ISSN 2278-3091
Volume 9, No.5, September - October 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse26952020.pdf
https://doi.org/10.30534/ijatcse/2020/26952020

An Approach on Cyber Protection Changes by way of a cohesive Red and Blue Working Committee

[1]Neetha K S, [2]Dr. Dayanand Lal.N , [3]Dr. Brahmananda S H, [4]Dr. Nijaguna G S, [5]Veena R C
[1]Assistant Professor, Department of CSE, Gitam School of Technology, India, nsrinath@gitam.edu
[2]Assistant Professor, Department of CSE ,Gitam School of Technology, India, dnarayan@gitam.edu
[3]Professor, Department of CSE, Gitam School of Technology, India, bsavadat@gitam.edu
[4]Assistant Professor, Department of ISE ,SEACET, India, nijagunags@gmail.com
[5]Assistant Professor, Department of CSE ,Gitam School of Technology, India, vchalapa@gitam.edu

ABSTRACT
Defensive system programs have progressed from interesting to necessary over the years and businesses across the globe are now realizing how important it is to continually invest in security. This move would make sure the business is successful in the markets. If the properties are not sufficiently protected, irreparable loss can arise and bankruptcy can result under some situations. Investing in defence alone is not enough, because of the emerging threat environment. Organisation's overall safety status must be strengthened. Investments in defending, sensing and reacting must also be matched. According to new risks and information protection issues, it is important to change the technique in order to prevent infringements. The conventional solution to avoiding infringement on its own does not promote continuing research, so in order to counter new risks, you will also improve your defence. The implementation of this pattern in the area of information protection was therefore a logical change.

Key words : Data Safety, Diffusion Trying, Ethical hacking, Red Crew, Safety Testing, Susceptibility Valuation

1. INTRODUCTION

As we all know today, the cybersecurity threat landscape can be dynamic and is continuously changing. Today's computer hacker utilizes a combination of both advanced and modern intrusion methods. In addition to that, different iterations of the current malware threat actors are being used regularly. Red Teaming would be a multi-layered, full-scope simulation of risks aimed at testing out how effectively an organization's staff and networks, applications and physical defence mechanisms can withstand a real-life enemy assault**.**

A red on blue answer session usually happens in a computer field, an area built for training and practice activities for information protection up. The cyber spectrum houses manufacturing or output-like systems for use in both the blue (defensive) and red (attack) circumstances. To promote the blue cases, the cyber range creates a framework which simulates the network of an organization being supervised by the security operations centre (SOC) team. Usually, this blue configuration combines the network management and emergency response technologies of choice for the enterprise.

Meanwhile, a sequence of real-world occurrences on the red crew, resemble cyber attackers trying to penetrate or damage the network and information networks of the enterprise. The red scenario is carried out by combining the latest automated assault tools with manual penetration testing techniques. Cyber ranges provide a number of versatile, customized options for businesses, allowing enterprises to concentrate on assault, security or a combination between both. In fact, the cyber spectrum can have additional in-house personnel to work on one hand or the other whether an organization chooses to concentrate its efforts on only one dimension.

A red team works beyond the box, it actively looks for innovative technologies and strategies to help secure the health of companies. Having a red team is a protest as it goes against laws and morality because you obey the tactics of white hats to prove that others have weaknesses in their processes. This are not stuff any of us do.

In order to be fully equipped for any intrusion or violation, technological hardening methods in both networks must be utilized to the effect of surface hackers. Hardening DNS is completely important, because it is one of the toughest measures to be ignored. To discourage DNS assaults, you should obey our instructions to further may the surface of attack.

Be familiar with software applications which require network monitoring for any unusual and potentially malicious

behaviour. After all network traffic, packets and current firewalls are screened and all operations in the company's networks are best managed.

2. LITERATURE SURVEY

According to Nelson and Kettani, PowerShell is an illustration of how the cyber warfare groups should implement a free software intrusion method. More post-exploitation frameworks written by PowerShell are likely to be conducted, spread and exploited over time by the cyber espionage groups. Defenders of the network would need to consider the use of these methods with the chain of attack and create solutions into their networks to avoid compromise. Here authors gives summary of PowerShell-written post-exploitation mechanisms and how cyber-espionage organizations use them. PowerSploit, PowerShell Empire and PoshC2 were the structures on which they have focused much. These structures were used in all phases of the attack chain. PowerShell was the most frequently used by cyber-espionage organizations was the conclusion made by the authors.

In this article the author gave the complete overview of powershell, starting with why attackers make use of powershell , phases of powershell, malwares, tools and frameworks and mitigation and protection. Here they gave explanation about PowerShell as they let the attackers to conduct illegal acts without having to implement any more binary data. It improves the chances of transmission still by letting their challenges without being determined. The reality about the PowerShell has also been illustrated as preinstalled application and a favourite tool for attacking. PowerShell allows few more Traces such as prolonged logging which are not turned on purpose.

Li, Zhenyuan et.al illustrated PowerShell language as a dynamically created script pieces at multiple stages and approaches for detection of attacks that are inherently vulnerable to disinformation. To address this challenge, author crafted PowerShell scripts with the first successful and lightweight deinformatic approach. To fix the issue of correctly defining retrievable code bits, they introduced a new solid understanding-based method that performs substring layer identification and emulation-based recovery in the abstract syntax tree of the PowerShell script. It also explained an example of the classic objective-oriented mining association algorithm and the recent discovery of 31 textual fingerprints for PowerShell threats to allow semantic detection.

The author discusses the challenges by designing and implementing their performance through too many unique detectors of suspicious PowerShell commands. Based on the "regular" natural language processing (NLPs), the proposed analysis consists of detectors and detectors dependent on character-level convolutionary neural networks. Detector efficiency was evaluated using a large real-world dataset. The analysis reveals that while detectors such as traditional NLP-detectors alone yield high efficiency, a hybrid detector that combines an NLP-based classifier with a CNN-based classifier offers the best results, since the other classifier may recognize fraudulent commands that manage to avoid the former. The study of these commands shows that some of the patterns that the CNN classifier automatically detects are inherently difficult to detect using the NLP techniques.

The author proposed a PowerShell process named PSDEM in this paper which has two layers to access previous PowerShell texts. The first demonstrates how to remove PowerShell scripts from the text's much-unknowable language. The other shows scripts that are de-obfuscating, which can involve decoding, modifying strings and diffusing file logic. Instead they're working with PSDEM-based de-obfuscation and automatic search tool in pdf files for harmful PowerShell scripts. Checking the effectiveness of the method from the expense and time utility of de-obfuscation and analysis results appeared to be acceptable. The study suggested improves the reliability and consistency of screening suspicious PowerShell scripts in microsoft word and provides a means for security specialists to obtain additional knowledge regarding threats.

3. METHODOLOGY PROPOSED

3.1 Group Red and Blue

Study on the Red and Blue team is nothing unusual. The initial definition was developed decades ago in World War I and emerged with the government, as was the case for certain words used in data privacy. The core idea was to use models to show an attack 's efficacy. The usefulness of models focused on actual strategies that the enemy might use is well known and used in both the military and computer security sectors.

3.1.1 Red Crew

Red Teams were international agency brought together to assess the efficiency of a compliance system. It is achieved by emulating the actions and tactics of suspected criminals in the most practical manner imaginable. The method is close, but not equivalent for, penetration monitoring, which requires the achievement of one or more targets. This assigned community checks the protection strategy of the company to see if it would fare toward real-time threats-until they really happen. Hiring candidates of diverse skills and specialties allows you fill out a defence red squad and insure you are researching and viewing a business from the multiple viewpoints of an

intruder. The implementation of the Red project team has also allowed companies to protect their assets more safely in the field of data protection.

The Red Team will consist of fully skilled experts, with unique skill sets, and they will need to be fully briefed regarding the current threat climate for the field of the enterprise. The Red Team would be mindful of the changes and understand if emerging challenges are evolving. In certain instances, and depending on the needs of the enterprise, Red Team leaders may have technical expertise to build and customize their own weakness to better exploit unique glitches that can affect the business. Your Red Team can constantly review the protection procedures during the year. In specific, their task would be to assess the networks and see if it can survive various attack methodologies without providing warning and fellow employees. It's also worth making the Red Team monitor the company when introducing a new protection product or application.

The main Red Team process takes shape as shown in the below(figure 1) approach:

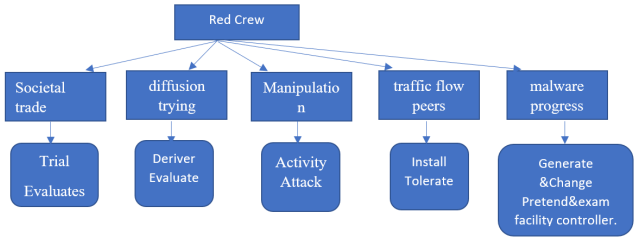

Figure 1: Red Team Operations

The Red Team would conduct social manipulation, infiltrate the system by attempting to circumvent the existing protection measures, often known as penetration testing. it will also exploit system and Network, generate traffic and develop new or customise malware. The project's goal is to find bugs and exploit them to get control to the assets of the organization.

3.1.2 Blue Crew

Blue Crew applies to the internal defence unit that protects against all actual threats and Red Crew. Blue Crew can be differentiated from regular defense departments of most organisations, since most security operations departments do not have a attitude of relentless caution against violence, which is the task and mindset of the real Blue Squad. The Blue Workforce must guarantee that the facilities remain protected and, in the event that the Red Family discovers fault and abuses it, they must immediately fix and log it as part of the knowledge gained. Below are some examples of the Blue squad's tasks when a rival may disrupt the device:

The core Blue Team phase takes place using the following method in Figure 2:

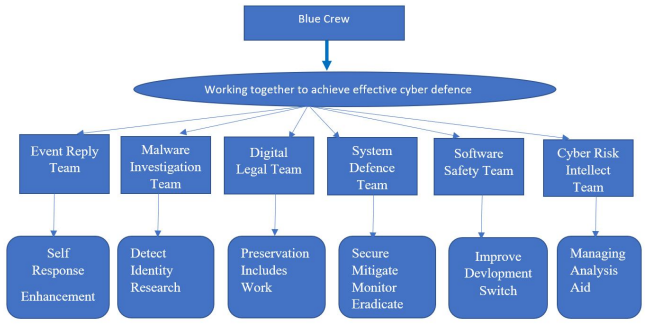

Figure 2: Blue Crew Operations

3.2 Implementation

The front-end effective discussion on, how attackers hack network system in different Scenarios work. Here two type of teams we find, in that blue teamers are known as Hunters, Red teamers are known as attackers. Since the Blue Teamers are working to attack the red teamers activities based on the various setup, that come across different case studies and the appropriate ways to investigate, study and gathering some of the forensic objects. Which may guide the blue crew to chase red teamers and monitor their actions and the signs left by them.

Set-Up

Throughout this segment, we will present some of the real-life scenarios and examining a variety of events by red teams. As stated earlier, we are going to see how a red teamer has original network connections and has performed any illegal behaviour all over the domain computers.

i. Case Study 1: Device to remote execution (Psexec)

Most of the red teamers use Psexec tools to conduct the remote monitoring and get their stuff completed and they depend on the default software (admin tools) which are whitelisted in certain instances. Psexec is a legal resource made accessible by Microsoft Sysinternals and many of the managers use this on windows system. The offenders people use this method to execute disruptive acts and execute remote commands.

A simple command is utilized to get a session at cmd.exe by using the order below figure 3:

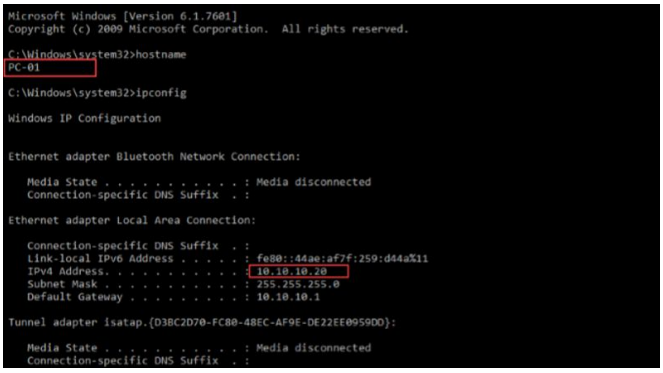

Figure 3: Psexec Suspicious Command

There is an artifact for understanding whether or not the Psexec was ever run by any person. If a user executes an order, a Psexec service is created (figure 4) on the destination computer and put a file on the C:\windows with the name Psexesvc.

Figure 4: PSEXESVC File on the Target Machine.

You can also detect the development of this service(figure 5) on the registry key underneath.

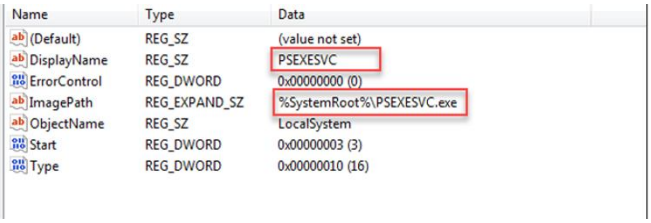

Figure 5: Registry Value for the Service (PSEXESVC).

Windows prefetch artifact:

We can identify the behaviour of Psexec from a recognized artifacts (prefetch). Prefetch on windows was a windows xp and windows server 2003 feature added to speed up the cycle of booting windows and launching a program. The prefetch is placed under %system Root%\prefetch. The prefetch file(figure 6) contain different information, such as: Name executable, count execution, information about the volume, file and directories referenced executable, and timestamps of course.

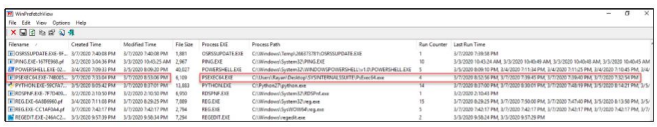

Figure 6: Prefetch Files

Shimacache Artifact:

Shimacache also known as AppCompatcache, is an application compatibility feature server developed by Microsoft and making use of windows operating system identify compliance problems with the software. It is used to scan easily, to determine whether for reliability the modules need to shim or not. The shimcache stores specific metadata such as: File full path, last modified time, file size, process execution flag. As a thread hunter, with shimcache we can chase the Psexec activity.

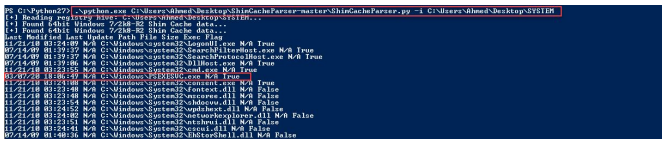

Figure 7: Shimcache Results.

On the figure 7 above you can see that we used shimcache parser method to retrieve the cache registry hive information.

ii. Case Study 2: Suspicious PowerShell Controls:

The attackers and the red teamers learn PowerShell very well. They use PowerShell to accomplish their tasks and ease the work. Popular PowerShell scripts are available and can be used for enumeration, privilege escalation and persistence. Here we will demonstrate in this scenario that an intruder has used suspicious PowerShell scripts and executed malicious commands to achieve the target of the attacker in the network.

As a danger hunter, to identify some form of harmful or questionable commands, we must also test the PowerShell events given in the below figure 8:

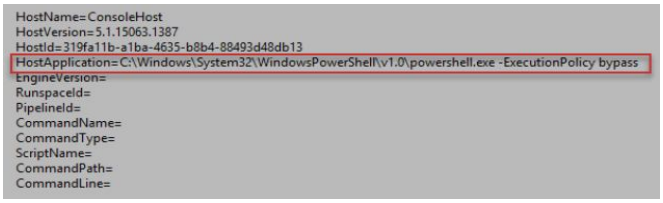

Figure 8: PowerShell Event ID (600).

Figure 9: Microsoft-Windows-PowerShell Event ID (4104).

In the above (figure 9)events, we see that some users have bypassed the execution policy of the PowerShell. This activity is usually done by malicious users to allow them for running such scripts, which by default the strategy is set to "Restricted" and it stops PowerShell scripts from being performed. The activities which runs the status of operations is being shown with the help of figure 6 and figure 7.

We were able to find the suspected case below(figure 10 and 11) after running the events:

Figure10:SuspiciousScript1Microsoft-Windows-PowerShell Event ID.

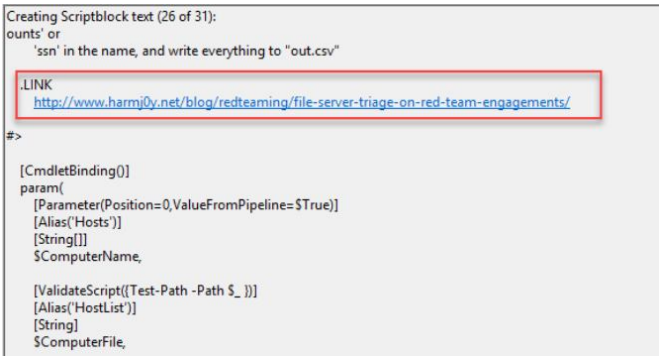

Figure11: SuspiciousScript2 Microsoft-Windows-PowerShell Event ID

We can see that the main computer(sys2) was running a malicious file. The script is power view, a famous PowerShell module whose main objective is to enumerate the target domain.

4. CONCLUSION

Now that multiple organisations have experienced losses as a series of organized threats, it is increasing the value of incident reports to better examine such losses. This report provides and explains facts about the use of techniques and their corresponding communication with machines, which are important for the event to be successfully analysed. Most devices cannot leave evidence that they have been performed with Windows default settings, which may prompt incomplete accident inquiries. To examine what the attacker did, a setup that needs additional reports to be obtained than those viewed through the default settings has to be designed. In the current conditions, where it is impossible to avoid network penetration, it is necessary to both recognize and develop the monitoring system to assess the amount of harm that happened during an incident in order to stop loss from spreading and to revisit protection measures after an incident. Other approaches which incorporate the usage of audit tools or similar are often used in addition to evaluating and planning responses which are not limited to the method of collecting additional logs utilizing normal Windows features as seen in this article.

REFERENCES

1. Nelson, Tj & Kettani, Houssain. (2020). Open Source PowerShell-Written Post Exploitation Frameworks Used by Cyber Espionage Groups. 451-456. 10.1109/ICICT50521.2020.00078].
2. https://docs.broadcom.com/doc/increased-use-of-powershell-in-attacks-16-en
3. Li, Zhenyuan & Chen, Qi & Xiong, Chunlin & Chen, Yan & Zhu, Tiantian & Yang, Hai. (2019). Effective and Light-Weight Deobfuscation and Semantic-Aware Attack Detection for PowerShell Scripts. 10.1145/3319535.3363187.
4. Danny Hendler, Shay Kels, Amir Rubin," Detecting Malicious PowerShell Commands using Deep Neural Networks "
5. Chao Liu, Bin Xia, Yunzheng Liu ,"PSDEM: A Feasible De-Obfuscation Method for Malicious PowerShell Detection".
6. N. Veerasamy, "High-Level Methodology for Carrying out Combined Red and Blue Teams," *2009 Second International Conference on Computer and Electrical Engineering*, Dubai, 2009, pp. 416-420, doi: 10.1109/ICCEE.2009.177.
7. J. Yuen, B. Turnbull and J. Hernandez, "Visual analytics for cyber red teaming," 2015 IEEE Symposium on Visualization for Cyber Security (VizSec), Chicago, IL, 2015, pp. 1-8, doi: 10.1109/VIZSEC.2015.7312765.
8. S. Zavala, N. Shashidhar and C. Varol, "Cybersecurity Evaluation with PowerShell," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 2020, pp. 1-6, doi: 10.1109/ISDFS49300.2020.9116258.
9. S. P. Liew and S. Ikeda, "Detecting Adversary using Windows Digital Artifacts," 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 2019, pp. 3210-3215, doi: 10.1109/BigData47090.2019.9006552.
10. S. Lim, J. Park, K. Lim, C. Lee and S. Lee, "Forensic Artifacts Left by Virtual Disk Encryption Tools," 2010 3rd International Conference on Human-Centric Computing, Cebu, 2010, pp. 1-6, doi: 10.1109/HUMANCOM.2010.5563320.
11. T. Tan, S. Porter, T. Tan and G. West, "Computational Red Teaming for physical security assessment," The 4th Annual IEEE International Conference on Cyber Technology in Automation, Control and Intelligent, Hong Kong, 2014, pp. 258-263, doi: 10.1109/CYBER.2014.6917471.
12. Effective and Secure Approach for Multi-Keyword Quest Graded over Authenticated Data, International Journal of Advanced Trends in Computer Science and Engineering, 2020, volume 9, number 2, pages 2278-3091,

Shobharani D, Parikshith Nayaka S K, Swasthika Jain T, Dr. Dayanand Lal

13. Mr. Parikshith Nayaka S K, Mrs. Shobha Rani, Dr. Dayanand Lal, Dr. M Anand. (2020). Convert Channel and Information Hiding in TCP/IP . *International Journal of Control and Automation*, *13*(02), 582 - 591. Retrieved from http://sersc.org/journals/index.php/IJCA/article/view/11199
14. Jacob, I. Jeena. (2020). Ensuring Network Security using Secured Privileged Accounts. International Journal of Emerging Trends in Engineering Research. 8. 1959-1963. 10.30534/ijeter/2020/80852020.
15. A modern themed system for patients security of data exposure in semi-convinced servers in the cloud, International Journal of Emerging Trends in Engineering Research, 2020, volume 8, number 8, pages 4123-4127 Parikshith Nayaka, S.K. and Dayanand Lal, N. and Shahapur, V. and Saritha, A.K. and Kousar, N.