

PREVIEW PREVIEW PREVIEW PREVIEW

Hacking

VOL. 19

NO. 02



RECONNAISSANCE STAGE OF ATTACK

STAGE ONE – RECONNAISSANCE

REVEALING KILLNET: THE POWER OF RECONNAISSANCE WITH DNS DUMPSTER

METHODS FOR ANALYZING THE HUMAN RESOURCE ASPECT OF CYBERSECURITY AND ESPIONAGE

IDENTIFYING ATTACKERS IN THE EARLY PHASE OF THE CYBER KILL

PREVIEW PREVIEW PREVIEW PREVIEW

EDITOR'S WORD

Dear Readers,

Welcome to the new Hakin9 ebook, titled "Reconnaissance Stage of Attack". This edition is dedicated to exploring the critical initial phase in the cyber kill chain: reconnaissance. As the gateway through which all subsequent attacks are launched, understanding and mitigating threats at this stage is essential for robust cybersecurity defenses.

This issue comprises articles that shed light on the varied aspects of reconnaissance—from the strategic use of tools like DNS Dumpster by groups such as Killnet, to the roles that human resources play in both perpetrating and defending against espionage. We will guide you through the nuances of modern reconnaissance methods, uncover the shadowy practices of dark web surveillance, and provide expert insights into identifying attackers early in their campaigns.

Our expert contributors, including leaders in digital security and seasoned analysts, offer deep dives into how threat intelligence can be effectively employed to anticipate and neutralize threats before they evolve into full-scale attacks. Additionally, the issue includes a special feature with Gilbert Oviedo, who answers pressing questions about reconnaissance tactics and defenses.

Each article in this issue is designed not only to inform but also to equip you with the knowledge and strategies needed to enhance your defensive measures against the sophisticated techniques employed by today's cyber adversaries.

Join us as we explore these pivotal themes, providing you with the insights necessary to understand the complexities of reconnaissance and fortify your defenses against the ever-evolving landscape of cyber threats. Whether you are a cybersecurity veteran or new to the field, this issue is an essential resource for staying ahead in the dynamic world of digital security.

Helena and the Hakin9 Team

HELENA.PIORUN@HAKIN9.ORG

Cover Image

Wiktoria Bukowska

Cover Design

Wiktoria Bukowska

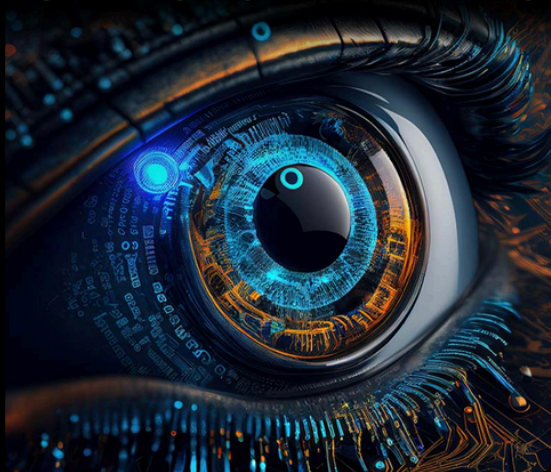
Reviewers

André Luiz, Momen Eldawakhly, Jonatan Perez, Alberto, Frank Moerdel, Steve, Shaw Cross, Salman Aslam, Craig, Shweta Chawla, Ihab, Michal Jachim, Mukund Sarma, Joern Kuhr, Blair Gormley, Ranjitha R, Steve Shaw Cross, Amit Chugh, Michele Albano, Emanuele Placidi, Jordan M. Bonagura, Setu, Matt Takas

04	UNVEILING CYBER THREATS: UNDERSTANDING RECONNAISSANCE IN THE CYBER KILL CHAIN AND THE IMPORTANCE OF THREAT INTELLIGENCE
16	REVEALING KILLNET: THE POWER OF RECONNAISSANCE WITH DNS DUMPSTER
26	METHODS FOR ANALYZING THE HUMAN RESOURCE ASPECT OF CYBERSECURITY AND ESPIONAGE
35	CYBER KILL CHAIN: RECONNAISSANCE
42	IDENTIFYING ATTACKERS IN THE EARLY PHASE OF THE CYBER KILL CHAIN
49	STAGE ONE – RECONNAISSANCE
63	UNVEILING DIGITAL SHADOWS: UNDERSTANDING MODERN RECONNAISSANCE TECHNIQUES
81	DARK WEB RECONNAISSANCE: THE ART OF UNCOVERING THE HIDDEN ADVERSARIES
88	STRATEGIES FOR DEFENDING AGAINST KILL CHAIN RECONNAISSANCE
100	SECURITY IMPLICATIONS OF SERVERLESS COMPUTING IN THE CLOUD

All trademarks, trade names, or logos mentioned or used are the property of their respective owners. The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

OSINT TOOLS & TTPs FOR PENTESTERS AND RED TEAMERS



OSINT TOOLS & TTPs FOR PENTESTERS AND RED TEAMERS (W48)

In this course, Eva Prokofiev, the prominent expert in the CTI and OSINT areas, will share with you her know-how and point of view on how to examine a target not only from a "pentester's angle", but also from other cybersecurity perspectives.

All trademarks, trade names, or logos mentioned or used are the property of their respective owners. The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

CYBER KILL CHAIN: RECONNAISSANCE

Priyanka Tomar

No wonder that cyber threats pose a significant risk to all of us be it individuals, organizations and nations. Cyber-attacks are becoming sophisticated day by day therefore understanding the attack methodologies used by cyber threat actors is crucial for defensive purposes. Here Cyber Kill Chain framework comes into play, it was developed by Lockheed Martin. The Cyber Kill Chain framework provides a well-structured approach to understand the various stages of a cyber-attack, from reconnaissance to data exfiltration. In this article, we discuss the first phase of the Cyber Kill Chain i.e. reconnaissance.

The Cyber Kill Chain Overview

The Cyber Kill Chain's concept has been drawn from military strategy which was adapted for cybersecurity purposes. It outlines the steps of a cyber-attack, allowing defenders to understand effectively intervene in the cyber-attack process. The seven stages of the Cyber Kill Chain are:

1. **Reconnaissance:** Collecting information about the target.
2. **Weaponization:** Cyber attackers develop or acquire the tools and methods necessary to exploit the vulnerabilities identified during reconnaissance. Weaponization can take various forms, including the creation of custom malware tailored to specific targets or the repurposing of existing exploits to suit the attacker's needs.
3. **Delivery:** Attackers deliver the malicious payload such as malware or exploit code to the target. The objective of the delivery phase is to successfully infiltrate the target

environment

4. **Exploitation:** Exploiting the weaknesses to gain access to the target device.
5. **Installation:** Establishing a foothold within the compromised device.
6. **Command and Control (C2):** Setting up communication channels for taking over the remote control of target device.
7. **Actions on Objectives:** Achieving the cyber-attacks goals such as data breach or disruption of the operation.

Each stage plays a critical role in the cyber-attack kill chain with defenders aiming to disrupt the chain at any stage to thwart the attack.

The Reconnaissance

Reconnaissance is the first stage of the Cyber Kill Chain, is considered the most critical part. It sets the foundation for the cyber-attack because it provides the vital information about the target. The goal of reconnaissance is to collect as much information as possible about the target so that next stages of the cyber attack can be planned effectively. These stages may be gaining unauthorized access, exploiting vulnerabilities or launching targeted phishing campaigns etc. By understanding the reconnaissance phase, organizations can implement measures to detect and prevent attackers from gathering information and initiating subsequent stages of the cyber kill chain.

In cyber warfare, adversaries increasingly turn to the dark web to procure reconnaissance data offered by cybercriminals. The dark web encompasses a plethora of websites, forums, shops, and marketplaces specializing in the sale of unlawfully obtained information. Utilizing personally identifiable information (PII) sourced from the dark web, hackers orchestrate social engineering attacks, such as phishing emails, domain name manipulation, and IP address spoofing. Beyond credentials, the dark web serves as a marketplace for cybercriminals to peddle malware, tools, and code, facilitating various malicious endeavors like code injection attacks.

As part of their reconnaissance efforts, cybercriminals seek out

vulnerabilities within target networks. These vulnerabilities often manifest in the form of outdated operating systems, vulnerable applications, insecure tools, and inadequately configured security firewalls. The dark web equips hackers with an arsenal of firewalls and antivirus evasion malware, enabling them to infiltrate networks clandestinely and evade detection.

Reconnaissance can be done in multiple ways such as :

1. **Passive Reconnaissance:** Collecting publicly accessible data related to the target from diverse sources such as social media platforms, corporate websites, or public databases, directories, and archives is a common tactic. This process involves obtaining domain names, IP addresses, and subdomains linked to the target through sources such as WHOIS records. Additionally, they may acquire email addresses, job listings published by the target organization and contact information. Attackers analyse publicly available historical data to gain valuable insights. Moreover, they can discern potential targets for social engineering maneuvers from the amassed information. Attackers might get details about the physical location of servers.
- **Active Reconnaissance:** It includes probing the target's network infrastructure for vulnerabilities. Attackers identify open ports and services on target systems using tools like Nmap because this information provides insight into the network architecture and potential vulnerabilities. Further they collect detailed information about the services running on open ports such as version numbers and configurations. This helps attackers identify known vulnerabilities that can be exploited. They use automated tools to scan for known vulnerabilities in software, operating systems, or network devices. This helps attackers identify potential points of entry into the target's systems. Attackers can capture and analyze network traffic to gather information such as usernames, passwords, or other sensitive data being transmitted over the network. Attackers scan wireless network in the target's vicinity to identify SSIDs,

encryption types and potential points of entry.

Techniques Used in Reconnaissance

Cyber Threat actors employ variety of techniques during the reconnaissance phase to collect intelligence about their target. Some common reconnaissance techniques are:

1. **Open-Source Intelligence (OSINT):** Cyber threat actors leverage publicly and freely available information from various sources like social media, company websites, job postings and news articles etc. to gather information about the target, organization's employees, technologies and infrastructure.
2. **Network Scanning:** Cyber attackers conducting scans on target's network to identify active hosts, open ports and services running on those open ports. Tools such as Nmap and Shodan are commonly used for scanning purpose.
3. **Vulnerability Scanning:** Identifying potential weaknesses or vulnerabilities within the target's network infrastructure is also part of reconnaissance process. Vulnerability scanning tools such as Nessus, Burpsuite, Nexpose and OpenVAS can automate this process because these tools scans for known vulnerabilities in network devices, servers and applications.
4. **Social Engineering:** Manipulating individuals within the target organization to reveal sensitive information or grant unauthorized access to the target falls under social engineering. This can be achieved through multiple techniques such as phishing emails, pretexting (creating a false scenario to obtain information), or impersonation (This may involve imitating another person's voice, appearance, or behaviour to deceive others into thinking they are that person).
5. **Dumpster Diving:** Physically or digitally searching through the target organization's trash or discarded documents to find valuable information such as usernames, passwords, financial documents or internal documents.
6. **DNS Enumeration:** Gathering information about domain names, subdomains and associated IP addresses of the target organizations. Multiple techniques can be used such as DNS

zone transfers, DNS querying, and DNS reconnaissance tools like DNSrecon, NSlookup, DNSenum etc .

7. **Website Analysis:** Analysing the target organization's website for information such as employee names, email addresses, internal systems, software versions and other potentially sensitive data.

Mitigating Reconnaissance Attacks

Considering the critical role of reconnaissance in the Cyber Kill Chain, organizations must employ robust strategies to mitigate reconnaissance attempts effectively. Some best practices for defending against reconnaissance attacks include:

1. **Implementing Security Controls:** Implementing robust security controls involves deploying necessary network safeguards such as firewalls, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). These defensive techniques actively surveillance network traffic and helps in identifying and thwarting reconnaissance activities. Firewalls regulate traffic flow while IDS and IPS analyze anomalies and promptly respond to potential cyber threats ensuring a fortified network environment against malicious intrusions or similar activities.
2. **Patch Management:** Regularly patching and updating software and systems to address known vulnerabilities helps in reducing the possibilities of successful exploitation during the reconnaissance phase.
3. **Network Segmentation:** Segmenting the network into smaller subnetworks is important for managing reconnaissance risks and deterring lateral movement of cyber threat actors. By dividing the network into more manageable and smaller units, constrains the scope of potential cybersecurity breaches and enhance overall cyber security posture of the organization. Also, it minimizes the impact of unauthorized access attempts.
4. **Monitoring and Logging:** Implementation of robust logging and monitoring protocols is aimed at detecting and analysing network traffic, system logs, and user conduct to identify

potential reconnaissance or malicious activities.

5. **Security Awareness Programs:** Regular cyber security awareness initiatives, coupled with simulated phishing drills, serve to fortify adherence to sound security protocols among staff. These efforts also play a pivotal role in empowering employees to discern and promptly report any dubious behaviours or incidents. By instilling a heightened sense of vigilance and competence, such programs contribute significantly to the overall resilience of the organization against potential security threats and breaches. Educating employees about the risks of social engineering attacks and imparting training on how to recognize and respond to suspicious emails, phone calls or other forms of communication.
6. **Information Sharing:** Participation in information-sharing endeavours within the cybersecurity community is essential for staying informed about emerging threats and the tactics employed by threat actors, especially during the reconnaissance phase. By actively engaging in these initiatives, individuals and organizations can enhance their awareness and preparedness against potential cybersecurity risks. Sharing insights, best practices, and intelligence not only fosters a collective defense posture but also facilitates the timely dissemination of critical information to thwart malicious activities.

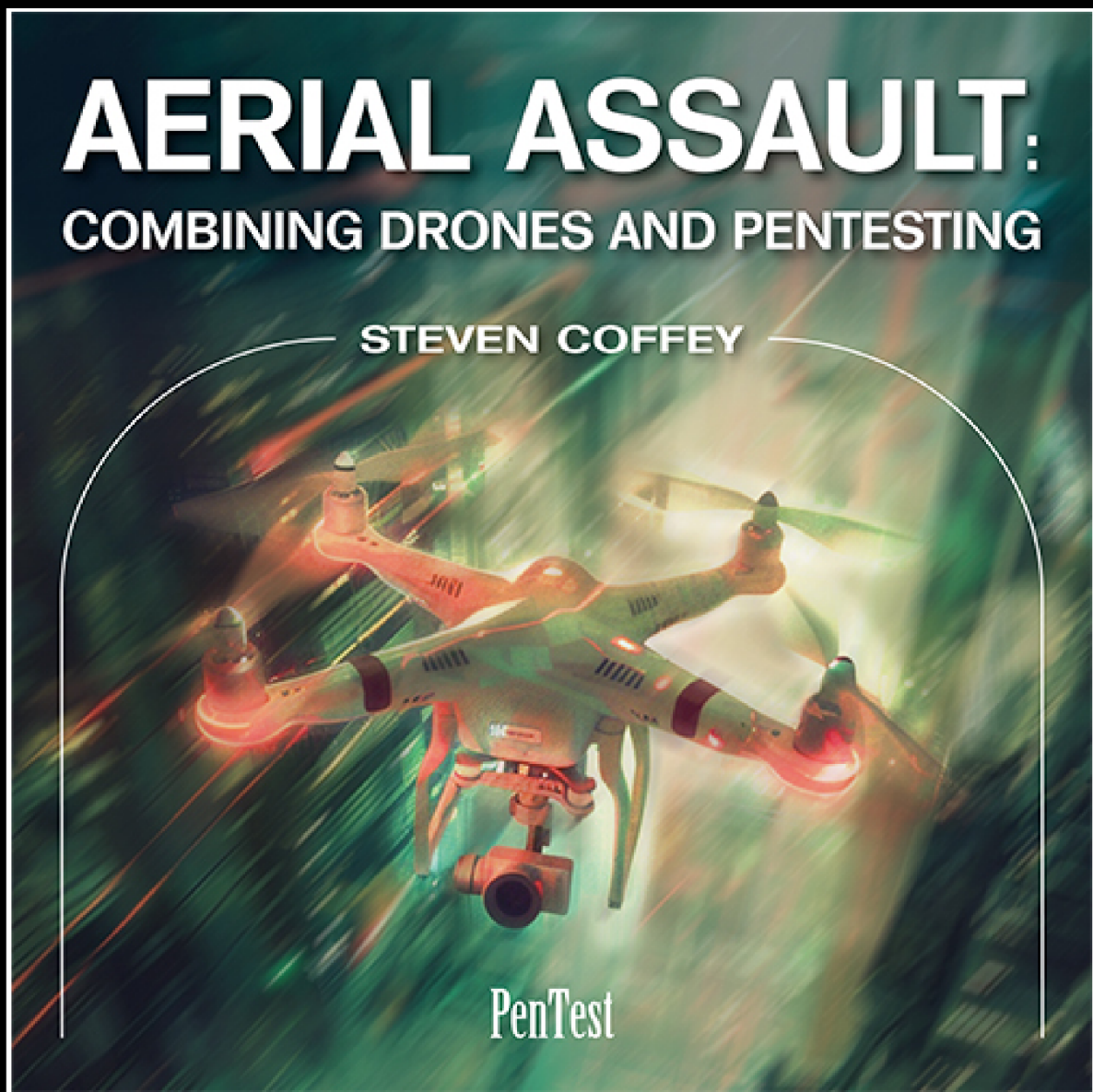
Conclusion

Reconnaissance plays an important role in the Cyber Kill Chain, serving as the foundation to understand how cyber-attacks are planned and executed. By understanding the techniques employed by threat actors during the reconnaissance phase and implementing effective defense strategies, organizations can significantly reduce their susceptibility to cyber threats. Through continuous vigilance, education, and collaboration, defenders can stay one step ahead of adversaries and safeguard their digital assets against malicious actors.

Priyanka Tomar

cyberpathshalaindia.com

NEW COURSE OUT NOW!



AS DRONES BECOME MORE ACCESSIBLE AND ADVANCED, THEIR POTENTIAL FOR BOTH OFFENSIVE OPERATIONS AND DEFENSIVE STRATEGIES GROWS.