

## Did Anyone Get the Name of That Hacker Who PWNED Me?

Lance Cottrell  
Ntrepid / Anonymizer

Session ID: BR-F43

Session Classification: Intermediate

Security in  
knowledge



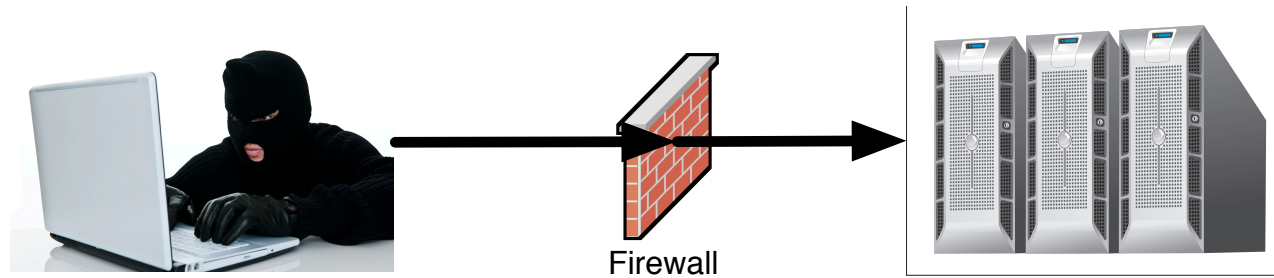
# When You Are Under Attack

You may ask:



**Did Anyone Get the Name of  
That Hacker Who PWNED Me?**

# As a Defender, You See....



IP: 37.123.118.67

Lat / Long: +54 / -2

Country: UK

Ping: 110ms

ISP: as13213.net (AKA UK2.net) server hosting

Open Ports: SSH, HTTP

# Was That Really the Attacker?





# What If You Could Spot People Hiding?

- ▶ Block Web Access
- ▶ Redirect to Honeypot
- ▶ Add Firewall Rule
- ▶ Deny Credit Card
- ▶ Flag in Logs



# How Do They Hide?

- ▶ Proxies
- ▶ VPNs
- ▶ Chained VPNs / TOR
- ▶ Botnets / Compromised Hosts
- ▶ Advanced Persistent Threats



# How You Can Spot Them

- ▶ Known Anonymity IP
- ▶ Open Proxy / VPN Ports
- ▶ Inappropriate / Non-consumer IP
- ▶ “Bulletproof” Host
- ▶ High Latency vs. Ping
- ▶ Protocol Leakage

## Track the Computer Itself



Your browser fingerprint appears to be unique among the 2,433,270 tested so far.  
Currently, we estimate that your browser has a fingerprint that collides at least 2.5 in a billion of existing references.  
The measurements we used to obtain this result are listed below. You can read more about our methodology, research tools, and some additional related fingerprinting in our [whitepaper](#).  
Help us increase our sample size: [Facebook](#) [Twitter](#) [LinkedIn](#)

# Browser Fingerprints

- ▶ Fingerprint May Stand Out
- ▶ Unusual OS / Browser
- ▶ System TOO Clean
- ▶ System TOO Hardened
- ▶ Lying In UserAgent String

Browser Characteristics	Value	Value
User Agent	10.2	10.2
OS	14.81	14.81
Browser Plugins	21.84	21.84
Time Zone and Clock Data	4.74	4.74
System Fonts	1.80	1.80
App Capabilities	0.43	1.34
Language	1	2

Learn about PanoptiClick and web tracking. [The PanoptiClick Privacy Policy](#). [Privacy Policy](#). [Learn about the Electronic Frontier Foundation](#).

# Virtualization Makes Your Job Harder

Advantages	Disadvantages
Easy to Clean	Cloned Each Time
No Cookies or Super-Cookies	Too Clean or Outdated Cruft
Detection as VM Requires Local Execution	Can Be Detected as VM

# Fortunately (for you), Good OPSEC is Hard

- ▶ Tools can be slow and cumbersome
- ▶ May go direct for “innocent” activity / reconnaissance
- ▶ May forget to use it
- ▶ Accidentally cross the streams of personas
- ▶ Correlate attacker print with all previous activity



# Why Should YOU be Stealthy

- ▶ Lurk in IRC and Forums
  - Discover Plans
  - Learn Techniques
  - Hide your interest & activity
- ▶ Bait Honeypots
  - Drop False Leads and Links
- ▶ Government
  - Has Other More Aggressive Options

# 10 Tips for Defender Stealth Part 1

1. Using a known anon IP is good
2. Use only VPN type privacy services
3. Use a VM for identity isolation and malware prevention
4. Use a different VM for each identity / activity
5. Vary your appearance and fingerprint for each VM

# 10 Tips for Defender Stealth Part 2

6. Files on the VM are definitionally contaminated
7. Check for DNS leakage
8. Ensure no local network or device is visible from the VM
9. Change clock, time zone, language, as appropriate
10. Stay on the right side of the law

# Thanks

Contact me at:

Email: [lance.cottrell@ntrepidcorp.com](mailto:lance.cottrell@ntrepidcorp.com)

Commercial / Gov: <http://ntrepidcorp.com>

Consumer: <http://anonymizer.com>

Blog: <http://theprivacyblog.com>

Twitter: @LanceCottrell

LinkedIn: <http://linkedin.com/in/LanceCottrell>

