

Bereich Elektrotechnik und Informatik

der Fakultät für Ingenieurwissenschaften
an der Hochschule Wismar

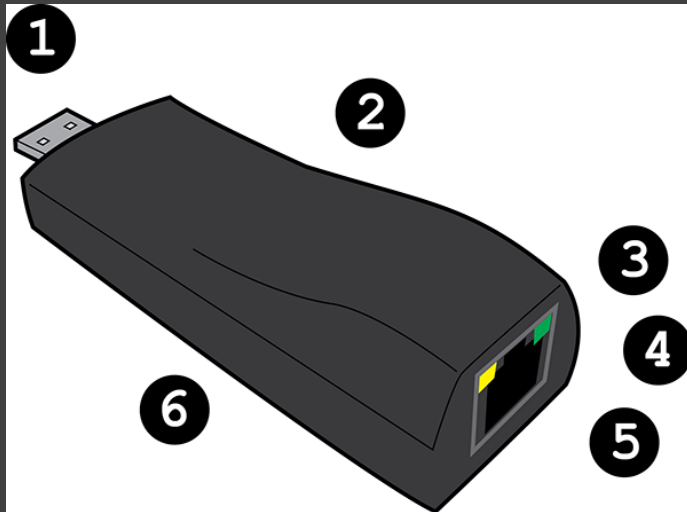
RubberDucky / LanTurtle / WifiPineApple

Hardware Hacking Tool Eine kleine Einführung

Dirk Zimmermann



Lan Turtle



```
172.16.84.1 - PuTTY
Turtle SSHell (v1)

Main Menu
  .-./*)
  _/_/_/_/ LAN TURTLE \/_/_/_/
  U U      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 DNSSpoofer 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 PC gesperrt ist,
die Benutzer Credential zu erfahren?



Lan Turtle

Es ist möglich

```
HTTP-NTLMv2-172.16.84.143.txt x
1 zimmermann::FIWI:1122334455667788:C1D8BFE410088DACA76729CF9E06A892:0101000000000000
2 zimmermann::FIWI:1122334455667788:C1D8BFE410088DACA76729CF9E06A892:0101000000000000
```



Lan Turtle

Aber nicht nur das, sonder auch

DNS Spoofing

MitM

Urlnarf usw.....



WiFi Pineapple nano

Verwendung

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



WiFi Pineapple nano

The screenshot displays the WiFi Pineapple nano dashboard. On the left is a vertical navigation menu with the following items: Dashboard, Recon, Clients, Filters, Modules (with a dropdown arrow), PineAP, Tracking, Logging, Reporting, Networking, Configuration, Advanced, and Help. The main content area features three large summary cards at the top: 'Uptime' showing 0 hours, 1 minute with a sub-section for 42% CPU usage; 'Clients Connected' showing 0; and 'SSIDs in Pool' showing 12 with a sub-section for 0 SSIDs added this session. Below these are three smaller panels: 'Landing Page Browser Stats' (No Landing Page Browser Stats Available), 'Notifications' (No Notifications), and 'Bulletins' (Load Bulletins from WiFiPineapple.com).

Uptime	Clients Connected	SSIDs in Pool
0 hours, 1 minute	0	12
42% CPU USAGE		0 SSIDS ADDED THIS SESSION

Landing Page Browser Stats
No Landing Page Browser Stats Available

Notifications
No Notifications

Bulletins
Load Bulletins from WiFiPineapple.com



WiFi Pineapple nano

The screenshot displays the WiFi Pineapple nano web interface. On the left is a sidebar menu with the following items: Clients, Filters, Modules (expanded), Manage Modules, DNSspoofer, Deauth, Evil Portal, Occupineapple, Online Hash Crack, Papers, and Portal Auth. The main content area is titled 'Controls' and includes a dropdown menu. Below this, the 'Dependencies' section shows a green 'Installed' button. The 'DNSspoofer' section features a dropdown menu with 'lo' selected, a green 'Start' button, and a toggle switch for 'Start on boot' currently set to 'OFF'. The 'Hosts' and 'Landing Page' sections are currently empty. The 'Output' section has an 'Auto-refresh' toggle set to 'OFF'. Below the output area is a filter input field containing the text 'Piped commands used to filter output (e.g. grep, awk)', a 'Clear Filter' button, and a 'Refresh Log' button. The output log itself shows the message 'DNSspoofer is not running...'.



Rubber Ducky



USB Device

Verhält sich wie eine Tastatur

Rubber Ducky

Einfache „Scriptsprache“

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

