VIAVI Solutions

Frequently Asked Questions (FAQs)

TeraVM
Cybersecurity Threat Database

Is there a difference between vulnerabilities and an exploit?

Yes, vulnerabilities do not necessarily represent EXPLOITS, for example:

- A vulnerability does not mean it can be attacked.
- Many vulnerabilities require pre-existing conditions, like Java installed.
- Many vulnerabilities require an attacker to be logged on, inside the system. In most cases the logon is required as a genuine user. The vulnerability is within the system or software that the user is logged into.
- A few Vulnerabilities are within network devices, like routers, switches, NAS devices. In a fair portion of sthese we just do not have the hardware to build and test the attack.

Do you just use CVE linked threats?

No, the CVE database is mainly a list of reported VULNERABILITIES, to validate security with those alone is akin to validating security for the lowest risk. We enable user add mixed traffic flows.

How many CVEs actually have exploits?

The number of published CVE's that have an exploit are minimal. It has been shown that in

2015 Jan to March:

- Published CVE's 1,611
- With exploits 109

2015 April to June:

- Published CVE's 1,440
- With exploits 5

Why is the TeraVM™ approach to security assessment different?

TeraVM's per flow architecture enables realism, with repeatability i.e. all TCP sessions are fully stateful. In addition, our per flow architecture enables you mix the Good, Bad and your own traffic signatures enabling you with the widest assessment capability.

In addition, TeraVM includes known exploits (verified, tried and tested) where our competitors use a set of pcaps which include suggested potential vulnerabilities.

Why is per flow so important?

Per flow is important as it provides the accuracy necessary to pin-point of the potential 10s of gigabits of traffic each threat signature getting through your security appliance.

Can I share the threat database among users?

Yes, the threat database is a licensed entity enabling you share among your users.

What reports do you produce?

TeraVM provides users with a number of reports which include key information such as CVE numbers, reports formats include CSV, pdf and html.

Can I add my own traffic signatures?

Yes, a user can add their own traffic signatures to a test use case, enabling you test with Good, Bad and your OWN, The traffic signatures can be saved and stored in a dedicated repository, which supports up a Terabyte of data.

What types of threats do you cover?

We focus on 3 key areas, giving the maximum coverage:

1. Network

   a. A vulnerability exploitable with network access means the Exploitable Scope is bound to the network stack and the attacker's path to the vulnerable system is at the network layer.

2. Adjacent Network

   a. A vulnerability exploitable with network access means the Exploitable Scope is bound to the network stack and the attacker's path to the vulnerable system is at the network layer.

   b. For instance, a vulnerability in this category would be a bug in application software that processes Ethernet frames.

3. Local

   a. A vulnerability exploitable with local access means the Exploitable Scope is not bound to the network stack and the attacker's path to the Exploitable Scope is via read / write / execute capabilities.

   b. If the attacker has the necessary Privileges Required to interact with the Exploitable Scope, they may be logged in locally; otherwise, they may deliver an exploit to a user and rely on User Interaction.

   c. An example of a locally exploitable vulnerability is a flaw in a word processing application when processing a malformed document.

Why is repeatability important?

Accuracy is key in security assessment and after each upgrade/update of the security appliance it's necessary to show no exposure has been opened. We can prove the reliability by running the same test cases over and over in a back-to-back mode, showing consistent results.

Can I easily scale my threat assessment to meet new bandwidth demands?

Yes, using the TeraVM virtual solution enables a highly scalable or an elastic test bed, enabling you to scale as you grow.

Can I run threat assessments from cloud managed platforms?

Yes, TeraVM is a virtual solution allowing you to turn it up on a number of cloud platforms including OpenStack.

How do you keep up with/track all new potential exploits?

We partner with a company specialized in this area, Idappcom, who has spent over a decade and more following the security industry, producing a number of security products, including the extensive threat database, which is part of TeraVM.

Who is Idappcom?

Idappcom was founded in 2004 to develop services focusing on application and user security, plus license management on PC's thru to mainframes. In 2009, through acquisition, Idappcom expanded its expertise in the specialized area of network security management and penetration testing.

Their objective is to create as many test traffic signatures as they can for the majority of the exploitable systems, for which a working exploit actually exists in the wild. Idappcom provide test cases for the majority of potential targets, which are vulnerable, by using exploits that are used by the majority of the attackers. So from a risk management view, they are protecting the most from attack, with the most.

How does Idappcom find and select Threat/Malware?

Idappcom produces both pcaps and security rules. Idappcom selection process is therefore based on 3 principles:

1. The rule published has to have been developed from a proven exploit in our pcap library

2. The pcap produced has to be based on an actual exploit that exists

3. Idappcom do not produce and publish any pcap for a vulnerability that does not have an exploit

The selection process gives clients the choice of a complete solution with TeraVM traffic emulation through to rules management or a supply of rules that have been developed from known exploits whilst not creating a new supply of exploits for known vulnerabilities.

How does Idappcom get these PCAP files?

Idappcom has a team of security specialists who are tasked with sourcing genuine attacks / threats. Once they have identified a threat and verified that is it a genuine one which will harm a system, if it penetrates it, they create a pcap of the traffic.

Idappcom conducts a lot of research of trusted threat monitoring sites such as Mitre CVE, Bugtraq, Security Focus, Vupen, Security Tracker, IBM/ISS, Secunia, OSVDB etc.

The process also involves monitoring "black hat" website and forums. From these sources their researchers gather metadata, the vulnerability detail and the exploit detail. They then correct any deliberate or accidental errors in the data before building the vulnerable instance and to ensure the exploit actually works before capturing the exploit traffic.

When will Idappcom be able to release PCAPs?

Idappcom issues an updated library of pcaps and security rules each calendar month. There is not a formalized time period for the release of new threat traffic as the vulnerabilities are announced / found by other organizations/ individuals.

Idappcom only investigates a vulnerability when it has been verified by the security community as being genuine and someone has declared that an exploit exists for it. Many vulnerabilities are announced long before anyone has managed to exploit them and create a real attack.

If an exploit has been proven to exist then Idappcom will always make an attempt to create a pcap for it, assuming that sufficient knowledge of the exploit exists in the security community.

How many PCAPs does Idappcom provide per/every month (average)?

Idappcom release between 100 and 150 new traffic files each month. On occasion this has been exceeded and up to 200 have been released. The requirements for IPS vendors is one of efficiency. They require the minimum number to provide enough variances to prove a rule works.

What are the advantages to using TeraVM with Idappcom?

TeraVM provides the ability of load generation with real flows and Idappcom are specialists in threat creation and mitigation. This contrasts with other market tools, as their focus is clearly on load generation, with threat mitigation as secondary thought.

The primary purpose of TeraVM with Idappcom is to provide our users with a method to test their network defenses using real world attacks in a safe and controlled manner and to correct any breaches through patching of security rules.

VIAVI Solutions

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

tvm-cybersecurity-faq-wir-nse-ae
30187433 900 0818