e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

CYBERSECURITY AUTOMATION USING CYBER KILL CHAIN

Trupti Zaware[*1]

[*1]Department Of Information And Technology, B. K. Birla College Of Arts, Commerce
And Science (Autonomous), Kalyan, Mumbai, India.

DOI : https://www.doi.org/10.56726/IRJMETS29648

ABSTRACT

Cybersecurity is additional crucial than ever within the fashionable society. Businesses and people square measure liable to cyberattacks attributable to the event of the web and the growing reliance on technology. The method of preventing unwanted access to or thievery from laptop networks and systems is thought as cyber security. Keeping your information secure from hackers is what it entails, in different terms. The point of network safety is to secure or at any rate, diminish advanced assaults for this multitude of angles. Network safety safeguards organizations against cybercriminals and the cyberthreats they turn out. Security mechanization is that the machine-based execution of safety activities with the capability to mechanically acknowledge, contributed and correct cyberthreats not withstanding human mediation by distinctive approaching dangers, triaging, and that specialize in cautions as they arise, then, at that time, responsive them in associate opportune style. cybernation is that the best thanks to decrease the degree of dangers and empower faster shunning. In this paper, we tend to describe the cyber kill chain with their all steps. The cyber kill chain may be a blueprint for in operation in an exceedingly staged manner, that incident response groups, forensics consultants, and malware researchers will use to notice and stop cyberattacks at completely different stages of the chain. This paper proposes associate approach to attach cyber kill chain with automation to seek out preventions or vulnerability. The most aim of cyber kill chain methodology is to assist businesses to scale back the danger of attack by understanding however law-breaking generally progresses. We will use the kill chain to assess existing security measures, establish vulnerabilities, and fix any security risks.

Keywords: Unauthorized Access, Triaging, Security Automation, Cyber Kill Chain, Vulnerability.

I. INTRODUCTION

The computerized kill chain is a change of the strategics kill chain, which is a little-by-little methodology that recognizes and stops enemy development. At first made by Lockheed Martin in 2011, the computerized kill chain approaches the various periods of a couple of typical cyberattacks and, moreover, where the information security gathering can thwart, recognize, or block aggressors. The computerized kill join is supposed to prepare for current cyberattacks, generally called advanced persevering risks (APTs), wherein foes contribute tremendous energy surveillant and organizing an attack. Most commonly these attacks included blends of malware, ransomware, trojans, caricaturing and social planning strategies to convey their course of action.

Insights on digital assaults are seldom predictable and ostensibly consistently a most realistic estimation, as they can reflects assaults that are accounted for; some effective assaults are not revealed and, even more, should go undetected. The Ponemon Establishment's Expense of Information Break Study distributed in Walk 2012 reports that the quantity of assaults from insiders is roughly 33% of every single recorded assault. While Verizon's 2017 tantamount report shows a lower extent of 25% up from 14% in 2013, which was twofold the genuine number of real goes after in the earlier year[1]. These figures show that the issue of insider assaults has not better over the most recent five years and as an industry, we are yet to get the issue under control.

Although it is still a supporting tool, the cyberattack lifecycle is less predictable and clear than it was ten years ago. For instance, it is quite reasonable to anticipate that digital attackers may omit or add procedures, especially at the most crucial stages of the lifecycle. This gives organizations less time and opportunity to identify and eliminate threats earlier in their lifespan. In addition, the prevalence of the kill chain concept may provide cyberattackers a hint about how organizations are setting up their defenses, which may help them avoid being identified at key points of the attack lifecycle.

II. RELATED WORK

Making a progressive system is a significant device for sorting out information and grasping existing issues and making a space arrangement. For instance, Lindorfer et al. in 2011 proposed an order for harming conduct of malwares considering recognizing natural variables[2]. They confronted issues with damaging codes and distinguishing instrument climate utilized for getting away from examination.

In 2014, the United States presented the "Network safety Intelligence Sharing Act[3]. Up until this point, the assault kill chain has been officially remembered for American law.

Conventional cyber defense has two inherent flaws: 1. The static nature of traditional systems gives attackers enough time to probe the target network and gather information; 2. Traditional network defense mainly focuses on the reactive response after attacks have occurred, rather than intervening in the early stages of the cyber kill chain[4].

Revell et al. conducted a study on devices for OSINT-based (Open source brilliantly) examinations. They centered on applications, websites, and administrations that the OSINT professionals are using[5]. They distinguished diverse OSINT devices and utilized their created evaluation system for security, unwavering quality, and lawfulness for cyber examinations. Their appraisal system comprised of report data, provider appraisal, outside evaluation, and practitioner's appraisal. In the report data, they evaluated the tool's value and traceable characteristics. The Supplier Assessment evaluated the claims, legitimate terms, and approaches utilization. In the outside appraisals, the surveys approximately the instruments from the outside clients, bolster, upkeep, vulnerabilities are evaluated.

With the persistent attack attempt, attack tools and techniques are becoming more sophisticated, obstruction-based security mechanisms are unable to meet the needs of counteract advanced unknown attacks[6]. Attack traffic will be forwarded to the shadow service instead of being blocked. This is because attackers can use a proxy against IP address blocked.

Introduction to Cyber Kill Chain model

According to the data gathered, the Lockheed Martin Cyber Kill Chain model essentially has seven stages:

Phase 1: Reconnaissance

During the reconnaissance phase of a cyber-attack, a malicious actor explores vulnerabilities and weaknesses that can be exploited within the network. As part of this, an attacker may harvest login credentials or gather other information, such as email addresses, user IDs, physical locations, and software applications.

Phase 2: Weaponization

Attackers could install back doors as a backup in case network administrators find and close their primary port of entry, allowing them to keep using the system. The attacker develops an attack vector, such as remote access malware, ransomware, a virus, or a worm, during the weaponization phase.

Phase 3: Delivery

Attack is started by the invader in the Delivery stage. For instance, they can provide harmful links or email attachments to encourage user action. The campaign's efficacy can be increased by combining this activity with social engineering strategies. The actions done will vary depending on the kind of attack they want to launch.

Phase 4: Exploitation

In the Exploitation stage, the malicious code is executed inside the casualty's framework.

Phase 5: Installation

Immediately taking after the Exploitation stage, the malware or other assault vector will be introduced on the victim's framework. This may be a turning point within the assault lifecycle, as the danger on-screen character has entered the framework and can presently accept control.

Phase 6: Command and Control

The virus can be used by the attacker in command and control to assume remote control of a device or identity inside the target network. They could also try to migrate laterally in the network at this point to increase their access and create new avenues of entry in the future.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:09/September-2022 Impact Factor- 6.752 www.irjmets.com

Phase 7: Actions on Objective

These steps could include data theft, destruction, encryption, or exfiltration by means of a virus, Trojan, or other attack.

In table 1, there is tabular format in which we are showing top threats with cyber threat kill chain attack workflow steps:

Table 1: Threats in workflow steps[7].

Top Threats	Cyber Threat Kill Chain Attack Workflow Steps						
	Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control	Actions on Objectives
Malware					✓	✓	✓
Web-Based Attacks		✓	✓	✓			
Web Application Attacks	✓			✓	✓		
Phishing	✓	✓	✓				
Spam		✓	✓				
Denial of Service	✓	✓				✓	✓
Ransomware					✓	✓	✓
Botnets						✓	
Insider threat	✓	✓	✓	✓	✓	✓	✓
Physical Manipulation/ Damage/ Theft/ Loss					✓		✓
Data Breaches							
Identity Theft	✓	✓	✓				✓
Information Leakage	✓	✓	✓	✓			✓
Exploit Kits		✓	✓	✓	✓		
Cyber Espionage							

Function of the cyber kill chain in cybersecurity:

The Cyber Kill Chain plays a major role in serving to organizations outline their cyber security strategy [8]. underneath this model, organizations should adopt services and solutions that modify them to:

- Sleuthing attackers at every stage of the threat lifecycle mistreatment threat techniques
- Stop access by unauthorized users
- Stop unauthorized users from sharing, storing, altering, exfiltrating or encrypting sensitive information
- Answer attacks in real time
- Stop the attacker's lateral movement inside the network

Lockheed Martin developed the CKC model, that explains the threat employing a series of stages, beginning with intelligence, and ending with actions on the target. Later, supported these studies, the model was dilated to seven stages, that area unit still in use these days.

The conventional kill chain has contributed to security protection; however, it additionally has clear drawbacks [9]. Defences directive attention toward perimeter-based security. By the standards of current cyber security technologies and procedures, each cyberattackers may doubtless be thought to be Associate in Nursing business executive. each internal threats and extremely subtle assaults area unit poorly handled by it.

In table 2, we tend to area unit about to do a straightforward tabular format of however security tools will be wont to apply discover and deny of every stage that is gift in Lockheed Martin's cyber kill chain.

Table 2: Detect and deny of each stage[10].

Reconnaissance	Detect • Web Analytics • Threat Intelligence • Network Intrusion Detection System
	Deny • Information Sharing Policy • Firewall Access Control Lists
Weaponization	Detect: • Threat Intelligence • Network Intrusion Detection System
	Deny: • Network Intrusion Prevention System
Delivery	Detect: • Endpoint Malware Protection
	Deny: • Change Management • Application Allow listing • Proxy Filter • Host-Based Intrusion Prevention System
Exploitation	Detect: • Endpoint Malware Protection • Host-Based Intrusion Detection System
	Deny: • Secure Password • Patch Management
Installation	Detect: Security Information and Event Management (SIEM) • Host-Based Intrusion Detection System
	Deny: • Privilege Separation • Strong Passwords • Two-factor Authentication

Command & Control	Detect: • Network Intrusion Detection System • Host-Based Intrusion Detection System
	Deny: • Firewall Access Control Lists • Network Segmentation
Actions on Objectives	Detect: • Endpoint Malware Protection
	Deny: • Data-at-rest Encryption

III. METHODOLOGY

This study suggests an approach based on vulnerability analysis utilizing several tools and a cyber death chain. Using this method will help detect risks at every step of their lifecycles.

As we said before, certain cyber-attacks are referred to as Advanced Persistent Threats (APTs), not only due to the attacker's skills but also due to their capacity for setting up and maintaining ongoing operations against a target. Security professionals won't only wait to respond to warning signs or symptoms of compromise. They actively search for dangers to stop them or lessen the harm[2].

The seven steps of the Kill Chain concept are an intelligence-driven approach to intrusion detection. These stages improve the visibility of an incursion and aid security teams in comprehending the strategies, tactics, and practices of an adversary. The steps come together to produce a chain-like integrated end-to-end process[11].

In table 3, we are distributed some known threats based on three categories. The main three categories are network threats, host threats, and application threats.

Table 3: Threats distribution

Network Threats	Host Threats	Application Threats
▪ Information gathering ▪ Sniffing and eavesdropping ▪ Spoofing Session hijacking and man in the middle attack ▪ DNS and ARP poisoning ▪ Password based attacks ▪ Denial of service attacks ▪ Compromised key attacks ▪ Firewall and IDS attacks	▪ Malware attacks ▪ Foot printing ▪ Profiling ▪ Password attacks Denial of service attacks Arbitrary code execution ▪ Unauthorized access ▪ Privilege escalation ▪ Backdoor attacks Physical security threats	▪ Improper data/input validation Authentication and authorization attacks ▪ Security misconfiguration ▪ Information disclosure ▪ Hidden-field tampering ▪ Broken session management ▪ Buffer overflow issues ▪ Cryptography attacks ▪ SQL injection ▪ Phishing Improper error handling and exception management

Vulnerability management:

To oversee shortcomings, a Vulnerability Management cycle ought to be described in the affiliation. It will in general be described as how to process and remediate potential shortcoming information nitty gritty by inside or external individuals or affiliations. ISO (International Standard Organization) gives terms, definitions, thoughts, and affiliation ideas to structure this activity through 2 vital rules:

• ISO 30111 - Vulnerability managing process. It deals with the assessment, crisis, and remediation of inside or somewhat declared shortcomings.

- ISO 29147 - Vulnerability disclosure. It deals with the marks of association between the different potential shortcoming uncovering accomplices (vendors, audits/penetration testing, thus on.)[12].

A shortcoming assessment is a five-step process effectively ensuring the trustworthiness of wellbeing systems across the association. The entire cycle is essential to shortcoming the leaders and IT Risk Management lifecycles. Coming up next are the means in shortcoming assessments, also to go about as an outline of how each stage functions[13].

Stage 1: Vulnerability Identification

The most vital phase in weakness is sorting out practical weaknesses of a machine while growing a total posting of each tracked down weakness. Weakness filtering is both verified and unauthenticated examines. Confirmed checks offer get right of passage to low-arrange data. Entrance giving a shot can pinpoint security blemishes and attack vectors overlooked. It is the sort of trial that assailants use to choose third-festival transporters or data spills.

Stage 2: Vulnerability Analysis

After sorting out weaknesses, indicate the added substances and the establishment reasons liable for those weaknesses. A main driver for a weakness is an old model of an open-supply library. Weakness supervisors must have the option to classify seriousness goes and determine strong arrangements.

Stage 3: Risk Assessment

The vital objective of Risk Assessments is to focus on the weaknesses Common Vulnerability Scoring System (CVSS) doles out a mathematical expense to the seriousness of the weakness. CVSS scores every weakness, beginning from zero to 10, and reaches from openness to influence.

Stage 4: Vulnerability Remediation

Remediation involves more than one gathering running together, which incorporate turn of events, chance control, consistence, tasks, and security gatherings. Different weakness control structures advocate common remediation methodologies for perceived weaknesses. Remediation steps range from refreshing running techniques, developing design control procedures, and fixing programming.

Stage 5: Vulnerability Mitigation

Since currently presently not all perceived weaknesses can go through remediation, forcing relief methods is the resulting heading of activity. Relief makes a specialty of bringing down the commonness of a chose weakness or lessening its terrible effect at the framework. Relief procedures incorporate presenting new assurance measures, evolving products, encryptions, attack floor the board, seller risk the executives, and nonstop security checking.

In table 4, there are recorded different sorts of digital weaknesses, organization name, item name, related malware, and CVSS (Common weakness scoring framework). By this data we can comprehend that where organization's item digital weakness is there with their related malwares, and scope of CSVV[14], [15].

Table 4: Vulnerability with CVSS

Cyber Vulnerability	Company	Product	Associated Malware	CVSS
CVE-2017-0199	Microsoft	Office	Latenbot Microsoft Word Intruder Hancitor Dridex FinFisher Silent Doc Exploit REMCOS PoohMilk Freenki	9.3

			FreeMilk Cerber	
CVE-2016-0189	Microsoft	Internet Explorer	RIG Exploit Kit Sundown Exploit Kit Magnitude Exploit Kit Terror Exploit Kit Magnier Neutrino Exploit Kit Astrum Exploit Kit Grandsoft Exploit kit Bleeding Life Exploit Kit Matrix Ransomware Disdain Exploit Kit Kaixin Exploit Kit	7.6
CVE-2017-0022	Microsoft	Windows	Neutrino Exploit Kit Astrum Exploit Kit	4.3
CVE-2016-7200	Microsoft	Edge	Neutrino Exploit Kit Sundown Exploit Kit Kaixin Exploit Kit RIG Exploit Kit	7.6
CVE-2015-8651	Adobe	Flash Player	RIG Exploit Kit Astrum Exploit Kit Matrix Ransomware Anguler Exploit Kit Ramnit	9.3
CVE-2017-1019	Adobe	Flash Player	Magnitude Exploit Kit Astrum Exploit Kit Nuclear Pack Exploit Kit DealersChoice Neutrino Exploit Kit Angier Exploit Kit Pangimop Cerber Locky	10
CVE-2017-0037	Microsoft	Internet Explorer/ Edge	Disdain Exploit Kit Terror Exploit Kit Cerber	7.6

Detection Phases:

Detection of the intrusion might occur throughout any section of the intrusion process [11]. Figure one shows associate degree early detection, throughout the delivery section. Figure a pair of shows associate degree example of detection in a very later section, C2.

Early detection phase:

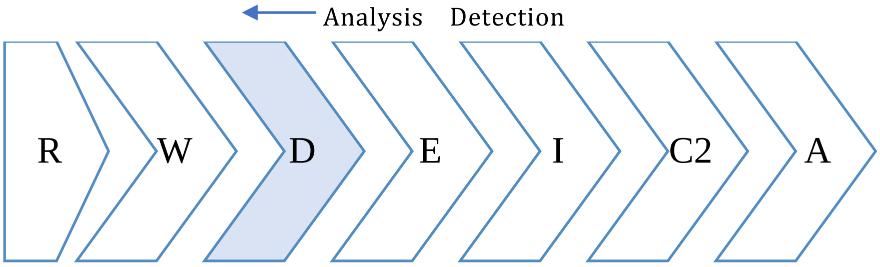


Figure 1: Early detection phases of the Kill Chain model

Late detection phase:

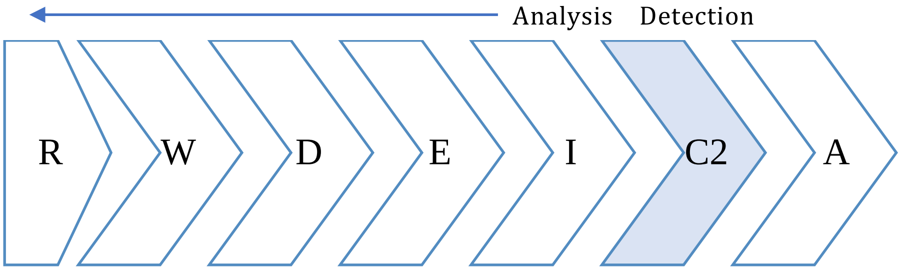


Figure 2: Late detection phases of the Kill Chain model

The Kill Chain Model is exclusive therein it combines intelligence from totally different phases to spot the character and degree of the intrusion.

IV. MODELING AND ANALYSIS

In this phase we are going to demonstrate the manner that we are able to use our totally different we tend token's location device for mechanization we tend to are mainly centers around weakness examination step therein we perform automation we are going to utilize basically Nmap nikto and Burp suite equipment these devices are effectively accessible on Linux operating framework similarly as ubuntu operating frameworks

Introduction and Applications of tools:

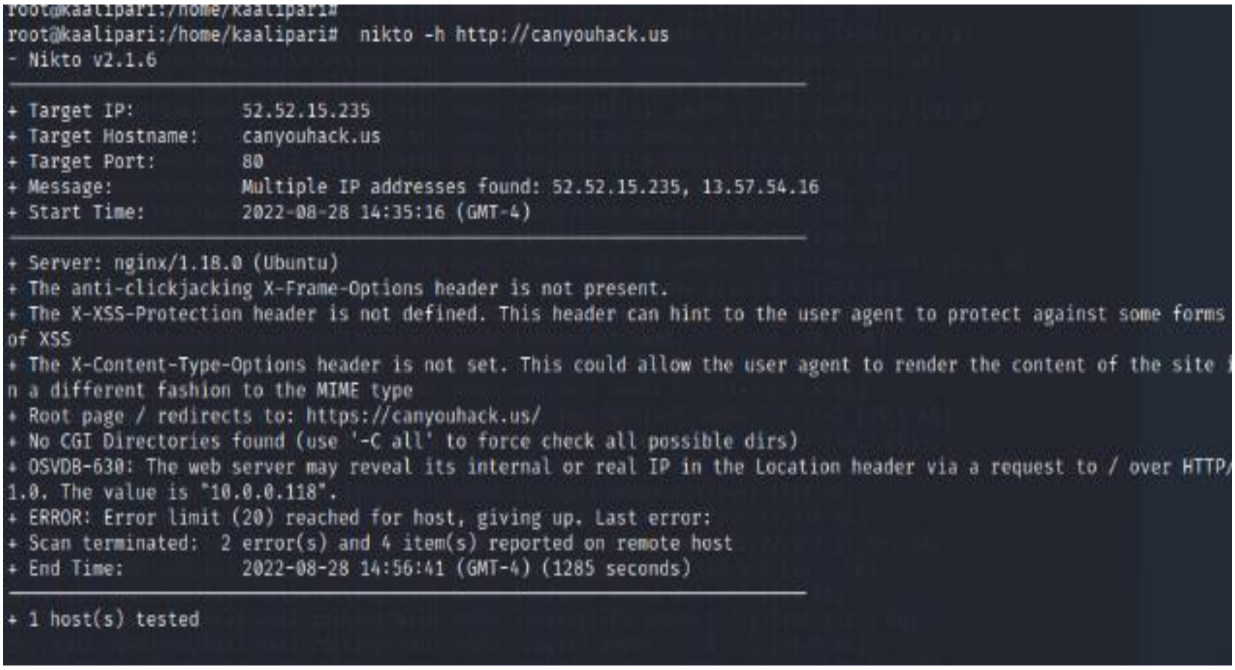
1. Nikto: Nikto could be an internet server filtering device that's meant to perform totally different knowledge social event and weaknesses analysis errands, for instance, gathering servers' knowledge, finding programming misconfigurations, characterizing default documents and comes running on an internet server, recognizing misconfigured or unsure records and comes, and distinctive obsolete internet servers and comes. The extent of those filtering undertakings is incredibly important.

Significant parts of Nikto:

- SSL support for UNIX operating system and Windows OS
- HTTP intercessor support
- Different ports and servers filtering
- Different result document styles
- Encoding ways (for IDS avoidance)
- Change ways for fishing
- Custom filtering selections
- Bogus positive decreasing procedures
- Certifications speculating for approval

Following is that the essential order for nikto. during this order we do not want any extraordinary selections or boundaries for begin the filtering.

nikto -h <target server> [16]



```
root@kaalipari:/home/kaalipari#
root@kaalipari:/home/kaalipari#  nikto -h http://canyouhack.us
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          52.52.15.235
+ Target Hostname:    canyouhack.us
+ Target Port:        80
+ Message:            Multiple IP addresses found: 52.52.15.235, 13.57.54.16
+ Start Time:         2022-08-28 14:35:16 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx/1.18.0 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms
of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site i
n a different fashion to the MIME type
+ Root page / redirects to: https://canyouhack.us/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to / over HTTP/
1.0. The value is "10.0.0.118".
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated:  2 error(s) and 4 item(s) reported on remote host
+ End Time:           2022-08-28 14:56:41 (GMT-4) (1285 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

The manner that nikto runs such unnumbered tests goes with it an unbelievable call for overseers and security engineers desperate to realize neglected script style problems and presumably malignant documents that leave you defenseless against assaults

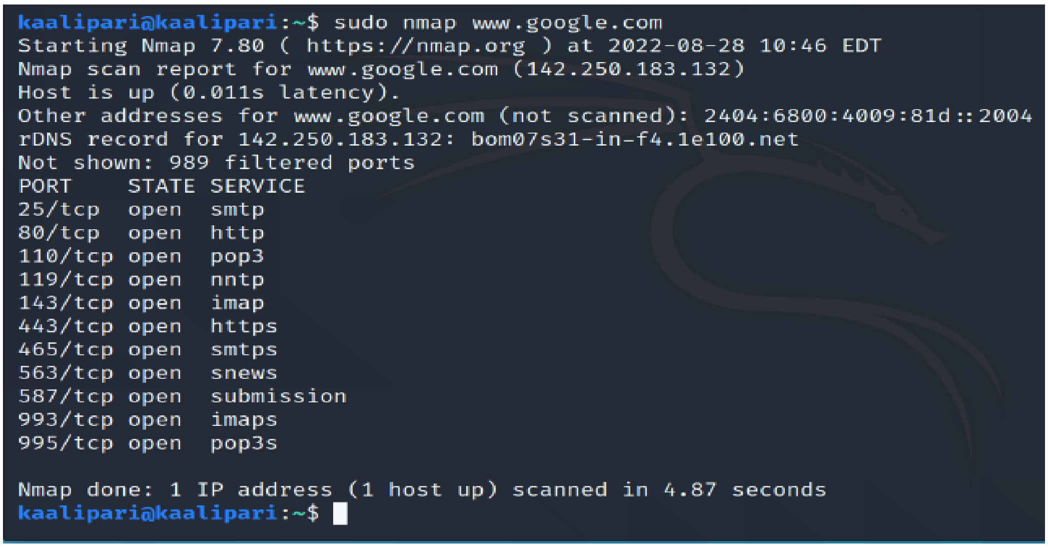
2. Nmap: Nmap is a corporation plotter that's used for network revelation and examining undertakings. the middle errands performed by the device incorporate live organization has revelation, finding varied administrations running on every host, flag snatching, and grouping knowledge regarding firewalls and parcel separating frameworks used by the target organizations. aside from network coming up with, Nmap contains a prearranging highlight that's used to look at types of organization weaknesses.

Significant highlights of Nmap:

- Further developed NSE practicality
- Better IPv6 support
- Quicker network filtering
- Better TLS/SSL examining
- Distinguishing operating frameworks running on network gadgets.
- Security examining.
- Network coming up with.
- Performing administration revealing through the ID of hosts and also the applications/forms they are running.

In Nmap we've usually got 2 basic orders by that we will end our weakness scan [17]:

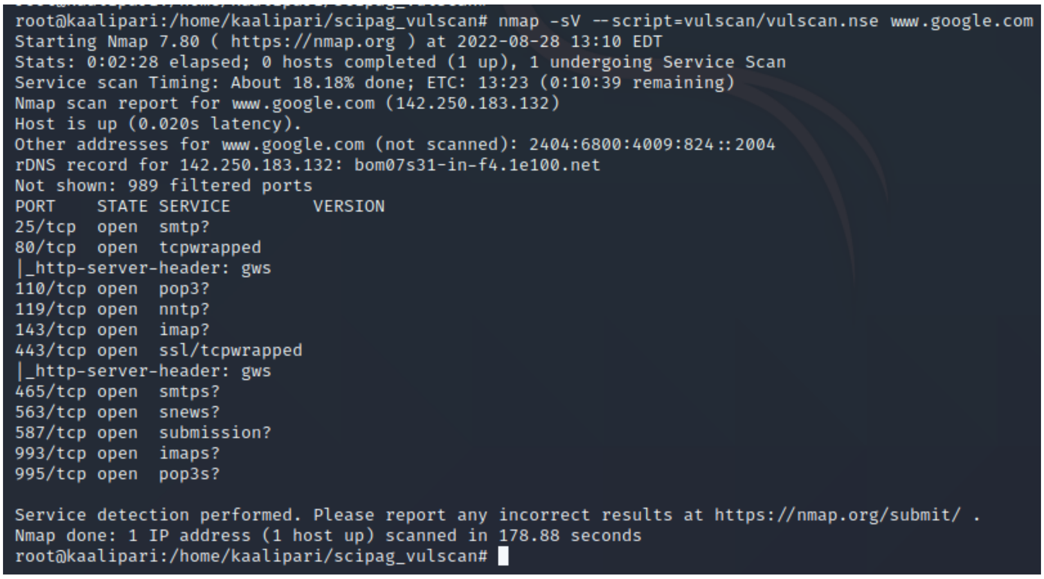
nmap www.example.com



```
kaalipari@kaalipari:~$ sudo nmap www.google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-28 10:46 EDT
Nmap scan report for www.google.com (142.250.183.132)
Host is up (0.011s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:81d::2004
rDNS record for 142.250.183.132: bom07s31-in-f4.1e100.net
Not shown: 989 filtered ports
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
110/tcp open  pop3
119/tcp open  nntp
143/tcp open  imap
443/tcp open  https
465/tcp open  smtps
563/tcp open  snews
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 4.87 seconds
kaalipari@kaalipari:~$ 
```

nmap -sV --script=vulscan/vulscan.nse www.example.com



```
root@kaalipari:/home/kaalipari/scipag_vulscan# nmap -sV --script=vulscan/vulscan.nse www.google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-28 13:10 EDT
Stats: 0:02:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 18.18% done; ETC: 13:23 (0:10:39 remaining)
Nmap scan report for www.google.com (142.250.183.132)
Host is up (0.020s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:824::2004
rDNS record for 142.250.183.132: bom07s31-in-f4.1e100.net
Not shown: 989 filtered ports
PORT     STATE SERVICE        VERSION
25/tcp   open  smtp?
80/tcp   open  tcpwrapped
|_http-server-header: gws
110/tcp open  pop3?
119/tcp open  nntp?
143/tcp open  imap?
443/tcp open  ssl/tcpwrapped
|_http-server-header: gws
465/tcp open  smtps?
563/tcp open  snews?
587/tcp open  submission?
993/tcp open  imaps?
995/tcp open  pop3s?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 178.88 seconds
root@kaalipari:/home/kaalipari/scipag_vulscan# 
```

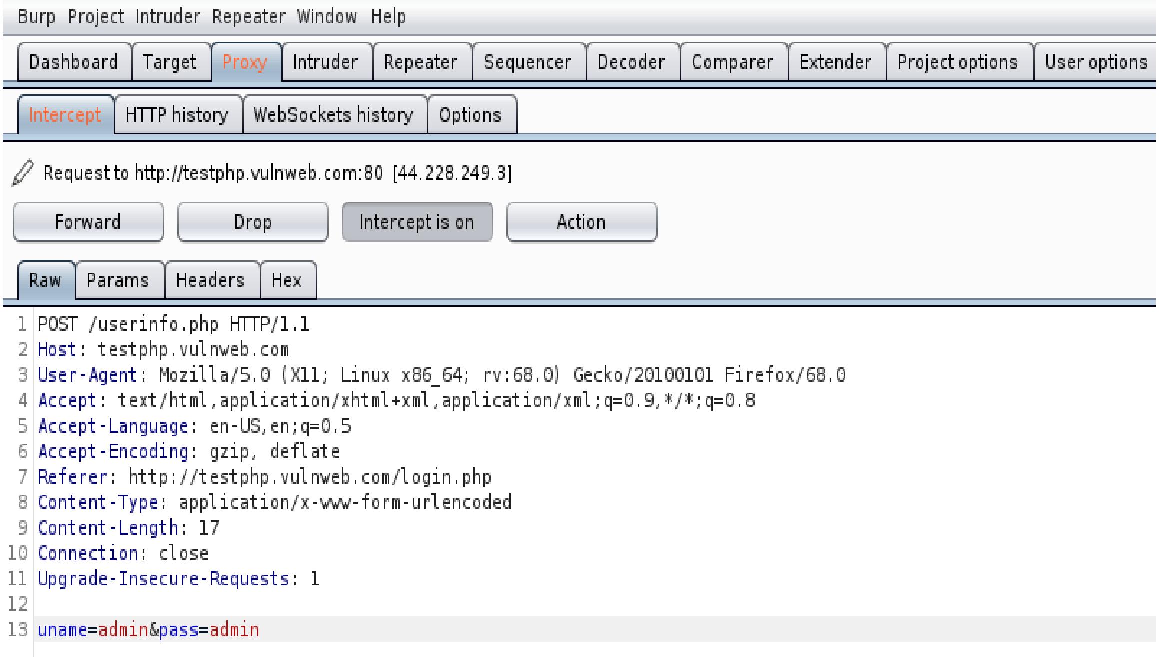
Nmap could be a illustrious instrument for programmers that is that the primary justification for why security specialists shrewdness to utilize it. With Nmap you'll accomplish one thing aside from hunt down open ports on your organization. It likewise finds knowledge out there to expected aggressors.

3. Burp Suite: Burp Suite could be a Java-based system for playacting internet application security testing. the various devices that compose the Burp Suite work to assist the total testing method. The Burp family likewise carries out totally different roles that create this summing up as a result of scanners. Burp has various security instruments like CI combine and list preventive intercessor. preventive intermediaries assist with deciding however applications answer things like stunning info delays or hindered network associations. Administrations solid against unfavorable circumstances have higher time and square measure safer against Internet-based assaults.

Significant highlights of Burp Suite:

- Easy Scan Setup
- Scalable Scan
- Scan fashionable internet
- Custom Configurations
- Risk Management Platforms

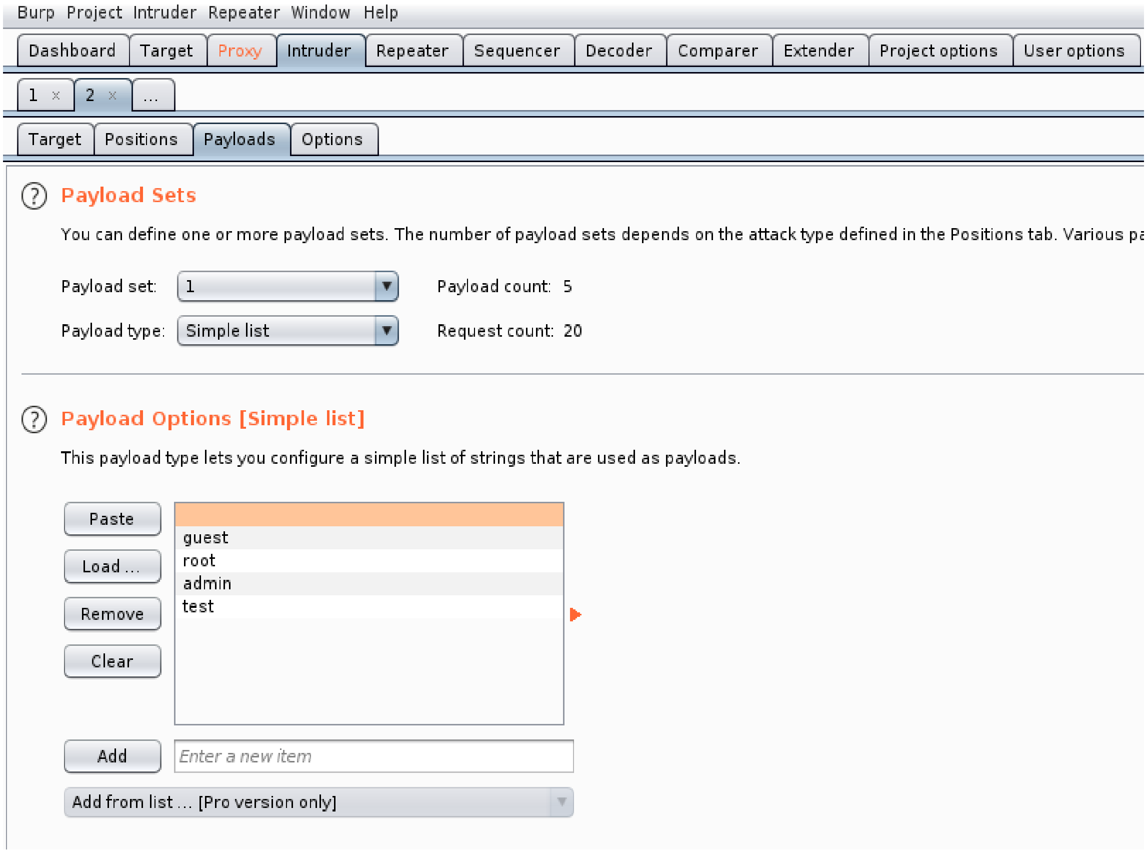
To utilize Burp Suite, you must set 127.0.0.1 as scientific discipline address to port range 808. Then found out associate degree intercessor shopper in your program.



Request to http://testphp.vulnweb.com:80 [44.228.249.3]

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testphp.vulnweb.com/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 17
Connection: close
Upgrade-Insecure-Requests: 1

uname=admin&pass=admin
```



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various pa

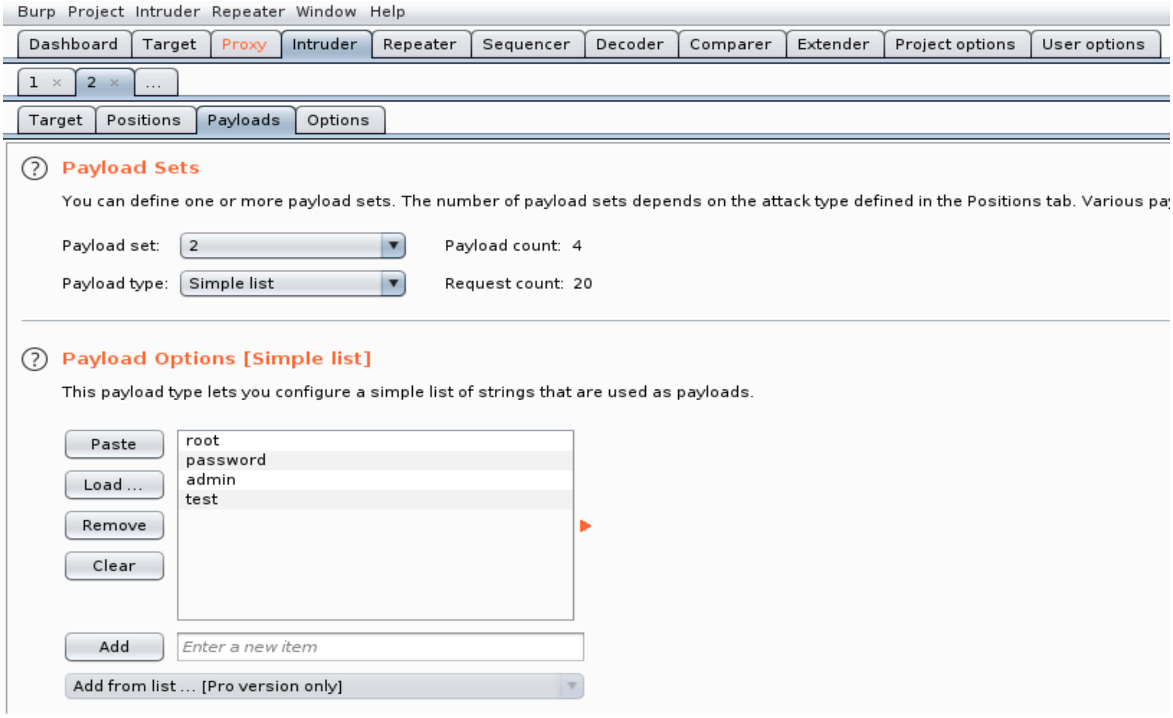
Payload set: 1 Payload count: 5

Payload type: Simple list Request count: 20

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

guest
root
admin
test



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various pa

Payload set: 2
Payload type: Simple list
Payload count: 4
Request count: 20

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
root
password
admin
test
```

The burp capturing intercessor will likewise be used to screen HTTP traffic among servers and shoppers squarely therefore people being checked won't understand you're look this is often valuable whereas perceptive for baneful inward organization traffic

V. RESULT

Vulnerability screening alludes to native associations and organizations to ponder the gamble of the vulnerable. There is square measure several styles of scanners accessible for your requirements. however, we tend to decide depends upon our expertise. If you're keen on filtering our home association, the Burp suite will be serious but within the event that you just square measure keen on establishing and addressing a colossal business climate, you got to explore for a couple of skilled scanners.

VI. CONCLUSION

Cyber-attacks are at the upward thrust. Beginning with simple attacks such as defacing homepages or obtaining personal information cyber-attacks have evolved into complex attacks such as stealing state secrets and attacking national infrastructure. Cyber-attacks consist of different types of attack elements. Many security studies have looked at the sophistication of cyber-attacks; However, research on the complexity of predictive attacks is lacking. We explore automation in vulnerability analysis using various tools. Additionally, we describe the features of the tools we use. We also collect information about which tools are best suited for different situations. This document helps security managers define strategies against threats in a multimedia service environment helps establish secure visibility of threats occurring in an organization and countermeasures for each stage of intrusion.

VII. FUTURE WORK

In future work we intend to perform definite weakness portrayal and countermeasures considering the apparatuses introduced in this review. This area of digital assault is exceptionally delicate and under a microscope in data security. This requires nonstop and far-reaching exploration to see new danger dangers and take advantage of regions to help counterproductive safeguard systems. The main power to battle digital assaults is innovation improvement. This engages aggressors and gives them a benefit in creating exploits and assault vectors since it requires around 206 days for an association to recognize and contain an assault. This work simply examined seven stages and how to diminish the assault surface to restrict the aggressor's progress. Each step of the digital kill chain is a strong and researchable region for scientists. Future bearings for work and exploration are as per the following:

1. Absolute executioner streak. We construct a quantitative kill fasten model to distinguish and break down assailant actions.

2. Quantitative examination of key hubs. We utilize quantitative investigation to track down key hubs to focus for preservation.

VIII. REFERENCES

[1] Adrian Duncan, Sadie Creese, and Michael Goldsmith, "A Combined Attack-Tree and Kill-Chain Approach to Designing Attack-Detection Strategies for Malicious Insiders in Cloud Computing," in 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, United Kingdom, Jun. 2019, pp. 1–9. doi: 10.1109/CyberSecPODS.2019.8885401.

[2] R. HosseiniNejad, H. HaddadPajouh, A. Dehghantanha, and R. M. Parizi, "A Cyber Kill Chain Based Analysis of Remote Access Trojans," in Handbook of Big Data and IoT Security, A. Dehghantanha and K.-K. R. Choo, Eds. Cham: Springer International Publishing, 2019, pp. 273–299. doi: 10.1007/978-3-030-10543-3_12.

[3] J. Du, X. Zhang, G. Suo, R. Guo, and G. Lu, "A Method of Network Behavior Recognition and Attack Scenario Reconstruction for Attack Kill Chain," presented at the Proceedings of the 2019 International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME 2019), Guilin, China, 2019. doi: 10.2991/wcnme-19.2019.23.

[4] Shuo Wang, Qingqi Pei, Yuchen Zhang, Xiaohu Liu, and Guangming Tang, "A Hybrid Cyber Defense Mechanism to Mitigate the Persistent Scan and Foothold Attack," Secur. Commun. Netw., vol. 2020, pp. 1–15, Oct. 2020, doi: 10.1155/2020/8882200.

[5] Muhammad Mudassar Yamin, Mohib Ullah, Habib Ullah, B. Katt, M. Hijji, and K. Muhammad, "Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security," Mathematics, vol. 10, no. 12, p. 2054, Jun. 2022, doi: 10.3390/math10122054.

[6] J. Lin, C. Liu, X. Cui, and Z. Jia, "Poster: A Website Protection Framework Against Targeted Attacks based on Cyber Deception," p. 2.

[7] Houssain Kettani and Robert M Cannistra, "On Cyber Threats to Smart Digital Environments," p. 6, 2018.

[8] "WHAT IS THE CYBER KILL CHAIN? PROCESS & MODEL." 2021. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/

[9] Xiaojun Zhou, Zhen Xu, L. Wang, K. Chen, C. Chen, and W. Zhang, "Kill Chain for Industrial Control System," MATEC Web Conf., vol. 173, p. 01013, 2018, doi: 10.1051/matecconf/201817301013.

[10] "Cyber Kill Chain: Understanding and Mitigating Advanced Persistent Threats." 2020. [Online]. Available: https://www.exabeam.com/information-security/cyber-kill-chain/

[11] Levent Ertaul and Mina Mousa, "Applying the Kill Chain and Diamond Models to Microsoft Advanced Threat Analytics," p. 7.

[12] T. Devaux, T. Massip, A. Ulliac, J.-L. Simoni, and P. Varela, "Automation of Risk-Based Vulnerability Management Based on a Cyber Kill Chain Model," p. 16, 2021.

[13] Pooneh Nikkhah Bahrami, Ali Dehghantanha, T. Dargahi, R. M. Parizi, K.-K. R. Choo, and H. H. S. Javadi, "Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures," J. Inf. Process. Syst., vol. 15, no. 4, pp. 865–889, Aug. 2019, doi: 10.3745/JIPS.03.0126.

[14] "Top 10 Cyber Security Vulnerabilities Used by Cyber Criminals Read more at: https://www.appknox.com/blog/top-10-cybersecurity-vulnerabilities." 2018.

[15] "Computer Vulnerabilities: How Safe Are Your Systems?" 2018. [Online]. Available: https://www.smarttech247.com/news/computer-vulnerabilities-safe-systems/

[16] "nikto." [Online]. Available: https://github.com/sullo/nikto

[17] "nmap." [Online]. Available: https://github.com/scipag/vulscan