Building and Implementation of Cyber Security Strategies under Linux Environment using Cybersecurity Kill Chain

Vinit A. Sinha
Assistant Professor
PGDCA, PRMIT&R Badnera-Amravati
Maharashtra, India

Vilas M. Thakare, PhD
Professor & Head
P.G. Dept. of Comp Science, SGBAU, Amravati,
Maharashtra, India

ABSTRACT

A cyber strategy is view towards various aspects of security needed in cyber space. It itself describes protection required to address data , network , technical system and persons who work in this area. This article explains the basic building of cyber strategy and implementation techniques using attack and defense team . The research explain role of Linux and cybersecurity kill chain, to elaborate cyber strategies and implementation of all these techniques. The whole work is redirected towards understanding threats and risks , while building internal and external testing cyber strategies. Cybersecurity kill chain is a security model that organises both tracking and prevention of intrusion at various phases. The article ended up with implementation techniques which are sensible and more effective towards making hardening of security to cyber space.

Keywords

Cyber strategy, Linux, Cyber kill chain

1. INTRODUCTION

Cybersecurity has many finger view of meanings , which can be clearly and practically categories as protection to individuals , small business owners ,firms conducting online business , for shared service providers and for the government. Somewhat cybersecurity treated as moving target constantly **[1].** Cyber strategy is way to create an practical approach to build a plan to provide a security circle around cyber assets like digital data , networks , technical system and IT persons.

2. NEED OF CYBER STRATEGIES

Organisation are dealing with cyber threats generated by professionals attackers and many of them run their own states , terrorists and cybercriminal group. Many time it is observed that cyber attackers have more expertise in cyber security than average IT employees . So that they can easily bypass major tool setup by IT organisation. Result out , today organisation need leakproof strategy to update their cyber defense system. Following fig.(1) shows occurrence of malware infection have been grown up from last 10 years, which express need of cyber strategy in clear ways **[2].**

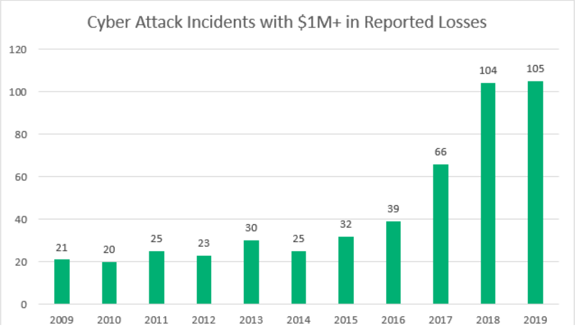


Figure 1 (Cyber Attack Statistics)

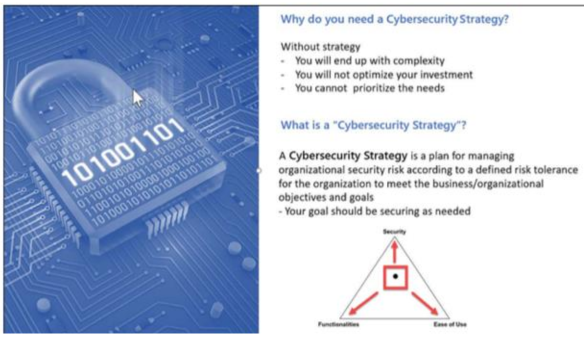
Describe below are strong reasons for implementation of cyber strategies.

A. Change in predetermination-
Predefine assumption sometime could be misleading tailored only towards objectives as compliance.

B. Organisations Standard –
Cyber strategies should be centralized for control and decision making purpose , which leads to level up standard of organisation.

C. Security tactics in brief –
High standard tactics are responsible for security of the organisations . This reflects on incidence response , threat recovery and business planning . Some times responses to attack may help stakeholder of organisation.

D. Security commitment to organisation for long period –
Cyber strategies provides security system to organisation using resources and efforts. It is good sign for investor and stakeholder of organisation.



Why do you need a Cybersecurity Strategy?

Without strategy
- You will end up with complexity
- You will not optimize your investment
- You cannot prioritize the needs

What is a "Cybersecurity Strategy"?

A **Cybersecurity Strategy** is a plan for managing organizational security risk according to a defined risk tolerance for the organization to meet the business/organizational objectives and goals
- Your goal should be securing as needed

Figure 2 (Need a cybersecurity strategy)

3. WAY OF CYBER STRATEGY (BUILDING)

In this we explained, how to build an cyber strategy.

A. Business Understanding –
For Securing the business , it should be understandable for ease. Goal of organisation is matter here for great work. Sometime risk management should be there for victory work. Here strategy with tactics for smooth work is needed , which tends to noiseless and fastest route to victory.

B. Threats and Risk Management –
Without risk no work is completed successfully. So the risk word combines ,

1. Potential event
2. Probability
3. Potential severity

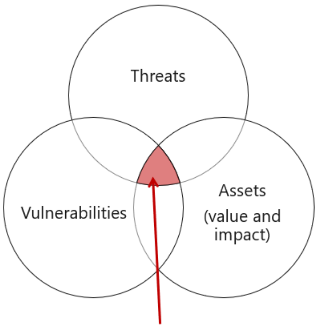


Figure 3 (Risk Combination)

C. Documents (Elements of cyber strategy) –

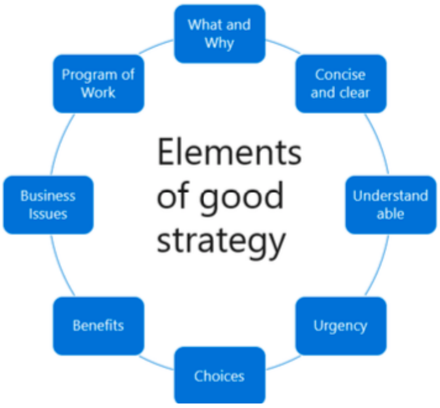


Figure 4 (Elements of cyber strategy)

Documentation is needy and it put key aspect of every strategy . It plays an critical role when combines with treatment setting and assurance of business continuity. It contains list of strategy which are needed to plan security system for any organisation. It also help to achieve business goal and align with business strategy . It is important to study mindset of hackers for his activity to implement effective cyber strategy , which we discussed in next section .

4. STRATEGIES USE IN CYBER-ATTACKS

1. External testing:- It involves attempts for breaching organisation externally in manner of outside its network. In this case attacks are directed towards public resources for testing purpose.

2. Internal Testing: - This strategies majorly used for attacks performs within organisation for compromise at low level.

3. Blind Testing: - 'Some time surprise will be more dangerous at prime time'. This strategy is totally based on giving surprise to organisation for severe damage.

4. Target Testing: - This type of testing is based on special target attack mode, which affect more and multiple attacks on single target for incresing chances to successful attack. But some times it gives less information as narrow space channel.

5. STRATEGIES USED IN CYBER DEFENSE

1. Extensiveness of defense : - This strategy includes layered pattern during hardening security of organisation. So attackers faces difficulties to enter into defense mechanism . Redundancy of security layers protect one each other during attack occurrence by hacker . This result to series of defense system always provide better solution on severe attacks.

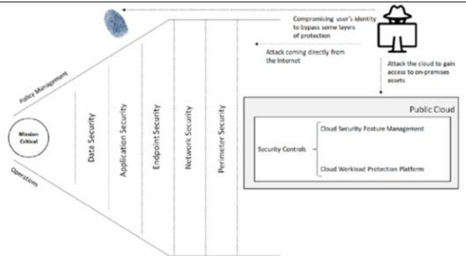

Compromising user's identity to bypass some layers of protection
Attack coming directly from the Internet
Attack the cloud to gain access to on-premises assets
Policy Management
Mission Critical
Operations
Data Security
Application Security
Endpoint Security
Network Security
Perimeter Security
Public Cloud
Security Controls
Cloud Security Posture Management
Cloud Workload Protection Platform

Figure 5 (Extensiveness of defense)

2. Breathiness of defense : - This strategy involves combination of traditional and advance security mechanism . Basically this strategy aims to hardening OSI model security at each layer. The web application firewall (WAF) are effective way to protect application against cyber-attack. With this method developers also use new tech methodology as OWASP (Open Web Application Security Project) , which result out standard level of security and basic information of common vulnerability.

6. IMPLEMENTATION TECHNIQUES OF CYBER STRATEGY (CYBERSECURITY KILL CHAIN)

It provides platform for mastering security . "*Thinking as an attacker to understand the motivation behind cyber-attacks and steps of performing an attack called as Cyber Kill Chain (CKC)*". CKC is in combination of different phases and description of how cyber-attacks generally taken out or executes to its result. It can be treat as model of security for organisation to detect as prevent intruder activities at various stages. CKC are more successfully used against various attacks as ransomware , hacking attempts and Advance Persistent Threats . Following figure 6 shows , how threat generators executes there activities in kill chain.

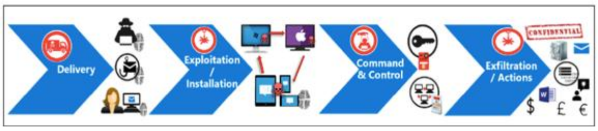


Figure 6 (Activities of Threat generators)

7. PHASES OF CYBERSECURITY KILL CHAIN

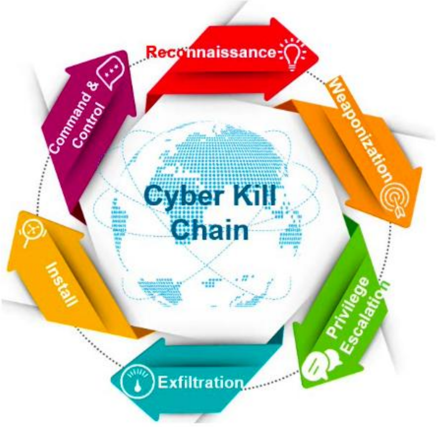


Figure 7 (Phases of Cyber Kill Chain)

1. Reconnaissance – In cyber-attack, threat generators trying to get information, which can be used to attack on system. This things includes host in network and related to vulnerability in same segment.

2. Weaponization – It is the cycle where tools are built for implementation of attacks on their targeted system. The method of creation of intruder file and insert into victim system is generally used.

3. Privilege Escalation – This is next step after weapon is ready . It include maintain access and traverse in network , while others are undetected.

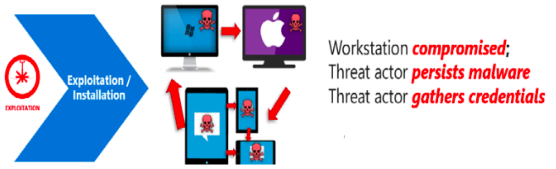
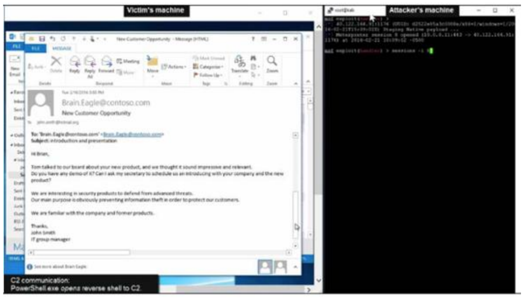

EXPLOITATION
Exploitation / Installation
Workstation compromised;
Threat actor persists malware
Threat actor gathers credentials

Figure 8 (Installation of weapon for target system)

4. Exfiltration – This phase is treat as successful step , while treatment generator is move around victims network with accessing to system and sensitive data from organisation. Threat generator some time move towards data storage location for tampering and extraction purpose.

   Following Figure 9 shows infected attachment in email of victim's system where hackers use shell terminalis to command and control centre which displayed on right hand side.



Brain.Eagle@contoso.com
New Customer Opportunity

To: 'Brain.Eagle@contoso.com' <Brain.Eagle@contoso.com>
Subject: introduction and presentation

Hi Brian,

Tom talked to our board about your new product, and we thought it sound impressive and relevant.
Do you have any demo of it? Can I ask my secretary to schedule us an introducing with your company and the new product?

We are interesting in security products to defend from advanced threats.
Our main purpose is obviously preventing information theft in order to protect our customers.

We are familiar with the company and former products.

Thanks,
John Smith
IT group manager

See more about Brain Eagle

C2 communication:
PowerShell.exe opens reverse shell to C2

```
msf exploit([illegible]) >
[*] [illegible] Staging Native payload ...
[*] Meterpreter session 3 opened [illegible]
[illegible]

msf exploit([illegible]) > sessions -i 3
```

Figure 9 (Attacker's Side View)

8. TOOLS USED IN CKC-

1. Nmap- It is an free and open source based network scanning tool.

2. Metasploit – This is framework based tools most popularly use by hackers used to attack on target system.

3. John the ripper – This is password cracking tools used by hackers to execute dictionary attacks.

4. Zenmap – This is helpbased tool for Nmap having easy GUI for maintaining network connection.

5. Wireshark – This is one of network sniffing packet tool for analysing the network use by both hackers and pen tester.

6. Aircrack-ng – It is most effective network tool. Some time dangerous pack of tools used for wireless hacking and most population a today's cyber space.

9. RESULT

Cyber kill chain explored the threat generator typical mindset and shows the way how he get target using simple and advance intrusion tools. We also discovered how cyber strategies improves defense system by different ways which are more effective. Above discussed study also explain ways through which defense system can interrupt threat stage development and attacks by using security tools. We also discussed how threat generator exfiltrate data from organisation for which they gain ease access. Threat generator also move forward to attack on victim's hardware to cause more damage.

10. CONCLUSION

The research work concluded with building of cyber security strategies with above mentioned techniques on the basis of needs. Today cyber space is full of risk and threats related severe cyber-attacks. This work explains the solutions with implementation of cyber key chain (CKC) having number of security tools. In future , this techniques of prevention may improve by applying network based smart tool like *Deauthor Board* , which is an non-conventional tool . With this an *Evil OSX* is effective tool based on Apple OS may help to build ecosystem . Future plan should be made up countermeasure of CKC based on penetration testing.

11. REFERENCES

[1] Steinberg, Joseph. *Cybersecurity for Dummies*. 1st ed. Indianapolis: John Wiley and Sons, 2019.

[2] 42 Cyber Attack Statistics by Year: A Look at the Last Decade | InfoSec Insights. (2021). Retrieved 13 January 2021, from https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/

[3] What is The Cyber Kill Chain and How to Use it Effectively | Varonis. (2021). Retrieved 13 January 2021, from https://www.varonis.com/blog/cyber-kill-chain/

[4] Beggs, Robert W. *Mastering Kali Linux for Advanced Penetration Testing a Practical Guide to Testing Your Network's Security with Kali Linux, the Preferred Choice of Penetration Testers and Hackers*. Birmingham, UK: Packt Pub., 2014. http://proquest.safaribooksonline.com/9781782163121.

[5] Rains, Tim, and an O'Reilly Media Company Safari. *Cybersecurity Threats, Malware Trends, and Strategies*, 2020. https://learning.oreilly.com/library/view/-/9781800206014/?ar.

[6] Sharma, Himanshu and O'Reilly for Higher Education (Firm). *Kali Linux - An Ethical Hacker's Cookbook - Second Edition*, 2019. https://www.safaribooksonline.com/library/view//9781789952308/?ar.

[7] Steinberg, Joseph. *Cybersecurity for Dummies*. 1st ed. Indianapolis: John Wiley and Sons, 2019.

[8] Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Computers in Industry, 114, 103165. https://doi.org/10.1016/j.compind.2019.103165.