tenable network security

Nessus Exploit Integration

v2

Tenable Network Security has committed to providing context around vulnerabilities, and correlating them to other sources, such as available exploits. We currently pull information from the most widely used exploit frameworks, including Core IMPACT, Immunity CANVAS, Metasploit, and the newly added Exploit Hub. Below are ways in which Tenable's products help you integrate this information into your vulnerability remediation strategy, including:

1. Nessus and PVS associated vulnerabilities with known exploits
2. Targeted vulnerability information for improving incident response
3. Alerting on new exploits on a continuous basis
4. Saving time on penetration tests by integrating vulnerability data

Exploitation Challenges

Traditional exploits required a skilled attacker to discover a flaw in a software package, and then write code, such as a buffer overflow, to exploit the vulnerability and gain the ability to take over the target. Recent advances in software protection have made this process much more difficult. Memory protection, such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR), has increased the time it takes to write a reliable exploit. Thus, the exploit contained in your favorite penetration testing framework may work on some systems once, then fail on that very same system on future attempts. The exploit may not work at all on other systems of different patch levels, processor architectures (32-bit vs. 64-bit), or service packs.

Attackers today have turned much of their focus to attacking web applications and client-side software. Web applications can be easily fuzzed to find vulnerabilities. That is, in order to find a software flaw the attacker must try different types of exploits against the parameters in a web application. This process can be largely automated and used to find common web application vulnerabilities such as Cross-site scripting (XSS), SQL injection, and command injection.

Client-side attacks present several different challenges for attackers. From an attacker's perspective, it can be difficult to discover which software, and which version is running on the clients' desktops in order to launch the appropriate exploit. Additionally, because the attacks are typically sent to a user via email the attack could end up compromising a home PC or public kiosk.

Four Ways Tenable Products Can Help

1. Exploitability Index

Nessus, the Passive Vulnerability Scanner (PVS), and SecurityCenter help you eliminate vulnerabilities that new kinds of exploits target by implementing an exploitability index. Each vulnerability identified by Nessus or PVS is cross-checked against publicly available exploits. If an exploit exists for a given vulnerability, the "Exploit Exists" flag is set to true within the results. Nessus and PVS have the most comprehensive coverage of exploits in the market today, identifying exploits from the following sources:

- Core IMPACT
- Immunity CANVAS (in addition to the D2 exploit packs)
- Metasploit
- Exploit Hub

There is no single framework or source of exploits that provides you with 100% coverage. By correlating exploits and vulnerabilities from multiple sources you get the benefit of expanded coverage.

Plugin ID: 45378 **Port / Service:** cifs (445/tcp) **Severity:** High

Plugin Name: MS10-018: Cumulative Security Update for Internet Explorer (980182)

http://www.microsoft.com/technet/security/bulletin/ms10-018.mspx

Risk Factor: High

CVSS Base Score
9.3 (CVSS2#AV:N/AC:M/Au:N/C:C/I:C/A:C)

CVSS Temporal Score
7.7 (CVSS2#E:F/RL:OF/RC:C)

Plugin Output
- C:\WINDOWS\system32\Msrating.dll has not been patched
  Remote version : 6.0.2900.3268
  Should be : 6.0.2900.3676

CVE
CVE-2010-0267
CVE-2010-0488
CVE-2010-0489
CVE-2010-0490
CVE-2010-0491
CVE-2010-0492
CVE-2010-0494
CVE-2010-0805
CVE-2010-0806
CVE-2010-0807

BID
38615
39023
39024
39025
39026
39027
39028
39030
39031
39047

Xref
OSVDB:62810
OSVDB:63327
OSVDB:63328
OSVDB:63329
OSVDB:63330
OSVDB:63331
OSVDB:63332
OSVDB:63333
OSVDB:63334
OSVDB:63335
MSFT:MS10-018

Vulnerability Publication Date: 2010/03/09

Patch Publication Date: 2010/03/30

Plugin Publication Date: 2010/03/30

Plugin Last Modification Date: 2011/01/04

Public Exploit Available: True

Exploitable With: Canvas (CANVAS), Core Impact, Metasploit (Internet Explorer DHTML Behaviors Use After Free)

The above alert from Nessus shows a Microsoft vulnerability exploitable with Immunity CANVAS and Metasploit.

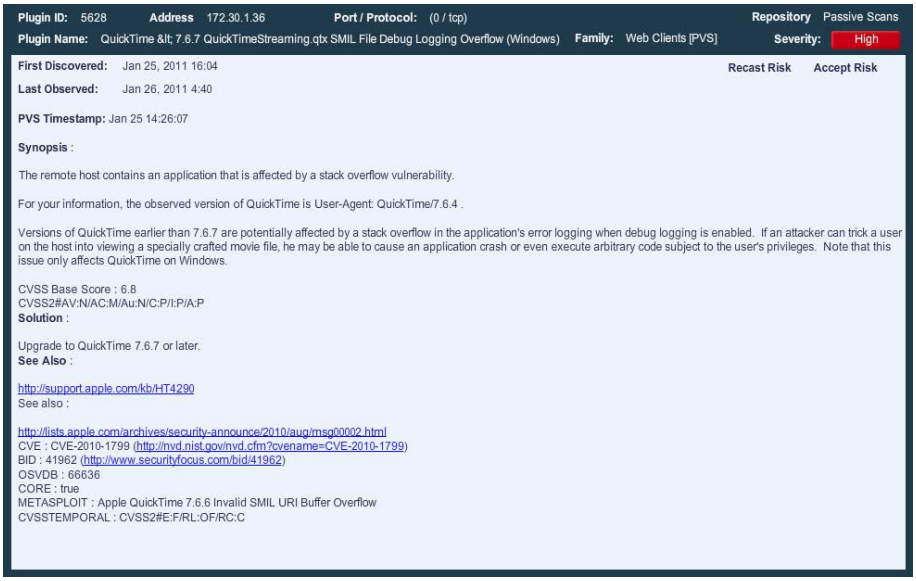
2. Targeted Vulnerability Information for Rapid Incident Response

The vulnerability data from your entire network can be sorted based on vulnerabilities for which there exists an exploit. You can further break this down into which framework, or source of exploits, the systems are vulnerable to. This means you can prioritize the remediation of vulnerabilities based on available tools. For example, if you believe Metasploit to be the most popular framework, due to its availability, and you've discovered Metasploit payloads on some of your systems that were compromised, you can prioritize and quickly identify anything on your network that could be compromised by Metasploit.

3. Continuous Alerting on New Exploits

Exploitability can be classified by asset type as well. For example, if the DMZ containing your Internet facing servers is scanned on a regular basis, you can query that data to see what is vulnerable to a known exploit. With SecurityCenter, you can set up an alert to notify you if one of those servers presents this condition.

Exploitability of vulnerabilities is discovered actively with credentialed and uncredentialed Nessus scans and passively with PVS, allowing for alerts on any network being monitored and coverage of client side vulnerabilities. As exploits are released, Nessus and PVS plugins are updated. This means you can scan for a vulnerability today, which has no exploit, but some time later receive an alert once an exploit gets published.



Above is an example from SecurityCenter showing a vulnerability in Apple QuickTime discovered by PVS Exploits for this vulnerability exist in both Core IMPACT and Metasploit.

4. Integrating with Penetration Testing to Save Time

Nessus is one of the most popular tools for integrating into exploitation frameworks. All of the popular frameworks, including Core IMPACT, Metasploit, and Immunity CANVAS support importing Nessus results into the tools. For example, you can scan a network using Nessus, export the results, and then import them into Core IMPACT. From there, Core IMPACT will have knowledge of the vulnerabilities found and allow you exploit them and deploy payloads.

Further integration has been added to two of the frameworks, Metasploit and Immunity CANVAS. These frameworks support the Nessus API, which allows them to talk directly to Nessus. A user can work within the exploit framework, initiate commands to launch a Nessus scan from the framework, and then pull down the report from the Nessus server and exploit vulnerabilities based on the results.

To gain even deeper insight into the targets during a penetration test you can use the "Pass the hash" technique to audit systems that you've successfully exploited. For example, on a penetration test you may have compromised a Windows host and gained access to its password hashes. You can then go back to Nessus and enter the hashes in the authentication section, and then have Nessus perform local patch checking and configuration audits.

Further Reading

- "Using Nessus and Metasploit Together" – Tenable Network Security Blog (http://blog.tenablesecurity.com/2011/08/using-nessus-and-metasploit-together.html) by Paul Asadoorian
- "Passively Detect all of your Exploitable Vulnerabilities" – Tenable Network Security Blog (http://blog.tenablesecurity.com/2011/01/passively-detect-all-of-your-exploitable-vulnerabilities-pvs-34-released.html) by Ron Gula
- "Nessus "Exploitable With" Field Updated" – Tenable Network Security Blog (http://blog.tenablesecurity.com/2011/02/nessus-exploitable-with-field-updated.html) by Paul Asadoorian

About Tenable Network Security

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management, and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG, and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit www.tenable.com.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive,
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com

tenable™ network security