************************************
Please pick a hostname
>
```

Figure 2



```
****************************************
* Network Settings                     *
****************************************
Current IP address 192.168.110.129
Would you like to configure a static IP address [y/N]
> ^^
```

Figure 3



```
tail: warning: --retry only effective for the initial open
==> /opt/rapid7/insightidr/logs/bootstrap.0.log <==
Apr 10, 2020 8:26:26 AM com.rapid7.razor.collector.bootstrap.impl.JavaLogHelper$Logger info
INFO: Collector Registration Status: Unregistered
Apr 10, 2020 8:26:26 AM com.rapid7.razor.collector.bootstrap.impl.JavaLogHelper$Logger info
INFO: RegistrationManager attempting to connect to the server: https://data.insight.rapid7.com/api/1
/collector/register
Apr 10, 2020 8:26:26 AM com.rapid7.razor.collector.bootstrap.impl.JavaLogHelper$Logger info
INFO: **** Agent key for this Collector is: c33e29b2-5b76-475e-9f64-858449feea5a
Apr 10, 2020 8:27:03 AM com.rapid7.razor.collector.bootstrap.impl.JavaLogHelper$Logger info
INFO: RegistrationManager attempting to connect to the server: https://data.insight.rapid7.com/api/1
/collector/register
Apr 10, 2020 8:27:03 AM com.rapid7.razor.collector.bootstrap.impl.JavaLogHelper$Logger info
INFO: **** Agent key for this Collector is: c33e29b2-5b76-475e-9f64-858449feea5a

==> /opt/rapid7/insightidr/logs/collector.log <==
^\/srv/collector-installer/bin/log-display.sh: line 3:  2859 Quit                   tail --retry -f
 /opt/rapid7/insightidr/logs/bootstrap.0.log /opt/rapid7/insightidr/logs/collector.log
_
```

Figure 4

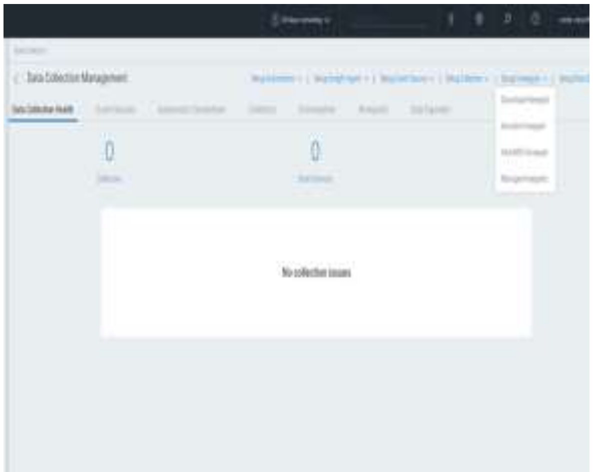


Figure 5

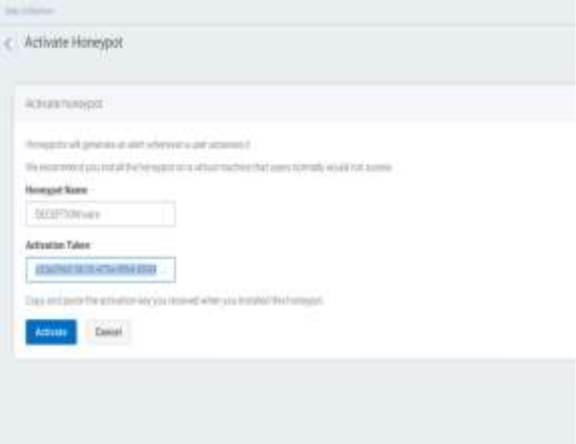


Figure 6

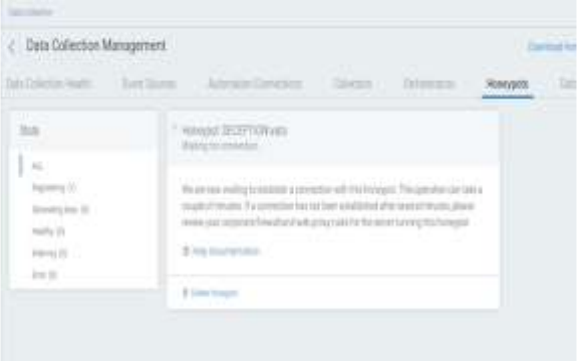


Figure 7

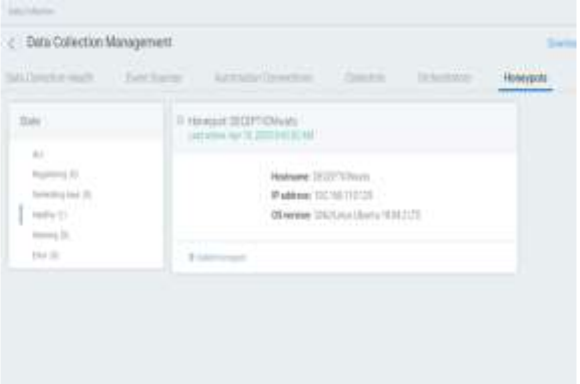


Figure 8

VI. RESULTS

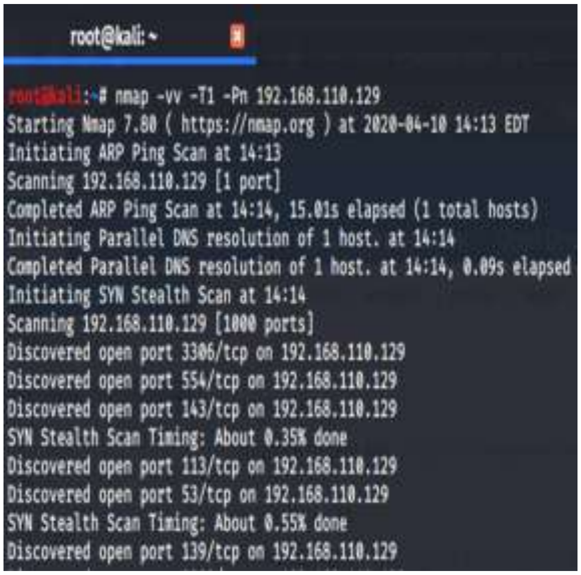
To test the result of demo deceptive model we are going to perform the nmap scan attack from outside the system, and resulting would be captured into our demo deceptive model which could be known by the alert given by the InsightIDR portal and mail also, here in following below steps alert generated on the portal is shown.

1.“Figure 9”Test the Honeypot

- Any access to the honeypot will cause an attentive to trigger.
- A common thanks to test the honeypot is to run an nmap scan, mimicking intruder behavior.
- You could run a regular discovery scan, a vulnerability scan, throw exploits, or try to brute-force the honeypot to trigger an occasion.

2.“Figure 10”After attempting to access the honeypot, wait some minutes then navigate to "Investigations" and verify that you just received a Honeypot Access alert.

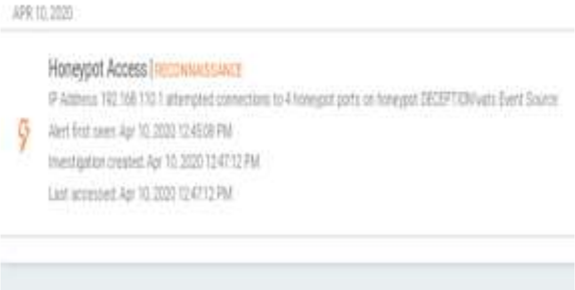
Figures of Test Results:



```
root@kali: ~

root@kali:~# nmap -vv -T1 -Pn 192.168.110.129
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-10 14:13 EDT
Initiating ARP Ping Scan at 14:13
Scanning 192.168.110.129 [1 port]
Completed ARP Ping Scan at 14:14, 15.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:14
Completed Parallel DNS resolution of 1 host. at 14:14, 0.09s elapsed
Initiating SYN Stealth Scan at 14:14
Scanning 192.168.110.129 [1000 ports]
Discovered open port 3306/tcp on 192.168.110.129
Discovered open port 554/tcp on 192.168.110.129
Discovered open port 143/tcp on 192.168.110.129
SYN Stealth Scan Timing: About 0.35% done
Discovered open port 113/tcp on 192.168.110.129
Discovered open port 53/tcp on 192.168.110.129
SYN Stealth Scan Timing: About 0.55% done
Discovered open port 139/tcp on 192.168.110.129
```

Figure 9



APR 10, 2020

Honeypot Access | RECONNAISSANCE

IP Address 192.168.110.1 attempted connections to 4 honeypot ports on honeypot DECEPTIONVats Event Source

Alert first seen Apr 10, 2020 12:45:08 PM

Investigation created Apr 10, 2020 12:47:12 PM

Last accessed Apr 10, 2020 12:47:12 PM

Figure 10

VII. DISCUSSION

Today When Hackers already have made their mind clear to come with full & find new endpoints to be exploited even in this global crisis and the Pandemic likely to be with us for certain period, we can't deny the fact of making some tough decisions as per our individual as well as organization's beneficial Applying innovative tactics like deceptive models for the system is a wise choice, however it could help for threat detection & prevention even in this cybernetic environment.

VIII. CONCLUSION

After the understanding of current requirements of cyber solutions of organizations and for that using new Deceptive Tactic components, behaviour and therefore the position of it on the system security prospect and evaluate the effectiveness when targeted by a cyber threat which materializes into a cyber-incident, one thing is obvious that the new Deceptive Tactic is efficient & well strategic Technology which might help to cut back the Cyber Attacks even from working home's difficult time. The flexibility to deploy easily, detect an intrusion & malware quickly puts this tactic into the primary line of defence in any organization's security model especially when world is facing this preposterous crisis. Also, with the assistance of this Deceptive Tactic, finally the prototype breaks that even after organization's plan and act against several cyber threats, the attackers will bear either by simple human mistakes or a zero-day vulnerability with the understanding and complete their wickedness. So for the top it conclusion line stated as "Deception Works Best When its Real".

IX. ACKNOWLEDGMENT

"If we knew what it was we were doing, it would not be called research, would it?"

"Try not to become a man of success, but rather try to become a man of value." (Miller, 1955, p. 64), I humbly agree with the renowned physicist and Nobel Laureate Albert Einstein quotes and would like to acknowledge everyone that contributed to "my value."

Love values are always comes firstly from my parents who facilitating all the time and availability possible, supporting me all the way.

Professional value from my guide Chandresh Parekh that believed in me and supporting me throughout.

The educational value of the Raksha Shakti University, Lavad and RSU campus, and all the teachers that had the skills and techniques to share their knowledge successfully.

Friendship value from of all my friends that listened to my challenges as their own and gave a true meaning of, "Don't make friends who are comfortable to be with. Make friends who will force you to lever yourself up."

To everyone that contributed to my value and help me with not only as a father, a mother, a person, a professional, a friend or an academic but also a mainstay of motivation for me whole time, I truly appreciated, please have my deepest gratitude.

REFERENCES

[1] Rapid7.com [Internet], www.rapid7.com, “Deception Technology - Tricks, traps, and technology”, Latest Access Time for website is 17 April 2020.

[2] Attivonetworks.com [Internet], www. attivonetworks.com, “Better Detectıon Agaınst Better Attackers - No Alert Fatıgue From False Posıtıves”, Latest Access Time for website is 16 April 2020.

[3] Sophia A. Faulkner, “Looking To Deception Technology To Combat Advanced Persistent Threats”, A Dissertation Project, Utica College. Published by ProQuest LLC (2017).

[4] Wikipedia. Deception Technology [Internet]. en.wikipedia.org, “Deception Technology: High Level View”, Latest Access Time for website is 1st April 2020.

[5] Xiao Han, Nızar Kheır, Davıd Balzarotti; “Deception Techniques In Computer Security: A Research Perspective – Multidimensional Classification”, ACM Comput. Surv., Vol. 1, No. 1, Article . Publication date: January 2019.

[6] António Jorge Palminha P into, “Deception Technology: A Strategic Decision for Information Security”, A Dissertation Project, Management Information Systems (M GIS), European University. June 2017.

[7] Rapid7.com [Internet], insightidr.help.rapid7. com, “Deception Technology – Use Honey Items”, Latest Access Time for website is 17 April 2020

[8] Rapid7.com [Internet], insightidr.help.rapid7. com, “Honeypot – How do they work”, Latest Access Time for website is 17 April 2020.