International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 7, Issue 2
February 2018

Data Science in Cyber Security: Network Security Threat Detection

Sunita Choudhary
Research Scholar
CET, MUST, Lakshmangarh

Anand Sharma
Asst.Prof. CSE
CET, MUST, Lakshmangarh

Abstract: *In this new era of digitalization, cyber-attacks are controlled by creative, intelligent and highly skilled humans. Ongoing synchronization allows an attacker to gradually learn more about the target network, adapt to any defensive measures, and advance the attack over time. If we have not implemented any network security threat detection feeds on our organization, it will reveal the ending of our upcoming gruelling journey. Network security threat detection focuses on individual platforms, systems, networks, endpoints or almost any other IT resource. Network security threats detection is very immature (and uncommon) in actual cyber-security operations. Presently cyber defenders generally discount these approaches in favour of signature detection and intuition. The advancement for this is probably unique, including understanding patterns, risk appetite and decision points. We require a complete understanding of all aspects of the data generation process. Data science will produce technical data that allows for "tactical" discovery of a potential compromise on a system that decide when to block and when to alert on something. This paper aims to implement the concept of data science for network security threat detection.*

Keywords : Data Science, Cyber Security, Threat Detection.

I. Introduction

Cyber security, which can also be said asInformation Technology Security, aims atproviding the protection mechanisms to networked devices, the WWW, various application & programs against unauthorized access mechanisms, security attacks& thefts. It is also defined as the body that encompasses techniques, technologies & methodologies specifically inculcated in order to provide protection to the networks, systems from intrusion accesses. .

Due to the rapid and voluminous growth of cyber attacks , consistent focus is a diligent requirement for the protection of personal data that subjects to sensitivity &business purposes. In order to claim and ensurewe have the imminent need of various cyber elements like Information security, Application security, Disaster recovery & Network security & User Education.

The alarming spread of security risks is a major challenging issue in front of cyber security. Some of the approaches that are in action since the traditional period are as under: CTO public sector (a security service provider to federal agencies including Defence Department organizations) & Adam Vincent have described the problem.

II. Purpose of Attack

Categories of attacks range from intellectual property theft, identity theft and critical infrastructure attacks, tofinancial frauds. It becomes tediouswhile judging the motivation behind the hackers for attacksTheft of credit card information and cyber crimes involving government agencies and public properties has taken the shape of trending interests of hackers.

III. Types of Threats

An attack is generally comprised of two kinds: Active & Passive. Active network attacks observe unencrypted data in order to find out the important and relevant information and on the other hand passive attacks aim atdecrypting the weak encrypted information/data and acquiring the relevant information by making in account of the unsafe network zones. Some of the cybersecurity threats are categorized as under:

A. Advanced Persistent Threats (APT)

The usual targets of an APT are generally

Academic Science
International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 7, Issue 2
February 2018

organizations or country offices for business related information thefts. It is a collection of several techniques of computer hacking that are directed by the hackers to target upon the decided entities.

B. Insider Data Theft

An insider threat is entirely concerned with the institutional information. It is the most harmfulattack to anyinstitutional organization that is run by the normal people like contractors, business associates or employees who directly have access to the relevant sensitive information of that particular institution. And this threat aims at stealing that private information.

C. Distributed Denial of Service (DDoS)

DoS attack tries to create invisible network resources so that users cannot b able to use those resources by shutting down the host services for a limited short period of time.

D. Trojan Attacks

A Trojan horse is one of the most harmful computer attack which misguides the target computer or the target user as a very important information and the user must definitely install it. Trojans are generally spread by internet downloading and uploading and random form fillings on internet.

E. Phishing

Phishing is a hit and trial method to acquire the important and relevant information of any target user like personal passwords, codes and usernames, bank account details etcby befooling as if a trusted and authenticated source or portal .

F. Physical attacks

These attacks basically target the hardware elements of a device or an array of devices. As IoT is an emerging technology that has been in widespread usage all over the globe because of its decentralized and distributed environment. Hence, the devices become more prone to such physical closure and attacks

G. Access attacks

Physical Access &Remote Access are the two major categories of access attacks that are mostly triggered down by the attackers. In a physical access, the intruder harms a physical device by acquiring unauthorised access to it physically whereas in a remote access, the major harm is done to the networked devices using the IP addresses.

H. Zero-day Attacks

A zero day also termed as an attack for security loophole in computer software that is not known to the party on the other end. Without the knowledge of the third party, the attacker tries to access and gain the required information using this particular hole.

I. Cyber-crimes

Cyber crimes involve computers both as a weapon and as a target depending upon the hacker's requirement. These crimes involve

identity theft, brand theft,intellectualproperty frauds, banking thefts etc.

J. Supervisory Control and Data Acquisition (SCADA) Attacks

SCADA system is most prone to several cyber attacks. The various methods in which the system can be attacked upon are:

i. Using Viruses or Trojans to completely take off the entire control of the computer/system.

ii. Using denial-of-service attacks for unauthorised intrusion.

IV. Threat Impacts

Below is the description of what impacts a threat leaves after attacking a system or a network:

A. Corruption of Information

Also called as information tampering. As its name suggests, it harms the information by corrupting the files and also that data which is in transition state on a particular network. Tampering of information means that the actual information or data gets modified in either of the ways, memory(hard disk) can also get affected .

B. Destruction of information

Best example can be given of is DOSs denial of service attacks that intentionally plan on tearing the information.

C. Disclosure of Information

Dissemination of the information to the outside users who are not authorised or part of the system or allowed to access is known as information leakage and disclosure. Examples: information exposure, intercepted information etc.

D. Theft of service

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 7, Issue 2
February 2018

Theft of applications and coputer programs, theft of important and confidential files and security codes as well as program codes and using that information for illegal use is theft of service.

E. Denial of service

Network blockage or intentional system blockage

F. Elevation of privilege

The various hit and trial methods like passwords guessing to get an intrusion to the system or any network to decode and get an unauthorised access.

G. Illegal usage

Usage of the general system functions to get and achieve the attacker's activities for illegal purposes.

V. Cyber Attack Detection

Detection of Cyber-attacksisdescribed as "the problem of identification of the individuals who pursue a legitimate but unauthorised access to a networked computer system and are misusing the privileges that they are havingwhich is also said as "Insider threats". It can also be stated as the identification of every single attemptthat is being made to for an illegal usage into a computer system without authorization

A. Host Intrusion Detection Systems (HIDS)

Host intrusion detection system means to control or observe a particular host machine. That isit calls to a domain of several intrusion detection systems that are the residents over a single host machine and also are monitored by an individual host computer. In order to capture data using a host machine exhibits the following characteristics as under:

i. File System –Any updates or changes on the host machine's file system bring about or indicates the various activities performed on the host computer.

ii. Network Events –Once the network stack properly processes and works upon the various communications taking place over the network, then only the detection system can intercept the information for the various intrusions being made.

iii. System Calls–System calls are also termed as high priority interrupts. All the system calls can be traced and observed once when the host kernel gets modified and a proper detection system gets positioned in the right place. This proper placement of the intrusion detection system will improve the richness of the information and will improve the process of detection.

B. Network Intrusion Detection Systems (NIDS)

A network cyber attack detection system (NCADS) functions by the proper placing of the network interface into a specific promiscuous mode, so that the entire network can be easily monitored. Monitoring of the network is an essential requirement because monitoring will yield the network packets which in turn will scan the entire network link and communication interface. Monitoring of attacks is not only crucial in terms of its addressing with the host machine but is also important because of the "ping-of-death" attack of which the system gets prone because that kill a host without even HCADS trigger.

C. Signature-based Malware Detection

It is also called as a pattern-matching approach as commercial antivirus is an example of signature based malware detection where a sequence of byte is scanned by a scanner within the entire program code with a purpose to keenly identify and reporting of a harmful deadly code. Syntactic analysis stage of a typical compiler is followed upon in order to detect such a malware by syntactically scanning a stream of code of instructions while he time of compilation. Although semantic analysis is not performed, this in turn becomes a limitation that can also come up as malware obfuscation during the program run period.

VI. Cyber Security Techniques

A. Access control and Password Security

We must ensure that we use different access mechanisms like OTPs, message authentication, third party security techniques in order to provide a secured access to our system. And designing a complex password which is not easy to guess or crack and regular updating or changing of the passwords to get a hold back from getting hacked.

B. Authentication of Data

While uploading and downloading of the data

and the document and various form filling websites, it must be totally noted and ensured that we are referring or using a proper and secured reliable source. Authentication of these downloaded documents and of the data is normally done by the various anti-virus software programs installed in the computer machines.That's why it is highly recommended to buy a reliable and licenced anti-virus that caters to all the needs and protects our system against threats.

C. Malware Scanners

Malware scanners are nothing but the software programs that aim at scanning the malware that have entered into the system by any means or gateways. Malwares are nothing special but the group of certain viruses like worms, wormholes, Trojans, logic bombs etc. Malwarebasicallydo the scanning of all the present files and information that may be harmed.

D. Anti-virus Software

Antivirus software is a computer program that is basically designed to provide the prevention & detection againstharmful software programs for example,boot sector virus and wormholes, Trojans etc. Mostly these anti-virusescome along with the package of auto-update feature that enables the application scope to trigger the actions of new upcoming viruses that are getting developed by the attackers in the market as they get identified.

Conclusion & Future Work

The detection systems of cyber attacks are different in the manner in which they collect and mine the data from the different sources and repositories and also in the different ample techniques the employ and use to apply various modifications and observations on a specific data item. The trending and uprooting technologies, along with the new cyber methods and threats that are up fronting, are nothing but the organizations that are in need of the new techniques and tools to perform their tasks as well as they seek intelligent methods to provide aid to their secured infrastructures. The detailed analysis of detection systems of cyber attacks is quite new as compared tothe other domains of research areas and this area has been undergoing a lot of future explorations ad much research work to go.

References

[1] Shailendra Singh, Sanjay Silakari," A Survey of Cyber Attack Detection Systems", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.5, May 2009.

[2] Amani Mobarak, AlMadahkah," Big Data In computer Cyber Security Systems" IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.4, April 2016.

[3] Prajakta Joglekar, Nitin Pise," Solving Cyber Security Challenges using Big Data" International Journal of Computer Applications (0975 – 8887) Volume 154 – No.4, November 2016.

[4] Adebayo Olawale Surajudeen, M.A. Mabayoje ,Amit Mishra, Osho Oluwafemi," Malware Detection, Supportive Software Agents and Its Classification Schemes", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.6, November 2012.

[5] Mohamed Abomhara and Geir M. Køien," Cyber Security and the Internet ofThings: Vulnerabilities,Threats,Intruders and Attacks" Journal of Cyber Security, Vol. 4, 65–88. doi: 10.13052/jcsm2245-1439.414, 2015.

[6] Dr. Savita Kumari Sheoran, Pratibha Yadav, "Research Perspectives in Security Threat Detection in Social Media Networks "International Journal of Advance Research in Computer Science and Management, Volume 5, Issue 1, January 2017.