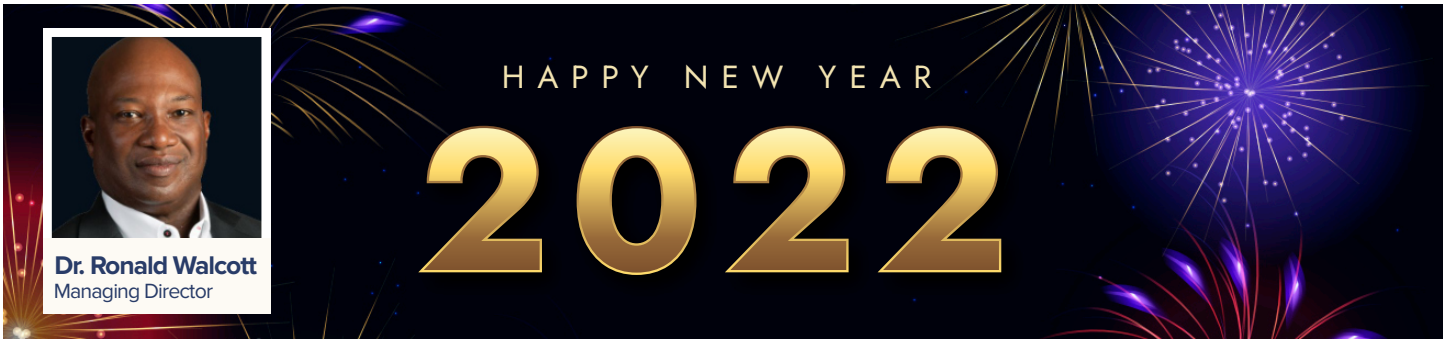
precision CYBERTECHNOLOGIES & DIGITAL SOLUTIONS

CYBER DIGITAL WORLD

NEWSLETTER

Volume 4: Issue No. 2 **December:** 2021



No company is free from risks and vulnerabilities. No matter how robust the digital infrastructure or how strict the cybersecurity measures are, there is always some level of risks.

This is why many businesses incorporate penetration testing (pen testing) in their risk assessment and security program.

In our previous issue, we looked at some measures that businesses can use to test the robustness of their networks. In this issue, we continue to discuss types of penetration testing.

Pen testing is intended to discover vulnerabilities. Trained security professionals perform approved pen tests, pretending to be hackers forcing their way past cyber defenses. This helps them to understand an organization's infrastructure and identify potential risks and vulnerabilities.

When the tests are completed, the organization can improve its security and prevent more malicious attackers from exploiting the same weaknesses.

of penetration testing that can be done to simulate exploits.

There are different types of pen tests.

Types of penetration testing

NETWORK INFRASTRUCTURE

Network Services

This is one of the most common types of pen tests. Its main objective is to evaluate vulnerabilities in the network infrastructure, including servers, firewalls, switches, routers, and printers. In addition, network penetration tests protect organizations from common network-based attacks (DNS level, proxy server, man in the middle, and others)

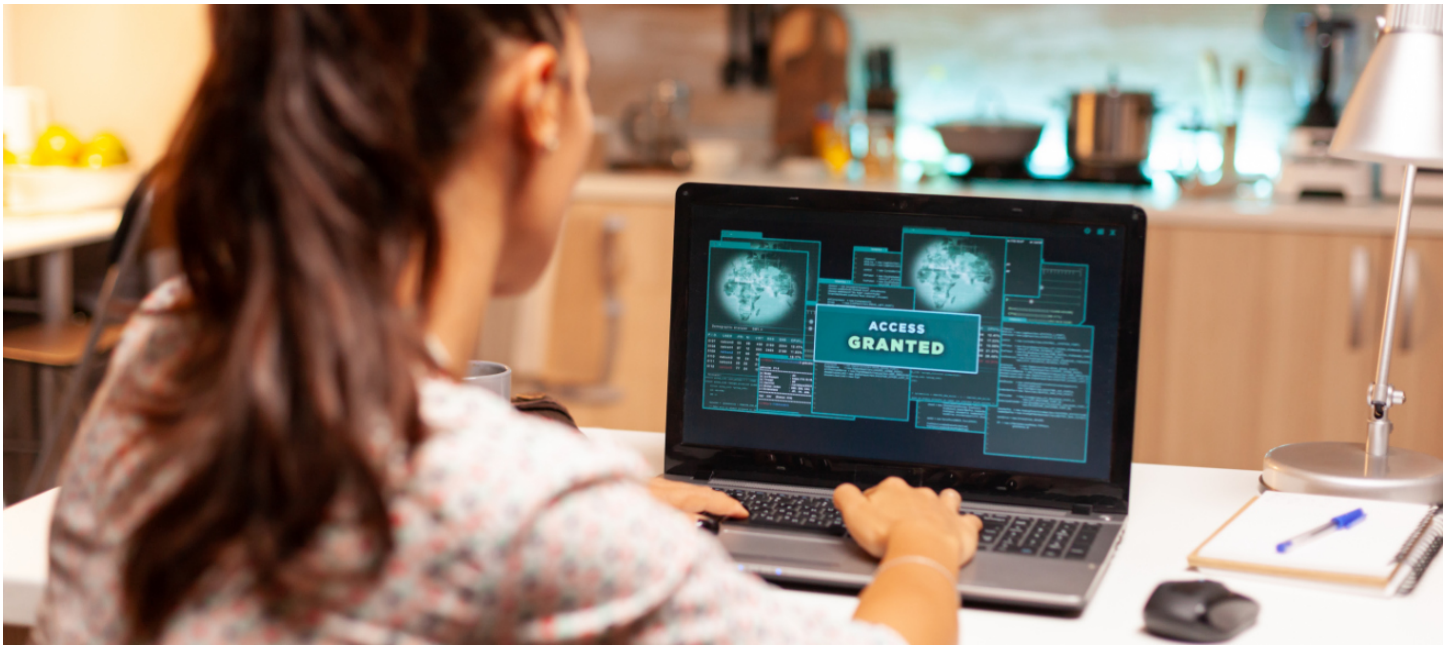
Network attacks may also include circumventing endpoint protection systems, intercepting network traffic, testing routers, stealing credentials, exploiting network services, discovering legacy devices and third-party appliances, and more.

WEB APPLICATION

True to its name, this test focuses on all web applications.

The tests focus on discovering security weaknesses of web apps or API's (application programing interfaces). Web applications tests are more specialized and complex, they require more time to evaluate and identify vulnerabilities. Web application issues may include SQL injec-

In this Issue:



tion, cross-site scripting, insecure authentication, and weak cryptography. These penetration techniques are constantly evolving and require periodic monitoring for new threats daily.

However, despite their cost and length, web application tests are crucial to a business.

WIRELESS

Wireless pen tests identify vulnerabilities related to the connections of various wireless devices to the wifi network. Wireless networks facilitate data exchange, but they are also a vulnerable entry point into an organization's (or its users') sensitive data, which is why they require a significant effort to strengthen their security provisions.

Additionally, businesses are using more mobile devices than ever before, but struggle to secure them. A wireless pen test will try to exploit corporate employees that use their devices on insecure, open guest networks.

SOCIAL ENGINEERING

Data from research suggests that more than 90 percent of all cyberattacks result from social engineering tactics. These attacks rely on poor judgment and human error rather than security gaps in software and operating systems. Social engineering pen tests are one of the most effective mitigation measures in cybersecurity, and several platforms provide a first approach to these kinds of tests.

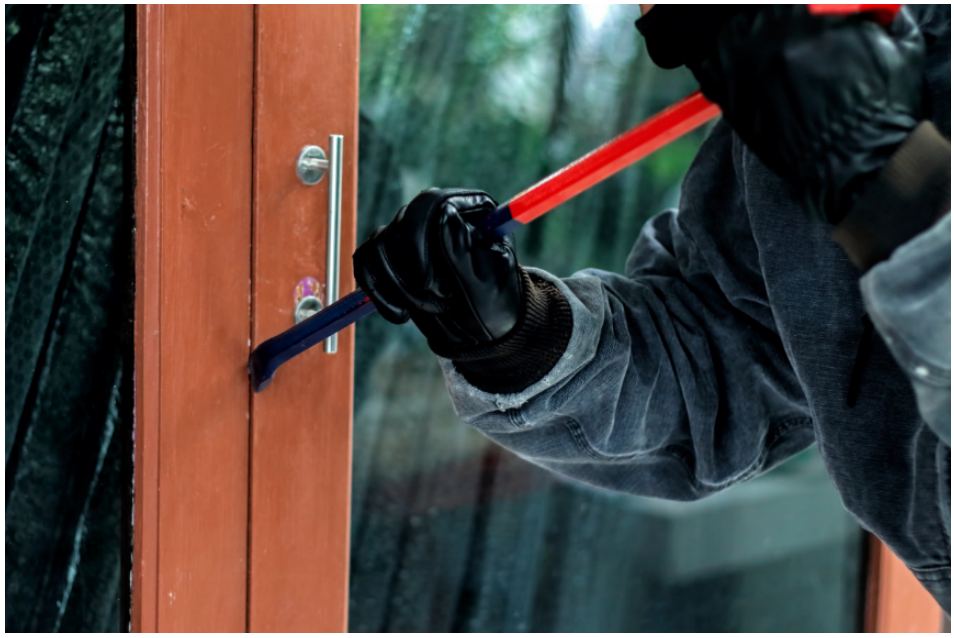
These tests can reveal how susceptible a business's employees are to these attacks. Small employee mistakes can grant adversaries their initial access to the business's internal network, at times with devastating results.

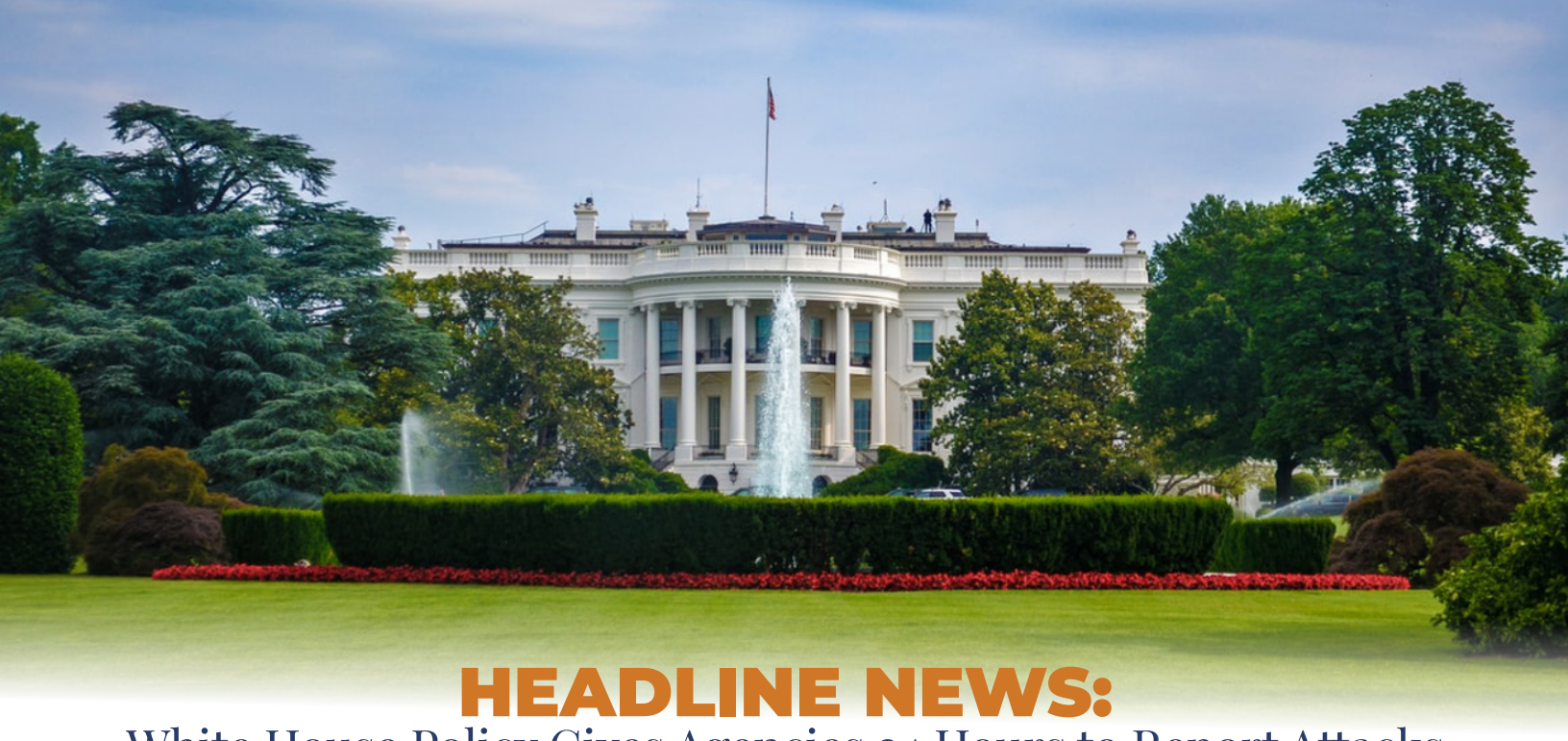
PHYSICAL

Finally, businesses can do a physical pen test which are designed to simulate threats to the organization's physical infrastructure: for example, someone getting unauthorized access to a restricted area. Through these analyses, it is possible to evaluate the weaknesses of a company's physical barriers and to strengthen the weakest ones.

Penetration testing is done to improve and mature your overall security.

So, what next? Find out in our next issue!





HEADLINE NEWS:

White House Policy Gives Agencies 24 Hours to Report Attacks

A new memo issued by the U.S. National Security Council within the Biden White House requires critical cybersecurity agencies to relay cyber incidents rising to national security threats to the council within 24 hours. The move is reportedly an effort to get cybersecurity advisers close to the president to assess incidents targeting critical infrastructure.

The NSC's policy, which will incorporate federal agencies such as the U.S. Cybersecurity and Infrastructure Security Agency, the FBI, and the Office of the Director of National Intelligence, tasks analysts with reporting incidents considered a major threat - including cyberespionage - within 24 hours, as first reported by CNN.

"The document ... is a process and a common methodology to help the U.S. government speak with one voice - nothing more and nothing less," a U.S. official tells ISMG. "It gives the NSC the framework to make an initial assessment of whether a cyber incident rises to the level of a national security concern. In many incidents, that assessment will change with time."

This comes on the heels of broader incident reporting considerations at the congressional level - including for critical infrastructure providers and some private sector organizations. Last week, Congress nixed an incident reporting mandate from its must-pass, annual defense spending bill, which passed the Senate on Wednesday.

A consensus version of the reporting mandate would have found critical infrastructure owners and operators reporting cyberattacks within 72 hours of detection, and payments to ransomware gangs would have been reported within 24 hours (see: Cyber Incident Reporting Mandate Excluded From Final NDAA).

MORE RESOURCES REQUIRED?

This new measure enacted by the NSC aims to determine whether additional resources may be needed to recover from a cyberattack, much like the May ransomware hit on Colonial Pipeline Co. In the wake of the attack, the company temporarily shut down its pipelines, spurring panic buying among consumers.

On the new policy, White House officials say findings relayed by the cyber agencies could prompt the creation of a working group within the NSC charged with remediating any economic fallout, according to CNN.

The NSC will reportedly adopt a color-coded system for reporting and incident severity, a system it first rolled out during the Obama administration.

Upcoming Events

HYBRID FINANCIAL SERVICES SUMMIT
January 25, 2022

VIRTUAL ANZ SUMMIT
February 16, 2022

868-610-7237
salesinfo@precision-cyber.com
www.precision-cyber.com
1st Floor, Brair Place, 10-12 Sweet Road
St. Clair, Port of Spain, Trinidad