

Task: CPE-basierte Inventur

Inhalt

- CPE-basierte Inventur durchführen

Einleitung

CPE steht für Common Product Enumeration. Es handelt sich um ein strukturiertes Benennungsschema für IT-Systeme, IT-Plattformen und Softwarepakete.

Mit anderen Worten: CPE bietet eine eindeutige Identifikationsnummer für praktisch jedes Softwareprodukt für das eine Schwachstelle bekannt ist.

Das CPE-Verzeichnis wird von MITRE und NIST gepflegt. MITRE pflegt ebenfalls CVE (Common Vulnerability Enumeration) und andere relevante Sicherheits-Standards.

Common Product Enumeration (CPE): Name Structure

A CPE Name is a URI with each name starting with the prefix (the URI scheme name) "cpe:".

`cpe:/{part}:{vendor}:{product}:{version}:{update}:{edition}:{language}`

Part

Each platform can be broken down into three distinct parts. A CPE Name specifies a single part and is used to identify any platform that matches the description of that part. The three distinct parts are:

h = hardware
o = operating system
a = application

Vendor

The second component of a CPE Name is the supplier or vendor of the platform element. For CPE, the name used for a supplier should be the highest organization-specific label of the organization's DNS name.

Additional Components

The last five components represent product, version, update, edition, and language information. These components are optional. A CPE can be written at different levels of specificity. A name can define product in general, a specific version of a product, or even a certain edition of that product.

Examples

```
cpe:/o:redhat:enterprise_linux:5  
cpe:/a:sun:jre:1.6.0  
cpe:/a:microsoft:ie:7  
cpe:/a:apache:tomcat:5.5.29
```

CPE-basierte Inventur durchführen

Die Inventur wird auf Basis eines beliebigen Scan-Vorganges aufgebaut. Allen vorgefundenen Produkte werden die entsprechenden CPEs zugeordnet.

Dies bedeutet auch, dass je umfangreicher und tiefgreifender die Scan Configuration gewählt ist, desto mehr Produkte werden identifiziert und tauchen dann in der Inventurliste auf.

1. Falls die Erkennungsleistung über lokale Sicherheitstests erhöht werden soll, dann sollte zunächst ein entsprechender Zugang konfiguriert werden. Falls noch nicht geschehen, erstellen Sie dafür einen entsprechenden Anwender auf den Zielsystemen (ein niedrig privilegiertes Benutzer-Konto reicht aus).

New Credential for Local Security Checks ?

Name:

Login:

Comment (optional):

Autogenerate credential

Password:

2. Nun werden die Zielsysteme (Targets) festgelegt und ggf. mit den entsprechenden Credentials verknüpft.

New Target ?

Name:

Comment (optional):

Hosts:

Credential (optional):

3. Als nächstes wird die Aufgabe (Task) erstellt indem die eine vorhandene Scan Configuration (z.B. "Full and Fast") mit dem entsprechenden Ziel kombiniert wird.



New Task ?

Name:

Scan Config:

Scan Targets:

Escalator (optional):

4. Der Scan wird gestartet in dem für den eben erstellten Task auf  geklickt wird. Es kann einige Zeit dauern, bis der Scan abgeschlossen ist. Den aktuellen Stand des Scans erhalten Sie indem Sie auf  klicken.

Reports for "CPE Inventory Task" ? 

Report	Threat	Scan Results				Download	Actions
		High	Medium	Low	Log		
Tue Feb 2 16:02:46 2010 Done	High	74	28	57	12	PDF <input type="button" value="Download"/>	 

5. Sobald der Status auf "Done" wechselt, ist der vollständige Bericht verfügbar. Sie können aber auch schon während des Scans die bereits gefundenen Ergebnisse einsehen.

Um sich nur die Ergebnisse der CPE basierten Inventur anzeigen zu lassen, läßt sich ein entsprechender Filter formulieren (Suchtext "CPE" und Bedrohungskategorie "Log").

Result Filtering

Results 1 - 2 of 2 This report as: PDF

Sorting: [port_ascending](#) | [port_descending](#) | [threat_ascending](#) | [threat_descending](#)

Text phrase:

Threat: High Medium Low Log

6. Hier ein Beispiel für ein Windows XP System.

Filtered Results

Host	High	Medium	Low	Log	Total
192.168.2.6	0	0	0	1	1
192.168.2.9	0	0	0	1	1
Total: 2	0	0	0	2	2

Port summary for host "192.168.2.6"

Service (Port)	Threat
general/tcp	Log

Security Issues reported for 192.168.2.6

Log general/tcp

NVT: CPE_Inventory (OID: 1.3.6.1.4.1.25623.1.0.810002)

The following products were identified during the scan and related to CPE (<http://cpe.mitre.org/>) identities. This list supports verification of software inventories. It may be incomplete and contains the best guesses based on various indicators during operating system, service and application detection routines.

```

IP|CPE
192.168.2.6|cpe:/a:sonicwall:global_vpn_client:4.0.0.835
192.168.2.6|cpe:/a:lumension_security:patchlink_update:2.4
192.168.2.6|cpe:/a:symantec:norton_antivirus:12.3.4.0
192.168.2.6|cpe:/a:tightvnc:tightvnc:1.2.9
192.168.2.6|cpe:/a:downstairs.dnsalias:home_ftp_server:1.10.1.1:39
192.168.2.6|cpe:/a:cisco:vpn_client:4.8.00.0440
192.168.2.6|cpe:/a:novell:edirectory:8.8.SP5.SP5
192.168.2.6|cpe:/a:sun:jre:1.6.0
192.168.2.6|cpe:/a:microsoft:ie:7
192.168.2.6|cpe:/o:microsoft:windows-nt:xp
192.168.2.6|cpe:/a:mcafee:epolicy_orchestrator:4.0.0.1421
192.168.2.6|cpe:/a:mcafee:agent:4.0.0.1421
192.168.2.6|cpe:/a:rhinosoft:serv-u:9.0.0.5
192.168.2.6|cpe:/a:apache:tomcat:5.5.28
192.168.2.6|cpe:/a:microsoft:windows_media_player:11.0.5721.5145
192.168.2.6|cpe:/a:sun:jre:1.6.0_13
192.168.2.6|cpe:/a:pg4win:pg4win:2.0.1
192.168.2.6|cpe:/a:kde-apps:kleopatra:2.0.11
192.168.2.6|cpe:/a:wireshark:wireshark:1.2.4
192.168.2.6|cpe:/a:novell:zmanager:2.7.0
  
```