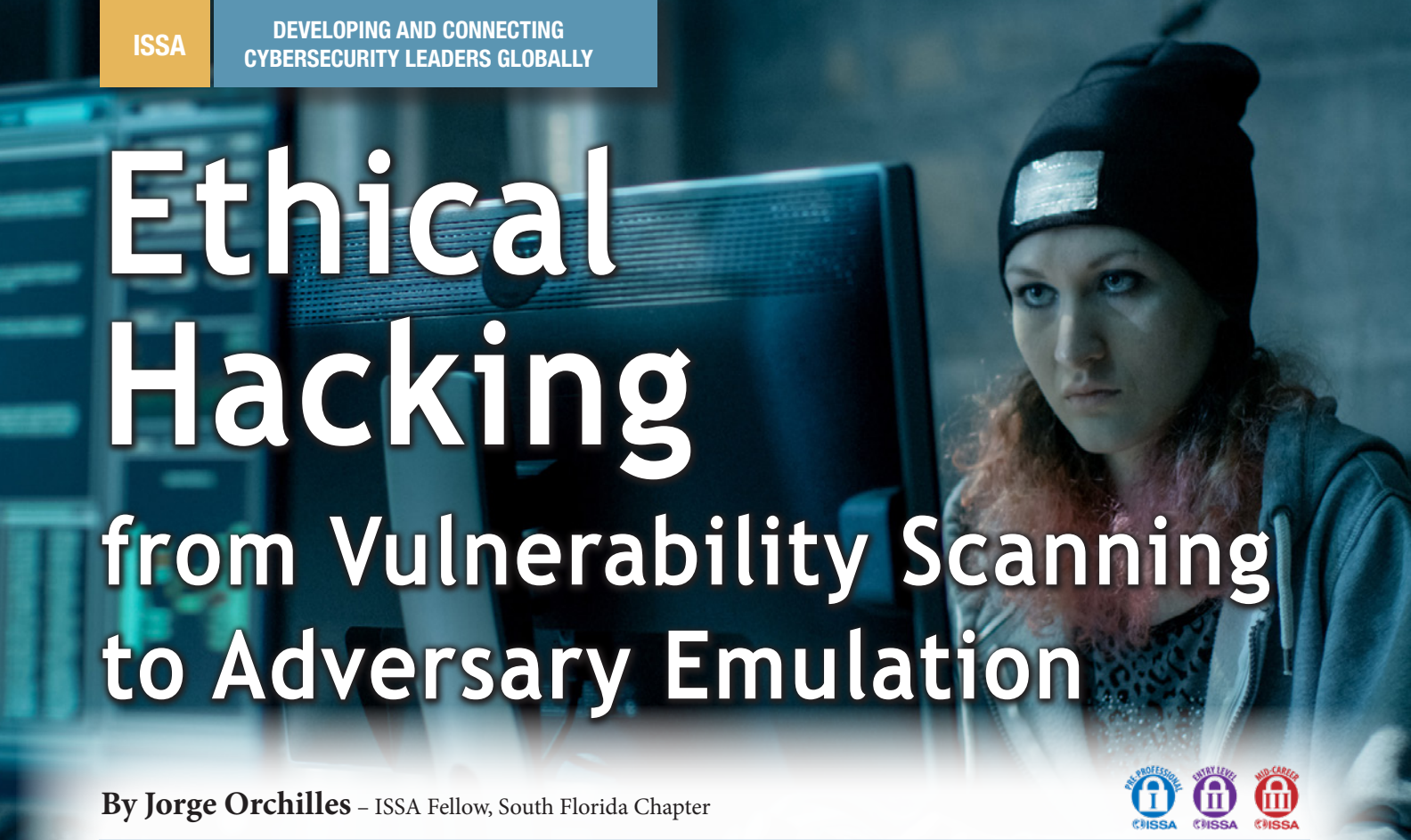

Ethical Hacking

from Vulnerability Scanning to Adversary Emulation

By Jorge Orchilles – ISSA Fellow, South Florida Chapter

One continually hears "ethical hacking" or "offensive security" terminology used incorrectly by regulators, customers, etc. This article attempts to clarify the definition so that we can all speak and push the industry to use the correct terminology.

Abstract

One continually hears "ethical hacking" or "offensive security" terminology used incorrectly by regulators, customers, etc. This article attempts to clarify the definition so that we can all speak and push the industry to use the correct terminology. These assessments are performed with a common goal: to provide business value. It is key to understand the needs of the regulator or customer before providing an ethical hacking service. We will cover the very basics of ethical hacking through the bleeding edge along with what tools can be used for each: vulnerability scanning, vulnerability assessment, vulnerability management, penetration testing, red team, purple team, and adversary emulation. These ethical hacking assessments rely on people (ethical hackers), process, and technology (tools). Our focus will be on the best tools for each with highlights of processes, frameworks, and methodologies.

Hacking and ethical hacking

The traditional definition of a hacker is a skilled individual who uses technical knowledge to overcome a problem. Unfortunately, the same dictionary, Merriam-Webster, has another definition of hacker as "a person who illegally gains access to and sometimes tampers with information in a computer system" [4]. For that reason, the information security industry started using the term *ethical hacker* to define someone with these skills that has permission to asses a target system or organization, permission being the keyword that differentiates between ethical and malicious, often called white hat and black hat, respectively. As an industry, we define an ethical hacker as a person who hacks into a computer network in order to test or evaluate its security. The main goal is to provide business value by improving the security of the organization.

There are many assessments an ethical hacker can perform against a target organization. Each has a different definition, goal, process, and tool set. We will cover them in the order most organizations implement them by covering the most basic ethical hacking assessments through the most advanced. This is not a formal maturity model but may be applied as such.

Vulnerability scanning

Scanning an organization for vulnerabilities with an automated scanner is the simplest of ethical hacking assessments one can perform. Scanners can be configured as blackbox, where they do not log into the target system; whitebox, where the scanner authenticates to the target system with creden-

tials via SMB or SSH; or agent based, where an agent is installed on the target system to call back to the management server.

- **Definition:** Automated (tool-based) scanning against assets (IPs or applications)
- **Goal:** Identify low hanging, known vulnerabilities pre- or post-authentication
- **Effort:** Small, requires tool investment
- **Focus:** Technology vulnerabilities, patches, configuration
- **Frequency:** Weekly to monthly
- **Customer:** System owners and operations teams
- **Process:** Point a network vulnerability scanner at some IPs. Point a web application vulnerability scanner at a website
- **Tools:** Tenable Nessus, Rapid7 InsightVM, Qualys, IBM AppScan, Burp Pro and MicroFocus Fortify WebInspect

There are many tools that perform vulnerability scanning and by far the largest market due to the simplicity and low requirement of skilled ethical hackers to operate the tools. The reports these tools provide are long and use the default risk ratings, which offers low value to business. Blackbox scans are prone to false positives as results are based on signature matching. My favorite is Tenable Nessus as the industry's most popular network vulnerability scanner. On the web application side, I have come to love Burp Pro scanning feature over the more expensive options.

Vulnerability assessment

With a vulnerability scan completed, an ethical hacker can validate the vulnerabilities manually to remove false positives and calculate an accurate risk rating. Vulnerabilities are assigned a Common Vulnerabilities and Exposure (CVE) ID and this is generally the starting point from a vulnerability scan result.

Ethical Hacker Tools

ATT&CK	CVE	Navigator
AttackerKB	VSS	Nessus
C2Matrix	Metasploit	SCYTHE

- **Definition:** Automated and manual assessment of assets in scope to find security vulnerabilities, which may or may not be used to get in or steal data
- **Goal:** Identify ALL vulnerabilities from assets in scope
- **Effort**: ~30 percent tools based and ~70 percent manual testing
- **Focus:** Assessments are broader and often include explicit policy and procedure reviews
- **Frequency:** Once per year or once per certification of product/version
- **Customer:** System owners, operations, engineers, application stakeholders
- **Process:** Verify each vulnerability identified by the vulnerability scanner
- **Tools:** Client-side tools that connect to the services in scope. For web applications, HTTP proxies such as Burp or OWASP ZAP

In a vulnerability assessment, the ethical hacker must verify the identified vulnerabilities, removing false positives, and calculating the correct risk score. The tools used are based on the service that the scanner deemed to be vulnerable. For example, if FTP is found, an FTP client may be used to ver-

ify the service and various configurations that may be vulnerable. For web applications, manual verification is done through HTTP proxies; my favorite is Burp Pro followed closely by OWASP ZAP.

Vulnerability management

At a high level, your organization should be patching at the same pace that the vendor releases patches. For example, Microsoft has patch Tuesday on the second Tuesday of every month. By the time the second Tuesday of the month comes, you should be fully patched with the patches released the previous month. Oracle does it quarterly. Prioritization then focuses on the real, urgent vulnerabilities that need to be patched at a much faster timeline than the "business as usual" [7]. There are various tools available to prioritize the patching of vulnerabilities.

- **Common vulnerability scoring system** (CVSS) – this is the industry standard and every CVE has a CVSS base score calculated and posted to the National Vulnerability Database (NVD) [5] – Ethical hackers should then calculate the temporal and environmental score for their organization
- **Exploit predictability scoring system** – new research presented at Blackhat 2019 to try and determine, through algorithms, the vulnerabilities most likely to be exploited – this is a new working group and work in progress [3]

- **AttackerKB** – new crowdsource, community project by Rapid7 where ethical hackers assess various vulnerabilities and determine attacker value and exploitability – yours truly was a beta tester and this site is now open to the public
- **Tenable vulnerability priority rating** – solution from Tenable for customers of Nessus that rates vulnerabilities based on two components: technical impact and threat [13]
- **Rapid7 real risk score** – solution from Rapid7 for customers of InsightVM that calculates scores based on the likeliness of an attacker exploiting the vulnerability in a real attack [8]
- **FireEye risk rating** – cyber threat intelligence-based rating performed manually by FireEye analysts based on impact and mitigating factors [11]

Penetration testing

Penetration testing goes a step further and exploits the vulnerabilities identified. This is the main differentiator from vulnerability assessment and penetration testing. Penetration testing involves gaining access to the target system through exploitation, further removing false positives, and calculating business risk.

- **Definition:** involves exploiting vulnerabilities under controlled circumstances in a professional, safe manner according to a carefully designed scope and rules of engagement
- **Goal:** Report all exploitable vulnerabilities and calculated business risk
- **Effort:** ~10 percent tools based and ~90 percent manual testing
- **Focus:** Technology and preventive controls
- **Frequency:** ~Once per year
- **Customer:** System owners, operations, engineering, and application stakeholders
- **Process:** Penetration Testing Execution Standard, Open Source Security Testing Methodology Manual, OWASP Testing Guide
- **Tools:** Metasploit, Immunity CANVAS, Core Impact

Penetration testing is mostly manual and requires ethical hackers to find exploits for the identified vulnerabilities so that they may exploited. My favorite tool for exploitation is the tool that has an exploit for the vulnerability I am targeting. When I teach the SANS Penetration Testing course [12], I always comment that if I could only use one tool during a penetration test, it would be Metasploit.

Metasploit has auxiliary modules that allow scanning, fuzzing, and brute forcing, among other items. It has over 1000 exploits already built in but can be used to identify vulnerabilities and create your own exploits. Those exploits need a payload to execute once successful and Metasploit also has many payloads, including the Metasploit interpreter, aka

	Language		UI			Agents			Channel										
Name	Server	Agent	Multi-User	UI	API	Windows	Linux	macOS	TCP	HTTP	HTTP2	HTTP3	DNS	DoH	ICMP	FTP	IMAP	MAPI	SMB
Apfell	Python	Python	Yes	Web	Yes	No	Yes	Yes	No	Yes	No	No	No	No	No	No	No	No	No
CALDERA	Python	Go	Yes	Web	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	No	No	No
Cobalt Strike	Java	C	Yes	GUI	No	Yes	No	No	Yes	Yes	No	No	Yes	Yes	No	No	No	No	Yes
Covenant	C#	C#	Yes	Web	Yes	Yes	No	No	No	Yes	No	No	No	No	No	No	No	No	Yes
Dali	Python	Python	No	CLI	No	BYOI	BYOI	BYOI	No	Yes	No	No	No	No	No	No	No	No	No
Empire	Python	PowerShell	Yes	Web	Yes	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	No	No	No
EvilOSX	Python	Python	No	GUI	No	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	No	No	No
Faction C2	.NET	.NET	Yes	Web	Yes	Yes	No	No	Yes	Yes	No	No	No	No	No	No	No	No	No
FlyingAFalseFlag	Python	C++	No	CLI	No	Yes	No	No	No	Yes	No	No	No	No	No	No	No	No	No
FudgeC2	Python	Powershell	Yes	Web	No	Yes	No	No	No	Yes	No	No	No	No	No	No	No	No	No
godoh	Go	Go	No	CLI	No	Yes	Yes	Yes	No	No	No	No	Yes	Yes	No	No	No	No	No
HARS	Python	C#	No	CLI	No	Yes	No	No	No	Yes	No	No	No	No	No	No	No	No	No
ibombshell	Python	PowerShell	No	GUI	No	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	No	No	No
INNUENDO	Python	Python	Yes	Web	Yes	Yes	Yes	Yes	No	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes
Koadic C3	Python	JScript/VBScript	No	GUI	No	Yes	No	No	No	Yes	No	No	No	No	No	No	No	No	No
MacShellSwift	Python	Swift	No	CLI	No	No	No	Yes	No	Yes	No	No	No	No	No	No	No	No	No
Merlin	Go	Go	No	GUI	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No	No	No	No	No	No
Metasploit	Ruby	C/Java/PHP/Python	Yes	CLI	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No	Yes
Ninja	Python	C#/PowerShell	Yes	CLI	No	Yes	No	No	No	Yes	No	No	No	No	No	No	No	No	No
Nuages	Python	C#	Yes	GUI	Yes	Yes	No	No	No	Yes	No	No	No	No	No	No	No	No	No
Octopus	Python	PowerShell	No	GUI	No	Yes	No	No	No	Yes	No	No	No	No	No	No	No	No	No
PoshC2	Python	PowerShell/C#/Python	Yes	CLI	No	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	No	No	No
PowerHub	Python	PowerShell	Yes	Web	No	Yes	No	No	No	Yes	No	No	No	No	No	No	No	No	No
Prismatica	Javascript/Python	JScript/.NET/Rust	Yes	GUI	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No	No
Red Team Toolkit	Python	C++	No	CLI	No	Yes	No	No	No	Yes	No	No	No	No	No	No	No	No	Yes
ReverseTCPShell	PowerShell	PowerShell	No	CLI	No	Yes	No	No	Yes	No	No	No	No	No	No	No	No	No	No
SCYTHE	Python	C	Yes	Web	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	No	No	No	No	No	Yes
SilentTrinity	Python	IronPython	Yes	CLI	No	Yes	No	No	No	Yes	No	No	No	No	No	No	No	No	No
Sliver	Go	Go	Yes	CLI	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes	No	No	No	No	No	No
Throwback	php	C++	Yes	Web	No	Yes	No	No	No	Yes	No	No	No	No	No	No	No	No	No
Trevor C2	Python	Python/PowerShell	No	CLI	No	Yes	Yes	Yes	No	Yes	No	No	No	No	No	No	No	No	No
Voodoo	Python	C++	Yes	Web	No	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No	No	No
WEASEL	Python	Python	No	CLI	No	Yes	Yes	Yes	No	No	No	No	Yes	No	No	No	No	No	No

Figure 1 – The C2 Matrix has a list of 40+ command and control frameworks along with their capabilities and features

Meterpreter. Lastly, Metasploit has post modules for post-exploitation, which make it a favorite. Immunity CANVAS and Core Impact have some but not all the mentioned features.

Red team

There are many debates on the definition of red team. Red Team Journal published this definition: "the practice of looking at a problem or situation from the perspective of an adversary" [10]. What is not debated is red team origins coming from military [1]. In the commercial sector of information security, red team is an independent group that, from the perspective of a threat or adversary, explores alternative plans and operations to challenge an organization to improve its effectiveness [9]. In information security, red team has a major focus on training and improving people, process, and technology. The only way to do red team wrong is to ignore the blue team. Red team focuses on testing the defenders, detection, and alerting.

- **Definition:** Red team emulates tactics, techniques, and procedures (TTPs) of adversaries to improve the people, processes, and technology in the target environment
- **Goal:** Make blue team better – Train and measure that blue team's detection and response policies, procedures, and technologies are effective
- **Effort:** Manual, some red team automation tools
- **Focus:** Detective controls, testing the defenders
- **Frequency:** Intelligence-led (new exploit, tool, or TTP)
- **Customer:** Blue teams, defenders
- **Process:** A framework for the regulatory use of penetration testing and red teaming in the financial services industry by Global Financial Markets Association [2]
- **Tools:** C2 Matrix, Cobalt Strike

There are so many tools available for emulating TTPs that I co-created an open source and community-driven project called the C2 Matrix. It stands for the Command and Control (C2) Framework Matrix. Command and control is one of the most important tactics in the MITRE ATT&CK matrix as it allows the attacker to interact with the target system and realize their objectives. There are many command and control frameworks available to emulate TTPs and this matrix documents the C2 capabilities, features, and detections for them (see figure 1). Choosing a favorite is difficult as they have different features that may be valuable to test against the target organization. For this reason, the C2 Matrix is my favorite tool as it allows me to choose the best framework to achieve the target business goals. It currently has 45 different C2s documented.

Purple team

Purple team is a virtual team made up of the red team and the blue team. The blue team are the defenders in an organization entrusted with identifying and remediating attacks, generally associated with security operations center or managed secu-

rity service provider (MSSP), hunt team, incident response, and digital forensics. The main difference is that a purple team exercise is non-blind, meaning the red team shows the blue team all TTPs performed and the blue team shows red team how they defend.

- **Definition:** A function, or virtual team, where red and blue teams work together to improve the overall security of the organization – Red team does not focus on stealth as they normally would
- **Goal:** Red team emulates adversary TTPs while blue teams watch and improve detection and response policies, procedures, and technologies in real time
- **Effort:** Manual
- **Frequency:** Intelligence-led (new exploit, tool, or TTP)
- **Customer:** Red team and blue team
- **Process:** Like red team process but fully disclosing to purple team
- **Tools:** C2 Matrix, SCYTHE

There are many tools available that simulate TTPs for purple team exercises. I prefer to use the same red team tools and focus the purple team exercise on the process. I did a presentation on performing high-value purple team exercises and provided a list of over 20 tools at the inaugural SANS Purple Team Summit. A post on medium has the video and list of tools [6]. We performed a breach and attack simulation (BAS) vendor shootout and chose to go with SCYTHE as it emulates the TTPs consistently, a very important requirement during purple team exercises.

Adversary emulation

An adversary emulation is a cyber threat intelligence-led exercise that can be performed as a red team engagement or a purple team exercise. The main difference is that an adversary with the capability, intent, and opportunity to attack the target organization must be selected. Once selected, it is especially important to understand how the adversary functions and the TTPs they use. With that completed, an adversary emulation plan may be created.

- **Definition:** A type of red team exercise where the red team emulates how an adversary operates, following the same tactics, techniques, and procedures (TTPs), with a specific objective similar to those of realistic threats or adversaries
- **Goal:** Emulate an end-to-end attack against a target organization – Obtain an holistic view of the organization's preparedness for a real, sophisticated attack –Improve overall security in organization
- **Effort:** Mostly all manual except for a couple adversary emulation tools
- **Frequency:** Twice a year or yearly
- **Customer:** Entire organization
- **Process:** MITRE ATT&CK, Unified Cyber Kill Chain
- **Tools:** ATT&CK Navigator, C2 Matrix, SCYTHE

Mapping the adversary TTPs to MITRE ATT&CK is a great start for an adversary emulation and can be performed with MITRE ATT&CK Navigator. With that mapping complete, an adversary emulation plan can be created and emulated by the red team (see figure 2). The red team would use tools that the adversary would use. This was the original use case for creating the C2 Matrix. My favorite tool for doing adversary emulation in a consistent and repeatable fashion is SCYTHE.

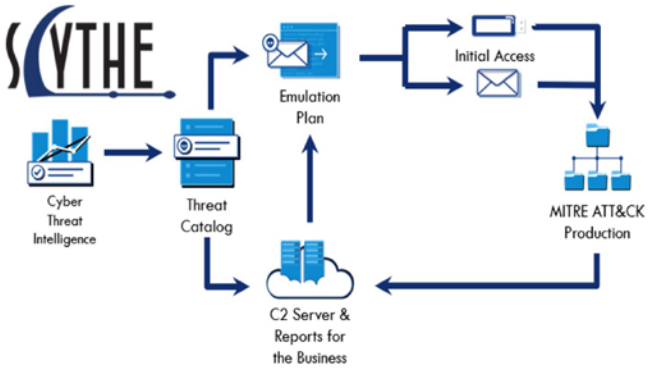

Figure 2 – SCYTHE leverages cyber threat intelligence to create campaigns that emulate adversaries and map to MITRE AT&CK.

Conclusion

It is important that we, as an industry, use the correct terminology. There are differences between these types of assessments, goals, and tools but the focus is to bring business value. Some organizations have matured following similar steps, from vulnerability scanning to adversary emulation, while others are in progress. Like everything in information security, there is no end state. Keep pushing to evolve from CVE to TTP as we all know we will be breached; the question lies in how we will respond. Please feel free to reach out and stay safe.

References

1. 4n7m4n,"Red Teaming: From the Military to Corporate Information Security Teams," Medium – https://medium.com/@antman1P_30185/red-teaming-from-the-military-to-corporate-information-security-teams-408c040bd87e.
2. GFMA,"GFMA Framework for the Regulatory Use of Penetration Testing in the Financial Services Industry," Global Financial Markets Association – https://www.gfma.org/correspondence/gfma-framework-for-the-regulatory-use-of-penetration-testing-in-the-financial-services-industry/.
3. Jacobs, Jay et al, "Exploit Prediction Scoring System (EPSS)," Arvix – https://arxiv.org/ftp/arxiv/papers/1908/1908.04856.pdf.
4. MW, "Hacker," Merriam-Webster – https://www.merriam-webster.com/dictionary/hacker.
5. NVD NIST, "National Vulnerability Database," NIST – https://nvd.nist.gov/.

6. Orchilles, Jorge. "Purple Team Exercise Tools," Medium – https://medium.com/@jorgeorchilles/purple-team-exercise-tools-a85187ce341.
7. Orchilles, Jorge. "Vulnerability Management Is Hard! How Do You Prioritize What to Patch? Medium – https://medium.com/@jorgeorchilles/vulnerability-management-is-hard-how-do-you-prioritize-what-to-patch-1fc8e163d740.
8. Rapid7, "Prioritize Vulnerabilities Like an Attacker," Rapid7 – https://www.rapid7.com/products/insightvm/features/real-risk-prioritization/.
9. Red Team, "Red Team Development and Operations: Definitions," Red Team Guide – https://redteam.guide/docs/definition-lexicon/.
10. RTJournal, "Climbing the Red Teaming Ladder," Red Team Journal – https://redteamjournal.com/blog/2018/11/climbing-the-red-teaming-ladder.
11. Sabel, Cameron and Jared Semrau,"Separating the Signal from the Noise: How Mandiant Intelligence Rates Vulnerabilities — Intelligence for Vulnerability Management, Part Three," FireEye, April 20, 2020 – https://www.fireeye.com/blog/threat-research/2020/04/how-mandiant-intelligence-rates-vulnerabilities.html.
12. ANS, "SEC560: Network Penetration Testing and Ethical Hacking," SANS – https://www.sans.org/course/network-penetration-testing-ethical-hacking.
13. Tai, Wei. "What Is VPR and How Is It Different from CVSS?" Tenable – https://www.tenable.com/blog/what-is-vpr-and-how-is-it-different-from-cvss.

About the Author

Jorge Orchilles, MS, led the offensive security team in a large financial institution for 10 years; is a SANS Certified Instructor; author of SANS SEC564: Red Team Exercises and Adversary Emulation, co-author of CVSSv3.1 and a threat-led penetration testing framework; C2 Matrix project lead; and 2020 NSI Technologist Fellow. He can be reached at jorge@orchilles.com.

Can You Handle a Nation-State Cyber Attack

Continued from page 10

curity team at all levels. Hiring skilled workers is notoriously difficult, so they wanted to make sure the team's skills were constantly improving and second to none. This, too, requires real-world training—the same type of immersive training NATO has created. For businesses, immersive cyber training is new. Experientially, it is a lot more like pilot simulator training than sitting in a classroom. Defenders work in realistic sessions and gain the skills needed to understand how attacks are unfolding and how to execute effective containment activities. The learning experience is called "gamified," meaning it is interactive and keeps the defender's attention.

According to Ian Quinn, director, joint operations center and head of global security education, outreach and awareness at Barclays, "As sophisticated attacks unfold, communication and process breakdowns occur because no previous generation training classes can prepare for them. Cyber range blue team exercises are simply the only way to surface and identify critical deficiencies. Immersive cyber skills training is a high-intensity endeavor that quickly uncovers gaps in skills and processes, enhances individual learning and cross-team collaboration, and feeds the data into a system for ongoing learning."

Barclays' approach begs the question: Can a company that embraces this operational training approach to cybersecurity stop a nation-state attack? In the end, no one is immune. There will simply never be enough technology to protect desirable targets. But the Barclays team has applied continuous training, assessments, and simulations to confront the most dangerous adversaries. In the process, it has increased their chances of effectively recognizing and taking immediate corrective actions to disrupt and contain them.

About the Author

Gordon Lawson is president at RangeForce. He has nearly two decades of experience in the security sector with a focus on SaaS optimization and global enterprise business development. He is a graduate of the US Naval Academy and holds an MBA from George Washington University. He may be reached at gordon@rangeforce.com.