HOW TO ASSESS YOUR SECURITY:

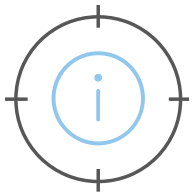
A Pen Testing Use Case Guide

A penetration test is the process of uncovering and exploiting security weaknesses in order to evaluate the security stance of an IT infrastructure. Using the techniques of a real attacker, pen testers intelligently determine risk and prioritize critical vulnerabilities for remediation.

Just as threat actors use tools to swiftly compromise an environment, pen testers use tools like Core Impact to streamline the process of gaining access by automating routine tasks so they can handle more dynamic issues. Additionally, such penetration testing tools can be used by security team members who may not have an extensive pen testing background, using them for tests that are easy to run, but essential to perform regularly, like validating vulnerability scans.

To better demonstrate how a pen testing solution like Core Impact can bolster your organization's security, we have put together several use cases of the fictional Acme, Inc., which show how Core Impact allows security teams to safely and efficiently test your environment using the same strategies as today's adversaries.

Use Case: Vulnerability Validation



Security Analyst Mary Jackson is in charge of running regular vulnerability scans of her organization's environment. The scanner turns up multiple vulnerabilities, and Mary is unsure of which vulnerability to try and resolve first.

DANGER:

Vulnerability scanners are an excellent security tool that examine an environment and uncover vulnerabilities that may be putting an organization at risk. A vulnerability scan report may list the corresponding Common Vulnerabilities and Exposures (CVE) number with each vulnerability, which is a unique id number that is assigned to known vulnerabilities. CVEs are given a rating using the Common Vulnerability Scoring System (CVSS) to classify how severe these vulnerabilities are on a scale of 0-10.

However, scanners can uncover hundreds, or even thousands of vulnerabilities depending on the size of an IT environment, so there may be enough severe vulnerabilities that the scoring system doesn't provide enough clarity on where to begin. Additionally, while this system may help give an idea of how much of a risk each vulnerability poses, it does not take context into account. While a vulnerability may be scored as a 10, it may not actually be posing as big of a risk to Acme because the vulnerability is on an isolated system that requires direct access. A vulnerability with a lower rating may actually have the potential to cause more damage based on its location and ability to be leveraged for further attacks.

Ultimately, vulnerability scanners are intended to provide a broad picture of your security posture, but more insight is needed to fully prioritize the list of vulnerabilities uncovered.

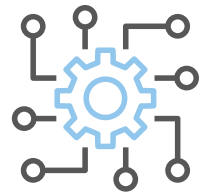
REMEDY:

Mary could use a penetration testing tool like Core Impact to fully prioritize the list of vulnerabilities uncovered. Penetration tests can validate vulnerabilities by investigating whether or not a vulnerability can be used to gain access, and if so, how difficult that effort would be. The results of such a pen test would produce a list based on the risk the vulnerabilities pose to the organization's specific infrastructure.

Core Impact integrates with numerous third-party scanners, like Frontline, Burp Suite, Nessus, and Qualys, directly importing their scan data to run an automated test for vulnerability validation. Core Impact will evaluate the scan's output and provide you with prioritized validation of your system's weaknesses.

Use Case: Automation

In order to extend their vulnerability management program, Acme would like to run penetration tests on a regular basis.



DANGER:

Oftentimes, organizations that look into building a penetration testing program assume they need to regularly use a third-party service or hire their own team of experienced testers. However, there has been an ongoing skills shortage in the field of cybersecurity that shows no sign of resolving anytime soon. In fact, according to the 2021 Pen Testing Report, 44% of respondents answered that lack of talent/skillset were why they did not run pen tests, and 48% of respondents said that hiring enough skilled personnel was one of their top pen testing challenges.

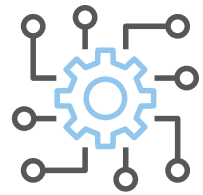
This can be an issue for both third-party and internal teams. Reputable, skilled, third-party pen testers can only run so many engagements, and may not be able to accommodate such a frequent cadence. Alternately, the organization's budget may not be able to sustain hiring pen testing services for more routine tests. For internal teams, experienced testers may not be available for hire, and those that are often come with a high price tag.

Manual pen testing can also be quite lengthy and labor intensive. Even though teams and individual testers use penetration testing tools, they are often relying on mix of multiple open-source tools, which means switching back and forth between solutions and manually combining information for reporting.

Because of these time and budget constraints, organizations may, at most, only be running tests annually, which is typically not sufficient. An organization may add additional assets or upgrade existing ones throughout the year, and their security should not have to wait so long to be validated. Further, retesting, which involves rerunning the same tests as a previous pen testing session, is critical in order to verify that remediation efforts were successful.

Use Case: Automation

In order to extend their vulnerability management program, Acme would like to run penetration tests on a regular basis.



REMEDY:

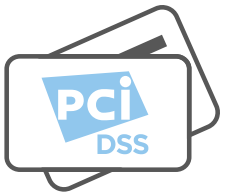
An automated pen testing tool like Core Impact can easily streamline the penetration testing process. Firstly, Core Impact addresses the pen testing skills gap. While experienced pen tests will always be needed for complex engagements, not every test requires an expert.

Core Impact enables team members who don't have a deep background in pen testing to be able to run basic, though vital, tests using Rapid Penetration Tests (RPTS). These step-by-step wizards safely guide a tester through exercises like network information gathering or privilege escalation. Even general tests that validate remediation can be straightforward and automated. This allows organizations to run tests more frequently while still maintaining efficiency, and without having to dramatically increase headcount.

Secondly, Core Impact's centralization both reduces console fatigue and standardizes reporting. As a comprehensive tool that can test across multiple vectors, every phase of the penetration testing process can be executed and managed in one place. Additionally, Core Impact offers multiple integration and collaboration capabilities with tools like Plextrac, Metasploit, Burp Suite, and Cobalt Strike for further centralization. With all of this information in one place, reports can be automatically generated instead of manually combining them piecemeal from different tools.

Use Case: Compliance

Since Acme has its own retail business, they are required to adhere to the PCI DSS security standards.



DANGER:

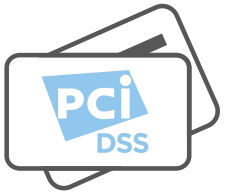
Most organizations must adhere to some type of industry or government security regulation, like SOX, GDPR, HIPAA, or NIST. In this case, PCI DSS is administered by the Payment Card Industry Security Standards Council and focuses on moving all retailers (and other industries) who use credit/debit cards into stronger and more predictably tested security postures, which can dramatically reduce credit card fraud.

Not adhering to PCI DSS can result in multiple issues. Firstly, these requirements are intended to safeguard an organization from data breaches, so failing to meet these best practices dramatically increases the risk of a successful attack. In the short term, breaches can disrupt or halt productivity. In the long term, they can take a great deal of time and money to recover from. Additionally, it may permanently damage the reputation of a business, which can result in fewer sales, and diminished confidence from investors. Not only that, credit card companies may no longer want a contract with the organization, so the business can no longer accept those cards for any transaction. Liability issues may also have to be resolved in court.

Lastly, failure to comply can also result in serious fines ranging from thousands to millions of dollars. It's also worth noting that part of PCI DSS, as well as many other regulations, is being able to prove compliance—those without thorough reporting or documentation may still end up failing an audit.

Use Case: Compliance

Since Acme has its own retail business, they are required to adhere to the PCI DSS security standards.



REMEDY:

The PCI standards currently consist of 12 main requirements, and over 200 sub-requirements. Requirement 11.3 mandates the development and implementation of "a methodology for penetration testing that includes external and internal penetration testing at least annually and after any upgrade or modification."

Luckily, penetration testing can kill two birds with one stone. If a penetration test has proper reporting, it can not only show that a pen test was conducted, but can also prove compliance to other requirements or sub-requirements. In fact, 99% of those surveyed for the *2021 Penetration Testing Report* said they used pen testing to maintain and demonstrate compliance for at least one regulation, such as SOX, HIPPA, or GDPR.

These regulations aim to protect sensitive data that is valuable to attackers, which can include customer or patient information, financial records, or even employee files. Periodic mandated testing ensures organizations stay compliant by uncovering and fixing security weaknesses that may be putting this data at risk. Additionally, for auditors, these tests can also verify that other mandated security measures are in place or working properly.

A penetration testing tool can make adherence to any regulation simple to implement, minimally disruptive, and budget-conscious. Core Impact provides an easy to follow and automated framework that can run internal and external tests, and also doesn't require the security team to have extensive pen testing experience. Additionally, Core Impact's automated reporting features ensure consistency and increase efficiency, creating a thorough record for all aspects of a pen testing engagement.

Use Case: Infrastructure Upgrade Validation

As Acme continues to grow and evolve, its IT environment must do the same. Consequently, additional servers are added, new solutions are added to the tool stack, and existing tools are upgraded to the latest versions.

DANGER:

Despite all efforts to create and distribute a secure product, there are countless software (and even some hardware) releases that contain vulnerabilities. So while upgrades and new assets bring exciting new capabilities and features, they also bring in the potential to become attack vectors for malicious actors seeking to gain access. Depending on the severity of the vulnerability, a threat actor could gain access to credentials, escalate privileges, or even take control of the root account.

Once vulnerabilities have been discovered, advisories are typically released with details on workaround patches, or other ways to mitigate risk. If an organization hasn't run a pen test after adding new assets, they may not be aware of how much of a risk it poses to their organization, or may not even know the vulnerability exists in their environment. Even when patches exist and are applied, they may not have been implemented correctly, leaving the vulnerability intact.

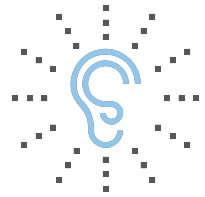
REMEDY:

As an organization's infrastructure changes, either through upgrades or adding additional assets, it's critical to pen test regularly. A single pen test serves as a baseline. An integral part of pen testing strategies is to retest frequently against that baseline. Retesting helps ensure that that security holes have been closed when remediation efforts have been made and can uncover new weaknesses that may be present in new assets or updates.

Having a pen testing tool like Core Impact can help to enable and streamline the retesting process. Organizations without a distinct internal team may rely entirely on third-party services, who they may only be able to enlist once a year. Having a pen testing tool allows any organization to run basic, routine tests, like validating vulnerability scans. These simple tests can be all that's needed to verify that new vulnerabilities are present.

Core Impact has a certified library of exploits that is kept up to date to test against the latest vulnerabilities. Additionally, Core Impact can save testing sessions when they are initially run, logging what attack paths were used. These tests can then be automatically rerun at a later time for remediation validation. Comparing reports from both tests can also show if any new vulnerabilities have been uncovered as well as revealing if patches were correctly applied and functioning.

Use Case: Increasing Workforce Awareness



Acme Inc. recently experienced several small breaches. While tools in their security stack detected and prevented these breaches from doing significant damage, security analyst Annie Easley is still concerned about where these breaches originated. Upon analysis, it is discovered that several employees received emails that they thought were from customers, and opened an attachment, not knowing it held a suspicious payload. Annie wants to know how aware the rest of the employees are of such dangers.

DANGER:

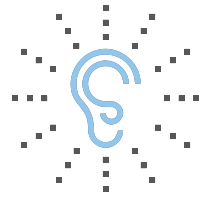
Software vulnerabilities can be patched and misconfigurations can be corrected, but there is no closing an organization's biggest security hole—its employees. Though phishing is an old technique, it is still an effective one that attackers regularly rely upon to solicit sensitive information or directly breach a system.

While spam filters can block out a portion of phishing emails, they are typically the most basic ones that are more easily recognized. However, many can still slip through, particularly spear phish, which are tailored for an individual or organization. These are much more sophisticated, and can either realistically imitate an official business, or appear to come from an individual they know.

Administrators may be able to put more powerful blockers up or have notifications of external email addresses for the company email service. However, employees still regularly check personal email from their workstations or in the case of remote work, personal computers sharing a Wi-Fi router with a work computer are inadvertently connected to the network.

Victims of phishing attacks may never realize that they were the ones to open the doorway to a breach. If they are unaware of this knowledge, they may very well open another phishing email without thinking twice.

Use Case: Increasing Workforce Awareness



Acme Inc. recently experienced several small breaches. While tools in their security stack detected and prevented these breaches from doing significant damage, security analyst Annie Easley is still concerned about where these breaches originated. Upon analysis, it is discovered that several employees received emails that they thought were from customers, and opened an attachment, not knowing it held a suspicious payload. Annie wants to know how aware the rest of the employees are of such dangers.

REMEDY:

Using a pen testing tool like Core Impact would enable Annie to be able to run sophisticated simulated phishing campaigns. These campaigns are designed to give an organization data on how vulnerable they are to such attacks.

Using Core Impact's phishing capabilities, Annie could harvest email addresses that are visible from the Internet as well as the organizational intranet. Phish can then be designed to appear as authentic as needed. If opened, these phishing simulations can launch network pen tests to show how much access could be attained once deployed, demonstrating just how dangerous a phishing attack can be. At the conclusion of each test, Core Impact generates a list of who opened these emails, providing insight into who is most susceptible to these types of attacks.

From there, this data can be used to design and implement effective instruction and training, teaching employees vigilance and techniques for recognizing and reporting phishing attacks. Additionally, running phishing simulations before and after training, or making it a regular practice in general, can provide valuable data about how successful these education efforts are.

Use Case: Advanced Threats

With more incidences of severe attacks on the news, Acme's concern of stealthy attacks grows. Could a seemingly minor threat vector serve as an entry point for an attacker to linger within the environment for a long period of time, allowing them to slowly work their way into more critical areas of the IT infrastructure to steal valuable data or severely disrupt operations?

DANGER:

Most cyber-attacks take a "hit-and-run" approach, using methods like DDoS or malware to achieve a simple goal of a single step breach. However, there are an increasing number of complex advanced threats that target high value objectives.

Such attacks are multi-layered, with attackers remaining in the environment long after the initial exploitation. Once they've gained an initial foothold, they'll work on strengthening it to get closer to their ultimate goal. For example, while they may use a successful phishing attack as their entry point, the end goal of the attack is not to remain on the initial victim's device. Instead, they'll begin to determine if additional users have access to the machine, what networks it can talk to, and where the local DNS servers or even domain controllers are. From there, they'll pivot, using another attack to gain access to other systems.

Since such attacks take more time and skill in order to gain additional access to a hard-to-reach target, they need to remain undetected and linger in the system. Consequently, attackers focus on "low and slow" attacks, which involve stealthily moving from one compromised host to the next, without generating irregular or unpredictable network traffic in order to hunt for their specific data or system objectives.

Unfortunately, many security teams are focused solely on initial exploitation, as their resources don't enable them to explore potential next steps of an attack.

Use Case: Advanced Threats

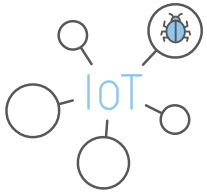
With more incidences of severe attacks on the news, Acme's concern of stealthy attacks grows. Could a seemingly minor threat vector serve as an entry point for an attacker to linger within the environment for a long period of time, allowing them to slowly work their way into more critical areas of the IT infrastructure to steal valuable data or severely disrupt operations?

REMEDY:

Acme's security team could use a penetration testing solution like Core Impact to run advanced penetration tests. In addition to information gathering and entry point attacks, such tools can also run tests to escalate privileges after a successful breach, allowing them to advance further into an IT environment.

Additionally, just as cyber-attackers use multiple tools, so must penetration testers. A security team could benefit from an adversary simulation solution to further play out an advanced persistent threat (APT) scenario. Solutions like Cobalt Strike can emulate a threat actor focused on stealth and post-exploitation so that cybersecurity professionals can determine whether an infrastructure's defenses are strong enough to detect or prevent an advanced adversary from moving closer to critical assets. In fact, Core Impact and Cobalt Strike even have interoperability features, like session passing, which allows an attack simulation to be played out from initial breach to an embedded actor.

Use Case: IoT and SCADA Testing



Acme's IT infrastructure does not just consist of servers and workstations. As a large manufacturing company, they have a SCADA system, as well as IoT devices, like the office's smart thermostat. Additionally, Acme permits remote work, so IoT devices in the homes of employees may also be connected to the network.

DANGER:

Many IoT devices have become critical to organizational productivity. Unfortunately, these added benefits are accompanied by security risks. IoT devices not only increase the attack surface, they further increase risk because they often lack traditional preventative layers like antivirus.

The danger of IoT devices is two-fold. First, threat actors may have a substantially easier time breaching the network using IoT devices as their entry points. While the IoT device may not provide significant access to sensitive information, it can be used as the initial link in an attack chain that will eventually lead them deeper into the network. For example, one large data breach began when a threat actor attained credentials to a HVAC system in a company's building.

Second, certain IoT devices and SCADA systems are essential to the primary function of an organization, so taking control of these devices or simply disabling them can completely cripple the business. This can even affect the functionality of cities or countries. For example, nuclear centrifuges were targeted by the Stuxnet worm.

REMEDY:

Uncovering any potential vulnerabilities in these devices through pen testing is a key way to ensure they are as secure as possible. Pen testers can use exploits that take advantage of flaws or weaknesses in an IoT device, demonstrating how a threat actor could gain access. Even efforts to make IoT more secure should be tested. Some organizations have attempted to connect IoT devices using a VPN as an added safeguard. However, threat actors can also target weaknesses in VPNs, such as those that have gone unpatched, so these should also be regularly assessed.

Core Impact has a robust, stable library of expert tested commercial-grade exploits, which is regularly updated. A partnership with ExCraft Labs, an expert cybersecurity research group, provides the option to add additional IoT exploit packs, allowing pen testers to comprehensively assess every piece of an IT infrastructure.

SUMMARY

Ultimately, these use cases show the dynamic ways pen testing tools can give organizations a security advantage, providing valuable insights that will help mitigate risk and protect essential assets. These use cases also provide a glimpse of the benefits of Core Impact, a robust, automated tool that provides both visibility into the security stance of your organization and a clear pathway towards remediation. With Core Impact, security teams can maximize their resources with a centralized solution that allows you to gather information, exploit systems using certified exploits, and generate reports, all in one place.

coresecurity
by HelpSystems

About HelpSystems

Organizations around the world rely on HelpSystems to make IT lives easier and keep business running smoothly. Our software and services monitor and automate processes, encrypt and secure data, and provide easy access to the information people need.

CS-GD-0222-SV