Red Team Knife to improve Cyber Security Education

Danilo Caivano[1,†], Adriano Gentile[1,*,†], Gennaro Del Campo[2,†], Davide Pio Posa[1,*,†] and Antonio Piccinno[1,†]

[1]Department of Computer Science, University of Bari Aldo Moro
[2]SER&Practices, Spin-off of the University of Bari Aldo Moro

Abstract

The increasing ubiquity of digital systems in daily life has significantly expanded the attack surface for cyber threats, demanding new tools and methodologies for effective defense. Traditional security practices are no longer sufficient in the face of evolving and sophisticated cyberattacks. Therefore, this paper introduces Red Team Knife (RTK), a tool designed to support cybersecurity education and practice by guiding users—both novices and experts—through structured penetration testing activities aligned with the Cyber Kill Chain model. RTK integrates widely-used red teaming tools (e.g., Nmap, Sqlmap, theHarvester) within a user-friendly graphical interface built on the MVC paradigm. It provides contextual guidance and execution support to enhance usability and streamline pentesting workflows. The tool was tested on vulnerable virtual machines (XVWA and OWASP BWA), demonstrating its ability to identify security flaws, assist users with targeted hints, and maintain a persistent knowledge base through result saving and restoration features. RTK represents a valuable contribution to cybersecurity training and operational efficiency. Providing a guided, modular, and extensible environment for penetration testing improves educational outcomes and real-world security assessments.

Keywords

Cybersecurity, Red team Knife, Education, Cyber Kill Chain

1. Introduction

It is undeniable that the ubiquity of computer systems in our daily lives has created new challenges for security professionals [1]. Where once the protection of sensitive documents was primarily a matter of choosing a lock that was resistant to physical attack, today the same challenge arises in a very different and highly digital context [2]. Digital technologies have radically changed the security landscape and introduced a new type of vulnerability. Rather than being physically stored in a specific location, document archives are now virtual and accessible from anywhere in the world via the Internet. This change has necessitated a new perspective on data protection, requiring computer security professionals to adapt to a rapidly changing environment continually[3]. In addition to changing vulnerabilities, the tools available to security professionals are also constantly changing. In today's environment, a cybersecurity professional must not only be aware of evolving digital threats, but also master the tools and techniques needed to effectively counter them [4].

In this dynamic scenario, knowledge of the available 'tools' becomes critical. Computer security professionals must be able to use a wide range of tools and technologies to protect data and digital infrastructures effectively [5]. Among computer security methodologies, penetration testing is emerging as a critical approach to assessing the effectiveness of an organization's defenses. This practice, commonly known as 'pentesting', consists of conducting simulations of controlled cyber-attacks in order to identify vulnerabilities and weaknesses in systems, thus enabling organisations to take targeted corrective action and strengthen their defences.

This research work aims to provide a set of tools that are accessible to both novices and experts performing computer system security testing, to ensure a more uniform and consistent workflow,

Joint Proceedings of IS-EUD 2025: 10th International Symposium on End-User Development, 16-18 June 2025, Munich, Germany.
*Corresponding author.
†These authors contributed equally.
danilo.caivano@uniba.it (D. Caivano); gentile97@studenti.uniba.it (A. Gentile); r.delcampo@serandp.com (G. D. Campo); d.posa3@studenti.uniba.it (D. P. Posa); antonio.piccinno@uniba.it (A. Piccinno)
© 2025 Copyright © 2025 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

CEUR-WS.org/Vol-3978/short-s3-11.pdf

similar to being guided by a 'compass'. The effectiveness of this 'Red Team Knife' will be tested by pentesting a real platform to produce a security report that identifies any existing vulnerabilities and associated risks.

2. Cyber Kill Chain

The Cyber Kill Chain model, originally developed to analyze cyber threats, consists of seven stages: Reconnaissance, Weaponization, Delivery, Exploit, Installation, Command & Control, and Actions [6]. This model enhances visibility into attacks and enriches analysts' understanding of adversary tactics [7]. However, its sequential nature limits its effectiveness against advanced persistent threats, leading to the proposal of a concurrent analysis model that mimics human mental processes [8]. The integration of Artificial Intelligence (AI) along the Cyber Kill Chain shows promise in enhancing defense capabilities, particularly in reconnaissance, intrusion, privilege escalation, and data exfiltration stages [9]. Understanding the technical aspects of each stage, including methodologies, techniques, and tools, is crucial for developing effective incident response and analysis capabilities [10]. When combined with advanced analytics and predictive modeling, the Cyber Kill Chain becomes critical for inside-out security [6].

Seven phases are defined in the cyber kill chain [11]:

1. *Reconnaissance*. The attacker gathers information about the target, such as vulnerabilities, system configurations, and user details, to plan the attack.
2. *Weaponization*. Malicious tools are created by the attacker, like malware or ransomware, to exploit the identified vulnerabilities.
3. *Delivery*. The malicious payload is delivered to the target, often through phishing emails, malicious links, or exploiting software vulnerabilities.
4. *Exploitation*. The malicious code is executed on the target system, exploiting the vulnerabilities to gain unauthorized access.
5. *Installation*. Malware or other malicious components are installed on compromised systems.
6. *Command and Control (C2)*. The attacker establishes communication channels to control compromised systems and execute their plans.
7. *Actions on Objectives*. The attacker achieves their goals, such as data theft, system disruption, or financial gain.

3. Red Team Knife (RTK)

A penetration test (or pentest) is an authorized simulated cyberattack on a computer system, performed to evaluate the security of the system. The pentest is performed to identify weaknesses or vulnerabilities, including the potential for unauthorized parties to gain access to the system's features and data. Thus enabling a comprehensive risk assessment to be carried out.

Red Team Knife[1] serves as an interface to a range of valuable red teaming tools (Figure 1), including: Nmap, Nmap vulnerability scanner, Feroxbuster, theHarvester, Dig, w4af, SMTP Email spoofer, Commix, Sqlmap. Therefore, the aim of Red Team Knife (RTK) is to provide a set of tools accessible experts and non-experts in cybersecurity activities performing security inspections on systems. It is evident that, despite the wide availability of accessible tools for penetration testing, there is a lack of a platform that provides comprehensive and structured support to perform a security analysis. Indeed, existing platforms are not yet well-established, or are only specialised in certain areas.

Therefore, the idea behind *RED Team Knife* emerged from the need to have a guideline during penetration testing activities. Despite the wide availability of publicly accessible tools, there is a lack of a platform that provides complete and structured support for conducting a security analysis. The existing platforms are either not yet established or are only specialised in certain areas. The aim of

[1] https://github.com/Red-Team-Knife/red_team_knife

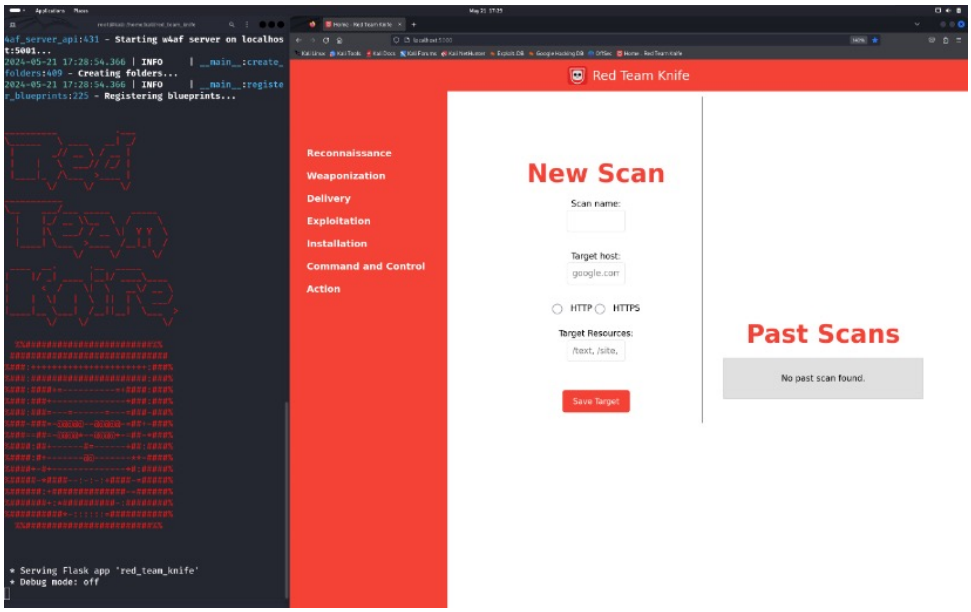

Figure 1: Red Team Knife Dashboard

'Red Team Knife' is, therefore, to provide an organic and interconnected set of tools, which intelligently guides the pentester during use.

These features can be useful both for those who are approaching the discipline of computer security for the first time, often in need of useful indications that are difficult to find immediately from other sources, and for those who already have experience in the field and simply want an improvement in their workflow, which can be greatly enhanced and extended with an effective graphic interface. The tool is designed to guide the user through the steps of the Cyber Kill Chain.

Finally, Red Team Knife aims to offer the possibility of saving and restoring, without excessive effort, the scans performed, so as to conduct an all-round analysis of the system concerned, keeping the results in a cohesive knowledge base.

RTK provides guidelines in the execution of penetration testing with respect to the phases of the Cyber Kill Chain. The tools made available to the user have been linked by providing useful hints proposing a possible continuation after a satisfactory result has been found. It is important to note that the w4af tool can make the user 'backtrack' to the use of Dig. This is because the tool provides useful information for both reconnaissance and weaponisation (Figure 2).

The adopted architectural paradigm is inspired by the MVC (Model-View-Controller) pattern, which comprises three principal components: *Model*, *View* and *Controller*. The Model is responsible for encapsulating the domain-specific structure and implementing the application functionality, i.e. the state and operations that can change the state, using an Observer pattern. The Model also maintains dependencies with the Controller and the View, which notifies of the change of state. The View is responsible for presenting information via a graphical interface, and when the information contained in the View undergoes an update by the responsible Model, the View receives a notification and will change its representation appropriately. Finally, the Controller is responsible for responding to actions that the user performs on the graphical interface.

In particular, the general operating principle of the application is based on the encapsulation of the tools by a controller, which manages the execution, locking and retrieval of the results.

Most of the included tools have command-line interfaces whose results, provided on standard output, are difficult to examine and de-serialise. To overcome this problem, the possibility of saving the results of the tool's execution to a file was exploited, which we refer to in our context as *temp_file*. The operation of the controller is thus as follows: receives an execution request in which target and options are specified; creates the command to be executed by formatting the options correctly; initialises a

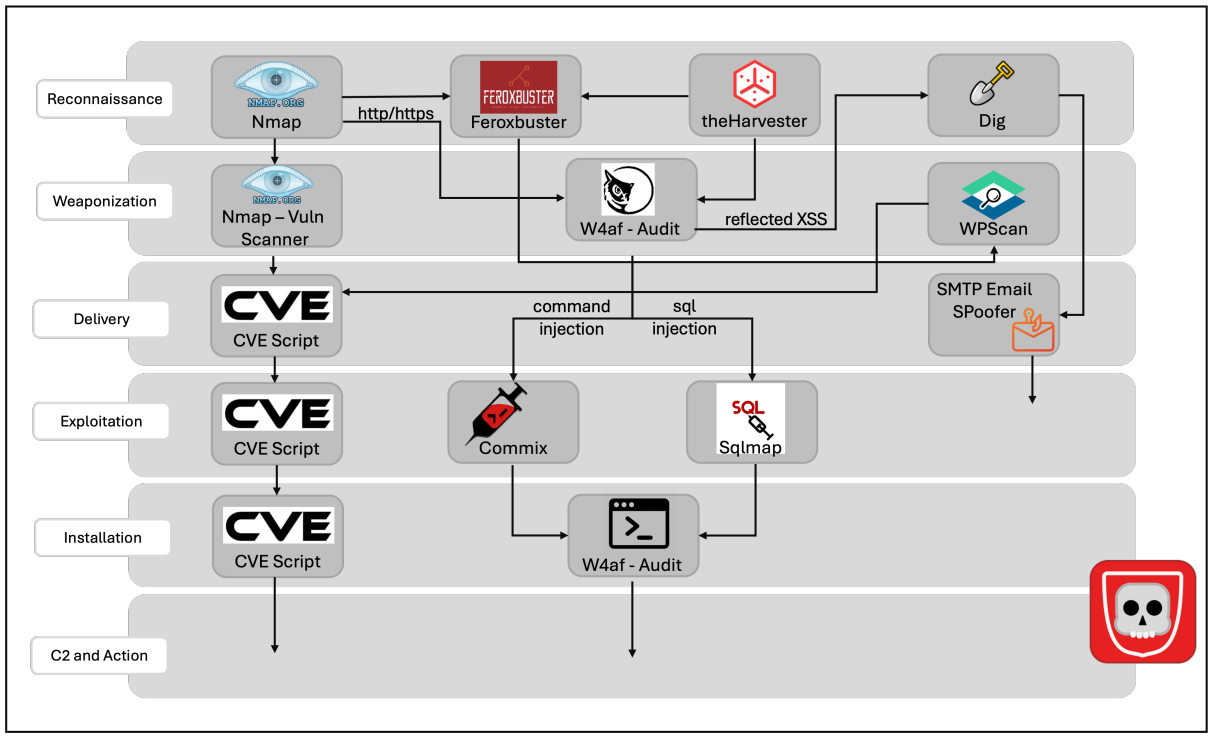

Figure 2: Cyber Kill Chain in Red Team Knife

thread instance in which to execute a command with *subprocessPopen()*; communicates with the thread to report any required stops; retrieves data from the *temp_file* that the command generated and stores it appropriately.

4. Experimentation

Preliminary testing of the system's operation was carried out using XVWA[2] and the OWASP Broken Web Applications project[3], by means of some virtual machines available online.

XVWA, an acronym for Xtreme Vulnerable Web Application, is a web application developed in PHP/MySQL with intentional vulnerabilities. It was specially designed to help computer security beginners in their learning. The 'Live ISO' version was used to start a virtual machine and use the service.

Both target machines were used for testing the integrated tools. Below is an example of the results of the vulnerability scan on XVWA with Nmap.

The SQL Injection section of XVWA makes it possible to clearly identify the parameter and type of request required to execute the attack. Below is an example of a hint command for running a shell via SQLMap (Figure 4).

The OS Command Injection section of XVWA has the same features as mentioned above, so it is an excellent target on which to test the tool's operation (Figure 5).

5. Conclusions

The Red Team Knife (RTK) is designed to provide both beginners and experienced professionals in cybersecurity with an accessible, structured, and integrated set of tools for penetration testing. It enhances the penetration testing workflow by offering guidance along the Cyber Kill Chain, supports

[2]https://github.com/s4n7h0/xvwa
[3]https://github.com/chuckfw/owaspbwa

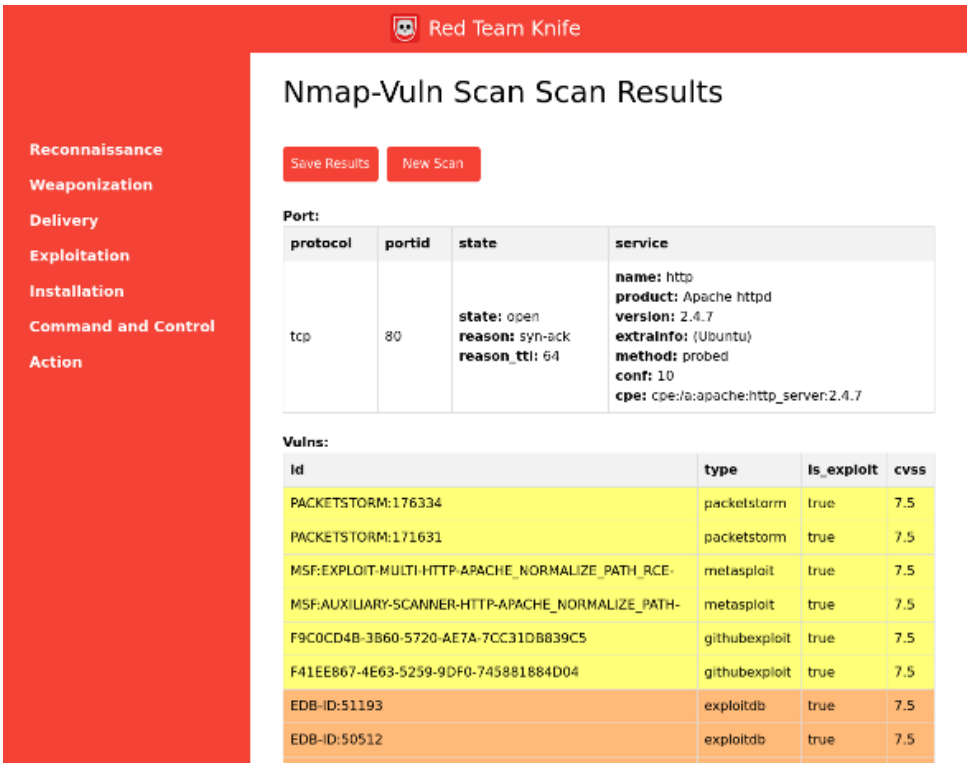

Figure 3: Vulnerability Analysis with Nmap on XVWA

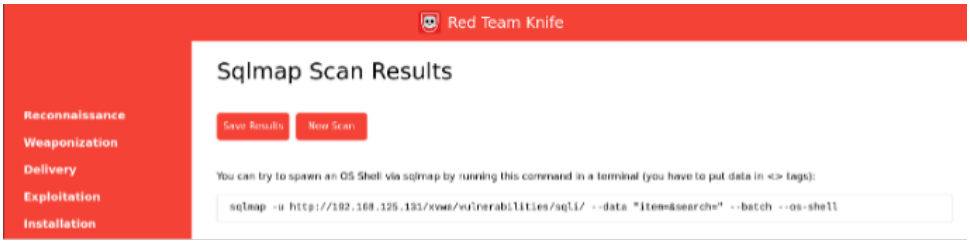

Figure 4: Hint command for running a shell via SQLMap

saving/restoring results, and wraps command-line tools in a more user-friendly interface using an MVC-based architecture.

Preliminary experimentation on known vulnerable platforms (like XVWA and OWASP BWA) demonstrated its usefulness in identifying vulnerabilities and guiding users through exploitation steps.

Overall, RTK aims to support cybersecurity education and practice by acting as a compass for effective and educational penetration testing activities.

Acknowledgments

This work was partially supported by the following projects: SERICS - “Security and Rights in the CyberSpace - SERICS” (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU; Accordo Quadro CrASte - “Cyber Academy for Security and Intelligence”.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

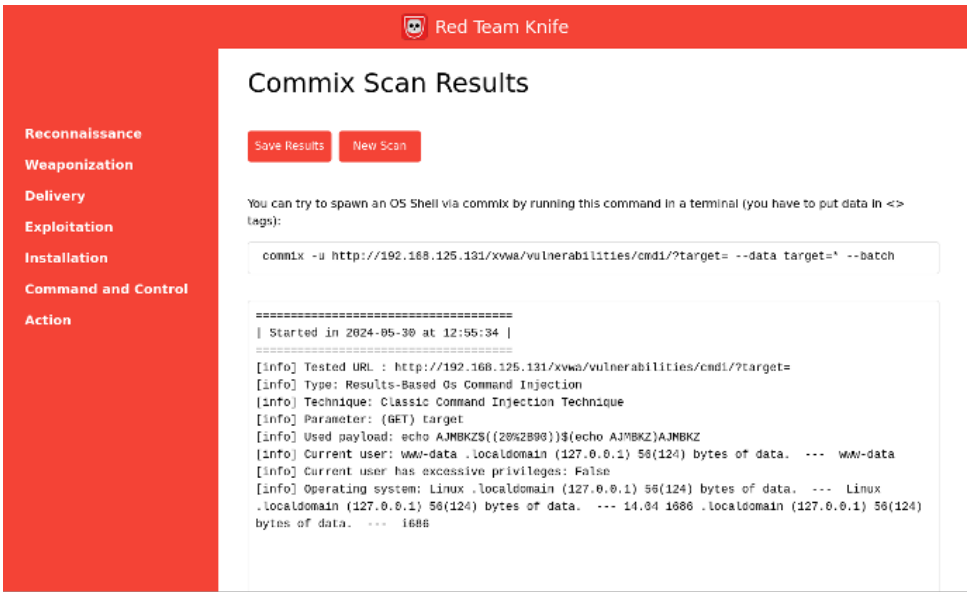

Figure 5: Hint command for running a shell via SQLMap

References

[1] M. T. Baldassarre, V. S. Barletta, D. Caivano, D. Raguseo, M. Scalera, Teaching cyber security: The hack-space integrated model, volume 2315, 2019. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85061370504&partnerID=40&md5=e8da8bde8df7b4a276e5517e34136832.

[2] M. T. Baldassarre, V. S. Barletta, D. Caivano, A. Piccinno, M. Scalera, Privacy knowledge base for supporting decision-making in software development, in: C. Ardito, R. Lanzilotti, A. Malizia, M. Larusdottir, L. D. Spano, J. Campos, M. Hertzum, T. Mentler, J. Abdelnour Nocera, L. Piccolo, S. Sauer, G. van der Veer (Eds.), Sense, Feel, Design, Springer International Publishing, Cham, 2022, pp. 147–157. URL: https://doi.org/10.1007/978-3-030-98388-8_14.

[3] M. T. Baldassarre, V. S. Barletta, D. Caivano, M. Scalera, Privacy oriented software development, in: M. Piattini, P. Rupino da Cunha, I. García Rodríguez de Guzmán, R. Pérez-Castillo (Eds.), Quality of Information and Communications Technology, Springer International Publishing, Cham, 2019, pp. 18–32. URL: https://doi.org/10.1007/978-3-030-29238-6_2.

[4] C. Catalano, A. Chezzi, V. S. Barletta, F. Tommasi, Defeating fido2/ctap2/webauthn using browser in the middle and reflected cross site scripting, Journal of Computer Virology and Hacking Techniques 21 (2025) 11. URL: https://doi.org/10.1007/s11416-025-00556-2. doi:10.1007/s11416-025-00556-2.

[5] V. S. Barletta, D. Caivano, M. Calvano, A. Curci, A. Piccinno, Craste: Human factors and perception in cybersecurity education, volume 3713, 2024, p. 75 – 81. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85198753881&partnerID=40&md5=35f9b858e583d214bb7a53c0a7dbf0da.

[6] I. Tarnowski, How to use cyber kill chain model to build cybersecurity?, European Journal of Higher Education IT (2017).

[7] M. S. Khan, S. Siddiqui, K. Ferens, A Cognitive and Concurrent Cyber Kill Chain Model, Springer International Publishing, Cham, 2018, pp. 585–602. URL: https://doi.org/10.1007/978-3-319-58424-9_34. doi:10.1007/978-3-319-58424-9_34.

[8] M. M. S. Khan, J. A. Giraldo, M. Parvania, Real-time cyber-physical analysis of distribution systems using digital twins, 2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) (2022) 34–39. URL: https://api.semanticscholar.org/CorpusID:254153621.

[9] I. Chomiak-Orsa, A. Rot, B. Blaicke, Artificial intelligence in cybersecurity: The use of ai along the cyber kill chain, in: N. T. Nguyen, R. Chbeir, E. Exposito, P. Aniorté, B. Trawiński (Eds.),

Computational Collective Intelligence, Springer International Publishing, Cham, 2019, pp. 406–416.
[10] T. Yadav, A. M. Rao, Technical aspects of cyber kill chain, in: J. H. Abawajy, S. Mukherjea, S. M. Thampi, A. Ruiz-Martínez (Eds.), Security in Computing and Communications, Springer International Publishing, Cham, 2015, pp. 438–452.
[11] E. M. Hutchins, M. J. Cloppert, R. M. Amin, et al., Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, Leading Issues in Information Warfare & Security Research 1 (2011) 80.