Exploits & IT-Standards

Elia Garzi, Sebastian Gruber 29.9.2021

Erfahrungsbericht

Metasploit 1

Exploit erklärt 2

Praxis 3

ISO Standards

4 Was sind ISO Standards

5 Was ist ISO 27000?

6 Was ist ISMS?

1 Erfahrungsbericht

Metasploit:

- Projekt zu IT-Sicherheit
- Ansammlung von Exploits
- Verschiedene Betriebssysteme

2 Exploit

Was ist ein Exploit?:

- Schwachstellen in Software
- z.B.Well known Ports

Schutz vor Exploit:

- Softwareupdates
- Stabiler Code

03

Praxis

Port Scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- -sV -O 192.168.19.128                                    1 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 16:25 EDT
Stats: 0:02:15 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 16:28 (0:00:04 remaining)
Nmap scan report for 192.168.19.128
Host is up (0.00096s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
```

Exploit

msfconsole

Schnittstelle zum Metasploit Framework

search function

Suchen nach exploit (Versionen)

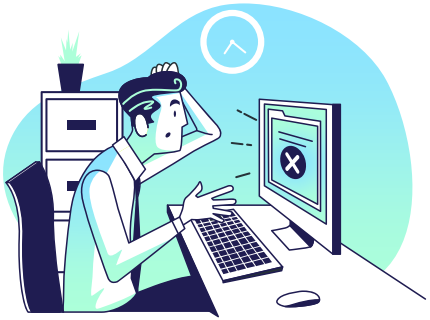
set RHOST

IP-Adresse des Angriffsziels

ISO Standards

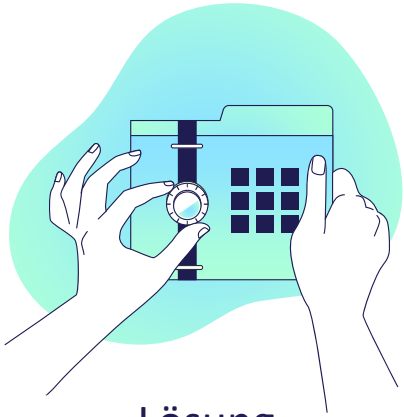
ISMS, ISO 27000

4 Wieso ISO Standards?



Das Problem

- IT-Sicherheit ist komplex
- IT-Sicherheit wird schnell chaotisch
- IT-Sicherheit teils Gesetzlich vorgeschrieben



Lösung

- Methoden vereinheitlichen
- Framework für IT-Sicherheit

5 ISO 27000

- Reihe Standards
- Informationssicherheit
- Information Security Management System

6 Die Bestandteile von ISMS

Informationssicherheit

Vertraulichkeit

Integrität

Verfügbarkeit

Unternehmensweit

Geht über die IT-Abteilung hinaus

Prozesse, Schulung, Management

Risikomanagement

Erfassung

Analyse

6 Der Weg zum ISMS

Noch Fragen?

Vielen Dank fürs Zuhören

RESOURCES

- https://bit.ly/39AVB0O
- https://bit.ly/2XPkqmW
- https://bit.ly/3zTPgIF
- https://de.wikipedia.org/wiki/Metasploit
- https://docs.microsoft.com/de-de/microsoft-365/security/defender-endpoint/enable-exploit-protection?view=o365-worldwide
- https://www.27000.org/
- https://en.wikipedia.org/wiki/ISO/IEC_27000