Ethical Hacking: Understanding Your Enemy's Tactics

- Understanding how attacks work is one of the most challenging aspects of defensive security.
- By familiarizing yourself with how hackers think and operate, you can better tailor your organisation's defences to emerging threats and trends.
- If you don't test defences against attacks, the only people who will be testing your network will be the bad guys.
- By learning offensive security, you will be able to test your defences and determine which aspects are operating correctly and where any gaps exist.

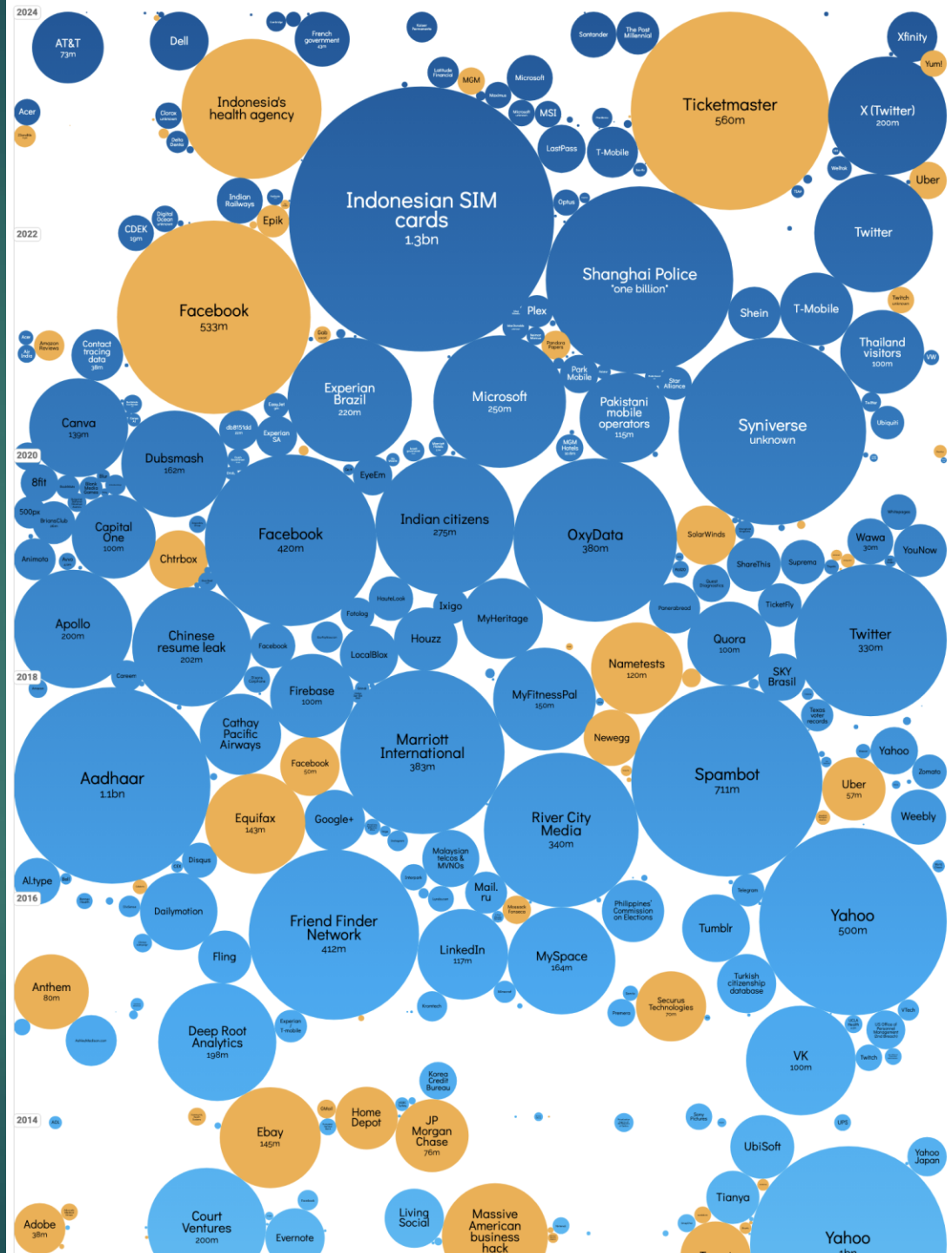
Hacker Motivation

- The criminal community is changing.
- Over the last few years, their motivation has evolved from the thrill of figuring out how to exploit vulnerabilities to figuring out how to make revenue from their actions and getting paid for their skills.
- Attackers who were out to “have fun” without any real target in mind have, to a great extent, been replaced by people who are serious about benefiting financially from their activities.
- Attacks are getting not only more specific, but also increasingly sophisticated.

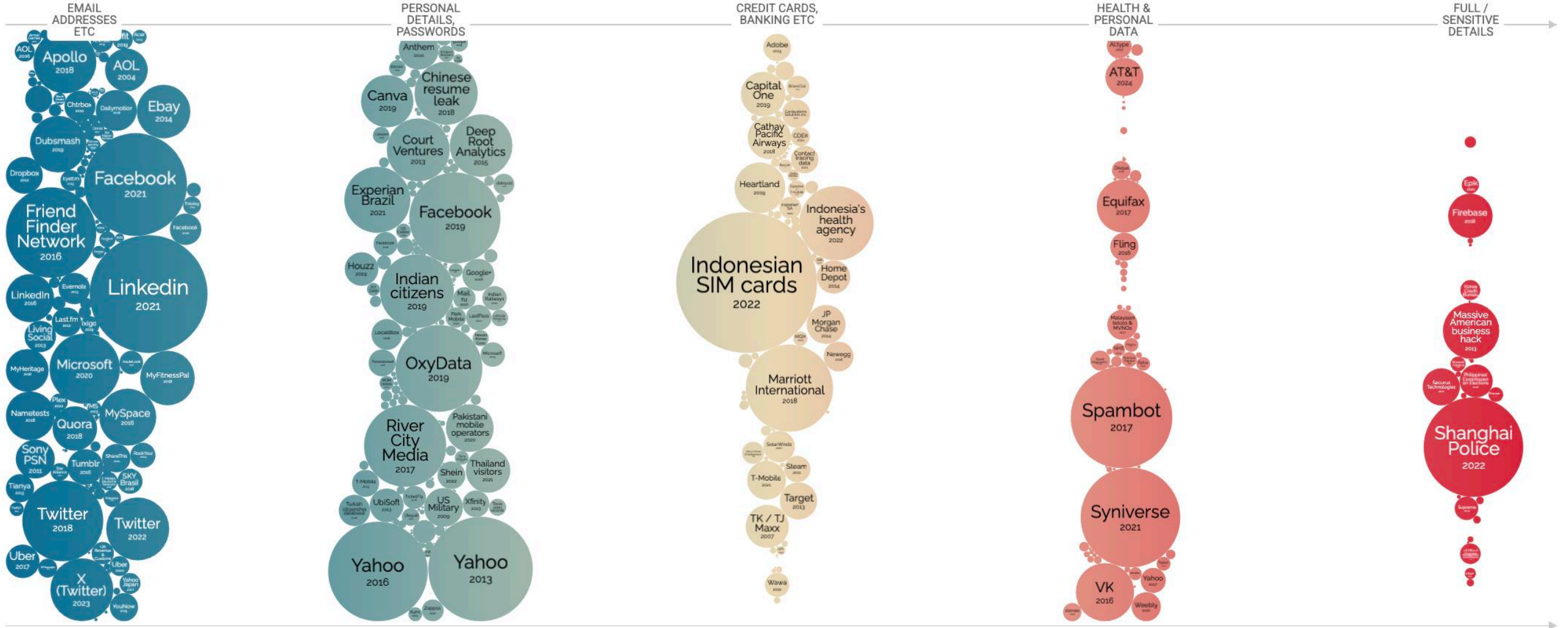
Sample Data Breaches

- In June 2024, 560 million records stolen from Ticketmaster including names, addresses, phone numbers, emails, purchases, and partial credit card numbers
- In July 2022, the data of over 1 billion Chinese nationals was stolen from the Shanghai Police. The stolen data included including names, addresses, places of birth, resident ID card numbers, phone numbers, photos, mobile phone numbers and information of criminal cases. It sold for 10 bitcoins.
- In March 2021, 533 million accounts had their data stolen from Facebook including phone numbers, full names, locations, email addresses, and biographical information.

- Graphic shows data breaches from 2010-Date
  - Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



Data Breaches by Data Sensitivity



Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Hacktivism

- In addition to attackers who are trying to profit, some attackers are politically motivated.
  - These attacks are labeled hacktivism.
- Both legal and illegal methods can be used to portray political ideology.
  - Is it right to try to influence social change through the use of technology?
  - Is web defacement covered under freedom of speech?
  - Is it wrong to carry out a virtual "sit in" on a site that provides illegal content?
  - As a response against 2022 Russian invasion of Ukraine, Anonymous performed multiple cyberattacks against Russian computer systems.
- One's viewpoint often determines what is ethical or not.

Zero-Day Attacks

- Some attackers also create and sell zero-day attacks.
- A zero-day attack is one for which there is currently no fix available.
- Whoever is running the particular software that contains that exploitable vulnerability is exposed, with little or no protection.
- The code for these types of attacks are advertised on special websites and sold to other attackers or organized crime rings.

Identifying Attacks

- Network administrators, engineers, and security professionals must be able to recognize when an attack is underway or when one is imminent.
- It may seem like it should be easy to recognize an attack as it is happening—but only for the very "noisy" or overwhelming attacks such as denial-of-service (DoS) attacks.
- Many attackers fly under the radar and go unnoticed by security devices and security staff. By knowing how different types of attacks work, you can properly recognize and stop them.

Predicting Attacks

- If network staff is educated on attacker techniques and they see a ping sweep followed a day later by a port scan, administrators know their systems may soon be under attack.
- Many activities lead up to different types of attacks, so understanding these will help a company protect itself.
- The argument can be made that we now have more automated security products that identify these types of activities -- so we don't have to see them coming.
  - But, depending on the software, those activities may not be put in the necessary context and the software may make a dangerous decision.
  - Computers can outperform any human on calculations and repetitive tasks, but we still have the ability to make necessary judgment calls because we understand the grays in life and do not just see things in 1s and 0s.

Hacking Tools

- Hacking tools are really just software tools that carry out some specific types of procedure to achieve a desired result.
- The tools can be used for good (defensive) purposes or for bad (offensive) purposes.
- The good and the bad guys use the same exact toolset; the difference is their intent when operating these tools.
- It is imperative for security professionals to understand how to use these tools and how attacks are carried out if they are going to be of any use to their customers and to the industry.

The Ethical Hacking Process

- To protect themselves, organisations may want to understand the impact and ability of an attacker. In this case, they may employ an ***ethical hacker***, also known as a ***penetration tester***, to simulate an attack against the environment.
- The techniques that penetration testers employ are designed to emulate those of real attackers without causing damage; they enable organisations to better protect themselves against attack.
- But customers and aspiring hackers need to understand how this process works.

Ethical Hacking vs. Vulnerability Assessment

- These activities have different goals, but are often confused with one another.
- During a vulnerability assessment, some type of automated scanning product is used to probe the ports and services on a range of IP addresses.
  - Most of these products can also test for the type of operating system and application software running and the versions, patch levels, user accounts, and services that are also running.
  - These findings are matched up with correlating vulnerabilities in the product's database.
  - The end result is a large pile of data that basically states, "Here is a list of your vulnerabilities and here is a list of things you need to do to fix them."

Ethical Hacking vs. Vulnerability Assessment

- The problem with most vulnerability scans is, although they indicate the severity of a vulnerability, they rarely indicate its impact.
- This is where penetration testing comes in.
- Vulnerability scanning allows you to identity a piece of software as being vulnerable to exploit; a ***penetration test*** takes this further by exploiting vulnerabilities and, for example, accessing sensitive information.
- Most vulnerability scanners indicate what might be vulnerable based on versioning and some more invasive checks, but a penetration test indicates whether the vulnerability scanner finding is real or a false positive.

pwned

- When penetration testers attack, their ultimate goal is usually to break into a system and hop from system to system until they "own" the domain or environment.
- Unlike a vulnerability assessment, a penetration test does not stop with the identification of a possible vulnerability.
- Penetration testers leverage identified vulnerabilities until they own the domain or environment.
  - Being "owned" means either having root privileges on the most critical Unix or Linux system or owning the domain administrator account that can access and control all of the resources on the network.
- Testers do this to show the customer (company) what an actual attacker can do under the circumstances and the network's current security posture.

Pen Testing Process

1. Ground Rules

- Set expectations and contact information between testers and customers.
- Identify the parties involved and who is aware of the test.
- Set start and stop dates and blackout periods.
- Get formalized approval and a written agreement, including scope, signatures, and legal requirements, frequently called a ***Statement of Work (SOW)***.

2. Passive Scanning

- Gather as much information about the target as possible while maintaining zero contact between the penetration tester and the target.
- Passive scanning, otherwise known as Open Source Intelligence (OSINT), can include:
  - Social networking sites
  - Online databases
  - Google, Monster.com, etc.
  - Dumpster diving

3. Active Scanning and Enumeration

- Probe the target's public exposure with scanning tools, which might include:
  - Commercial scanning tools
  - Network mapping
  - Banner grabbing
  - War dialing
  - DNS zone transfers
  - Sniffing traffic
  - Wireless war driving

4. Fingerprinting

- Perform a thorough probe of the target systems to identify:
  - Operating system type and patch level
  - Applications and patch level
  - Open ports
  - Running services
  - User accounts

5. Select Target System

- Identify the most useful target(s).

6. Exploiting the Uncovered Vulnerabilities

- Execute the appropriate attack tools targeted at the suspected exposures
  - Some may not work.
  - Some may kill services or even kill the server.
  - Some may be successful.

7. Exploiting Privilege

- Escalate the security context so the ethical hacker has more control.
  - Gaining root or administrative rights
  - Using cracked password for unauthorized access
  - Carrying out buffer overflow to gain local versus remote control

8. Documenting and Reporting

- Document everything:
  - What was found
  - How it was found
  - The tools that were used
  - Vulnerabilities that were exploited
  - The timeline of activities and successes
  - Etc.

What Would an Unethical Hacker Do Differently?

1. Target Selection
   - Motivated by a grudge or for fun or for profit.
   - There are no ground rules, no hands-off targets, and the security team is definitely blind to the upcoming attack.
2. Intermediaries
   - The attacker launches his attack from a different system (intermediary) than his own, or a series of other systems, to make it more difficult to track back to him in case the attack is detected.
   - Intermediaries are often victims of the attacker as well.

What Would an Unethical Hacker Do Differently?

3. Penetration testing steps described previously
   - Scanning
   - Fingerprinting
   - Selecting target system
   - Exploiting the uncovered vulnerabilities
   - Escalating privilege
4. Preserving Access
   - This involves uploading and installing a rootkit, backdoor, trojaned applications, and/or bots to assure that the attacker can regain access at a later time.

What Would an Unethical Hacker Do Differently?

5. Covering Tracks
   - Scrubbing event and audit logs
   - Hiding uploaded files
   - Hiding the active processes that allow the attacker to regain access
   - Disabling messages to security software and system logs to hide malicious processes and actions
6. Hardening the System
   - After taking ownership of a system, an attacker may fix the open vulnerabilities so no other attacker can use the system for other purposes.

What Would an Unethical Hacker Do Differently?

7. Not so much documentation