Weapons of a Pentester
Understanding the virtual & physical tools used by white/black hat hackers
PRESENTER: Nick Aleks
Disclaimer

This presentation is intended for professional SECTOR attendees and may contain information, content or opinions that could offend overly sensitive persons.

I will showcasing and demoing tools that could be used to breach computers, networks, and security controls.

For those of you prone to overwhelming fear, don’t worry, by pouring a complete circle of salt around yourself and your computer, you can ensure that no harm will befall upon you or your pets.

By no means am I endorsing the illegal use of these tools.

No individuals, equipment or animals were harmed while developing this presentation.

I speak for no one, no one speaks for me.
Nick Aleks

@Nick_Aleks
nick@alekssecurity.com
Penetration Tester;

DEFCON Toronto – DC416
dc416.com
Organizer;
The Presentation
The right tool – for the right job

- The tools I will be show casing and demoing are not organized in any particular order.
- I gave this presentation in my first talk ever @ BSIDESTO 2015 (Weapons of a Hacker)
- In fact when Brain and Jackie asked me to give this talk I decided to add a few more tools to demo
The 10 Hacks

Today were hack'n:

- Hack Locks
- Hack Radio
- Hack Computers
- Hack Websites
- Hack Wi-fis
- Hack USBs
- Hack Frameworks
- Hack Browsers
- Hack IoT devices
- Hack RFID
Satisfaction Guaranteed
In order to promise you guys a great presentation experience this is what I have done

- Saved a bunch of good karma
- Haven’t had a drink in 24 hrs
- Sold Fred’s soul to the Demo Gods
- Popped a Senzu bean

---

**SACRIFICE AGREEMENT**

This Sacrifice Agreement ("Agreement") is made and effective:

**BETWEEN:**

FREDERIC DORRE (the "Sacrifier"), an individual with a soul

AND

DEMO GODS (the "Recipient of said soul"), the Demo Gods

The parties to this Agreement may be referred to individually as "Party" and jointly as "Parties."

**RECITALS**

A. The Seller is the owner of a soul and is willing to sell it to the Recipient;
B. The Recipient is willing to accept the Seller’s soul for the purpose of pleasing the Demo Gods between the time of 1:05 pm - 2:15 pm on the 15th of November at the INCTOR Security Education Conference in Toronto, Ontario. The Recipient does not disclose or resell the soul to any third party nor make use of the soul in any manner except as set out below.

**AGREEMENT**

The Parties agree as follows:

1. "Selling of the Soul" will be accepted by JAMES ARLEN on behalf of the Recipient (DEMO GODS). Upon successful signing of this agreement the soul shall be transferred from the Sacrifier to the Recipient.
2. "Effective Date" November 15, 2017 to Indefinitely

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date first above written.

On behalf of: On behalf of:
DEMO GODS: RECIPIENT

Authorized Signature Authorized Signature

James Arlen Frederic Dorre
Print Name Print Name
Hacking Locks
Physical Security
Pentesting physical security controls

Usually, when talking about computer or network security, most of the focus is, of course, on the digital side. We've talked about firewalls, intrusion detection systems, security software, and so on. But the physical side of security is often just as important, if not more. All the firewalls in the world won't help you if your server is hosted on premises, inside some closet where any customer or employee can go in, pick it up, and walk out the door. That's why things like locks, biometric scanners, and cameras are important.

2 Billion commercial and residential door locks are sold a year in the US.
The Art of picking
How does one pick a lock?

A tension wrench (or torque wrench) is used to apply a torque to the cylinder, while a lock pick (or picklock) is used to push individual pins up until they are flush with the shear line.

Raking or scrubbing a pin tumbler lock is usually done before individual pins are pushed up. While applying torque with the tension wrench, a lock pick with a wide tip is placed at the back of the lock and quickly slid outwards with upward pressure so all the pins are pushed up.
THE SNAP GUN

SPARROWS
LOCK PICKS
Snap gun
The automated lock picking gun

How does it work?
The snap gun strikes all of the bottom pins at once with a strong impact, and then withdraws again. The bottom pins transfer their kinetic energy to the top pins and come to a complete stop without penetrating the lock housing.

How long does it take?
10-30sec

If you have practices, and made the right sacrifices ;)
THE SNAP GUN DEMO...
Hacking Radio
Hacking RF Systems
Doors, Gates, Barriers, Cars, Comms

Radio Frequency Hacking
HAM radio hackers have been breaking into RF devices for years now. Billions of devices across North America utilize RF to operate. Typically these devices use sub 1 GHz frequency range.

RF signals use modulations (ASK, FSK, OOK) to transmit data.
Different RF Modulations
ASK, FSK, PSK

Fixed vs Rolling Codes
Some Radio Operated Security Controls
Doors, Gates, Barriers, Cars
**YARD Stick 1**

Sub 1GHz RF transmitter & receiver

**What is it?**

Yet Another Radio Dongle can transmit and receive digital wireless signals at frequencies below 1 GHz.

**Capabilities?**

- Half-duplex transmit and receive
- Mods: ASK, OOK, GFSK, 2-FSK, 4-FSK, MSK
- Data rates up to 500kbps
- Full-speed USB 2.0

**How does it work?**

YARD stick 1 comes with RfCat firmware installed. RfCAT allows you to interactively control the dongle with a python shell.
What are we hacking today Nick?
Oh I’ll show you
SHOW ME THE MONEY!!!!!!!
YARDSTICK 1
HACK DEMO
Hacking WIFI
(if that's the case, I have a lot of homes)
Wifiphisher

What is it?

Wifiphisher is a security tool that mounts automated phishing attacks against WiFi networks in order to obtain secret passphrases or other credentials. It is a social engineering attack that unlike other methods it does not include any brute forcing.

Step 1 • Victim becomes deauthenticated from their access point

Step 2 • Victim joins a rogue access point.

Step 3 • Victim is being served a realistic router config-looking page

Step 4 • Victim types password
Key Features

What makes this cool?

- All it takes is one person to fall for the attack and the entire network becomes compromised.
- Encryption type doesn’t matter. WEP/WPA/WPA2
- Open source. Python, HTML, CSS, JS
<table>
<thead>
<tr>
<th>num</th>
<th>ch</th>
<th>ESSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>xasaki</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>conn-xf41c18</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>Thomson06D09C</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
<td>BIG_B00BS</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>Wind WiFi 5V4Weg</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>Petter Pan</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>CONNX 1</td>
</tr>
<tr>
<td>8</td>
<td>6</td>
<td>CONN-X_6486</td>
</tr>
<tr>
<td>9</td>
<td>6</td>
<td>OTENET_6364</td>
</tr>
<tr>
<td>10</td>
<td>7</td>
<td>conn-xe0fc94</td>
</tr>
<tr>
<td>11</td>
<td>9</td>
<td>hol wifi</td>
</tr>
<tr>
<td>12</td>
<td>11</td>
<td>man-max</td>
</tr>
<tr>
<td>13</td>
<td>11</td>
<td>@Agra</td>
</tr>
</tbody>
</table>
Jamming Interface

Jamming devices:

DHCP Leases:
1433061912 40:f3:08:fb:3c:42 10.0.0.62 android-6c49980910fe9418 01:40:f3:08:fb:3c:42

HTTP requests:
[*] GET 10.0.0.62
[*] POST 10.0.0.62 wphshr-wpa-password=crippledblackphoenix

[] Closing
Router firmware upgrade
The Requirements
How can we start playing with wifiphisher

Needs

- Kali Linux
- Two wireless network cards, one capable of injection

TP-LINK TL-WN722N

- 150 Mbps
- 4dBi detachable antenna
- $12 on amazon
PROVE IT
Hacking Networks
The LAN Turtle
What is this little USB?

The LAN turtle is a covert Systems Administrative And Penetration testing tool.

It is a stealth remote access, network intelligence gathering and man-in-the-middle
Housed within a generic “USB Ethernet Adapter Case”, the LAN turtles appearance allows it to blend into many environments

Drop it on a LAN and access it from anywhere via SSH, Meterpreter and Open VPN.
Key Features

What makes you like turtles?

- Works like a standard USB Ethernet adapter, bridging the connection and powering the device
- Connects to any standard Ethernet network. Static or DHCP with the MAC address of your choice
- MITM DNSSpoofing attacks – phishing websites
- Pivot with a permanent meterpreter session in metasploit
Hack Computers
The USB Rubber Ducky - Intro

What is this little USB?

This little “thumb drive” takes social engineering to the next level – it isn’t really a usb... it’s a keyboard with a encoded payload that automatically types commands into the computer.

USB Rubber Ducky is a Keystroke Injection Platform
Key Features – Great Community
What makes this cool?

- Simple & Customize Pre-assembled attacks from online repositories
- Online tool kit for simple reconnaissance, scanning, exploration, and reporting
- **Simple ducky payload generator** for Linux with Password Cracker, Meterpreter and Netcat Integration
- Ducky-Decode firmware and encoder adding mass storage, multiple payloads, multilingual and much more
Use Cases

A review of some of the things you can use it for

**Recon**
- Computer Information
- User Information
- USB Information
- Shared Drive Information
- Program Information
- Installed Updates
- User Document List
- Basic Network Information
- Network Scan
- Port Scan
- Copy Wireless Profile
- Take Screen Captures
- Copy FireFox Profile
- Extract SAM File

**Exploitation**
- Find and Upload File (FTP)
- Disable Firewall
- Add User
- Open Firewall Port
- Start Wi-Fi Access Point
- Share C:\ Drive
- Enable RDP
- Create a Reverse Shell
- Local DNS Poisoning
- Delete a Windows Update

**Reporting**
- Save Report to Target Machine
- FTP Report to External Host
- Email Report to GMAIL Account
- Save Files to USB Drive
Ducky Price
Where to go if you want your own

Buy it here:

<table>
<thead>
<tr>
<th>Red Team Quantity</th>
<th>Price</th>
<th>Discount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buy 1</td>
<td>$42.99 ea</td>
<td>0% Off</td>
</tr>
<tr>
<td>Buy 2</td>
<td>$38.69 ea</td>
<td>10% Off</td>
</tr>
<tr>
<td>Buy 4</td>
<td>$36.54 ea</td>
<td>15% Off</td>
</tr>
<tr>
<td>Buy 8</td>
<td>$34.39 ea</td>
<td>20% Off</td>
</tr>
<tr>
<td>Buy 16</td>
<td>$32.24 ea</td>
<td>25% Off</td>
</tr>
</tbody>
</table>
The LAN Turtle

What is this little USB?

The LAN turtle is a covert Systems Administrative
And Penetration testing tool.

It is a stealth remote access, network intelligence
gathering
and man-in-the-middle
Housed within a generic “USB Ethernet Adapter Case”, the
LAN turtles appearance allows it to blend into many
environments

Drop it on a LAN and access it from anywhere via SSH,
Meterpreter and Open VPN.
Key Features
What makes you like turtles?

Works like a standard USB Ethernet adapter, bridging the connection and powering the device

Connects to any standard Ethernet network. Static or DHCP with the MAC address of your choice

Simple ducky payload generator for Linux with Password Cracker, Meterpreter and Netcat Integration

Open source downloadable modules (netcat, autossh,
Questions?