Hacking Demonstration
Dr John McCarthy Ph.D. BSc (Hons) MBCS
Deploying effective cyber security is one of the 21st century's greatest challenges for business.

The threats facing businesses in the digital sphere are increasing. Whilst awareness of cyber threats is growing an understanding of how we can combat these attacks fall short of the ideal.

We face a range of threat actors from governments and cyber criminals through to script kiddies. All of these present challenges.
Introduction

At this event, we will demonstrate a range of hacking techniques and methods commonly used to disrupt or gain entry into IT systems.

We will examine the attack vectors hackers use, and through practical demonstrations show how they achieve their goals.

Finally, we will offer solutions and guidance on how to mitigate the attacks demonstrates.
Cyber risk 'a clear and present danger', says Bank of England information security chief

He said that cyber risk should not be left to IT teams to manage on their own.

"The first thing is to get away from the perception that cyber is just a technology problem that can be solved entirely through engineering solutions,“

"There is a tendency for boards to look at it, fear that it’s too technical to understand, and then delegate the whole issue to technologists – who duly deliver some technological fixes.

The trouble with that is that most cyber-attacks are not exclusively – or even mainly – technical in nature. People and processes are every bit as important.
Unknowable Threat Landscape

There are well over 100,000 known computer viruses

Anti-virus is only 50% effective at best

Anti-virus will not protect against zero day attacks

Life is getting easier for the hackers and harder for us
The Internet of Things

8.7 billion connected devices in 2012

50 billion devices will be connected by 2020

Due to the nature of the networks we need to protect them globally

Whilst a great deal can be done to protect an individual port.

Ultimately all networks are connected and therefore have to be viewed in this way.
Cyberspace has become the fifth domain of warfare, after land, sea, air and space.

Infiltrating networks is pretty easy for those who have the will, the means and the time to spare.

Governments know this because they are such enthusiastic hackers themselves. Penetrating networks to damage them is not much harder. And, if you take enough care, nobody can prove you did it.
Hacking Search Engines

Expose online devices.
Webcams, routers, power plants, iPhones, wind turbines, refrigerators, VoIP phones.

Take a Tour  Free Sign Up
# Hacker Sites on the Dark web

## Forum

<table>
<thead>
<tr>
<th>Forum</th>
<th>Threads</th>
<th>Posts</th>
<th>Last Post</th>
</tr>
</thead>
<tbody>
<tr>
<td>Announcements</td>
<td>8</td>
<td>241</td>
<td>Forum Updates And Change...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>02-27-2017 by Admin</td>
</tr>
<tr>
<td>Introductions</td>
<td>1,074</td>
<td>2,478</td>
<td>Hulu intro</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>03-04-2017 by july</td>
</tr>
<tr>
<td>Cyber News</td>
<td>424</td>
<td>1,056</td>
<td>Google performs fine restructuring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>03-28-2017 by Adag</td>
</tr>
<tr>
<td>Offtopic</td>
<td>302</td>
<td>1,429</td>
<td>Sigant Mail issues?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yesterday by octopush2</td>
</tr>
<tr>
<td>Newbie Questions</td>
<td>269</td>
<td>1,262</td>
<td>good temp email provider</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>02-03-2017 by <em>M1S4003</em></td>
</tr>
</tbody>
</table>

## Marketplace

<table>
<thead>
<tr>
<th>Forum</th>
<th>Threads</th>
<th>Posts</th>
<th>Last Post</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVV / Fullz / Dumps</td>
<td>20</td>
<td>618</td>
<td>Goodwin's Luxury Quality...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Today by enterprise</td>
</tr>
<tr>
<td>Accounts / Logs</td>
<td>2</td>
<td>120</td>
<td>Payzal 4 sell</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>03-01-2017 by 9111111</td>
</tr>
<tr>
<td>Security Services</td>
<td>2</td>
<td>55</td>
<td>Professional anonymous V...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>03-03-2017 by phpthreads</td>
</tr>
<tr>
<td>Hosting / Spam / Traffic</td>
<td>1</td>
<td>38</td>
<td>Email Spam Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>02-11-2017 by D3132</td>
</tr>
<tr>
<td>Malwares / Exploits / Crypters</td>
<td>7</td>
<td>393</td>
<td>Medusa IRC DDoS Botnet RT</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>03-01-2017 by Johannith126</td>
</tr>
<tr>
<td>Other Services</td>
<td>2</td>
<td>24</td>
<td>Layer 7 HTTP DDoS - $25/4...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yesterday by max20000</td>
</tr>
<tr>
<td>Unverified Sales</td>
<td>392</td>
<td>1,782</td>
<td>Web Based Bunch Exploits...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>03-02-2017 by jck</td>
</tr>
<tr>
<td>Wanted Section / Job Offers</td>
<td>421</td>
<td>1,454</td>
<td>swap cracks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>02-01-2017 by deadmausoci</td>
</tr>
</tbody>
</table>
The Attack Vectors

**Reconnaissance** - Google Dorking

**Reputational Damage** – Defacing of Corporate website

**Breaking the Perimeter** – Compromising a network device

**Network Disruption and Corruption** - DNS poisoning

**Social Engineering** – The consequences of gaining physical access

**Physical Hacking Tools** Rubber Ducky - Kon-Boot - Lan Turtle
Reconnaissance
Open-source intelligence (OSINT) is intelligence collected from publicly available sources.

In the intelligence community (IC), the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources)

It is not related to open-source software or public intelligence.
Tools Hackers May Use

Hackers can spend months undertaking data gathering about your company.

Common Tools

Maltego
Shodan
Social Engineer Toolkit
Google Hacking Database
Google Dorks
Google Dorks

Google Dorking, is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use.

Done carefully the website will never know you have visited it by using the google cached pages.
A Google dork is a search string that uses advanced search operators to find information that is not readily available on a website.

**site:** returns files located on a particular website or domain.

**filetype:** followed (without a space) by a file extension returns files of the specified type, such as DOC, PDF, XLS and INI. Multiple file types can be searched for simultaneously by separating extensions with “|”.

**inurl:** followed by a particular string returns results with that sequence of characters in the URL.

**intext:** followed by the searcher’s chosen word or phrase returns files with the string anywhere in the text.

**site:**targetwebsite.com **inurl:**admindork

```plaintext
site:publicintelligence.net filetype:pdf intext:“sensitive but unclassified”
```
The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers.

Our aim is to serve the most comprehensive collection of exploits gathered through direct submissions, mailing lists, as well as other public sources, and present them in a freely-available and easy-to-navigate database.
# Google Dork Examples

<table>
<thead>
<tr>
<th>Date</th>
<th>Title</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-03-03</td>
<td>inurl:/profile.php?lookup=1</td>
<td>Files Containing Usernames</td>
</tr>
<tr>
<td>2017-03-02</td>
<td>&quot;your default password is&quot; filetype:pdf</td>
<td>Files Containing Passwords</td>
</tr>
<tr>
<td>2017-03-01</td>
<td>inurl:&quot;reset:-pwd &quot; ~ User&quot;</td>
<td>Pages Containing Login Portals</td>
</tr>
<tr>
<td>2017-03-01</td>
<td>extsvc.inurlbwsdl</td>
<td>Web Server Detection</td>
</tr>
<tr>
<td>2017-03-01</td>
<td>inurl:$filesrc=**** ~&quot;Current&quot; ~&quot;asp&quot;</td>
<td>Footholds</td>
</tr>
<tr>
<td>2017-03-01</td>
<td>inurl:&quot;Admin:.aspx )&quot; &quot;~Login&quot;</td>
<td>Pages Containing Login Portals</td>
</tr>
<tr>
<td>2017-02-24</td>
<td><em>CF-Host-Origin-IP</em> <em>CF-Int-Brand-ID</em> <em>CF-RAY</em> <em>CF-Visitor</em> <em>github</em> *site:github.com *site:cloudflare.com</td>
<td>Advisories and Vulnerabilities</td>
</tr>
<tr>
<td>2017-02-23</td>
<td>Ittrack inurl:hts-log.txt exttxt -github.com</td>
<td>Files Containing Juicy Info</td>
</tr>
<tr>
<td>2017-02-16</td>
<td>inurl:sendmessage.php?type=skype</td>
<td>Advisories and Vulnerabilities</td>
</tr>
<tr>
<td>2017-02-14</td>
<td>intitle:&quot;Login - OpenStack Dashboard&quot; inurl:&quot;dashboard&quot;</td>
<td>Pages Containing Login Portals</td>
</tr>
</tbody>
</table>
Demonstration 1 – Using Google Dorks
Defacing of a Corporate website

Forbes
Japanese Govt
Barack Obama
What's app
HSBC
Ashley Madison
Trump Hotels
Reputational Damage

- Loss of income
- Bad PR
- Lack of Public trust
- Brand Erosion
- Potential Law suits
- Crisis Management
- Increased expenditure
Demonstration 2 – Defacing a Website

KNOW YOUR ENEMY
Breaking the Perimeter - Compromising a network device
Breaking the Perimeter - Compromising a network device

Consequences

Man in the Middle attacks

Complete ownership

Entry into the corporate network.

Full control of network traffic for whatever is behind the router and access to that infrastructure.

Deploying a Kali on the network
Demonstration 3 – Breaking the Perimeter
Network Disruption and Corruption

DNS cache Poisoning
DNS Poisoning

Consequences

Steal usernames and passwords
Redirect to fake sites
Steal credit information etc.
Redirecting to exploit kits
Once they are past Physical security its game over….

Commercial Tools Hackers may use

**Kon-Boot** – bypass windows, mac and Linux login

**Rubber Ducky** – run scripts “as a keyboard”

**Lan Turtle** – create a shell with remote access
Demonstration 5 – Commercial Hacking Tools

USB Rubber Ducky

- Write
- Encode
- Load
- Deploy

The most lethal tool ever to grace an unsuspecting USB port.

- Write script with a simple scripting language or valve packed payload including:
  - WinAPI with detailed trojan
  - Ransom, shell, binary launch
  - PowerShell, ninja tools injection
  - Powershell config & execute
  - Create WINPE and SYSTEM

- Encode
  - Crack x32 and x64 version
  - Crack x32 and x64 version

- Load
  - Run the script on the USB drive
  - Pre-cache the payload

- Deploy
  - Pre-cache the payload
  - Load the payload

The Rubber Ducky delivers the script to the USB drive, and the payload is executed in seconds.

KON-BOOT

USB Bootable Remedy for lost passwords

- Remedy for lost passwords
- USB bootable solution
- Simplicity and ease of use

KON-BOOT is a secure solution for recovering lost passwords, offering a simple and efficient approach to address this common issue.
Don’t underestimate physical security

Train all your staff to be aware of Social engineering techniques – and remind them!

Over 80% of all hacks involve humans

Never forget the basics – patch management etc.

Good Network management can do a great deal to help

The necessity of disk encryption

Good Cyber Security is a cycle not an end point

Good practice can do much to alleviate the problem