WEEK 3
RED TEAM RECON

TIMOTHY SEWE OGODE(CSSA0423076)

CYBER SHUJAA

2.2 INTRODUCTION TO CYBERSECURITY

Table of Contents

2.2 INTRODUCTION TO CYBERSECURITY

1. INTRODUCTION

In red team operations, reconnaissance plays a crucial role in gathering information about a target without raising suspicion. The goal is to learn about the target's infrastructure and personnel to effectively orchestrate attacks. This report focuses on passive reconnaissance techniques that do not alert the target or create unnecessary noise. By utilizing methods such as WHOIS and DNS-based reconnaissance, advanced searching, Google hacking, and specialized search engines, one can discover subdomains, gather publicly available information about hosts and IP addresses, find email addresses, uncover login credentials and leaked passwords, and locate leaked documents and spreadsheets. The knowledge and insights gained from passive reconnaissance lay the foundation for successful red team operations in later stages.

2. Taxonomy of Reconnaissance

Reconnaissance, or recon, can be divided into two categories: passive reconnaissance and active reconnaissance. Passive reconnaissance involves gathering information about the target without interacting with it directly. This method relies on publicly available data obtained from third-party sources, such as Open Source Intelligence (OSINT). Examples of information collected include domain names, IP addresses, email addresses, employee details, and job postings. Passive reconnaissance helps build an initial understanding of the target. On the other hand, active reconnaissance involves interacting with the target by sending requests and packets to observe its response. This approach provides further insights beyond what passive recon reveals. Active recon can be conducted externally, focusing on the target's external assets accessible from the Internet, or internally, carried out from within the target company's network.

3. Built-in Tools

WHOIS is a request and response protocol that allows querying WHOIS servers for domain information. By using the "whois" command, we can retrieve valuable details about a domain, such as registrar information, creation/update dates, and contact details. DNS queries can be performed using tools like "nslookup," "dig," or "host," which provide information about DNS records associated with a domain. These tools can reveal A records, AAAA records, and more. Traceroute/tracert is used to trace the network path between our system and a target host, displaying the routers (hops) along the way. This information helps in understanding the network infrastructure. The combination of these tools facilitates passive reconnaissance by collecting publicly available data without generating suspicious traffic.

4. Advanced Searching

It highlights the importance of efficient search engine usage and introduces popular search modifiers that can enhance search results. There is a significance of protecting confidential information, as search engines may inadvertently index sensitive data such as internal documents, spreadsheets with usernames and passwords, and vulnerable web servers. Utilizing resources like the Google Hacking Database (GHDB) to identify potential vulnerabilities and exploring additional sources of information, such as social media platforms and job ads, which can provide valuable insights without directly interacting with the target.

2.2 INTRODUCTION TO CYBERSECURITY

5. Specialized Search Engines

In terms of WHOIS and DNS, there are additional resources to consider. WHOIS history provides historical domain registration data, particularly useful when privacy measures were not utilized. ViewDNS.info offers free advanced DNS services, including reverse IP lookup for identifying shared hosting and associated domain names. These tools enhance the understanding of domain histories and shared server environments.

6. Recon-ng

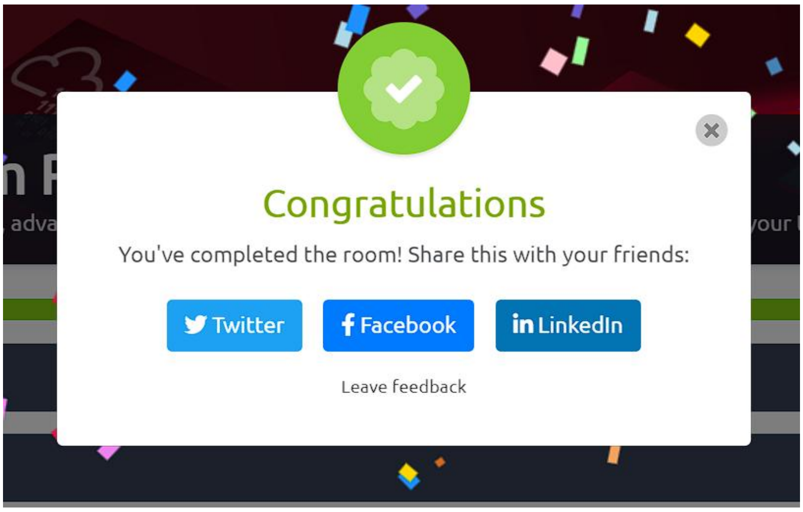
Recon-ng is a powerful reconnaissance tool widely used in red teaming operations. It allows red teamers to gather valuable information about their targets by leveraging various open-source intelligence (OSINT) sources and techniques. With Recon-ng, red teamers can perform automated data gathering, such as Footprinting domains, discovering subdomains, finding email addresses, and much more. It provides a flexible framework that enables red teamers to customize and automate their reconnaissance processes, ultimately aiding in the identification of potential attack vectors and enhancing the overall effectiveness of the red team's reconnaissance phase.

7. MALTEGO

Maltego is another popular tool utilized in red team reconnaissance. It provides a visual and intuitive interface for conducting OSINT investigations and link analysis. Red teamers can use Maltego to gather information from various sources, such as social media platforms, public databases, DNS records, and online communities. By mapping relationships and connections between different entities, Maltego helps red teamers gain insights into the target's infrastructure, potential vulnerabilities, and associated entities. It enables red teamers to visualize complex information, identify patterns, and make informed decisions during the reconnaissance phase of a red team engagement.

8. CONCLUSION

In red teaming, it is crucial to gather as much information as possible about the target. As the landscape evolves, we need to explore new avenues for data collection. We have covered essential tools like whois, dig, and tracert, along with utilizing search engines for passive reconnaissance. Additionally, we highlighted Recon-ng and Maltego, powerful tools that consolidate information from various sources. This knowledge expansion enhances our understanding of the target, enabling us to identify vulnerabilities, conduct targeted scans, and launch effective phishing campaigns. The more information we gather, the more refined our attacks become, increasing the likelihood of success.



Congratulations

You've completed the room! Share this with your friends: