red alert IT

Frequently Asked Questions

How long does it take for an assessment to run?

- It typically depends on the number of systems that are being targeted, along with the number of opened ports and services running on those systems. It's safe to estimate approximately 45 seconds to 3-4 minutes per IP address depending on the number of services running.

What is considered an IP address when creating a scheduled assessment?

- Anything that has an IP address on the network. This includes phones, network devices, printers, IP cameras, etc. While many individuals may believe that excluding devices such as printers may be necessary to preserve IP addresses, it should be noted that any device on a network could present a risk to the environment.

Do you recommend excluding certain devices?

- **No**. Every device that has an IP address could potentially present a risk to the environment at some point in time, depending on their functionality. Even some of the devices that appear to pose the smallest risk to the environment could potentially be used by an attacker.

If I scan an entire subnet range, will the whole range count against my IP address limit?

- **No**. If you provide a /24, for example, and there are only 5 live systems within that network, then your IP address count will only be reduced by 5. vPenTest does not consider the range, or location(s) included in the assessment when it comes to the IP address count. The only thing that matters is the number of systems that are actually active within the environment.

Is vPenTest geared more towards web app pen tests or network system pentest?

- vPenTest is focused strictly on network security pentests, including the following activities: 05. Is vPenTest geared more towards web app pen tests or network system pentest?
    - Host Discovery/Info Gathering
    - Authentication-based attacks
    - Man-in-the-middle attacks
    - Exploitation & Post Exploitation

How does vPenTest differ from a vulnerability assessment?

- A vulnerability assessment simply informs an organization about the vulnerabilities that are present within their environment. However, a vulnerability assessment does not attempt to exploit those vulnerabilities to determine the potential impact of successfully exploiting those vulnerabilities. This is not a flaw with vulnerability scanners; they just simply aren't designed to do this. vPenTest differs in that it is able to perform exploitation and post-exploitation techniques to demonstrate to customers how successfully exploiting a vulnerability could potentially lead to further access to systems and/or confidential data within their environment.

What is the biggest difference with vPenTest compared to a traditional penetration test?

- Traditional penetration tests are extremely time consuming, whereas vPenTest can run numerous tools simultaneously, wait for them to complete, automatically analyze the results, and determine its next move. This saves a significant amount of time from simply running one command at a time. Furthermore, vPenTest reduces the time spent reporting from 6 hours (average between reporting, QA, etc.) to less than a minute. That's a 29,900% speed increase per assessment that it saves. See the below Infographic for additional benefits provided by vPenTest compared to traditional penetration testing