Cybersecurity: Building a Better Defense with a Great Offense

David M. Cooke, Associate of Science

COVA CCI Undergraduate Research, Fall 2021

David Cooke is an undergraduate student at Old Dominion University, Norfolk, Virginia. Pursuing a Bachelor of Science; in Cybersecurity.

Table of Contents

Abstract

The current industry standard for cybersecurity is risk mitigation, which is the identification, evaluation, and categorization of threats that are posed to an organization's network. The goal is to prevent attacks and if an organization is attacked popular standard is to react and remedy the attack. This form of cyber defense isn't very reassuring to an organization and its users, once an attack is executed based on a study conducted by Booz Allen the average time an advanced persistent threat (APT) dwells on a victims' network before it's discovered is 200-250 days. That's plenty of time for a malicious third party to extract valuable and personal data from an organization's network on its users and the organization. To prevent vulnerabilities like this organizations, need to reevaluate their network security methods and a newly proposed method of cyber defense is a cyber offense. Cyber Offense as a defense is already seen in some organizations but not widely accepted, these forms of offense can include but aren't limited to threat hunting, red teaming, and ethical hacking.

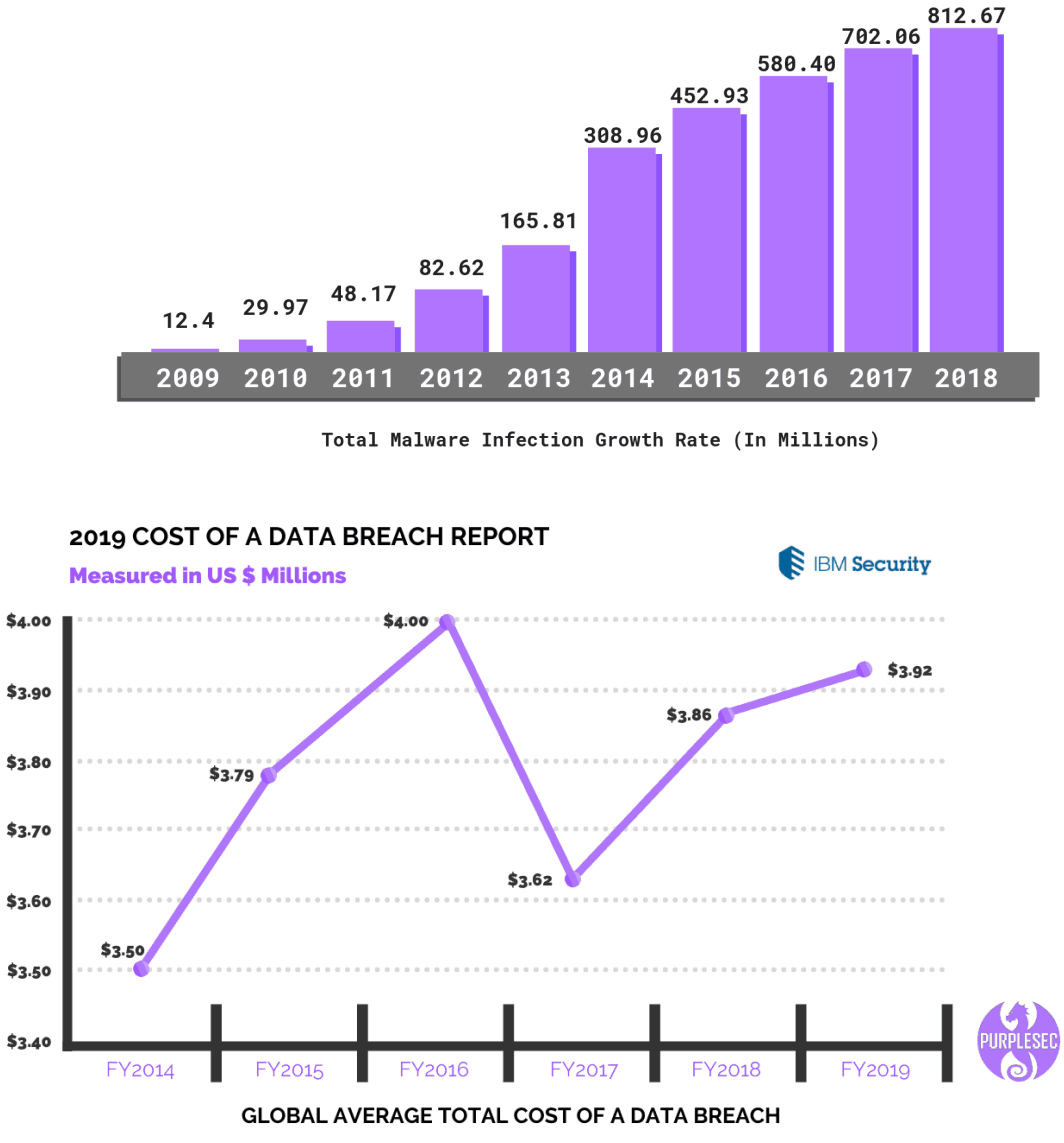
Introduction

Offensive security can be defined as a proactive, adversarial way of defending computer systems, networks, and users. The two types of offensive often explored are “Red Teaming’ and “Penetration Testing” However, these aren’t the only types of testing or methods for offensive security, but they are the main types used by companies in today’s scope. To start grasping the raw proposition of offensive security you need to understand its forms and applications. Often Red Teaming and penetration testing are terms that people use interchangeably however, they have different end-goals as well as fundamental differences, both are quite distinct. Red Teaming is a goal-based adversarial testing processing, it is an organization-wide approach that also measures how well an organization will respond to an attack. This method is meant to imitate the way an attacker would try to compromise an organization, where there’s a definite goal and every step made is to work towards that goal. Penetration testing on the other hand has a specific target such as a server, database, web application, social engineering, etc... In this method, the whole organization isn’t attacked instead vulnerabilities are only looked for if they’re associated with the target. This method prevents you from knowing if any vulnerabilities threaten the whole organization if they aren’t related to the investigated target. Both are viable tools that are important in building efficient offensive security, to achieve true protection you should have both in place so you make sure you can find as many vulnerabilities as possible, get them alerted and taken care of. These tools are just the surface of what posing offensive security can help provide your organization in terms of defense. Another type of offensive security that should be highlighted is “Threat Hunting” this method of offensive security’s purpose is to locate and isolate a threat that’s already present and made it through your current security solution. This method of offensive security is important because cyberspace is ever-growing, and threat actors

find new ways to infiltrate organizations and extract data every day so consistently searching for threats within your organization can help prevent a major attack waiting to happen. These three methods of an offensive cyber defense help build a more effective and efficient security posture, and overall do a better job at protecting your data from attackers than a typical cyber defense.

The Threat

Figure 1



As shown in Figure 1, the number of malware infections in 2018 was more than 65x the amount only 9 years prior in 2009 an alarming growth rate for what is the most expensive attack an organization can suffer. On average, a malware attack will cost a company $2.4 million US dollars, as well as 50 days in time remediating the exploit. One of the most common types of malware, ransomware saw a 40% surge in 2020 and was up 102% in the first half of 2021 compared to 2020. Malware can lead to even more turmoil for a company if it leads to a data breach which has an average cost of $3.92 million for companies worldwide and typically takes 191 days to identify and remediate. The cost of a data breach has come down since its peak in 2016 which was when Yahoo!, LinkedIn, and the Democratic Party, amongst many more suffered from a data breach but is still considerably high than it was 5 years ago in 2014, as shown in Figure 2. In the next two years, almost 30% of companies are expected to experience a data breach. (IBM) This is a result of an estimated 30+ million cyber-attacks there is every year. The biggest concern here with the rapid growth of cyber threats companies face is that while 43% of cyber-attacks target small businesses (Verizon 2021 Data Breach Investigations Report), 73% of these businesses are unprepared to deal with the said attack (2019 Hiscox Cyber-readiness Report). These statistics highlight a risk that these companies face and trigger a call-to-action for better security amongst them.

The Solution

Organizations must be ready to detect and respond to security breaches and events, standard mitigation measures in place aren't enough. Organizations need to become proactive and deliver a better defensive front by seeking out and eliminating risk before an agent can exploit them. Companies must understand the risk associated with a security breach, how to implement an effective penetration testing team, red team, as well a threat hunting team or at

least a group of people who can cover these fronts. Organizations must map out a home field and understand their assets, servers, and computer systems. Establishing a security posture that involves offensive security programs identifies flaws in prevention, detection, and remediation for incidents. Establishing a transparent environment amongst your security specialist in your organization is essential to a strong defense, as well as ensuring it is manageable and measurable. Synchronization of offensive tools in addition to your already existing defense will help ensure you're protected to the best ability your organization has to offer.

Penetration Testing

Exploring specific vulnerabilities with penetration testing within your organization determines what is exploitable and to what degree the information or network that's vulnerable could be exploited by an attacker. Penetration testing is executed by "white hats" which are essentially ethical hackers that determine what damage can be done to your organization by using ethical means of exploitation. There are two broad types of vulnerabilities that are considered when penetration testing, they are logical and physical vulnerabilities. Logical vulnerabilities include any of the organization's computers, devices, software, and applications. Physical vulnerabilities include any tangible security within the organization, as well as its employees' risk of social engineering. Many organizations don't have employees that are skilled in penetration testing and often need to outsource, if this is the case organizations must make certain that the outsourced associates aren't only performing blind tests but also knowledgeable ones. Knowledgeable tests are important for identifying internal risk and threats from agents that used to be an employee of the organization as internal risk exist and should not be overlooked. At the end of a penetration test, the results need to be posted and should be certain to include all vulnerabilities found as well as recommended remediation. The results should be given to the

security team, owners, as well as appropriate upper-level management to form transparency within the organization for the risks that exist. Once vulnerabilities are found they need to be addressed and mitigation will be delivered depending on the cost, severity, and value of the assets that are exposed.

Red Teaming

Your role when defending on the red team is to attack, you are posing as an attacker and are supposed to act as such. In this role, you perform all the steps a threat agent would, the typical approach for this is you'll first perform reconnaissance. Reconnaissance is also known as footprinting is the information gathering phase of red teaming, in this phase, you gather as much information as you can on the organization and establish an attack surface. Search for IP address blocks, identify related web pages, any APIs (Application Program Interfaces) that may be exposed, even employee names this is the foundation to what you're looking for a red team member. What separates red teaming from penetration testing is the assessment, when a red team searches for vulnerabilities they look at the whole organization, refer to Figure 3. Where a penetration test sees a potential target, a red team will see that and everything around it. The red team assessment sits atop its adversarial objectives and its adversary capabilities like an umbrella and considers different techniques that you can employ. A good breakdown of this is electronic, social, and physical components that are exploitable, as well as some other method that's help work towards the end goal. Refer to figure 4, for a visual representation and examples of components considered when making a red team assessment. All these aspects go into clearly defining and ranking risk for vulnerabilities that an adversary can attack and building a model of what a coordinated attack would look like from an adversary's perspective.

Figure 3

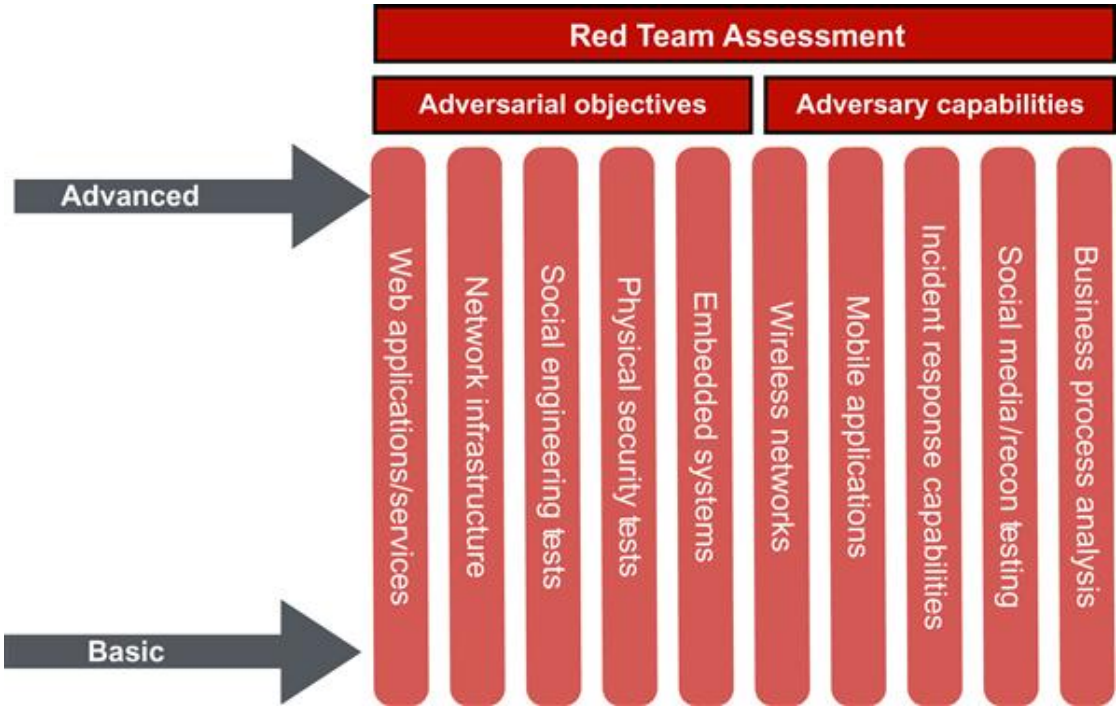


Figure 4

Electronic	Social	Physical	Other activities
Software	Phishing	Access control technologies	OSINT recon
Network	Phone-based	Physical facility security	Business process analysis
Wireless technologies	IM/chat	Access badge processes	Attack intelligence/ modeling
Platforms and infrastracture	Social media mining	Employee and vendor onboarding	Incident response evaluation
Mobile technologies			Risk management
Embedded technologies			Role-based social engineering

Threat Hunting

Taking offensive security, a step further for an organization, threat hunting can be considered an advanced security analysis process as it utilizes a deep understanding of the organization or its network to locate a subtle, deeply embedded attacker than a typical SOC (Security Operation Center) will find. This process is essential to mitigate damage and eliminate the risk that a company may face, dealing with the increasing number of attackers and threats an infiltration can almost be considered inevitable so being able to protect yourself after you've already taken a hit is becoming increasingly important for organizations. Threat hunting is mostly self-directed, a good hunter is capable of investigating, developing, teaching, being able to learn, and adjust. Threat hunting is typically started by an analyst's self-driven intuition about odd behavior on a network, it is rarely ever triggered by an IDS (Intrusion Detection System). Once a trigger is found the hunt begins and an analyst develops hypotheses on what threat exists or even simply if there is a threat present, they are in a logistical battle with the security processes going on and contending with it for data access. An analyst will pull the data as well as refine their hypothesis, then select data that contributes to their hypothesis and evaluate it. After this process is complete, they develop an expert belief on what threat is present, this can be presented in many forms it being a report. Software, or a new configuration for the defense of the network. Threat hunting is a supportive tool to your security it is a research process and can be considered as normal operations but viewed as going a step above. Combine this with the analytical tool, and threat analyst you already have to broaden your security and help ensure your organization is protected.

Challenges

Building an offensive front for your cyber defense is the optimal solution for eliminating the rising risk of cyber-attack however it has its barriers. Many organizations have reported that they have been largely unsuccessful in preventing cyber-criminals from exploiting their systems. In a survey conducted by Fortinet, a global leader in cybersecurity solutions 90 percent of organizations surveyed suffered at least one intrusion in the year. Many experiences lost productivity, operational outages impacting revenue, and even some had their physical safety put at risk. The survey also discovered that half of the organizations surveyed did not even have a security operation center and nearly four out of 10 did not have Security Information and Event Management (SIEM). Also, 47 percent had not implemented internal network segmentation and 59 percent did not implement network access control. A lot of this lack of security can be blamed on funding 58 percent of the organizations did say they were receiving a budget increase, but 15 percent were instead receiving a decrease. The only solution to solving what is a prevalent problem amongst organizations especially smaller businesses is through more awareness and with the increasing risk that cyber cyber-attacks pose to organizations we'll continue to see more growth of security measurements and implementations.

Offensive Security Beyond the Desk

Beyond the scope of an organization, you're starting to see offensive security used in various ways around the world, very notably for political gain. There have been cyber-attacks in recent history that have threatened national security and the critical infrastructures of a nation. The Internet of Things (IoT) is commonly used to refer to any physical device that is connected to the internet, collecting, and sharing data. The Mirai botnet which is known as the first IoT

malware was used to attack the Dyn network server which is mostly used within the United States. The attack rendered popular apps Twitter, PayPal, and many other major online services unable to provide their service due to the incredible amount of network traffic the botnet put on the server. This was a major cause of concern because of the scale of the attack, and it showed the new risk that is now present for a collection of devices that are slowly starting to become essential parts of day-to-day life and function. This amongst other new threats of sophisticated cyber-attacks calls for an evaluation of new major threats posed to the populous, there's now the threat of individuals, nations, and cybercrime organizations. This has caused the exploration of new methods of cyber defense to help fight in what can be referred to as cyberwarfare.

Conclusion

The threat is apparent, and the need for better security is obvious to satisfy this need organizations need to explore new methods of cyber defense and offensive security very well is a great solution. Through tried-and-true methods of offensive security risks are efficiently mitigated saving organizations millions in loss, productivity, and trust. Cyberspace is ever-changing and with every new development there's a new risk that comes along with it and to prevent potential attacks, organizations should begin to implement offensive methods such as penetration testing, red teaming, and threat hunting. The hurdles that are in front of them will continue to be cleared as the awareness of these threats becomes more prevalent. The extent of risk that people face is beyond just an organization or its users, nations are starting to face increased risk, and to protect the home-field the field they will have to adapt. As the functions that computers, devices, networks, and more technology continue to be embedded in our day-to-day life an evaluation will be done, and new methods will come forth to protect this new space.

Bibliography

2021 Cyber Security Statistics Trends & Data. (2021, August 06). Retrieved November 22, 2021, from https://purplesec.us/resources/cyber-security-statistics/

Bavisi, S. (2009). *Computer and Information Security Handbook*. Amsterdam: Elsevier.

Costin, A. (n.d.). Difference between pen testing, red teaming, & threat hunting. Retrieved November 22, 2021, from https://www.mindpointgroup.com/blog/difference-between-pen-testing-red-teaming-and-threat-hunting

Dalziel, H. (2015). *Next Generation Red Teaming*. Waltham, MA: Elsevier.

Issued by ITWeb Security Summit 2020. (2020, August 26). Report: 90% of OT leaders have experienced at least one intrusion in the past year. Retrieved November 22, 2021, from https://www.itweb.co.za/content/rxP3jqBmNJAMA2ye

Kim, K., Alfouzan, F., & Kim, H. (2021, August 23). Cyber-attack scoring model based on the offensive cybersecurity framework. Retrieved November 22, 2021, from https://www.mdpi.com/1239456

Krasnov, J., & Rose, A. (2020, July 06). An introduction to offensive security. Retrieved November 22, 2021, from https://www.bc-security.org/post/an-introduction-to-offensive-security/

Medairy, B. (n.d.). The future of cybersecurity: The best defense is a good offense. Retrieved November 22, 2021, from https://www.boozallen.com/s/insight/blog/future-of-cybersecurity.html#

Michael Collins. (2018). Threat Hunting. O'Reilly Media.

Phases of hacking. (n.d.). Retrieved November 22, 2021, from https://www.greycampus.com/opencampus/ethical-hacking/phases-of-hacking

Rehberger, J. (2020). *Cybersecurity attacks - Red Team Strategies: A practical guide to building a penetration testing program having homefield advantage*. Birmingham, UK: Packt Publishing.

Rountree, D. (2011). *Security for Microsoft Windows System Administrators: Introduction to Key Information Security Concepts*. Burlington, MA: Syngress.

Stouffer, C. (n.d.). 115 cybersecurity statistics and trends you need to know in 2021. Retrieved November 22, 2021, from https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html