Bereich Elektrotechnik und Informatik

der Fakultät für Ingenieurwissenschaften
an der Hochschule Wismar

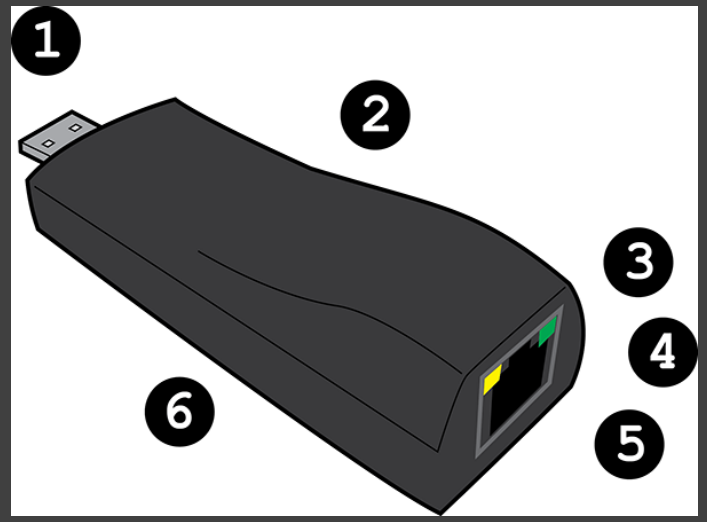
RubberDucky / LanTurtle / WifiPineApple

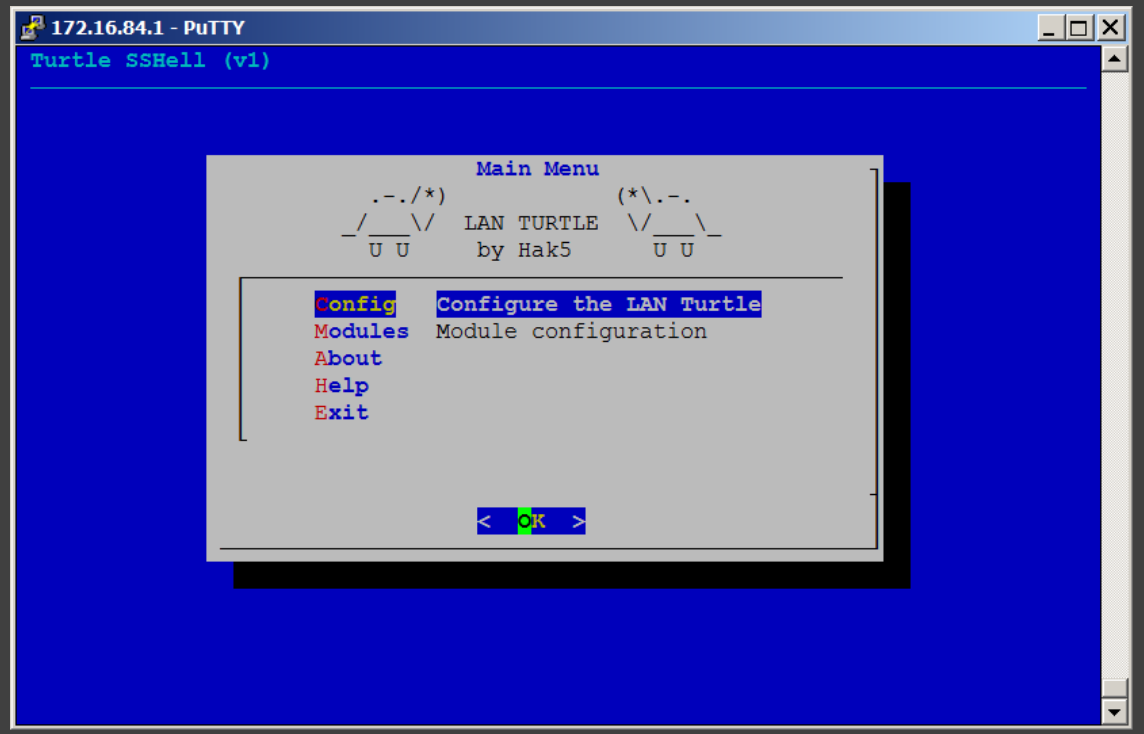
Hardware Hacking Tool Eine kleine Einführung

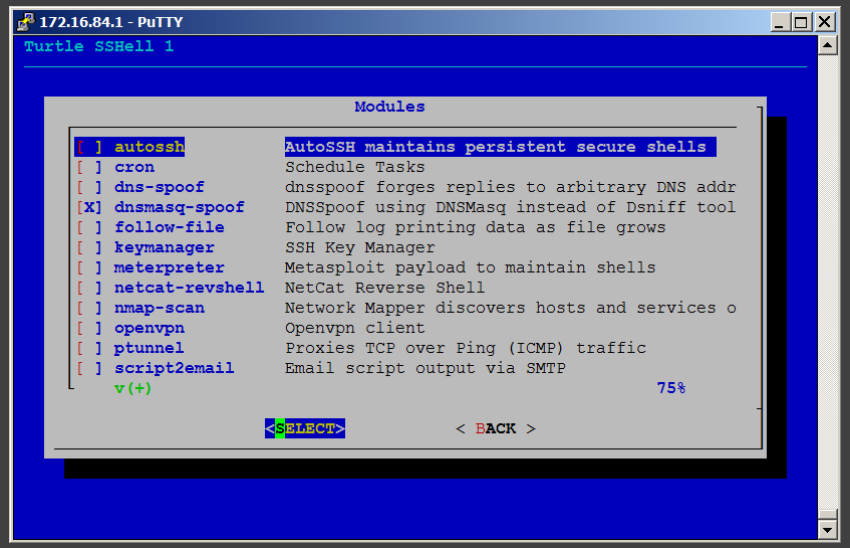
Dirk Zimmermann

HOCHSCHULE WISMAR
UNIVERSITY OF APPLIED SCIENCES TECHNOLOGY, BUSINESS AND DESIGN

Lan Turtle


1
2
3
4
5
6


172.16.84.1 - PuTTY
Turtle SSHell (v1)
Main Menu
.-./*)
_/___\/
U U
LAN TURTLE
by Hak5
(*\.-.
\/____
U U
Config Configure the LAN Turtle
Modules Module configuration
About
Help
Exit
< OK >


172.16.84.1 - PuTTY
Turtle SSHell 1
Modules
[ ] autossh AutoSSH maintains persistent secure shells
[ ] cron Schedule Tasks
[ ] dns-spoof dnsspoof forges replies to arbitrary DNS addr
[X] dnsmasq-spoof DNSSpoof using DNSMasq instead of Dsniff tool
[ ] follow-file Follow log printing data as file grows
[ ] keymanager SSH Key Manager
[ ] meterpreter Metasploit payload to maintain shells
[ ] netcat-revshell NetCat Reverse Shell
[ ] nmap-scan Network Mapper discovers hosts and services o
[ ] openvpn Openvpn client
[ ] ptunnel Proxies TCP over Ping (ICMP) traffic
[ ] script2email Email script output via SMTP
v(+)
75%
<SELECT> < BACK >

Lan Turtle

Zugangsdaten von gesperrtem PC in 20 Sekunden geklaut
https://www.heise.de/security/meldung/Zugangsdaten-von-gesperrtem-PC-in-20-Sekunden-geklaut-3316752.html

Snagging credits from locked machines
https://room362.com/post/2016/snagging-creds-from-locked-machines

Thesis

Ist es möglich, wenn ich dem Betriebssystem ein USB Ethernetadapter vorgaukel,
und der User eingeloggt aber der der PC gesperrt ist,
die Benutzer Credential zu erfahren?

Lan Turtle

Es ist möglich

HTTP-NTLMv2-172.16.84.143.txt

```
1  zimmermann::FIWI:1122334455667788:C1D8BFE410088DACA76729CF9E06A892:010100000000000
2  zimmermann::FIWI:1122334455667788:C1D8BFE410088DACA76729CF9E06A892:010100000000000
```

Lan Turtle

Aber nicht nur das, sonder auch

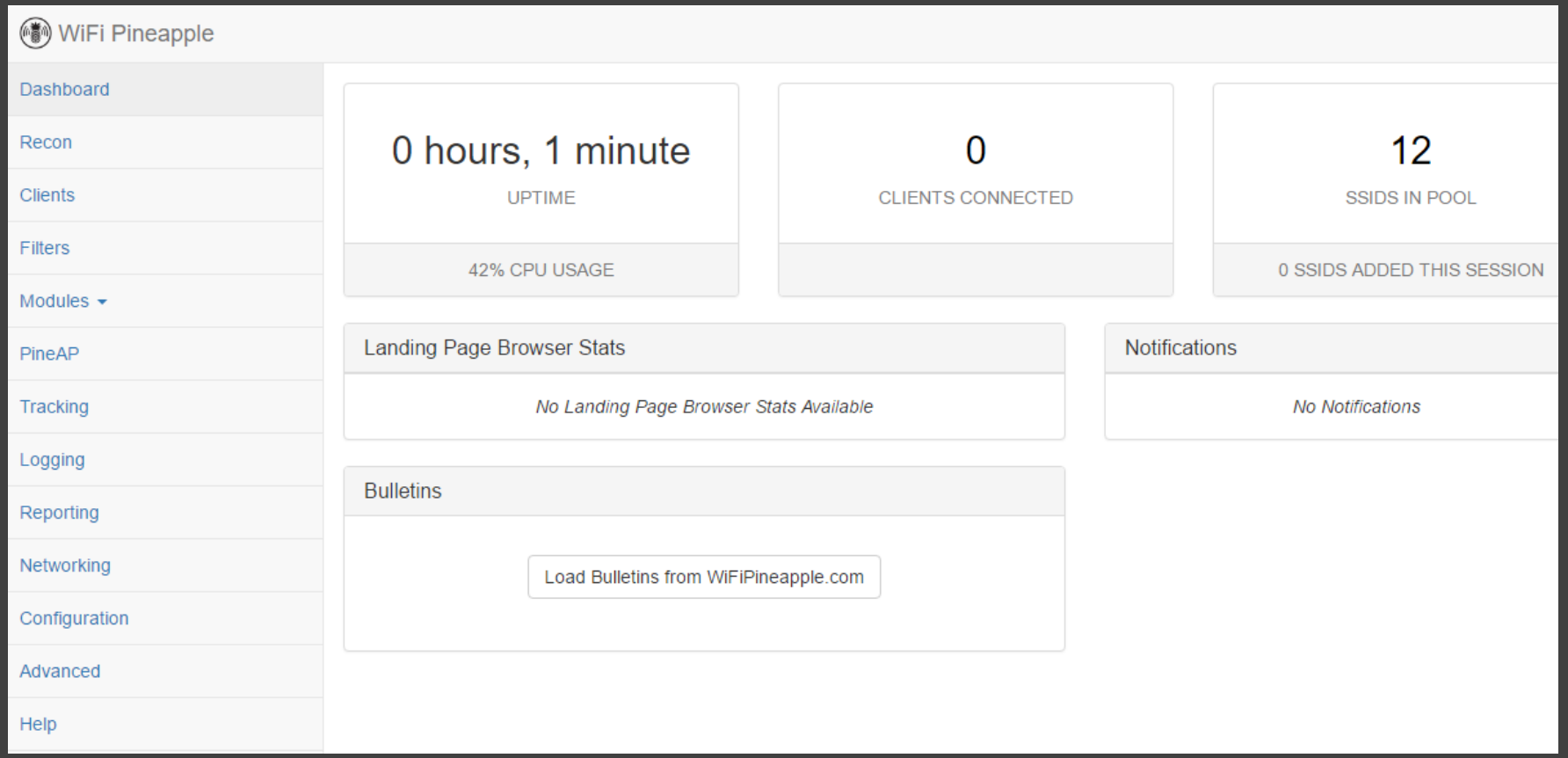
DNS Spoofing
MitM
Urlsnarf usw.....

WiFi Pineapple nano

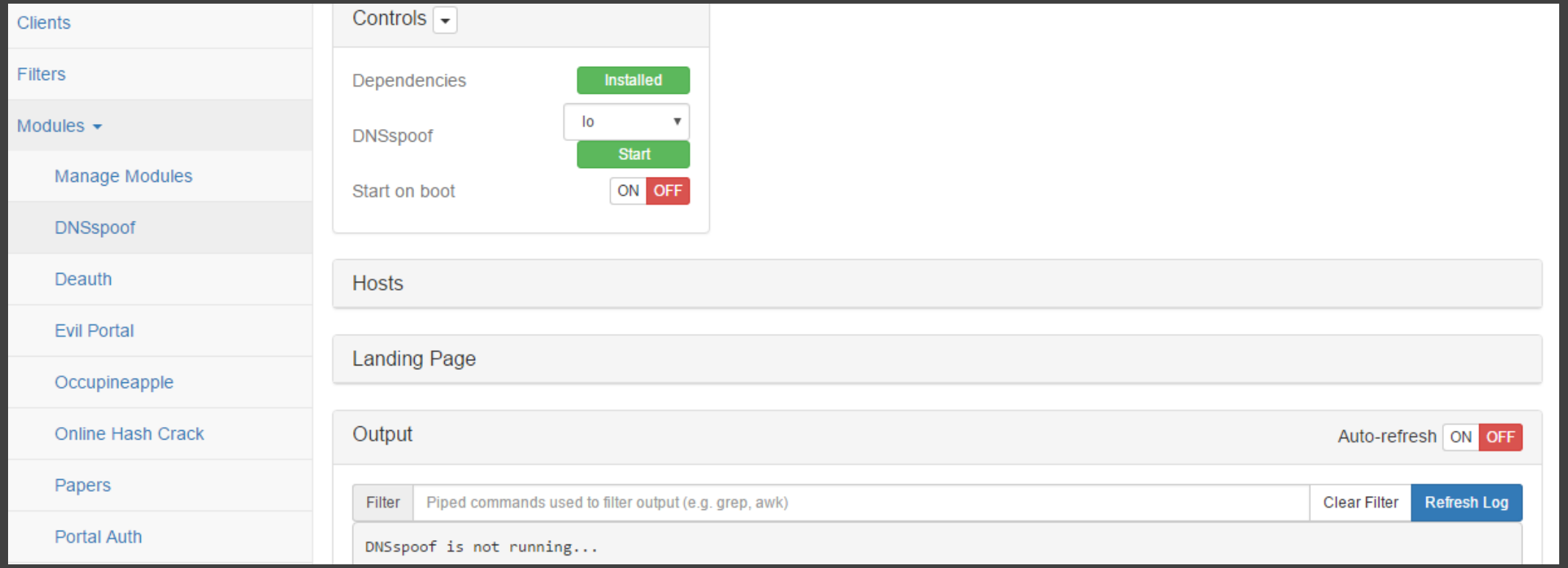
Verwendung

Als Accesspoint, Rouge Access Point,
Mit Funktionen wie MitM, usw

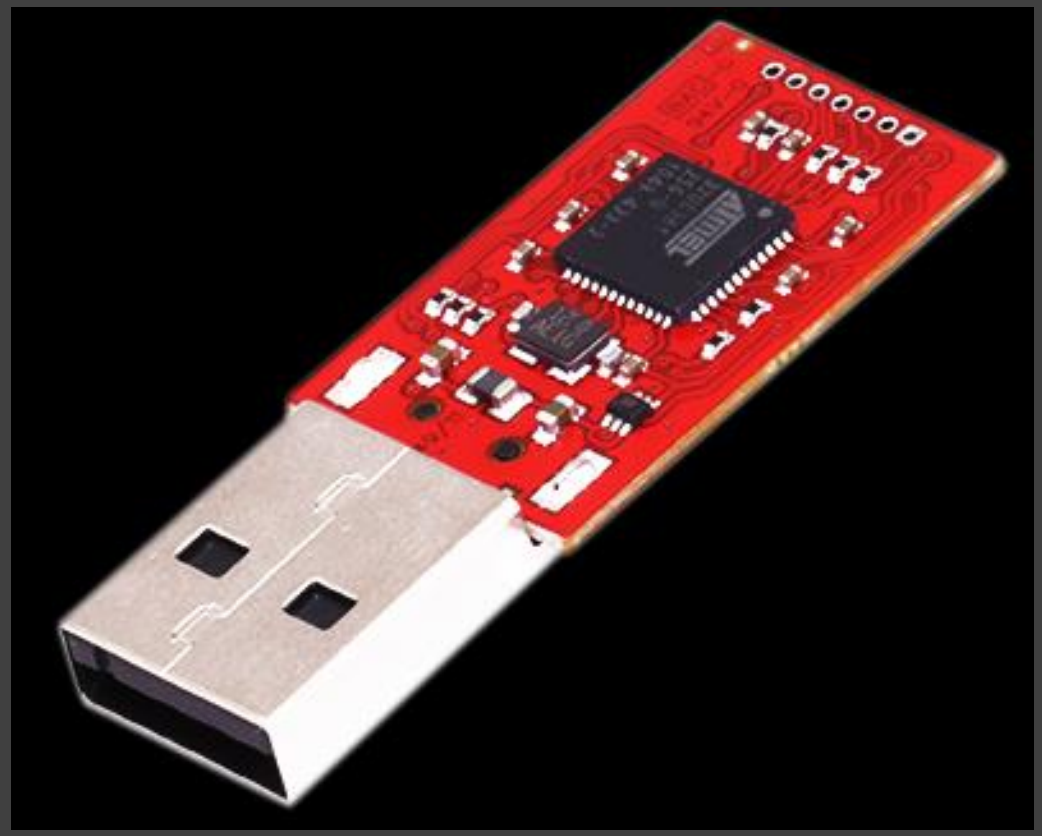
WiFi Pineapple nano



WiFi Pineapple nano



Rubber Ducky



USB Device
Verhält sich wie eine Tastatur

Rubber Ducky

Einfache „Scripsprache“

```
DELAY 5000
CONTROL ESCAPE
DELAY 100
STRING iexplore
http://www.betaarchive.co.uk/imageupload/1283877178.or.61533.jpg
ENTER
DELAY 4000
```

Online Payload Generator
https://ducktoolkit.com/

Rubber Ducky

Vorteil:
Kein spezielles Wissen für den „Anwender“ nötig
Tastatureingaben werden automatisiert übertragen

Nachteil:
Login muss gewährleistet sein
Unter Windows teilweise mit Powershellscripten
Und teilweise Administrativen Zugriff