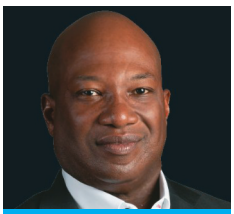
precision CYBERTECHNOLOGIES & DIGITAL SOLUTIONS

CYBER DIGITAL WORLD

NEWSLETTER

Volume 5: Issue No. 1 January 2022



Dr. Ronald Walcott
Managing Director

2022 is off to a great start, and the industry is buzzing with news about innovation and the latest trends. Desire for sustainable energy, the availability of wireless/broadband connectivity, and use of technology for medical procedures ranked as major drivers, while 3D printing, the use of robots for labour, and cloud computing were highly ranked as potential disruptors.

You can count on PCDS to keep you apprised of industry trends and the latest security and cyber technology developments.

In the last couple of issues we looked at types of penetration testing. But you may be wondering what happens when the pen test is completed?

Your Penetration Test Is Done, Now What?

After the pen test is completed a detailed report is generated. The report will be laid out in several sections including: an executive summary, a breakdown outlining what took place and recommendations on how further risks can be managed.

THE SUMMARY:

Penetration test reports generally begin with a summary of the findings. The intention is to provide a clear picture of the results for company executives, who can consider actionable takeaways without needing to process the entire report. The summary would reveal where the pen testers bypassed security controls and what they were able to uncover within the system. This breakdown is usually explained in a non-technical way to ensure that any reader can understand. It will also outline recommendations for security improvements, including what was first advised, as well as the short-, medium- and long-term goal for enhancing security measures.

Breakdown of the attack and what took place:

This section of the report provides in-depth particulars of the pen testers engagement. It clearly describes each phase of the attack process and what was done to compromise the system.

For example, if the pen tester used social engineering tactics, the report would show where they got the information that was used to trick your employees.

Pen testers also share exactly how infiltrated your system (for e.g. , through a series of phishing emails to build rapport and trust before sending a malicious link).

All the information will be detailed in the report, to enable you to understand the context of how the attack was executed and the resulting gaps in your security.

In this Issue:

YOUR PENETRATION TEST IS DONE, NOW WHAT?

HEADLINE NEWS: MICROSOFT EXCHANGE FIXES DISRUPTIVE 'Y2K22' BUG

UPCOMING EVENTS

The breakdown of your report will also explain the full scope of the outcome. This may show, , that the pen tester was able to place simulated malware onto your employee's computer packaged in a seemingly-normal software update installation. From there, the pen tester will indicate the path they took to acquire login credentials, access data, and whatever other information or systems they obtained after infiltrating your infrastructure.

RECOMMENDATIONS

Once the company has insight into the results of the pen test they can then look at the recommendations for mitigating the risks.

Every risk will be ranked in order of priority as critical, high, medium or low. The level of impact would also be considered and the risk threshold.

Recommendations will vary and should be customized based on the findings of the test.

For example, in the short term, critical technical changes to solve glaring issues may be needed and in the medium term, increasing security awareness training may be a high impact option to safeguard against further exposure and risks.

Upcoming Events

HYBRID FINANCIAL SERVICES SUMMIT
January 25, 2022

VIRTUAL ANZ SUMMIT
February 16, 2022

VIRTUAL ZERO TRUST SUMMIT
February 22, 2022

HEADLINE NEWS:

Microsoft Exchange Fixes Disruptive 'Y2K22' Bug

Remember Y2K? When widespread disruption was feared since systems that rendered dates as two digits needed to be updated to work with four digits?

Well, Microsoft Exchange recently issued a workaround to fix a fatal error that disrupted email delivery due to a date check failure with the change of the New Year.

In a statement, the company indicated: "We have addressed the issue causing messages to be stuck in transport queues of on-premises Exchange Server 2016 and Exchange Server 2019. The problem relates to a date check failure with the change of the new year and it is not a failure of the AV engine itself,"

WHAT IS THE ISSUE?

"The version checking performed against the signature file is causing the malware engine to crash, resulting in messages being stuck in transport queues," Microsoft stated.

Microsoft advised that it created a solution to address the problem of messages stuck in transport queues on Exchange Server 2016 and Exchange Server 2019, because of a latent date issue in a signature file used by the malware scanning engine within Exchange Server. However, it specified that, "Customer action is required to implement this solution."

"E-mail is a critical communication tool for every organization, and we expect it to work like we expect the lights to turn on when we flip the switch," stated John Bambenek, principal threat hunter at digital IT and security operations company Netenrich.

Mr. Bambenck continued: "This bug highlights the difficulty of robust coding where straight-forward functions, like date-checks, may look good to code scanners or in code review, but still cause critical failures."

SOLUTIONS OFFERED

Microsoft recommends an automated solution to fix the issue. Users are advised to download a script from here and before running it users should change the execution policy for PowerShell scripts by running 'Set-ExecutionPolicy-Execution Policy RemoteSigned'.

"Run the script on each Exchange mailbox server that downloads antimalware updates in your organization (use elevated Exchange Management Shell). Edge Transport servers are unaffected by this issue. You can run this script on multiple servers in parallel," Microsoft says.

Frequently Asked Questions:

WHAT IS THE DIFFERENCE BETWEEN A PENTEST AND A VULNERABILITY SCAN?

Vulnerability assessments and penetration tests are the most common techniques to uncover and fix cybersecurity flaws within your technologies. While some similarities exist between the two, they are often misinterpreted as the same thing although they yield very different degrees of analysis.

Vulnerability scanners are generally used by IT staff in order to check network infrastructures for known vulnerabilities that may have been introduced during their implementation. Penetration tests, by contrast, identifies both well-documented vulnerabilities, as well as those that have never been seen before, while providing evidence of their potential impact on your company.

CAN YOUR PENETRATION TESTS IMPACT MY BUSINESS OPERATIONS?

Various steps are taken over the course of the project to prevent the potential impact of our tests on the stability of your technological environment and the continuity of your business operations.

For this reason, a communication plan will be put in place at the beginning of the project to prevent and mitigate any potential impact. A representative of your organization will be identified to act as the main point of contact to ensure rapid communication in the event of a situation directly impacting the conduct of your daily operations, or if any critical vulnerabilities are identified, for which corrective measures need to be implemented quickly.

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