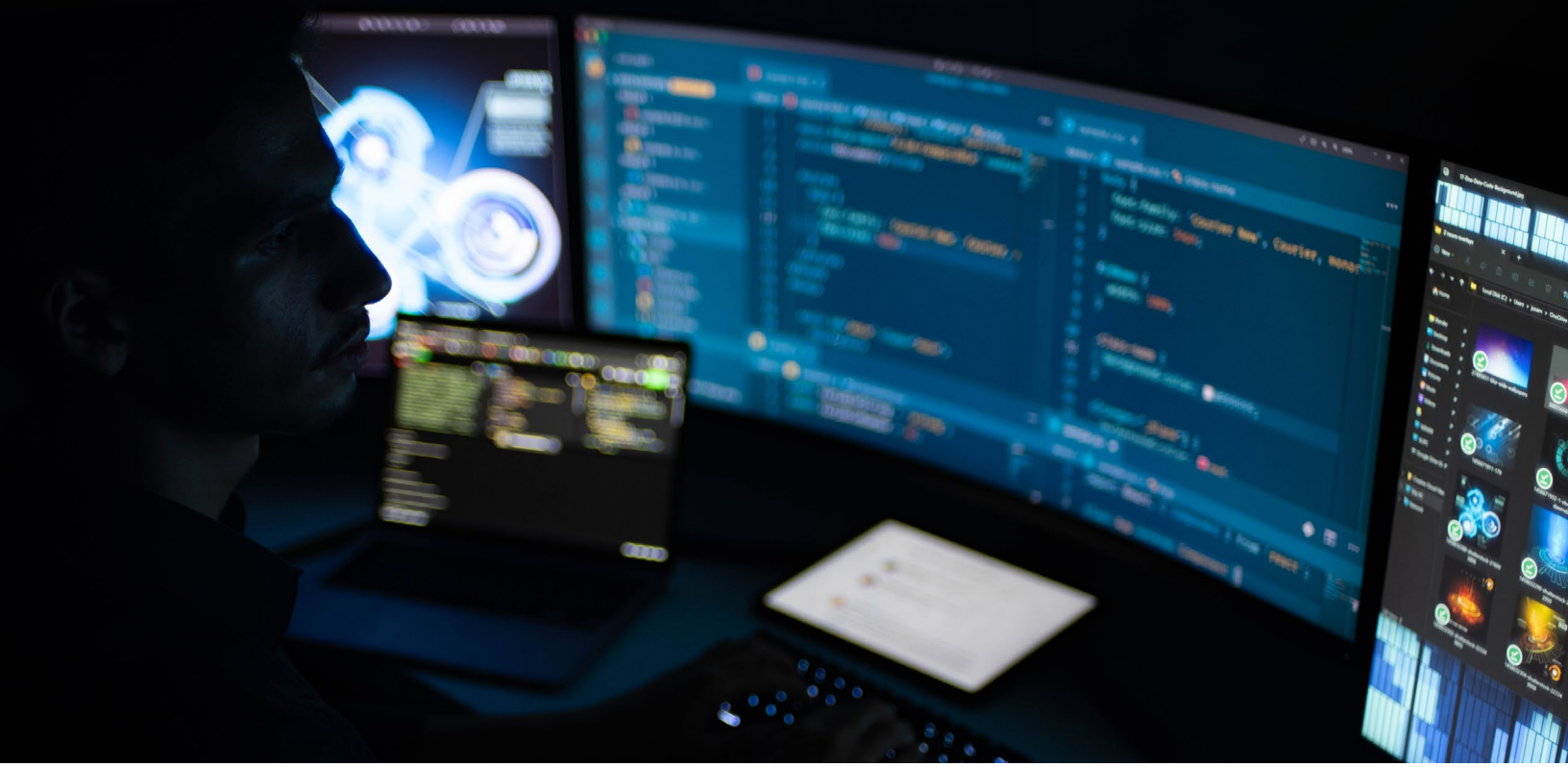
SPONSORED BY

CLONE SYSTEMS®

An ethical hacker's guide to customized penetration testing

What's new, what's old and what has changed in penetration testing



SC Media

CRA Business Intelligence

ebook
An SC Media publication

How penetration testing applies to cloud computing, smart devices and PCI DSS 4.0

Penetration testing is a craft as old as the cybersecurity profession, but attack tactics and the vulnerabilities they exploit have increased dramatically in recent years. ***Paul Wagenseil*** *unpacks what has changed and which new tools are available.*

OUR EXPERTS:

Tom Nianios
Senior Security Engineer, Clone Systems

Elyse Hamilton
Director, Customer Growth, Clone Systems

Ty Coffee
Managing Director, UHY

Norman Comstock
Managing Director, UHY

Scott Goodwin
Principal, Cybersecurity and Privacy Advisory, PKF O'Connor Davies LLP

Jason Stockinger
CRISC, CISSP, Director, Global Information Security, Royal Caribbean Group

Joshua Weiss
CEO, TeliApp

Penetration testing to gauge the security of computer networks dates to the 1970s. Many of the pen-testing techniques developed over the decades since still apply, as human nature remains unchanged and outdated technology continues to be used worldwide.

Yet innovation is a constant factor in pen-testing. In the past few years, testers have widened the scope of their targets to include Internet of Things devices and cloud servers and have incorporated machine learning and artificial intelligence into their toolkits.

"As a pen tester, you're always looking for new ways, and more automated ways, to do things," says Jason Stockinger, Director of Global Information Security at Royal Caribbean Group.

More specifically, for organizations that process more than six million payment-card transactions per year, penetration testing is an essential part of compliance with the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS 4.0, going into full effect by March 2025, adds new compliance requirements for any organization that accepts credit, charge or debit cards, regardless of the number of cards processed. As a result, the scope of associated pen tests will be widened.

What's new in pen testing, and what's old

The concept of penetration testing is simple: probe and try to penetrate an organization's defenses, especially those pertaining to computer networks, websites, web applications and other digital assets, all with the authorization of the targeted organization's management.

Pen testers are not malicious hackers, but professionals who are often certified information systems security professionals (CISSPs) or have similar credentials. They may sneak into buildings to gain access to server rooms, set up hidden Wi-Fi devices to capture network traffic and passwords, probe websites and web apps for exploitable vulnerabilities, send phishing emails to staffers, or even drop malicious USB sticks in parking lots.

> ***"You can't ignore the fact that because you move [your assets to the cloud], you need more security controls over there, because you have zero visibility now."***
>
> — Tom Nianios | *Senior Security Engineer, Clone Systems*

The goal is to see how far into an organization's systems an attacker can get, to discover how much data can be exploited or stolen, and, finally, to present a report to the organization's management explaining its security weaknesses, the associated risks and how those risks and weaknesses can be remediated.

By paying good guys to break in and having them show you how they did it, the theory goes, you can better defend yourselves against the bad guys.

Seven phases of a penetration test

Planning and scoping

The testers select the approach, scope and basic methodology. The client often dictates the scope, and many pen-testers will mix methodologies for maximum effectiveness.

Reconnaissance and information-gathering

The testers learn as much as possible about the targeted organization, often with the assistance of automated information-collection tools.

Scanning and discovery

The testers check for weak spots in the targeted organization's defenses and try to see how hard it is to get into protected areas. In a network pen-test, for example, this would involve probing and mapping the visible network and then trying to break into the network.

Gaining access

The active part of the pen-test begins as the testers break into protected areas. This can be done with a planned, manned "hands-on-keyboard" attack, but an automated pen-testing tool can do it too.

Maintaining access and going in deeper

Testers will try to establish persistence and move laterally throughout a network, preferably covering their tracks to avoid detection.

Reporting and risk analysis

The testers will report to the client organization's leaders on the state of the organization's security, what could happen and what can be done to fix things. The report should not be cursory, but instead very detailed and take an hour or two to present. This is perhaps the most important part of the pen test.

Remediation and verification

In some cases, the pen testers may come back for a second run to make sure the recommended steps have been taken and that mitigation has been successful.

Despite huge advances in software and security over the years, however, the basic methods of pen-testing tend to stay mostly the same.

"[It's] like breaking into a house. What are you going to do — bypass the alarm, bypass security, wear a hoodie, and so forth? The technique hasn't changed," says Tom Nianios, Senior Security Engineer at Clone Systems, a Philadelphia-based managed security service provider (MSSP) that offers pen tests and pen-testing tools as part of its services.

Likewise, many of the various standard methodologies that pen testers use as guides have been around for decades.

"The standards focus on stuff that's still relevant," says Nianios. "It's still relevant because it wasn't specific to vulnerabilities, which are constantly updating. It was specific to the methodology someone would use and the techniques someone would use to compromise an environment, which still stands correct today."

Standard methodologies used in penetration tests

- **Information System Security Assessment Framework (ISSAF)**: No longer updated but may still be useful as a guide to conducting a penetration test.
- **MITRE ATT&CK framework**: Developed as a guide to shore up defenses by analyzing real-life, step-by-step attacker tools and techniques. Its methods are often used by pen-testers to break into targets.
- **National Institute of Standards and Technology (NIST) Special Publication 800-115**: Provides guidance on planning and conducting a pen test and analyzing and remediating the findings. Corresponds to the widely used NIST Cybersecurity Framework (CSF) and to NIST SP 800-53, a mandatory compliance framework for most U.S. federal government agencies and contractors.

  "For a lot of our managed service customers," says Nianios, "we follow the NIST attack framework as far as pen-testing is concerned, because that focuses on techniques, and we can compare it with what's found in the results from a red-team assessment."
- **Open-Source Security Testing Methodology Manual (OSSTMM)**: Developed for security audits rather than penetration tests, but widely used by pen testers as a framework.

  "OSSTMM is a good standard in general, whether we're talking about IoT, cloud, or on-prem, just because of the technology and tools that are used there," says Nianios. "It touches a lot around physical security as well."
- **Open Worldwide Application Security Project (OWASP) Testing Guide**: Focuses on web applications and security controls. Includes checklists and lists of tools.
- **Penetration Testing Execution Standard (PTES)**: Very comprehensive and widely used. Walks pen testers through the entire process, from pre-test planning to post-test reporting.

"OWASP in particular is the de facto methodology for testing web applications, IoT devices and APIs," explain Ty Coffee, Principal, and Norman Comstock, Managing Director at UHY Consulting in New York. "ISSAF, NIST, and PTES may be geared more toward on-prem networks, cloud infrastructure, telecommunications, and wireless."

Many pen-testers use the standard methodologies as starting points rather than as prescriptive frameworks and will mix and match items from different methodologies to reach maximum effectiveness.

"Often, a blend of methodologies or a customized approach that combines elements from multiple methodologies may be the most effective for a given penetration testing engagement," says Joshua Weiss, CEO of TeliApp, a software-design, development and technology-infrastructure firm based in New Jersey.

Older pen-testing tools are also useful because so much antiquated software is still used by consumers and organizations alike. Asked which pen-testing tools and techniques should be deprecated or abandoned, Nianios can't think of any.

"I don't think we're at that state," he says. "A lot of customers and organizations have deprecated technology. There are customers out there that still run Windows XP, Windows 2008. I'm talking about Fortune 500 companies. You would use the same methodologies that you used 20 years ago to compromise their systems."

Automate everything

What is new in penetration testing is an increased reliance on automation. Automated tools themselves are nothing new; the network-mapping tool nmap dates from 1997. But their sophistication has become astonishing.

For example, some network-penetration tools can automatically plant backdoors in a network and set up command-and-control servers to direct malware from the internet.

> ***"If you're doing infrastructure as a service, [the cloud provider] is not going to allow you to pen-test past a certain point. If you start probing that, it'll be a breach of contract."***
>
> — Jason Stockinger | *CRISC, CISSP, Director, Global Information Security, Royal Caribbean Group*

Other tools can create complex phishing attacks with the click of a mouse, automatically scour the internet for available information on a targeted organization's employees and vendors, or automatically compile reports to be delivered at the end of a penetration test.

"The vast majority of tools that are executed by penetration testers, or real threat actors, are going to implement some level of automation, whether it's managing social-engineering campaigns or collecting system information," says Scott Goodwin, a principal in the Cybersecurity and Privacy Advisory practice of consulting firm PKF O'Connor Davies LLP. "This is simply because it makes testing more efficient."

Clone Systems itself offers an automated pen-testing program that clients can run themselves, although more hands-on tests involving human testers are also available.

"We offer an automated scripted test, which probably covers the majority of very simple scopes and environments," says Elyse Hamilton, Director, Customer Growth at Clone Systems. "If they're not that technically savvy, and the environment of the test is not too large, what we do is a hybrid model. And with that hybrid model, we just utilize our scripted tool, and we kind of manage it for them."

For the biggest organizations, "we do fully managed," Hamilton adds. "That would be for just larger complex environments, the people that are API-testing special applications."

To decide which option a particular organization should choose, "it's just dependent upon their level of comfortability with doing it themselves," Hamilton says. "Do they need a little bit of assistance, or do they need a fully managed hands-on pen-test by a CISSP?"

We are now seeing pen-testing tools and techniques that use machine learning and artificial intelligence. A ChatGPT pen-testing tool, PentestGPT, is available on GitHub. The role of AI in pen testing will only increase, said the experts we spoke to.

"I think it's going to play a huge role," says Nianios. "It makes anyone capable of writing programs or scripts, or modifying data that's available, to compromise a specific network or bypass specific technologies and techniques."

That may or may not democratize penetration testing. It will certainly democratize cybercrime. For that reason alone, pen testers need to incorporate AI into their toolkits.

"Among us security professionals, we are scared to death of artificial intelligence," says Stockinger. "But we need to be embracing it like the bad guys are embracing it. ... We should be using this stuff in our sandboxes more than the bad guys in order to come up with repeatable defense patterns, because the bad guys are going to be using this to attack us."

AI is set to put pen-testing automation into hyperdrive at the possible cost of a lack of human understanding of what it finds.

"My assumption is that we will have AI-driven penetration testing tools [that] are capable of identifying, exploiting, and reporting on known vulnerabilities in specific areas with relatively little human interaction," says Goodwin.

Staring through the scope

Two other fundamentals of penetration testing are approach and scope. The approach determines how much access to and information about the target is given to the pen-testers before the test. The scope determines which parts of the targeted organization's systems will be tested.

A black-box approach gives the pen tester little information and zero access to the target organization's network or facilities. A white-box approach grants both network access and detailed information about the organization's inner workings.

> *"There are customers out there that still run Windows XP, Windows 2008. I'm talking about Fortune 500 companies. You would use the same methodologies that you used 20 years ago to compromise their systems."*
>
> — Tom Nianios | *Senior Security Engineer, Clone Systems*

On the face of it, the black-box approach might seem to be more realistic in mimicking the actions of a real-life attacker. But a white-box approach may more thoroughly explore all the possible ways that a skilled and determined attacker could exploit a network once internal access has been achieved.

Types of pen tests grouped by approach

- **Black-box, aka opaque, test**: The tester has no special access to the target but must break in as a regular attacker would. A black-box test can take several weeks and may cost many thousands of dollars, depending on the extent and scope of the targeted areas. Variants include "blind" tests, in which the tester is given only the name of the target organization, and "double-blind" tests, in which the organization's IT and/or security teams get no warning of the pen test.

  "Whatever, whoever is going to try to hack your environment, they're going to use black-box testing," says Nianios.

- **External test**: Similar to a black-box test in that the organization's outward-facing network defenses are probed. This is best for testing internet defenses.

- **Gray-box, aka semi-opaque, test**: The tester has limited access to the target network, as would a logged-in customer or unprivileged employee. Best for testing identity and access management.

- **Internal test**: As in a white-box or gray-box test, the pen-tester gets partial or full access to the organization's internal network. Best for testing internal access management and zero-trust defenses.

- **White-box, aka transparent, test**: The tester has full access to and knowledge of the targeted facilities or network, like a sophisticated attacker who broke in, established persistence and was moving laterally. In a variant called a "targeted" or "lights-on" test, the tester may work with defenders to find and fix specific flaws. A white-box test generally takes less time and money than a black-box test of similar size and scope. This type is best for testing application and API security and may be safest for probing cloud assets, because a black-box test could cross the line into areas governed by the cloud service provider.

Also relevant are vulnerability scans, which are not penetration tests at all in that they don't try to break into anything. Instead, they check for common security flaws and misconfigurations and may suggest ways to remediate those flaws.

For many mid-sized or large organizations, part of the PCI DSS compliance process is having internal vulnerability scans performed quarterly by PCI-certified Approved Scanning Vendors (ASVs) such as Clone Systems. The company offers an automated PCI-compliant ASV scan that clients can run themselves.

Scope is even more important than approach. It determines what gets probed and what type of pen-test should be performed. There are different types of pen tests for networks and infrastructure, wireless networks, social engineering, web applications, physical facilities, and many other types of systems.

> ***"Among us security professionals, we are scared to death of artificial intelligence. But we need to be embracing it like the bad guys are embracing it."***
>
> — Jason Stockinger | *CRISC, CISSP, Director, Global Information Security, Royal Caribbean Group*

If you're having a pen-test done for PCI DSS compliance, for example, you'll want to run a network pen-test to probe the integrity of the cardholder data environment (CDE), or all the areas in the network where payment-card data may be entered, processed or stored, ranging from online checkout pages to point-of-sale terminals to cloud servers.

If you run a retail website, you'll also want to pen-test the web applications that let customers browse and pay for items.

"I recommend two different types of scans [for PCI DSS]," says Stockinger. "There's a network-level scan, where you're literally just checking the windows and doors of everything. And then there's also a web-application scan or something that is a little bit more OWASP, or the Open Web Application Security Project."

Types of penetration tests grouped by scope

- **API**: Targets the application-program interfaces that let different programs interact with each other.
- **CI/CD**: Targets the continuous integration/continuous deployment software-development life cycle (SDLC), often through automated static or dynamic application security testing (SAST/DAST).
- **Client-side**: Targets consumer and end-user software, often searching for common web security issues.
- **Cloud**: Targets cloud assets and servers. This often requires a new set of skills and tools, and testers must avoid crossing into a cloud service provider's area of responsibility.
- **Containers**: Targets walled-off processes running on on-premises, cloud or hybrid servers.
- **Internet of Things/embedded devices**: Targets "smart" commercial and consumer devices used in workplaces such as thermostats, conference-room TVs, refrigerators, and smart speakers.
- **Mobile apps**: Targets mobile apps on both client and server side.
- **Mobile devices**: Targets smartphones and tablets, including operating systems, radio communications and physical access.
- **Network**: Targets an organization's external (often internet-facing) and internal network defenses.
- **Physical**: Targets access to facilities, such as offices, server rooms or maintenance rooms. Many pen tests involve impersonating an employee to gain access to protected areas from which network penetration can begin.
- **Remediation verification**: Targets vulnerabilities and flaws detected during earlier pen tests and vulnerability scans to check that they've been fixed.
- **Social engineering**: Targets employees or customers of targeted organizations to trick them into providing access to protected networks.
- **Web application**: Targets web-based application and processes, whether from the client or server side.
- **Wireless**: Targets an organization's Wi-Fi or fixed-cellular network access.

Putting the cloud in scope

In recent years, the potential scope of penetration tests has widened to include cloud servers and assets. Pen-testing cloud environments often requires learning new techniques because data and applications may be distributed among a cloud service provider's servers, or between a client's on-premises servers and the cloud.

"It is a new set of skills. And it is a new set of methodologies," says Nianios. "However, it's easier in my opinion because all the security controls that they had in place on-site, all these layers that they've added over the years, they don't exist over there [in the cloud]."

Not all customers see the necessity of pen-testing their cloud assets, according to Nianios. Some believe that because something's now in the cloud, it's automatically more secure.

"I mention to all of our clients that are either hybrid mode or moving to the cloud [that] you can't ignore the fact that just because you move there, you need more security controls over there, because you have zero visibility now," he explains.

Lack of visibility is a constant issue, both due to the limitations imposed by the division of responsibility between cloud providers and clients, and to the often-unchecked proliferation of cloud assets that arises from the ease and affordability of spinning up new instances.

> ***"We will have AI-driven penetration testing tools [that] are capable of identifying, exploiting, and reporting on known vulnerabilities in specific areas with relatively little human interaction."***
>
> — Scott Goodwin | *Principal, Cybersecurity and Privacy Advisory, PKF O'Connor Davies LLP*

The shared-responsibility model imposes additional boundary restrictions. A cloud pen-tester should only probe those areas under the control and responsibility of the client; break into areas that "belong" to the cloud service provider, and the client may be violating the service agreement.

The frequent lack of clarity among cloud customers about where exactly the client's responsibility ends and the cloud provider's begins only further muddies the issue.

Before pen testers probe cloud assets, "they really need to dig into the licensing and contractual agreements that that organization would have with the cloud provider," Stockinger explains. "For example, if you're doing infrastructure as a service, [the cloud provider] is not going to allow you to pen-test past a certain point. If you start probing that, it'll be a breach of contract."

Despite the difficulties, penetration tests for the cloud have become a necessity. Cloud misconfigurations often leave valuable data unprotected, ready for any snooper to find. Rogue instances set up and forgotten by poorly supervised employees can be left running without detection.

Automated tools have been developed to probe cloud assets, and cloud service providers themselves often offer scanning tools. Goodwin points out that PCI DSS 4.0 includes a new requirement that cloud service providers support their clients during pen tests.

"This requirement [11.4.7] places additional responsibilities on cloud service providers to work with their customers through scoping issues and, potentially, remediation of vulnerabilities that cannot be addressed without the support of the service provider," he says.

Leveraging the Internet of Things

Pen testers are also probing Internet of Things and "smart" and embedded devices, especially those devices commonly found in workplaces. Many consumer-grade smart devices in the office are never updated or even catalogued by IT teams, leading to a shadow IT deployment that can be leveraged as a potential attack vector.

"For example, the Amazon Alexas that have become super popular. I know executives that have them in their offices," says Stockinger.

"But what they don't realize is that if that [Alexa] rides the same wireless network as the corporate network, that can create a bit of compromise for the network," he adds. "If those things aren't kept up-to-date, or if they're not connected appropriately, they can absolutely be an injection point for the bad guys."

Likewise, a "smart" TV in a conference room can be infected by a pen tester or a real-life attacker posing as a janitor with a USB stick. The TV is often connected to a video-conferencing system, and an attacker might easily be able to spy on meetings or even capture images of who's in the room.

"For even a Fortune 500 company, who goes in the conference room and updates the smart TV?" asks Nianios. "No one's going to notice that for the next 20, 30 days until someone's going to go in there and figure out why it can't go to Netflix."

To properly secure smart devices, Stockinger says, it's not enough to isolate them from valuable company assets by putting them on separate network segments.

"You've got to do some network testing on those. You've got to do the wireless penetration testing," he explains. "You also need to look at your hardware and your firmware, and the protocols that those things are communicating on the IoT devices."

Pen testing and PCI DSS 4.0

PCI DSS requires that organizations in its Level 1 category — those that process more than six million Visa, MasterCard or Discover transactions per year, or smaller numbers of American Express or JCB transactions — undergo yearly pen tests along with annual audits carried out by certified assessors. Organizations that process fewer cards may also need to undergo audits and pen tests in the wake of a data breach or other major security incident.

In these cases, the scope of the pen test is an organization's cardholder data environment (CDE) — basically any digital system that touches payment-card data.

> ***"[PCI DSS 4.0 is] really taking a strong look at the segmentation controls around the CDE and ensuring that any pieces that are being handled by a third-party, such as the firewall or PIN pads, are operating as we would expect."***
>
> — Ty Coffee & Norman Comstock | *Principal & Managing Director, UHY Consulting*

The general methods and tools for pen-testing for PCI DSS 4.0 compliance are not fundamentally different from those used for earlier versions of PCI DSS. A standard external network penetration test as defined by any major methodology, as well as an OWASP-type web-application pen-test, remain the fundamentals. But the scope has widened to include some other areas.

"Scope is super important when you're assessing yourself for PCI," observes Stockinger, adding that "PCI 4 aligns a little bit better with the NIST Cyber Security Framework," which Stockinger says has "a new area for governance, which is basically risk assessment."

PCI DSS 4.0 adds a requirement (6.4.2) that mandates the use of an automated tool to detect and prevent web-based attacks on web applications. On March 31, 2025, this will replace an earlier requirement (6.4.1) that web apps merely get vulnerability scans.

A brand-new requirement (6.4.3) orders that all organizations that maintain online retail websites need to manage, verify and inventory all scripts running on payment pages appearing on an end user's browser, and to prevent unauthorized code or scripts from running on those pages.

A complementary new requirement (11.6.1) mandates the implementation of a "mechanism," either manual or automated, that checks payment-page content and HTTP headers at least weekly for evidence of tampering and unauthorized changes.

Organizations can substitute this mechanism with a customized approach that makes certain that malicious "skimming" code cannot be added to payment pages without an alert being generated.

Goodwin suggests that pen testers try to manipulate payment pages directly to ensure PCI DSS 4.0 compliance, such as by trying to inject malicious code or by finding and tweaking stored data.

Conclusion: Web apps and APIs

Web-app pen-testing, ideally using the OWASP framework, was already part of PCI DSS pen-testing. These new requirements add application-program interfaces, or APIs — the software structures that permit two or more different programs to work with each other — to the scope of PCI DSS testing.

"Before, APIs were kind of the secure thing that no one can compromise," says Nianios. "But now, APIs are within scope. You need to test the web-application API, and you need to test the web application, obviously, with the OWASP standard."

The new standard also stresses network segmentation as it relates to the cardholder data environment, so that aspect needs to be thoroughly tested as well.

"[PCI DSS 4.0 is] really taking a strong look at the segmentation controls around the CDE and ensuring that any pieces that are being handled by a third-party, such as the firewall or PIN pads, are operating as we would expect," say Coffee and Comstock of UHY Consulting.

Even though it would be outside the general scope of PCI DSS penetration tests, Goodwin suggests that a social-engineering test might be useful.

"While PCI DSS 4.0 does not explicitly require social engineering as a component of penetration tests, it is still one of the most common ways organizations are initially breached," he says. "From a purely risk-based perspective, it makes sense for any organization processing cardholder data to engage in periodic adversarial social-engineering exercises."

However, every information-security professional knows that no matter what the test or its purpose, no penetration test, audit or vulnerability scan is going to catch every potential exploitable flaw or weak point.

"You can pen-test everything that you think is in your environment, everything that you've scoped in," says Stockinger, "and you can still miss the thing that the bad guy is going to use to exploit you."

MASTHEAD

EDITORIAL

SVP OF AUDIENCE CONTENT STRATEGY

Bill Brenner | bill.brenner@cyberriskalliance.com

SALES

CHIEF REVENUE OFFICER

Dave Kaye | dave.kaye@cyberriskalliance.com

DIRECTOR, STRATEGIC ACCOUNTS

Michele Guido | michele.guido@cyberriskalliance.com

Don't sleep on PCI 4.0. Compliance

Take notice and get ahead with Clone Systems.

Are you ready for all of the changes looming right around the corner? PCI 4.0 is the latest version that introduces stricter requirements and advanced security measures.

We have successfully helped thousands and thousands of businesses world-wide achieve and maintain compliance, and we would welcome the opportunity to do the same for you.

Learn more now at **clone-systems.com**. It's fast and easy.

CLONE SYSTEMS®