VIAVI

VIAVI Solutions

Application Note

Next Generation Firewall Validation

Security Hardening for Next Generation Firewalls

The new security threat agenda

As networks and functionality evolve, so too does the cyber threat landscape. Today, networking is undergoing a massive transformation, with many network functions now being offered as a virtualized appliance. The key question for many now - is how robust and reliable are the next generation of firewalls.

The goal of this application note, is to deliver a simple validation methodology which will be understood by all, ensuring that the applied security provides protection for the latest emerging threats. Threats and malware now manifest themselves in many unique forms and do not discriminate between applications of network functions.

Attack variance and ferocity can take many forms e.g. Cross-site Scripting, Data Manipulation, Denial Of Service, etc and are delivered using a range of network protocols:

- UDP: (using a variety of ports)
- TCP: (using a variety of ports)
- SSH
- SSL
- SIP/SDP
- RTSP
- POP/SMTP
- ICMP
- IGMP
- HTTP
- FTP
- DNS
- DHCP

Source: TeraVM Cybersecurity Database

Cybercriminals looking to gain access will adopt a range of attack strategies, looking to pinpoint weaknesses in order to breach the security perimeter. A fundamental defense methodology will begin by ensuring the basic security practices have been adopted i.e. the next generation firewall has been patched for latest threats.

Understanding the attack target

Understanding the level of security vulnerability that is potentially at play, is to understand who the likely threat target is and the applications in use. As everyday users of common software packages, it's fair to say that all of us are exposed and are potential targets, it's clear from the list highlighted below that attackers are looking to use widely used applications in their relentless pursuit of exposing security vulnerabilities:

• Browsers: Chrome, Firefox, Internet Explorer, Opera, Safari

• Email: Outlook, Thunderbird

• Photographs: StudioLine, Adobe Photoshop

• Word Processing: OpenOffice, Microsoft Word

• Data Processing: Microsoft Excel

However, exploit strategies are not isolated to just consumer like applications, network or server side applications are now also a target. For example take a web hosting service - offering end users simple web sites for business (or indeed personal use), as part of the hosting service package there are common administration tools and services, which are also being targeted e.g.

• Operating System Choices: Linux, Windows Server

• Server side language tools: PHP, JS

• Content management systems: Joomla, PHP-Fusion, Wordpress

Indeed anything that is connected to an IP network becomes a target and this includes network appliances:

• Dell SonicWall

• Cisco ASA

• Juniper Junos

Clearly from the samples above, there is a huge diversity of attack types and potential exploits. Hence to assure security hardening the best approach is to cover as many scenarios as possible.

Introducing TeraVM

TeraVM is an application emulation and security performance solution, delivering comprehensive test coverage for application services, wired and wireless networks. TeraVM is offered as a virtualized solution enabling the flexibility to run anywhere - lab, datacenter and the cloud, with consistent performance coverage, ensuring that highly optimized networks and services can be delivered with minimal risk.

TeraVM offers a wide range of application emulation and performance validation for system under test (SUT) ideal for VNFs, physical appliances and/or hybrid deployments which may use cloud bursting techniques.

TeraVM Cybersecurity Database

TeraVM delivers a comprehensive cybersecurity database of up to 12 thousand unique threats. Each and every one of these unique threats has violated an application or service and are independently researched, verified and packaged to provide the most comprehensive coverage of real world exposure of vulnerability, in a safe and controlled environment.

A significant portion of the TeraVM threats have a common vulnerabilities and exposures (CVE) number. However, many of the newly researched threats have yet to be CVE classified. This unique foresight enables users of TeraVM the opportunity to validate security with the latest threat activity.

Over half of the total threats in the TeraVM Cybersecurity Database have a Common Vulnerability Scoring System (CVSS) in excess of 7 (with 10 being the most severe). CVSS is an open industry standard which approximates the ease of exploit and the impact of exploit. Industry reports show once vulnerabilities are published, they are most likely to be recorded as a security breach.

99.9% of the exploited vulnerabilities were compromised more than a year after the CVE was published.

Source: Verizon Data Brach Investigation Report

Validation challenges for Next Generation Firewalls

The Challenge - validate what?

For many the challenge is to define a robust methodology to validate security performance. This can be a daunting task, with uncertainty of what/how the security perimeter should be validated. On top of this, the challenge is further complicated by the need to maintain the relevance of the test methodology, as the cyber threat-scape continually adopts.

Work Smarter not harder!

Cobham Wireless addresses these unique challenges through TeraVM. TeraVM enables users with a comprehensive cybersecurity database (CSDB) with thousands of unique threats. Each of the unique threats has been researched and validated by a third party (Idappcom) in which each of the threats have been shown to cause security breaches.
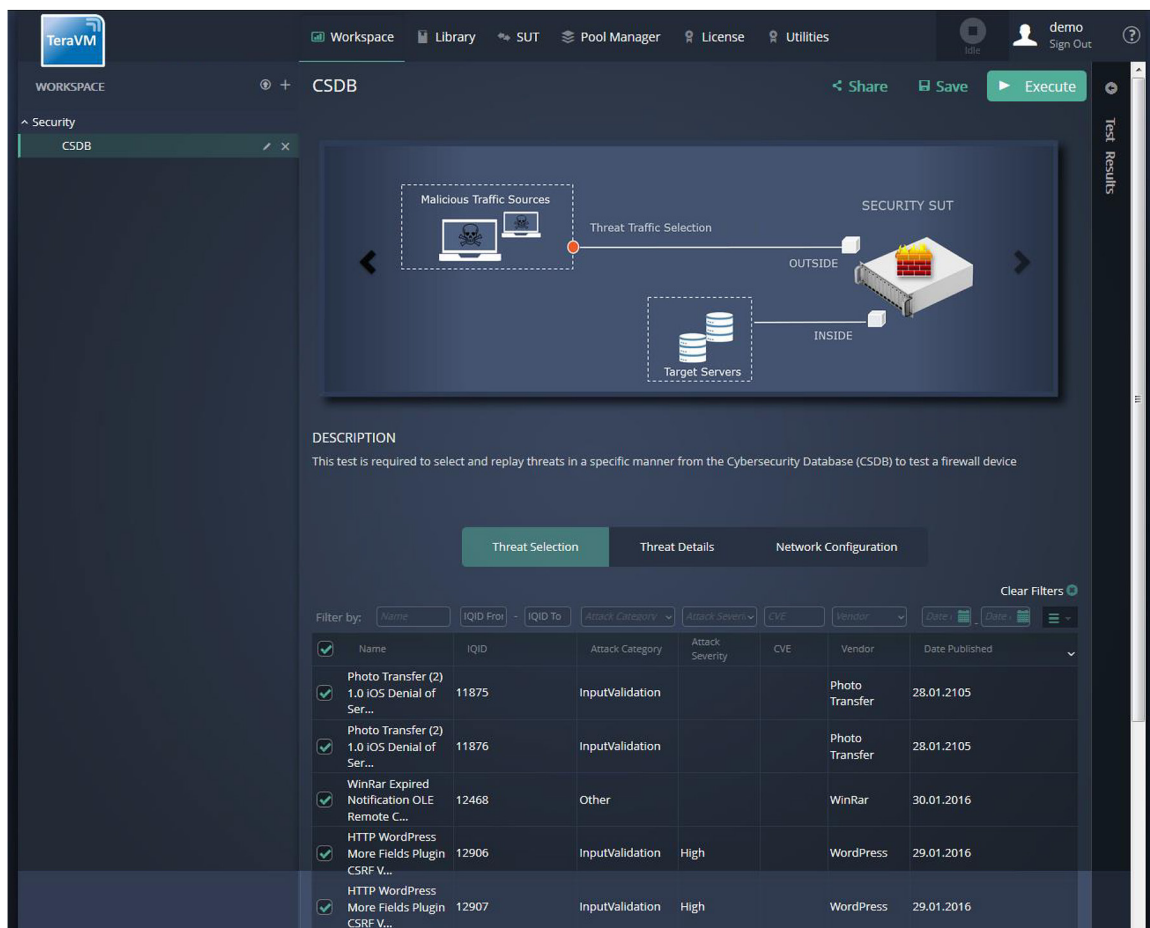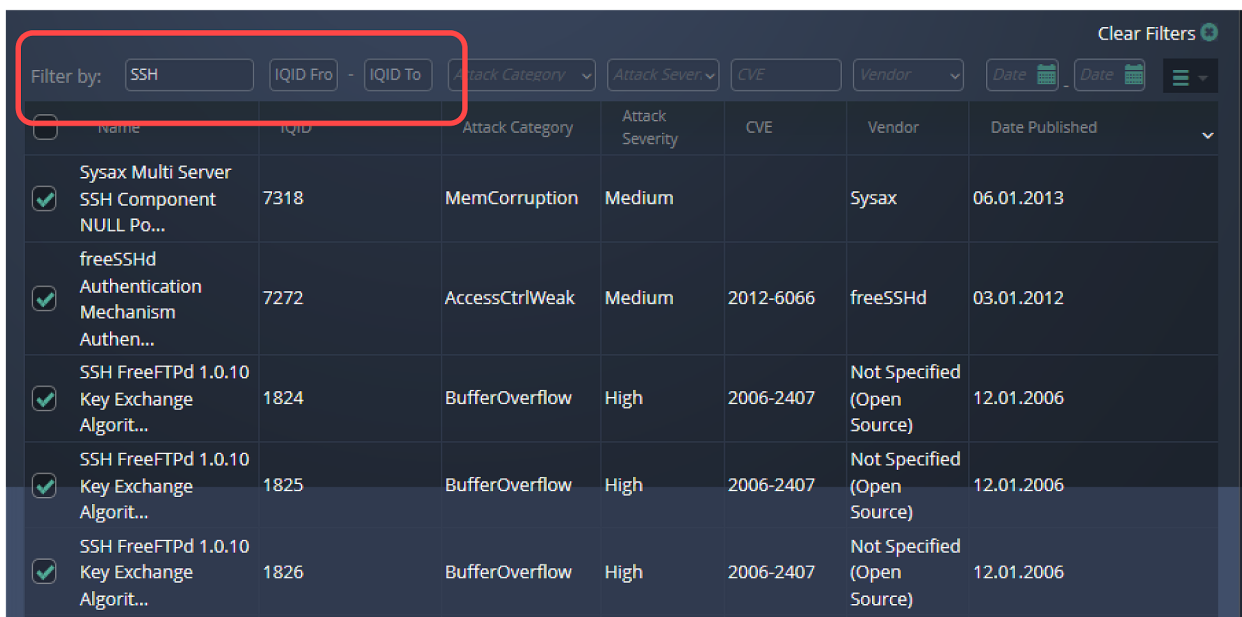

Figure 1 TeraVM Cybersecurity Database user interface

The TeraVM CSDB is delivered as an easy to use HTML5 web based interface enabling ease of selection of threats, resolving the "how to" challenge. The intuitive filtering solves the user problems of understanding as to what to validate with. Users simply select from any one of the many filters, the threats they wish to use in the validation run.

The most effective test is to validate the security appliance or system under test (SUT) by running all the threats, looking to see the level of exposure on the current patching/version of the security system.

However, a more efficient way is to know the potential target and applications running behind the security perimeter. By selecting the right TeraVM CSDB filters, users can quickly assess for potential exposures at a number of levels from protocol layers to application types.

Figure 2 Example TeraVM CSDB filter in action - selection example is for SSH based threats

NOTE: The TeraVM CSDB is updated regularly with the latest threats; sourced from industry expert groups e.g. CVE, Bugtraq, ISS and Idappcom. These independently verified threats are packaged into TeraVM ensuring no malice to the user's environment.

Security hardening validation methodology

So far the application paper notes the challenges associated with enabling performance validation for the security perimeter and presents a solution, in this section a simple methodology is presented.

A suggested goal of the methodology is to efficiently use the security professional's time so as to maximize the time spent patching all discovered vulnerabilities.
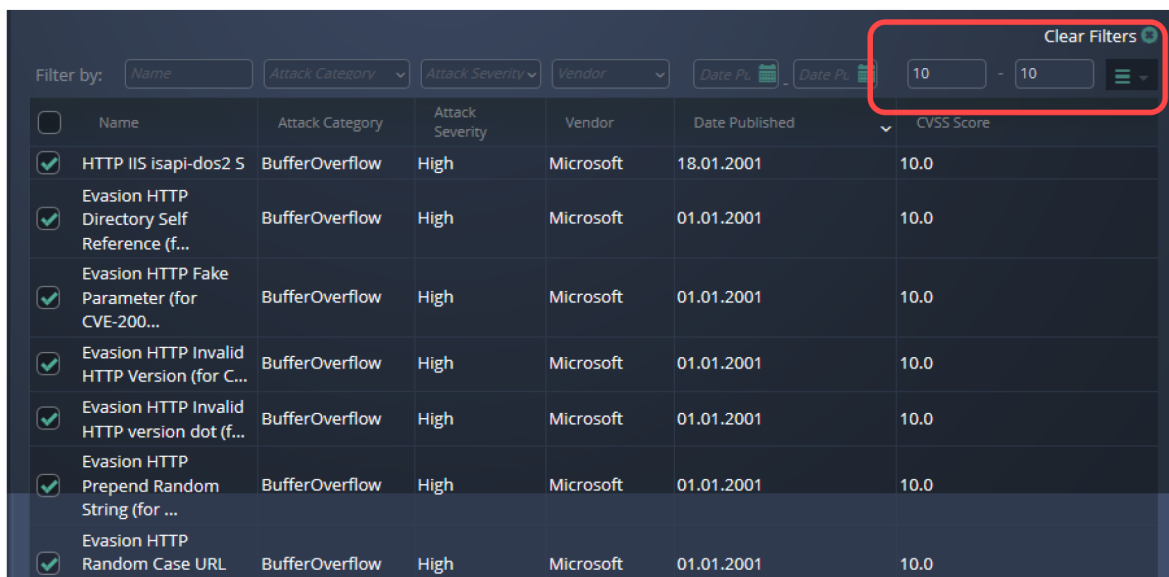
The counter attack plan is simple – patch, patch and patch:

1. Uncover exposures with maximum probability of a breach i.e. CVSS = 10

2. Patch

3. Repeat step 1 for CVSS = 9 to 7

4. Patch

5. Repeat for medium probability exposures i.e. CVSS = 6 to 4

6. Patch

7. Evaluate security effectiveness to stop malware (port scan and blacklist rules)

8. Patch

Our counter attack plan is as such that the security professional spends 90% of their time hardening the security perimeter.

Uncovering weakness with high probability of breach exposure

Using TeraVM's CSDB simply select the CVSS filter and enter a value of 10, execute the test run. It really is that simple with TeraVM!

Figure 3 TeraVM CSDB CVSS filters set to 10

When and where to patch the security appliance?

Once the test commences, the test will cycle through each of the individual threats. A key time saver with TeraVM (which enables a user to patch on the fly) is that it provides visibility in real time of the state of each of the threats i.e. blocked or not. A fail in the TeraVM UI suggests that the security perimeter is vulnerable as the threat was not blocked.
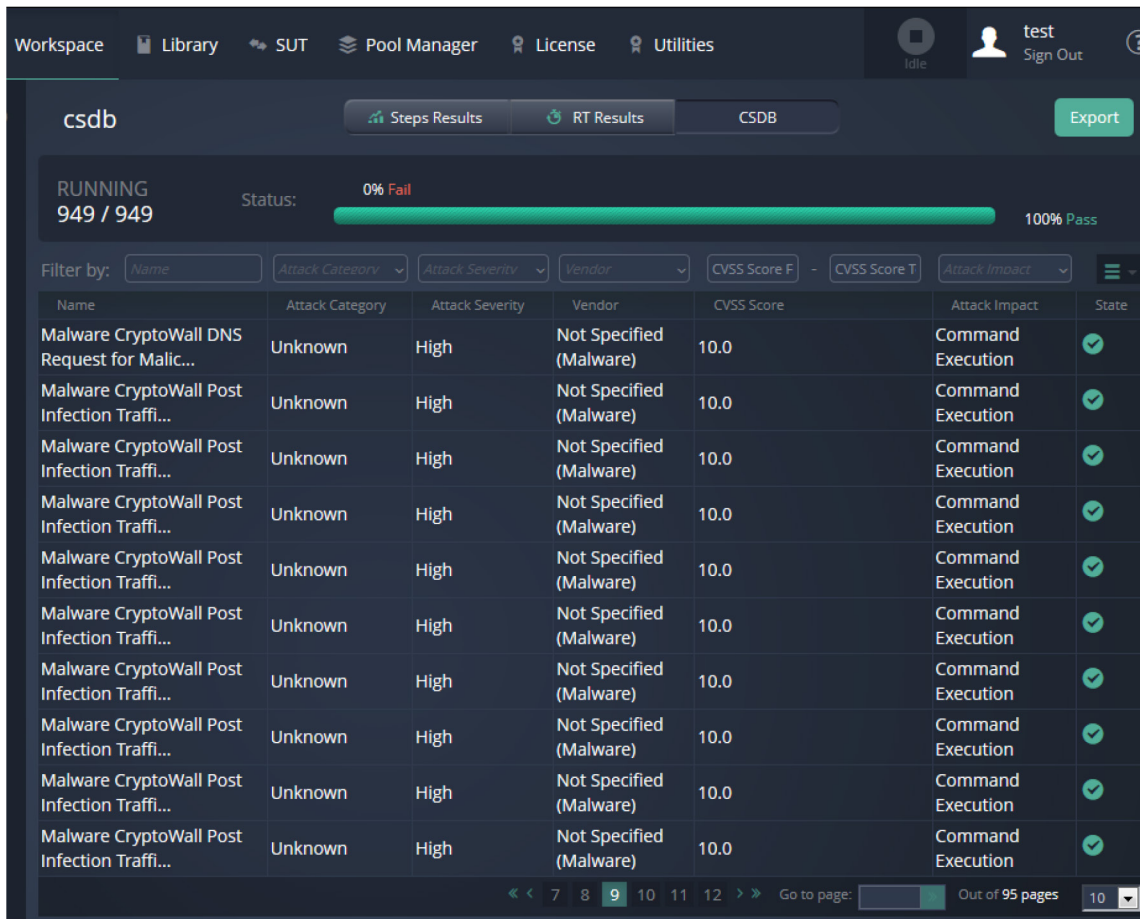

Figure 4 TeraVM CSDB presents live Pass/Fail criteria during the test execution

With the initial first steps completed in the methodology approach, the security professional can be confident that they have blocked the most severe of threats. The next 4 steps of the methodology is essentially repeating the process above and by the end the security professional has a very robust security

Shoring up defenses to block malware

The final piece of the security hardening exercise (step 7) is to ensure that no unnecessary ports are open, by running a simple port scan for the listening ports. By locking down the port range, this helps to ensure that any malware that may have been delivered through a benign source such as a document file format does not have the ease to connect to a command and control server.

Clearly a number of legitimate ports must remain open, at this point the aim is to ensure that the security perimeter can block traffic trying to connect out to the command and control server. An effective validation approach is take public and/or commercially available URL blacklists and attempt to connect to them again from the safety of the TeraVM.

Blacklist blocking validation

Connecting to TeraVM's central test library, users can download both a domain name service (port 53: DNS lookup) use case and/or web service (port 80/443: HTTP) use case. Both these simple test cases provide the user of TeraVM with an easy way to assess that the hundreds of thousands of blacklisted urls are being blocked. User's simply upload the url list into TeraVM, executes the test and sees the effectiveness of the security perimeter to block the bad, all within a few minutes!
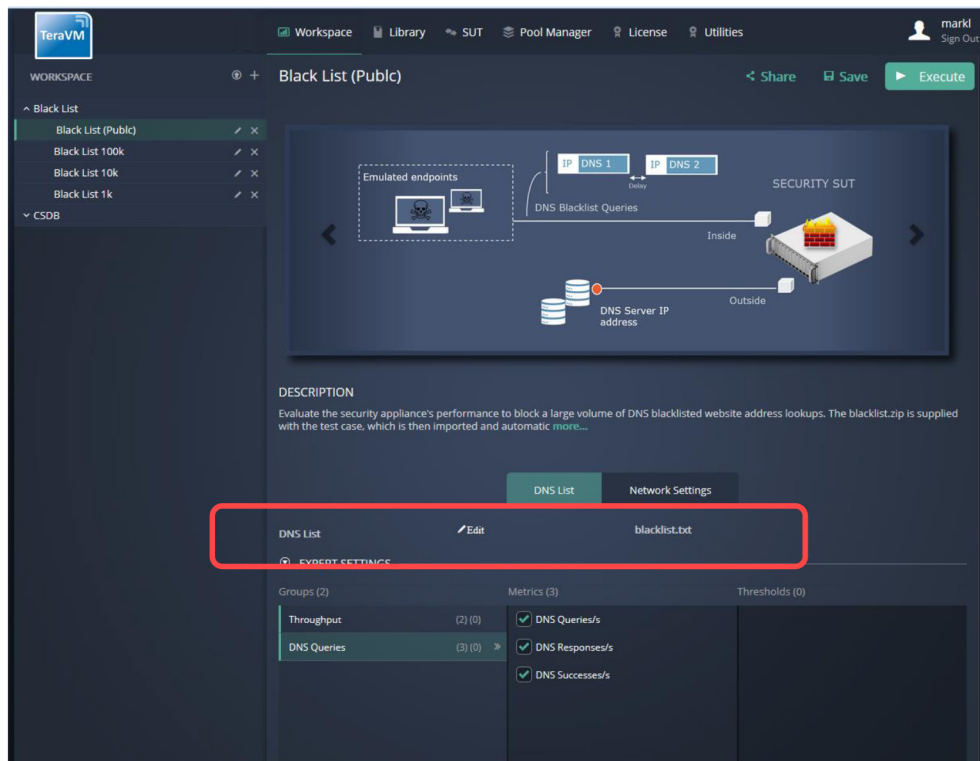

Figure 5 Import and validate the ability to block hundreds of thousands of blacklisted urls

Conclusion

The application note provides for an efficient and effective methodology to help assess and harden security. The application note highlights the challenges we all face when it comes to implementing good security; that is of understanding the threat-scape and the time to implement good security policies to cover all eventualities.

Understanding what is being protected is essential to help to define the possible threat-scape. It enables the security professional to quickly define an efficient validation methodology to assess the security perimeter.

Efficiencies are further gained by selecting the right tool such as TeraVM. TeraVM provides for a simple and easy to use interface which reports live all the possible vulnerabilities that the current policies/patch version that are running on the security appliance may have. The TeraVM cybersecurity database offers thousands of unique and industry proven threats, which have known and documented exploits.

The live threat reporting, which is only available in TeraVM, means the security professional can spend more time working on the key job of security hardening (rule creation and/or patching). Furthermore, TeraVM provides for an effective means to assess the security perimeter's ability to block potential malware exploits through validation with hundreds of thousands of the latest blacklisted URLs. This helps to ensure that the attacker's command and control servers don't get easy access to the inside of the security perimeter.

A further security challenge and headache is to stay ahead of the game. Security best practices highlight the need to stay up to date with regular patching. TeraVM as the prime security validation solution provides for regular updates through the TeraVM strike center. With the added advantage, that the already existing test cases become even more robust, as the latest threats are added to the cybersecurity database. All of which helps to ensure maximum protection for the future.

By selecting the right validation partner today, helps to maximize the overall return on investment for security hardening and validation, for many years to come!