CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Systematische Schwachstellensuche (Linux)

CloudCommand GmbH chr.schumacher@gmx.tm

Systematische Schwachstellensuche (Linux)

Die systematische Schwachstellensuche in **Linux-Systemen** ist ein wichtiger Bestandteil der IT-Sicherheit.

Dabei werden Schwachstellen erkannt, bewertet und dokumentiert, um Sicherheitslücken zu schließen, bevor sie ausgenutzt werden können.

Informationssammlung (Reconnaissance)

Systeminformationen:

```
uname -a          # Kernel-Version
lsb_release -a    # Distribution und Version
cat /etc/os-release
```

Informationssammlung (Reconnaissance)

Netzwerkinformationen:

```
ifconfig / ip a          # Netzwerkschnittstellen
netstat -tuln            # Offene Ports und Dienste
ss -tuln                 # Alternative zu netstat
route -n                 # Routing-Tabelle
```

Informationssammlung (Reconnaissance)

Benutzer und Gruppen:

```
cat /etc/passwd
cat /etc/group
whoami                  # Aktueller Benutzer
id                      # Benutzer-ID und Gruppen
```

Schwachstellenscans und Sicherheitsüberprüfungen

Lokale Schwachstellenprüfung:

Lynis (Sicherheitsaudit):

```
sudo apt install lynis
sudo lynis audit system
```

Schwachstellenscans und Sicherheitsüberprüfungen

Rootkit-Scans:

chkrootkit:

```
sudo apt install chkrootkit
sudo chkrootkit
```

rkhunter:

```
sudo apt install rkhunter
sudo rkhunter --check
```

Schwachstellenscans und Sicherheitsüberprüfungen

Schwachstellen in Paketen überprüfen:

Debian/Ubuntu:

```
sudo apt update && sudo apt upgrade
sudo apt install debsecan
debsecan --only-fixed
```

RedHat/CentOS:

```
sudo yum update
sudo yum install yum-security
sudo yum updateinfo list security all
```

Netzwerk- und Port-Scanning

Nmap (Netzwerkscan):

```
sudo nmap -sS -sV -O <IP-Adresse>
sudo nmap --script=vuln <IP-Adresse>
```

Netzwerk- und Port-Scanning

Netcat (offene Ports testen):

```
nc -zv <IP-Adresse> 1-65535
```

Netzwerk- und Port-Scanning

Nikto (Webserver-Scan):

```
sudo apt install nikto
nikto -h http://<IP-Adresse>
```

Schwachstellen-Scanner und Management-Tools

OpenVAS (Komplettlösung für Schwachstellenscans)

Installation (Debian/Ubuntu)

```
sudo apt install openvas
sudo gvm-setup
sudo gvm-start
```

Schwachstellen-Scanner und Management-Tools

Nessus (kommerziell, kostenlose Version verfügbar)

- Webseite:
  https://www.tenable.com/downloads/nessus?loginAttempted=true

VulnScan-Skripte:

- Verwende vorhandene **Nmap-Skripte** für CVE-Scans.
- Integriere Schwachstellendatenbanken wie **CVE** oder **Exploit-DB**.

DANKE!

Gibt es noch Fragen?

CloudCommand