DEFENDERBOX Funktionsumfang

Modul 1

EXTERNE ANGREIFBARKEIT

Externe Schwachstellenanalyse

- Portscan (1-65635)
- Cross Site Scripting
- SQL Injection Exploits
- JQuery
- SSL/TLS Best Practice Check
- HTTP-Header Security Check

Content-Security-Policy	Strict-Transport-Security	Zu jedem Eintrag der Liste erhalten Sie eine Bewertung	Übersicht aller gesetzten HTTP-Header	Security Check auf fehlende Header

- Weitere Gruppen von Schwachstellentests mit Anzahl der Checkmodule

AIX Local Security Checks (11656)	Alma Linux Local Security Checks (1647)	Amazon Linux Local Security Checks (5111)	Artificial Intelligence (151)	Backdoors (123)
Brute force attacks (25)	CentOS Local Security Checks (5152)	CGI abuses (6322)	CGI abuses : XSS (709)	CISCO (2487)
Databases (1039)	Debian Local Security Checks (9777)	Default Unix Accounts (172)	Denial of Service (110)	DNS (238)
F5 Networks Local Security Checks (1491)	Fedora Local Security Checks (20087)	Firewalls (582)	FreeBSD Local Security Checks (5806)	FTP (288)
Gain a shell remotely (282)	General (581)	Gentoo Local Security Checks (3732)	HP-UX Local Security Checks (1983)	Huawei Local Security Checks (12400)
Junos Local Security Checks (715)	MacOS X Local Security Checks (2743)	Mandriva Local Security Checks (3641)	MarinerOS Local Security Checks (1742)	Misc (4493)
Netware (14)	NewStart CGSL Local Security Checks (1483)	Oracle Linux Local Security Checks (7496)	OracleVM Local Security Checks (614)	Palo Alto Local Security Checks (203)
Peer-To-Peer File Sharing (109)	PhotonOS Local Security Checks (3789)	Policy Compliance (75)	Red Hat Local Security Checks (17804)	Rocky Linux Local Security Checks (1468)
RPC (39)	SCADA (457)	Scientific Linux Local Security Checks (3291)	Service detection (634)	Settings (123)
Slackware Local Security Checks (1629)	SMTP problems (154)	SNMP (34)	Solaris Local Security Checks (3823)	SuSE Local Security Checks (25316)
Tenable.ot (2772)	Ubuntu Local Security Checks (8582)	Virtuozzo Local Security Checks (341)	VMware ESX Local Security Checks (143)	Web Servers (1900)
Windows (7330)	Windows : Microsoft Bulletins (3261)	Windows: User management (29)		

DEFENDERBOX Funktionsumfang

Modul 1

EXTERNE ANGREIFBARKEIT

Externes Pentesting

- Portscanning
- CVE Scanning
- Webanwendungen
- SNMP v1/v2/v3
- Erraten von verwendeten Benutzerkennungen auf

SSH	Telnet	RDP	MySQL	Mongo DB
MS SQL	Redis	Maria DB	PostgreSQL	HTTP Basic Auth
HTTP Web Forms	FTP	SNMP	SMB	

- Prüfung auf die Verwendung von Standardkennungen mithilfe von Wörterbuch-Angriffen mit bekannten Standardanmelde-informationen nach Standardanmelde-informationen suchen

FTP	SSH	Telnet	RDP	MySQL
Mongo DB	MS SQL	Redis	Maria DB	PostgreSQL
Web	SNMP	SMB		

- Aktives Ausnutzen von gefundenen Sicherheitslücken. Bezieht sich auf Module, die die Umgebung verändern. Alle Module versuchen, sich selbst zu bereinigen, aber es besteht eine kleine Chance, dass die Bereinigung fehlschlägt.

ADCSESC4-Angriff – Fehlkonfigurierte Templates Zugriffskontrollen	Anonyme Docker-Engine-Schreibprüfung	Anonymer Druckerzugriff	Anonyme ZooKeeper-Schreibprüfung	Atlassian Crowd und Crowd Data Center – Entfernte Code-Ausführung (CVE-2019-11580)
Bluekeep (CVE-2019-0708)	CVE-2022-26923 (Certifried) Privilege Escalation - Erstellung eines Maschinenkontos	Elasticsearch-Schreibprüfung	FTPWrite-Prüfung	Erweitertes LLMNRund NetBIOS-Poisining
Begrenztes LLMNRund NetBIOS-Poisoning	Net-NTLMAuthentica-tion-Roercion	Net-NTLMHash-Vermittlung	ManageEngine ServiceDesk Plus PreAuth RCE(CVE-2021-44077)	Zoho ManageEngine ADSelfService Plus APIAuth-Umgehung (CVE-2021-40539)
Bluekeep (CVE-2019-0708)	Sicherheitslücke bei Cisco Smart Install (CVE-2018-0171)	EternalBlue (MS17-010)	EternalChampion/ EternalSynergy/ EternalRomance (MS17-010)	Explodierende Dose (CVE-2017-7269)
HP iLO Web APIRemote Code-Ausführung (CVE-2017-12542)	Heartbleed (CVE-2014-0160)	Serverdienst-Schwachstelle (MS08-067)	Subdomain-Übernahme	Unsicheres JMX(H3-2020-0022)
VMWare vCenter Server Zugriffssteue-rungsschwachstelle (CVE-2020-3951	VMWare vCenter Server-Plugin-Schwach-stelle mit Remotecode-Ausführung (CVE-2021-21972)	VMWare vRealize Operations Manager SSRF-Schwachstelle (CVE-2021-21975)		

- Weitere OSINT-Module

Abfrage RIPE Datenbank (DB)	CENSYS

DEFENDERBOX Funktionsumfang

Modul 2

DARKNET

Darknet Recherche

Öffentlich auffindbare Informationen zur Website

- Verfügbare Metadaten & technische Details
- Verlinkungen & Referenzen auf externen Seiten
- Offene Ports und potenzielle Angriffspunkte

Erfassung aller mit der Domain verbundenen E-Mail-Adressen

- Identifikation öffentlicher und geleakter E-Mail-Adressen
- Zuordnung zu bekannten oder kritischen Datenlecks

Abgleich mit „Have I Been Pwned“

- Überprüfung, ob und in welchen Datenlecks Ihre E-Mail-Adressen kompromittiert wurden
- Details zu den betroffenen Datenlecks (z. B. Name, Art der kompromittierten Daten, Zeitpunkt des Leaks)

Detaillierter Report mit Risikobewertung

- Auflistung aller gefundenen Informationen
- Einschätzung der potenziellen Risiken
- Konkrete Handlungsempfehlungen zur Risikominimierung

DEFENDERBOX Funktionsumfang

Modul 3

INTERNE ANGREIFBARKEIT

Internes Pentesting

Asset Discovery

Network Segmentation Analysis

Information Gathering

Ports	HTTP-Header	Webanwendungen	SNMP v1/v2/v3	mDNS
SSH	VNC	RDP	Telnet	

CVE Scanning

Ports	HTTP-Header	Webanwendungen	SNMP v1/v2/v4	SSH
WMI				

Credential Verification

Verwendung von Domänenbenutzeranmeldeinformationen

Passwort-Spraying von Azure-Cloud-Benutzern mit gängigen Passwörtern. Es besteht eine geringe Wahrscheinlichkeit, dass Konten gesperrt werden.	Überprüft den Zugriff auf Dienste und Freigaben mit lokaler Benutzerauthentifizierung (ohne Domäne).	Überprüft den Zugriff von Windows-Domänenbenutzern durch Authentifizierung mit Anmeldeinformationen gegenüber dem SMB-Service, der auf dem Windows Domain Controller läuft.	Ermöglicht das Passwort-Spraying von Domänenbenutzern mit gängigen Passwörtern. Standardmäßig wird ein Benutzer nur zweimal alle 60 Minuten versucht.

Service Brutforce

Durch unzähliges Ausprobieren von Benutzernamen und Passwort-Kombinationen versucht NodeZero in das System einzudringen.

SSH	Telnet	RDP	MySQL	Mongo DB
MS SQL	Redis	Maria DB	PostgreSQL	"HTTP Basic Auth/ HTTP Web Forms"
FTP	SNMP	SMB		

Service Discovery

In der Diensterkennungs-Phase testet NodeZero die gefundenen Services auf spezifische, häufig vorkommende Sicherheitslücken, die durch eine falsche Konfiguration entstehen.

Dabei werden unter anderem Authentifizierungsverfahren, die Verschlüsselung von Verbindungen oder Ausführungs- und Zugriffsrechte unter die Lupe genommen.

SSH	Telnet	DNS	MySQL	Mongo DB
MS SQL	HTTP	SSL/TSL	LDAP	SNMP v1/v2/v4
HTTP Header	FTP	SMTP	SMB	

Footprinting der Anwendungsumgebung

Insbesondere Versionsnummern stellen für Angreifer eine wertvolle Information dar. NodeZero untersucht, welche Technologien die Webseite in einem HTTP-Header, einem Cookie oder im Code preisgibt.

Das Footprinting umfasst Programmiersprachen, Content Management Systeme, Webserver, Frameworks oder Libraries. Eine eindeutige Bewertung gibt an, wie kritisch die ermöglichte Detektion der jeweiligen Technologie einzuschätzen ist.

für Angreifer sichtbare Technologien aufdecken	Scan der HTTP-Header, Cookies und des Webseiten-Codes

DEFENDERBOX Funktionsumfang

SECURITY

Wöchentliche Security-Prüfung

- Enthalten sind die Module 1. und 3. der Initialen Cybersicherheitsprüfung (Modul 2 bei Bedarf)

Modul 1 Modul 3

- Analyse der Abweichung / Veränderung zwischen der letzten Prüfung und der aktuellen Prüfung
- Alarmierung bei gravierenden, neuen Sicherheitslücken (CVE-Score >=8)

Zusätzliche Security-Prüfung

- Zusatzprüfungen alle 2-3 Monate

AD-Audit	Greybox-Testing: wie weit kommt ein Angreifer mit Testaccounts auf verschiedenen Ebenen	Netzwerk-Lasttest: wie reagiert das Netzwerk bei internen, erheblichen Lastspitzen

---

DEFENDERBOX – Ihre proaktive Sicherheitsmaßnahme in NIS-2

Die **DEFENDERBOX** ist Ihre proaktive Sicherheitsmaßnahme, wenn es um Prävention, Ermittlung und Bewältigung von Sicherheitsvorfällen geht.

EINFACH. SCHNELL. CYBERSICHER. identifiziert die **DEFENDERBOX** Schwachstellen und Sicherheitslücken in Ihrer IT-Infrastruktur - bevor es zu einem Cybersicherheitsvorfall kommt.

Der **DEFENDERBOX** "**Rapid Response Service**" von NodeZero sorgt dafür, dass Ihr Unternehmen sofort benachrichtigt wird, wenn das Angriffsteam neue Schwachstellen entdeckt und hinzugefügt hat. So können Sie Ihre eigene IT-Infrastruktur in Bezug auf neue Einfallstore für Hacker testen und diese ggfls. schließen, oft noch, bevor die Schwachstellen öffentlich bekannt werden.

Als Partner von **phished.io** bieten wir zudem Cybersecurity Awareness und Social Engineering Schulungen und Tests für alle Beschäftigten an.

Profitieren Sie von einer ganzheitlichen Sicherheitsstrategie.

Kontaktieren Sie uns!
vertrieb@defenderbox.de
Tel 02732 / 7652088