Breach Your Castle for Better Security

Asymmetric warfare is "the application of dissimilar strategies, tactics, capabilities and approaches used to circumvent or negate an opponent's strengths while exploiting his weaknesses."[1] Similar to guerrilla or unconventional warfare, the term implies a conflict between opponents of widely disparate resources and capabilities. Asymmetric warfare is often characterized by a small, resourceful and determined force fighting a much larger, technologically advanced and organized army. The objective of asymmetric warfare is not to overwhelm the enemy, but to harass and weary the enemy until the cost of victory becomes untenable.

Security has become a kind of disproportional war, in which defenders are engaged in a constant fight and face difficult odds. Experience proves that even the most sophisticated, best-protected networks are vulnerable to innovative, motivated and dedicated attackers who practice quick strike tactics that make use of automation, taking advantage of human weaknesses and abusing blind spots in complex IT environments. Enterprise and organizational security teams have to discover and patch every vulnerability and address every piece of malware—known and unknown—to minimize the threat of a successful attack. Meanwhile, the enemy needs to find only one vulnerability, one seam in the firewall or one moment of human weakness to find a way in and steal money, abscond with valuable intellectual property, and compromise enterprise and personal privacy.

Innovation abounds in the development of security solutions and techniques, but it also expands the universe of devices and services that an enterprise must maintain and manage to have state-of-the-art security. Paradoxically, innovation can serve to undermine security by adding to the complexity of constant updating, patching and testing that are needed, and by increasing the volume of noisy alerts that overwhelm security teams. The average large enterprise has to sort through approximately 17,000 malware alerts every week to find the 19 percent that are considered reliable.[2]

Breach Your Own Castle

It is necessary to develop a better process to offset security deficiencies and find a better way to inform defenders of weaknesses—one that understands how a potential attacker views, prioritizes and targets an infrastructure, and then how the attacker reaches the ultimate target. If an enterprise can breach its own castle before the adversary and proactively understand how the people, processes and technologies within its security framework respond, the enterprise can:

- Address issues before they are exploited
- Train security operations teams in the most likely incident response scenarios
- Optimize its security investments

Today, most security validation is performed by specialized consultants and ethical hackers. The skill sets of these professionals differ widely, and the pool of available, offensive cyber security talent is shrinking. In addition, regardless if enterprises hire specialized consultants or ethical hackers, enterprises are validating and analyzing infrastructure annually, at worst, and quarterly, at best. Point-in-time validations cannot keep pace with the ever-changing risk to business from new users, new endpoints, new applications and new hacking techniques.

Automation is the only way to resolve this weakness and keep pace with hacker breach methods and highly dynamic enterprise networks. By automating

Danelle Au
Is vice president of strategy at SafeBreach. She has more than 15 years of experience bringing new technologies to market. Prior to SafeBreach, Au led strategy and marketing at Adallom, a cloud security company acquired by Microsoft. She was also responsible for security solutions at Palo Alto Networks, driving growth in critical IT initiatives like virtualization, network segmentation and mobility. Au was cofounder of a high-speed networking chipset start-up, coauthor of an IP communications book, and holds two US patents for voice over IP (VoIP) and secure real-time transport protocol (SRTP) innovations.

adversarial actions, based on up-to-date threat intelligence, and analyzing vulnerabilities and weaknesses in the full context of systems and network relationships, a chief information security officer (CISO) can see how an actual attack can occur and what its ultimate impact will be. If CISOs can continuously validate the enterprise security posture from the perspective of the hacker, they can take necessary action in advance to mitigate attacks and stay ahead of the enemy.

The perspective on the need for automation in cyber security is not new. A December 2014 Forrester Research report stated, "Given the consequences of data breaches, businesses can no longer rely on passive, manual procedures to defend against them."[3] It is clear that the security community understands that automation is inevitable to succeed against attackers. Progress is already being made to automate incident response and orchestrate security policies to multiple security products. The next phase of the evolution is automation of the adversary's actions.

Automating the Hacker

Technology has emerged to automate the hacker.[4] Operating as internal security red and blue teams that alternately attack and defend in cyberwar games, simulators that are placed across the infrastructure play the role of the hacker. These simulators execute a variety of hacker breach methods that a real attacker uses, probing the network for security gaps and, when successful, moving along the kill chain to achieve their objective, such as locating and exfiltrating target data. A centralized management system collects and analyzes successful breach methods and scenarios to identify the source of the breach so that it can be fixed. In this way, automated breach simulations represent a potentially major advance for beleaguered CISOs and security teams, but only if the automated simulations and scenarios operate under meaningful parameters and achieve specific objectives for the enterprise, including:

- **Validate security posture across the entire kill chain**—A hacker thinks about getting from the initial point of penetration to the target. To properly identify risk for an enterprise, simulations must support validation across the entire kill chain—from infiltration to lateral movement and data exfiltration. This validation not only more accurately reflects the mind-set of an attacker, but also provides options to learn how and where to break the kill chain.
- **Incorporate comprehensive hacker playbook methods**—Hackers continue to refine their tools and techniques, including the types of malware that are being used. Hacker breach methods, similar to content signatures for an intrusion prevention system (IPS), should continue to be updated based on actual breaches and investigative data.
- **Inside out and outside in**—Attackers can be insiders or external threats. Simulators should be supported across the network, cloud and end points, and they should account for both internal and external attackers.

"Automated breach simulations represent a potentially major advance for beleaguered CISOs and security teams, but only if the automated simulations and scenarios operate under meaningful parameters and achieve specific objectives for the enterprise."

- **Real-world simulations**—Breach methods must be executed in production environments for the most accurate representation of hacker actions. To accomplish this successfully, breach simulations cannot impact users and the environment. This impact has been the

predominant fear with existing tools. Any security solution that breaks systems, affects users or impacts productivity is unlikely to be approved by management.

The Value of Breach Simulations

Simulating breach scenarios has various benefits. If an enterprise is spending time, money and other resources on security defenses (e.g., firewalls, IPS, secure web gateway, endpoint security), automating a hacker scenario and executing breach methods allows the enterprise to challenge these defenses and ensure that the investment it has made is paying off. The results of a successful simulated breach can be used to justify a change in approach if the C-suite or board needs to be convinced that the *status quo* is not sufficient. In fact, before enterprises choose a security vendor, they can quantify the vendor's efficacy using breach simulations. Validating that security products are working as expected is important. Due diligence needs to happen before implementation, after implementation and throughout the product life cycle.[5]

Breach simulation tools can also provide the means to more effectively deploy threat intelligence. A common frustration among security analysts is that the overwhelming volume of threat intelligence keeps them from being effective at addressing the threats that are specific to their enterprise. For example, attack patterns that show the targeting of financial services enterprises may be of little concern to a CISO responsible for protecting the high-value intellectual property of a manufacturer. Retailers may need to know and prepare for the latest techniques that are being used to compromise point-of-sale systems and recognize that attacks against health care institutions pose a minimal risk to their operations.

Being able to simulate breaches via an automated platform also allows security teams to identify breach scenarios and make more intelligent adjustments that disrupt and disable critical attack paths that the simulation identifies. Breach simulation also optimizes resources by making the security team more efficient in its day-to-day operations. Consider how security red teams operate. These teams are typically the elite security professionals with the right offensive-security mind-set who execute breach scenarios in enterprises today. If these professionals can offload foundational validation to an automated hacker, they can focus on identifying more unique threats for the enterprise. At a time when IT security skills are in high demand, employing breach simulation can mean getting the most out of the team.

"At a time when IT security skills are in high demand, employing breach simulation can mean getting the most out of the team."

Using threat intelligence feeds accelerates the response cycle and gives enterprises an opportunity to provide weapons to the available information in advance of a potential attack, turning hacker innovations into a stouter defense.

Finally, breach simulations can help to train security operations teams to be ready for a breach. By simulating a breach and ensuring the right alerts are being triggered, teams can build the muscle memory for incident response.

Automated Breach Simulations vs. Existing Tools

Does the use of breach simulations mean that it is time to replace the specialized tools that are already in the enterprise? The answer is no. A virtual hacker

or a breach simulation platform should serve as a complement to tools such as:

- **Security information and event management systems (SIEMs)**—They collect and analyze logs from a variety of network and security devices. Although they correlate events across different systems, they do not actually simulate and identify breach scenarios across the entire kill chain. Alerts from breach simulations can be sent to SIEMs to train security operations center (SOC) teams on expectations in the event of a breach.
- **Vulnerability management systems**—They are an essential component of any security strategy; however, although patching is critical, a hacker's playbook is not limited to vulnerabilities. A completely patched environment can still be breached. A breach simulation platform complements vulnerability management systems by identifying breach scenarios using a complete set of hacker breach methods, and does so in a safe way.

Environment Impact

One of the biggest advantages of breach simulations is that they run continuously, are safe and provide the kill chain perspective, in comparison with hacking tools, such as Metasploit, that may wreak havoc in an environment. Because simulations are performed between simulators, the impact to users and the environment is minimal other than a slight kilobyte increase in network traffic.

High-quality breach method databases can help to avoid breach simulation false positives. When a breach simulation platform plays the role of a hacker, the breach method database—the breadth and depth of breach methods—is the best determinant of the efficacy of the simulation. Enterprises should select breach simulation vendors based on the caliber of the vendor-offensive security researchers able to maintain and update these breach methods. Tools such as Wireshark, Process Explorer, FileMon, NetMon and Netflow can be used to inspect traffic that is created by breach simulations and ensure that the product is working as expected.

Should Enterprises Play the Role of a Hacker?

Globally, enterprises are projected to spend US $73 billion in cyber security solutions in 2016 and more than US $101 billion by 2020,[6] yet breaches keep happening. The answer is not in building taller, thicker walls for the castle. Instead of throwing more money at the problem, enterprises need to begin to think smarter, anticipate the enemy's next move and act in advance. Enterprises need to be bold enough to challenge their security controls, train their SOC teams so they know what to expect in the event of a breach and predict breach scenarios so they have the benefit of time to address them.

The time for a new, more innovative, automated, proactive way to validate security is now. Enterprises should play the hacker and breach their own castles.

Endnotes

1 United States Army Asymmetric Warfare Group, "Mission," 2015, *www.awg.army.mil/About.asp*
2 Lemos, R.; "Survey Says Security Products Waste Our Time," ARS Technica, 16 January 2015, *http://arstechnica.com/security/2015/01/survey-says-security-products-waste-our-time/*
3 Blankenship, J.; J. Kindervag; S. Balaouras; G. O'Donnell; H. Shey; S. Schiano; T. Lyness; P. Dostie; "Rules Of Engagement: A Call to Action to Automate Breach Response," Forrester Research Inc., 3 August 2016, *www.forrester.com/report/Rules+Of+Engagement+A+Call+To+Action+To+Automate+Breach+Response/-/E-RES87221*

4 Jackson Higgins, K.; "Startup Offers Free Cyberattack Simulation Service," *Information Week Dark Reading*, 2 December 2015, *www.darkreading.com/attacks-breaches/startup-offers-free-cyberattack-simulation-service/d/d-id/1323382*
5 Sanabria, A.; "The Biggest Mistake Enterprises Make When Purchasing Security Products and Services," Peerlyst, 29 September 2016, *www.peerlyst.com/posts/two-of-the-biggest-mistakes-enterprises-make-when-purchasing-security-products-and-services-adrian-sanabria*
6 Smith, E.; M. Shirer; "Worldwide Semiannual Security Spending Guide," International Data Corporation Research Inc., press release, October 2016, *www.idc.com/getdoc.jsp?containerId=prUS41851116*