krome

DATA SHEET

Remote Vulnerability Assessment

With a constantly evolving attack surface, new vulnerabilities are discovered each day; what would you find on your network? Unsecured remote connections? Out of date equipment? Missing patches? Unsupported operating systems? Configuration issues? Malware installed? Viruses?

How do you identify, quantify and prioritise the remediation of these vulnerabilities?

Our vulnerability assessment, powered by Nessus Pro, provides a point-in-time assessment that will identify and analyse your current network vulnerabilities, on both internal and external devices and applications. Our scan will highlight where your systems are vulnerable and will report on your remediation actions, in order of severity and priority.

Our Assessment Process

In order to identify and scan the devices inside your environment, we will require remote access to a virtual machine or physical server/pc on your network. We scan your environment externally from machines within our datacentre.

Using the Nessus Pro scanning tool we will initiate an internal and external vulnerability scanning assessment which will identify any areas of weakness, including software flaws, missing patches, malware and misconfiguration across a variety of operating systems, devices and applications.

The scan can be targeted at any device with an IP address including:

- Network devices
- Mobile devices, for vulnerabilities against policies
- Operating systems
- Applications within devices, ranging from small driver update utilities to complex Office productivity suites

The scan provides a point-in-time analysis which our team of consultants will review. Using the data collected, we will provide a detailed report summarising all of the security vulnerabilities discovered, along with a suggested plan for resilience improvement, clearly prioritising the remediation issues required.

If required, we can work with you to remediate any issues found as a separate remediation project, or we can leave you to make the required changes internally. Following the initial scan, we will provide a further scan 30 days later to ensure that any remediations made, have been successful. Further new vulnerabilities could also be captured at this point.

This can be delivered as a single point-in-time assessment to help you quickly understand where you have vulnerabilities or we can run this regularly for you as part of a managed service.

Identify Devices via IP range

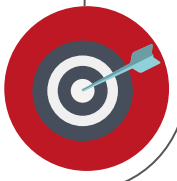
The scanning tool can be remotely deployed to any device within your IP range.

Vulnerability Scan

The internal and external scan will identify any current vulnerabilities or areas of weakness.

Comprehensive Report

A detailed review and report is provided, prioritising the remediation issues required.



Remediation

Assistance (if required) with the implementation of remediation solutions.

Re-Scan (30 days later)

A further scan 30 days later to ensure that any remediations made, have been successful.

Example Report Information

The report will provide you with a full list of vulnerabilities found per host and will RAG categorise them by their severity, showing the critical, high, medium, low and informational status on each host scanned.

HOST NAME

8	15	15	10	104
CRITICAL	HIGH	MEDIUM	LOW	INFORMATION

Severity	CVPP	Plugin	Name	IP Address
CRITICAL	10.0	123950	KB4493478: Security update for Adobe Flash Player (April 2019)	
CRITICAL	10.0	127841	KB4511553: Windows 10 Version 1809 and Windows Server 2019 August 2019 Security Update	
CRITICAL	10.0	128646	KB4516115: Security update for Adobe Flash Player (September 2019)	
HIGH	9.3	123948	KB4493509: Windows 10 Version 1809 and Windows Server 2019 April 2019 Security Update	
HIGH	9.3	125059	B4494441: Windows 10 Version 1809 and Windows Server 2019 May 2019 Security Update (MDSUM/RIDL) (MFBDS/RIDL/ZombieLoad) (MLPDS/RIDL) (MSBDS/Fallout)	

The report will also provide a detailed summary of the suggested remediations to take across all hosts, highlighting the number of vulnerabilities associated to each action across the environment, for example:

Taking the following actions across 23 hosts would resolve 8% of the vulnerabilities on the network.

Action to take	Vulns	Hosts
Install KB4551853	168	6
Oracle Java SE 1.7.0_261 / 1.8.0_251 / 1.11.0_7 / 1.14.0_1 Multiple Vulnerabilities (Apr 2020 CPU): Upgrade to Oracle JDK / JRE 14 Update 1 , 11 Update 7, 8 Update 251 , 7 Update 261 or later. If necessary, remove any affected versions.	58	1
VMware Tools 10.x < 11.0.0 Privilege Escalation (VMSA-2020-0002): Upgrade to VMware Tools version 11.0.0 or later or apply the workaround mentioned in the vendor advisory	44	22
Windows Malicious Software Removal Tool Elevation of Privilege Vulnerability: Upgrade to the relevant fixed version referenced in the advisory	23	23

If you would like us to assist in the remediation, then using the data captured in the scan, we can either provide you with remote or on-site assistance to resolve the vulnerabilities detected. Alternatively, we can leave you with the report to make your own internal updates. We can then re-scan your environment again up to 30 days later to ensure that the remediation was successful.

Advanced Vulnerability Assessment Service

In addition to our standard vulnerability assessment, we can also provide an added level to the service. Using other cyber security products within our portfolio we can deploy further inspection tools to analyse your cyber security provisions. A firewall assessment, for example, in which we passively inspect and analyse your traffic in a non-intrusive manner, providing detailed information on how many known and unknown threats were identified, what applications are delivering malware/exploits, identify high-risk processes and applications, and provide an overall check on the effectiveness of your current Firewall. We can also assess your current levels of password security and the policies around them, providing you with a summary of any users that are using insecure passwords, expired passwords, and privileged account access.

If you would be interested to learn more about how our vulnerability assessment services can help you to understand where your systems are the most vulnerable, and the steps required to protect your critical data, please contact us on **01932 232345**.

Krome Technologies
Head Office | Krome House | Pound Road | Chertsey | Surrey | KT16 8ER
01932 232345 | sales@krome.co.uk | www.krome.co.uk