Managed Service: Network Vulnerability Scanning

Protect7
your application security experts

Unsere Kunden wählen uns aufgrund unserer Fachkompetenz. Diese Stärke und unsere Erfahrungen setzen wir nicht nur im Bereich Web Application ein sondern auch beim Network Vulnerability Scanning Service. Mit modernen Tools zur automatischen Schwachstellen-Identifikation und manueller Analyse ist unser Service optimal, um die Scanfrequenz von exponierten IP Adressen zu erhöhen, oder um Compliance-Anforderungen erfüllen zu können.

Unsere Scans werden alle einer manuellen Verifikation unterzogen, was wir als "teilautomatisierten Test" bezeichnen. Damit sind alle Ergebnisse immer False-Positive bereinigt und je nach Modul auch in einem definierten Umfang um False-Negativ (nicht identifizierte Schwachstellen) reduziert. So können wir sicherstellen, dass unsere und Ihre Qualitätsansprüche erfüllt werden.

Recurring Scan:

Der Service entfaltet seinen Mehrwert vor allem dann, wenn ein Kunde seine externen IP Adressen regelmässig prüfen lässt. Aus diesem Grund ist die Basis des Service auf eine wiederkehrende Durchführung ausgelegt. Dadurch kann trotz einem reduzierten Testaufwand gegenüber einem vollwertigen manuellen Test, die Test Abdeckung (Coverage) mit jeder Durchführung erhöht werden. Dies weil nicht immer die gleichen Services in der Tiefe geprüft werden. Dadurch reduziert sich automatisch die False-Negative Quote. Zudem kann die zwischenzeitliche Schwachstellen Behebung verifiziert werden.

Preisübersicht/Preisgestaltung normales Setup

Modul	Grundkosten [klein/normal]	Preis/IP externer Scan
MN1-Opportunistic	550.- / 850.-	20.-
MN2-Balanced	550.- / 850.-	60.-
MN3-Advanced	550.- / 850.-	95.-

Preise pro Scanintervall und Modul. Die Grundkosten unterscheiden sich ob weniger als 8 IP Adressen (klein) oder mehr überprüft werden.

Im Abo fällt die initiale Gebühr nur 1 mal an.

Unsere Preise sind ausgerichtet an einem Scan über alle tcp- und ausgewählten udp Ports und einer wiederkehrenden Durchführung.

Mögliche Zusatzkosten	pro Network-Range
Initialisierungsgebühr	250.-
Spezial Scan-Setup	125.-

Beachten Sie für weitergehende Tests auch die Hinweise auf unserer Website zum Unterschied von automatischen versus manuell durchgeführten Sicherheitsanalysen (Penetration Tests).

Sie erhalten

- Regelmässige Übersicht über mögliche Schwachstellen und deren Schweregrad für Ihre exponierten IP Adressen
- Sehr gute Test Möglichkeit oder als Ergänzung zu manuellen Penetration Test
- Erhöhung der Test-Frequenz gegenüber jährlichen Penetration Tests
- Kontinuierliche Sicherheits-Analyse (zur Erfüllung von Governance Anforderungen)
- Auch für interne Scans erhältlich

Ihr Vorteil

- Sie müssen in Ihrer Organisation das nötige Know-How nicht aufbauen
- Speziell auf Netzwerk Services ausgerichtetes Verfahren
- Basis-Informationen über das Sicherheitsniveau Ihrer Web-Applikationen
- Risiko Reduktionen dank erhöhter Test-Frequenz
- Weniger False-Positives
- Weniger False-Negative
- Standardisiertes Reporting
- Erfüllung von Compliance-Anforderungen
- Qualität und Preise wählbar

Sämtliche Preisangaben in CHF und exkl. MwSt.

MANAGED SERVICES

Managed Network Vulnerability Scanning

Protect7
your application security experts

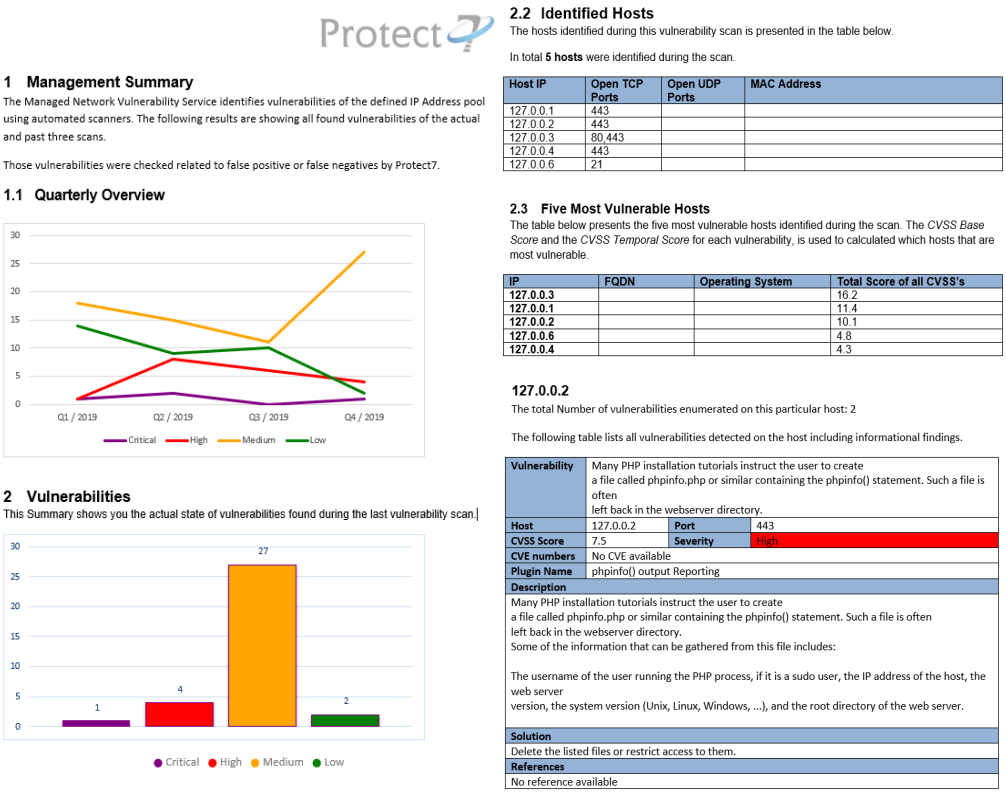
Service Übersicht

Feature	MN1- Opportunistic	MN2- Balanced	MN3- Advanced
Automated scan[1]	✓	✓	✓
Manual testing	basic	balanced	advanced
Manual False positive validation	✓	✓	✓
Manual False negative reduction		✓	✓
Recurring tests - remediation verification	✓	✓	✓
Recurring tests - coverage improvement		✓	✓
Report per scan	✓	✓	✓

Hinweis: Der manuelle Test-Aufwand inklusive Dokumentation beträgt pro IP bei MN2: 15 Minuten und bei MN3: 25 Minuten

Reporting

Der Report enthält die Resultate aus dem Scan, False-Positives bereinigten und um False-Negative identifizierte Schwachstellen ergänzt und wird im PDF–Format bereitgestellt.



Protect7

1 Management Summary

The Managed Network Vulnerability Service identifies vulnerabilities of the defined IP Address pool using automated scanners. The following results are showing all found vulnerabilities of the actual and past three scans.

Those vulnerabilities were checked related to false positive or false negatives by Protect7.

1.1 Quarterly Overview

2 Vulnerabilities

This Summary shows you the actual state of vulnerabilities found during the last vulnerability scan.

2.2 Identified Hosts

The hosts identified during this vulnerability scan is presented in the table below.

In total **5 hosts** were identified during the scan.

Host IP	Open TCP Ports	Open UDP Ports	MAC Address
127.0.0.1	443		
127.0.0.2	443		
127.0.0.3	80,443		
127.0.0.4	443		
127.0.0.6	21		

2.3 Five Most Vulnerable Hosts

The table below presents the five most vulnerable hosts identified during the scan. The *CVSS Base Score* and the *CVSS Temporal Score* for each vulnerability, is used to calculated which hosts that are most vulnerable.

IP	FQDN	Operating System	Total Score of all CVSS's
127.0.0.3			16.2
127.0.0.1			11.4
127.0.0.2			10.1
127.0.0.6			4.8
127.0.0.4			4.3

127.0.0.2

The total Number of vulnerabilities enumerated on this particular host: 2

The following table lists all vulnerabilities detected on the host including informational findings.

Vulnerability	Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory.		
Host	127.0.0.2	**Port**	443
CVSS Score	7.5	**Severity**	High
CVE numbers	No CVE available		
Plugin Name	phpinfo() output Reporting		
Description			
Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory. Some of the information that can be gathered from this file includes: The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.			
Solution			
Delete the listed files or restrict access to them.			
References			
No reference available			

MANAGED SERVICES