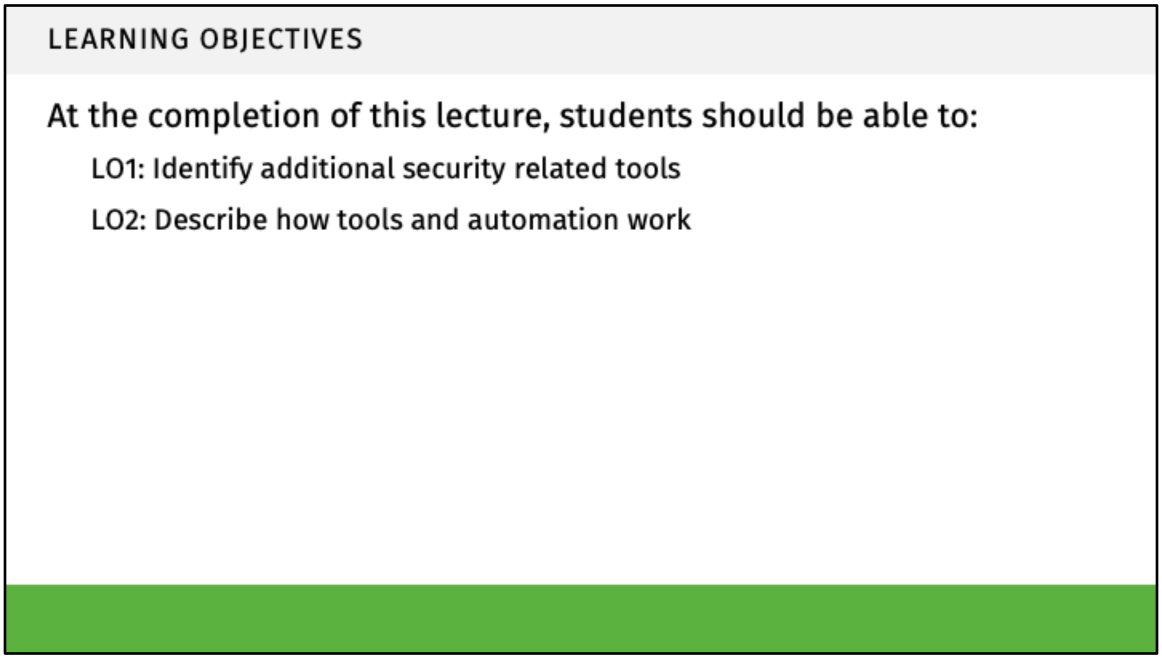
APP100

Tools and Tool creation



LEARNING OBJECTIVES

At the completion of this lecture, students should be able to:

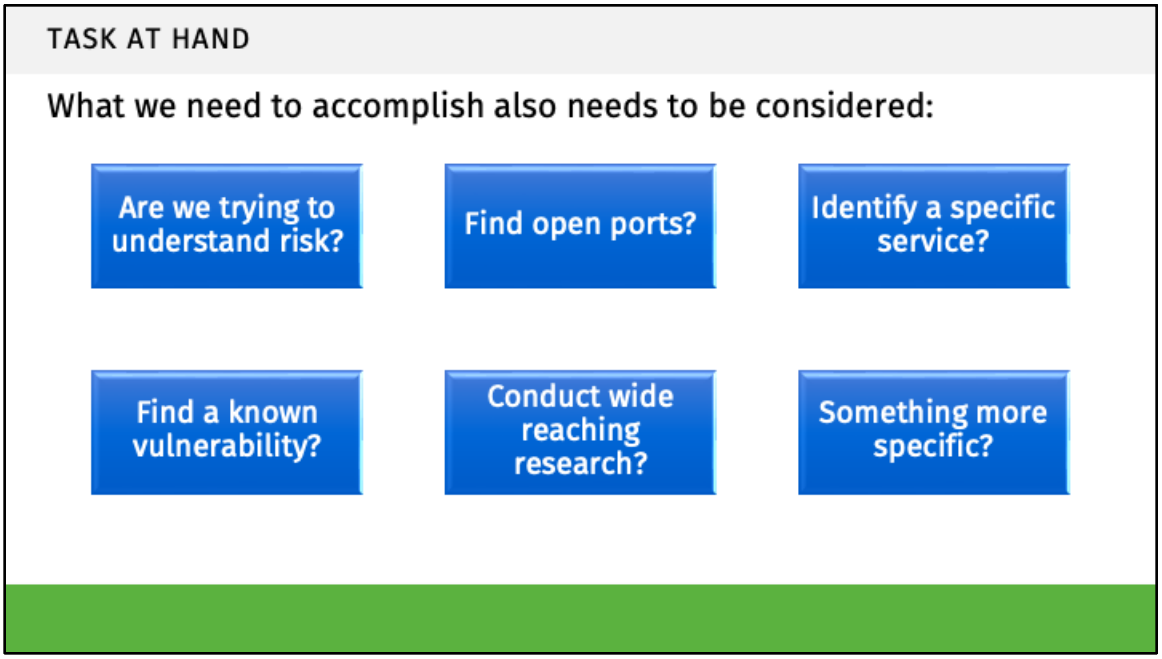
- LO1: Identify additional security related tools
- LO2: Describe how tools and automation work

TOOLS

Wielding the proper tool makes all the difference:

- Most tools are good for a small set of tasks
- OSINT tools
- Scanning tools
- Exploitation tools/frameworks
- Development tools
- Web technology discovery tools (Wappalyzer)

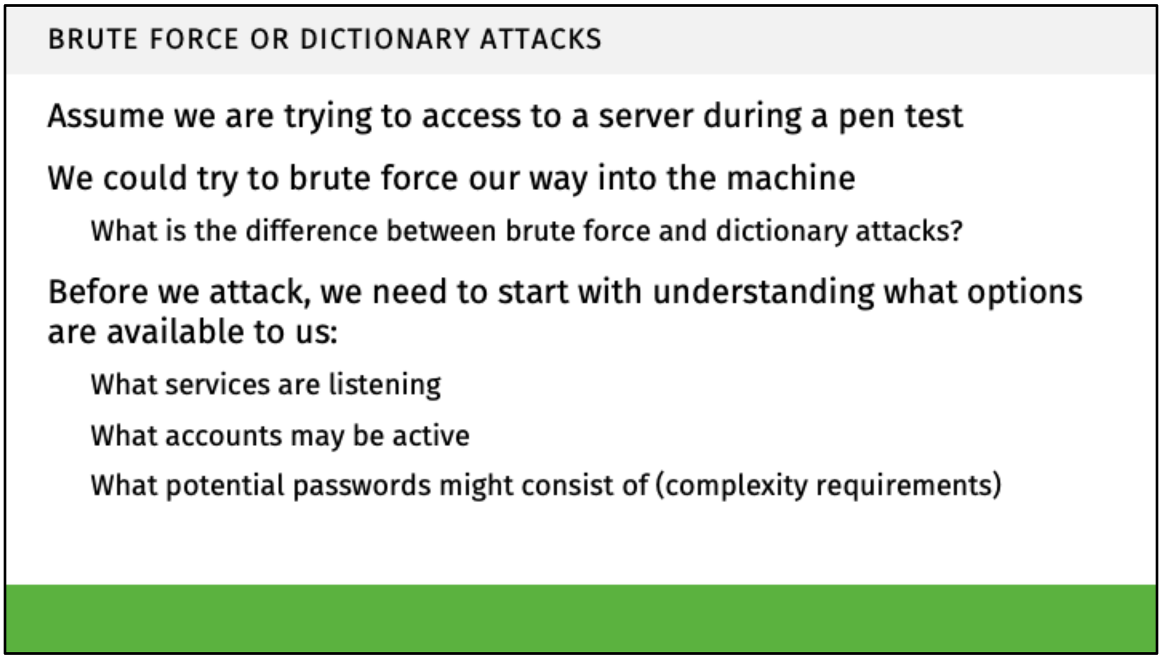
This Photo by Unknown Author is licensed under CC BY-NC



TASK AT HAND

What we need to accomplish also needs to be considered:

- Are we trying to understand risk?
- Find open ports?
- Identify a specific service?
- Find a known vulnerability?
- Conduct wide reaching research?
- Something more specific?



BRUTE FORCE OR DICTIONARY ATTACKS

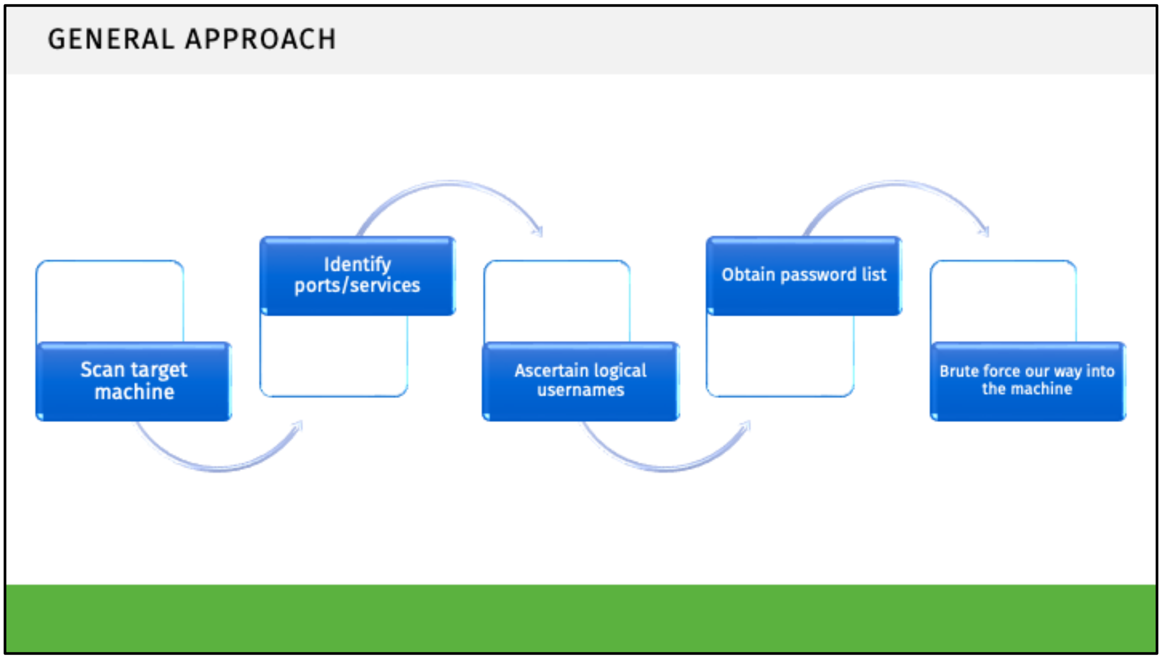
Assume we are trying to access to a server during a pen test

We could try to brute force our way into the machine

- What is the difference between brute force and dictionary attacks?

Before we attack, we need to start with understanding what options are available to us:

- What services are listening
- What accounts may be active
- What potential passwords might consist of (complexity requirements)



GENERAL APPROACH

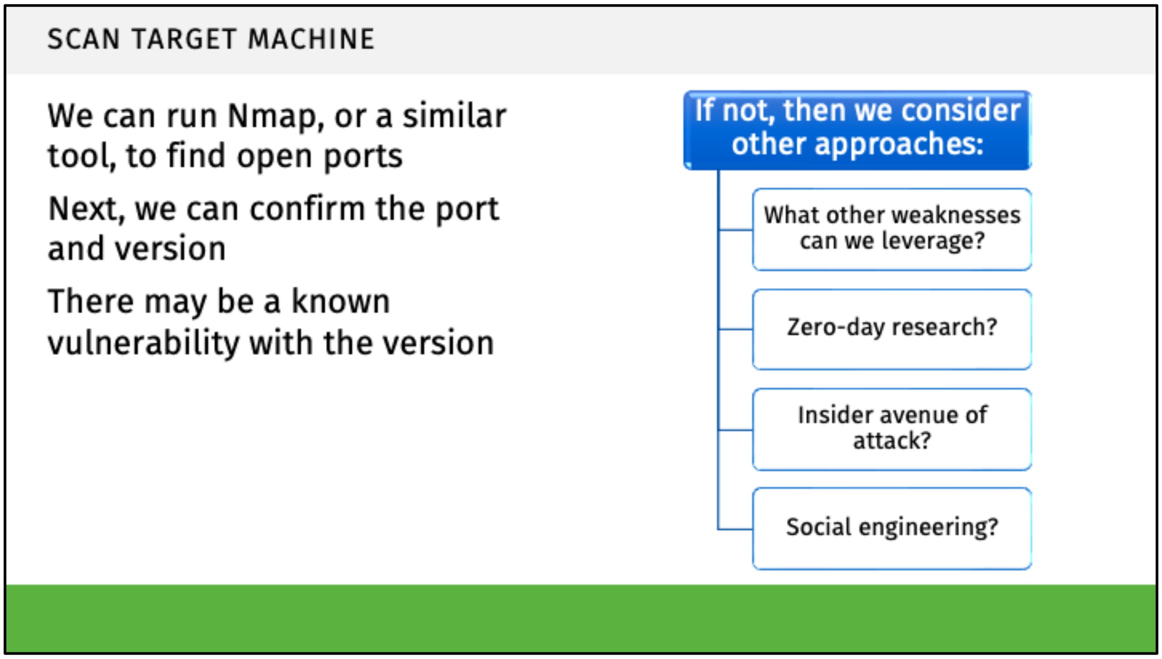
Scan target machine

Identify ports/services

Ascertain logical usernames

Obtain password list

Brute force our way into the machine



SCAN TARGET MACHINE

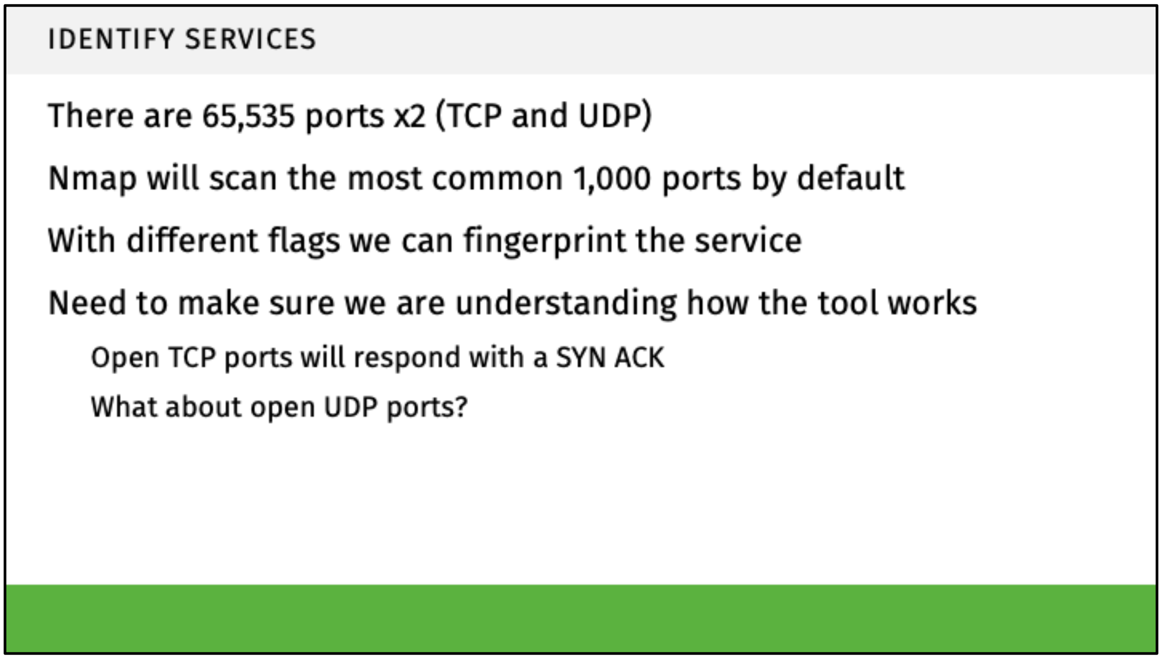
We can run Nmap, or a similar tool, to find open ports

Next, we can confirm the port and version

There may be a known vulnerability with the version

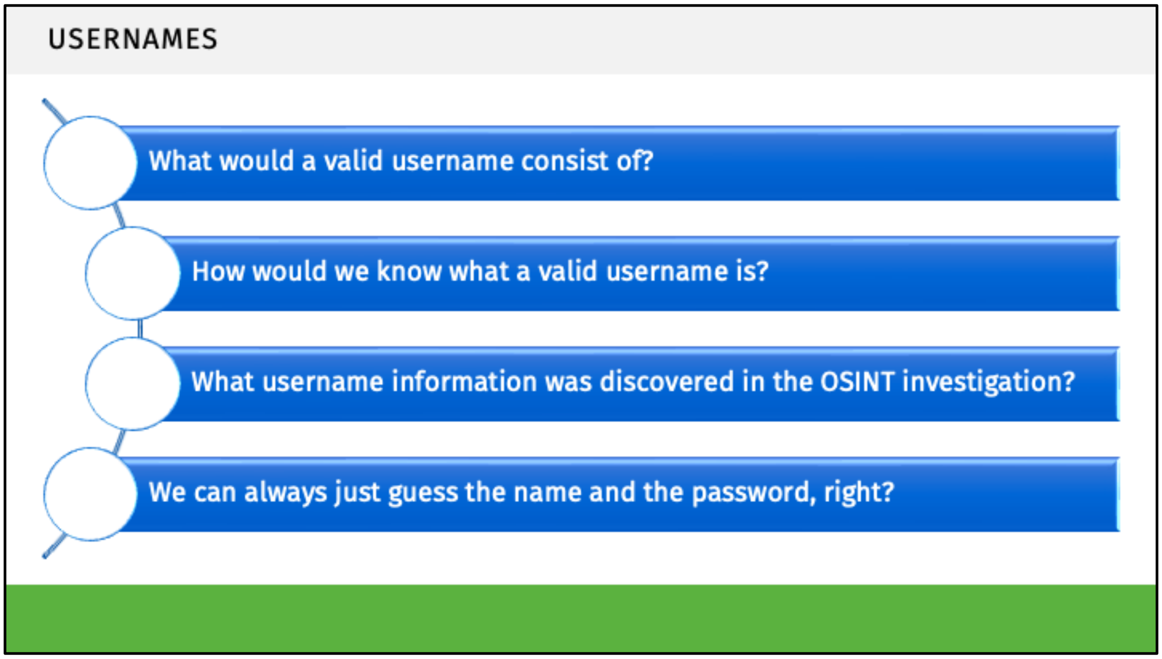
If not, then we consider other approaches:

- What other weaknesses can we leverage?
- Zero-day research?
- Insider avenue of attack?
- Social engineering?



IDENTIFY SERVICES

- There are 65,535 ports x2 (TCP and UDP)
- Nmap will scan the most common 1,000 ports by default
- With different flags we can fingerprint the service
- Need to make sure we are understanding how the tool works
  - Open TCP ports will respond with a SYN ACK
  - What about open UDP ports?



USERNAMES

- What would a valid username consist of?
- How would we know what a valid username is?
- What username information was discovered in the OSINT investigation?
- We can always just guess the name and the password, right?

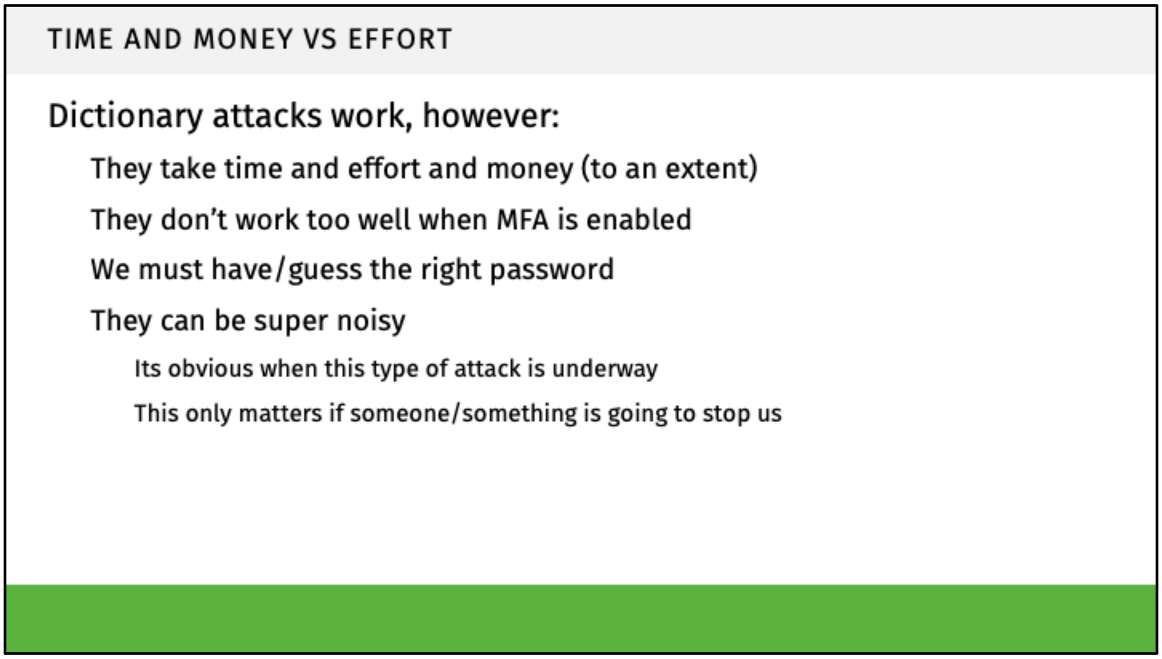
PASSWORD LISTS

Built into Kali by default

Online resources also have large lists of password

Data breach results can be useful for stuffing attacks

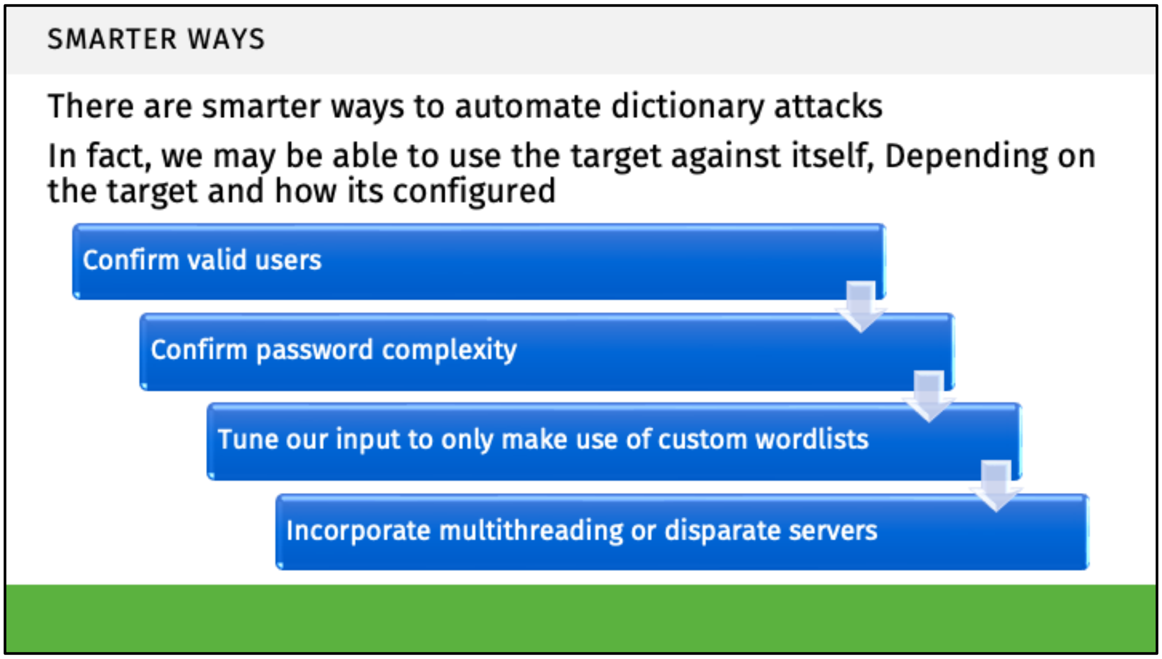
This Photo by Unknown Author is licensed under CC BY



TIME AND MONEY VS EFFORT

Dictionary attacks work, however:

- They take time and effort and money (to an extent)
- They don’t work too well when MFA is enabled
- We must have/guess the right password
- They can be super noisy
  - Its obvious when this type of attack is underway
  - This only matters if someone/something is going to stop us

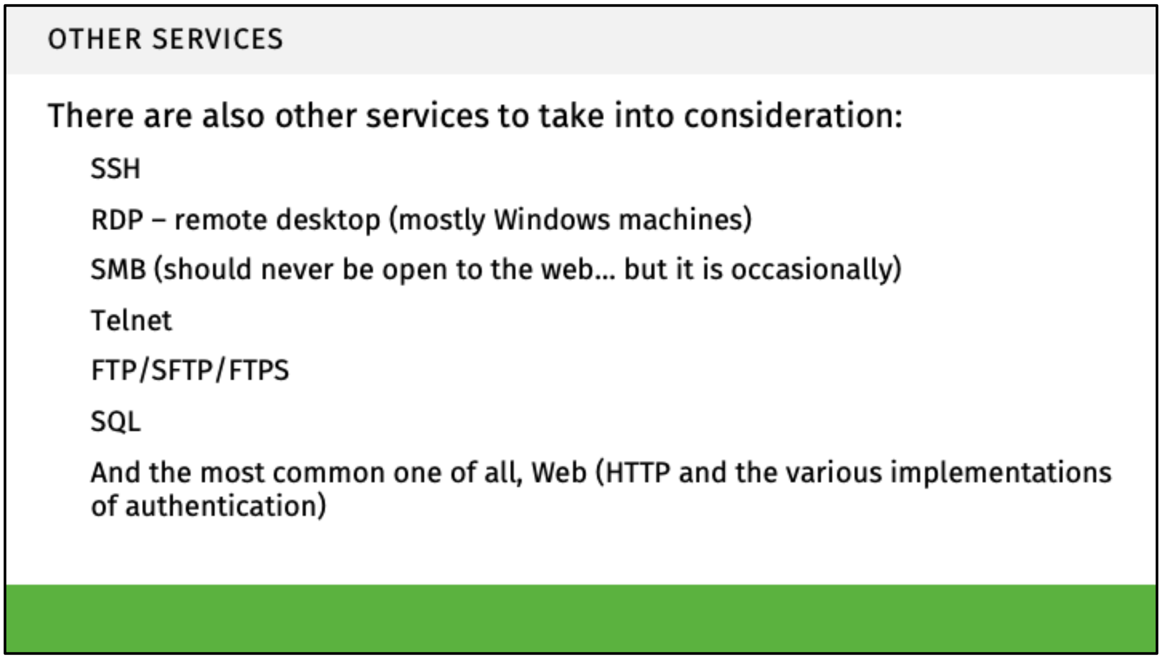


SMARTER WAYS

There are smarter ways to automate dictionary attacks

In fact, we may be able to use the target against itself, Depending on the target and how its configured

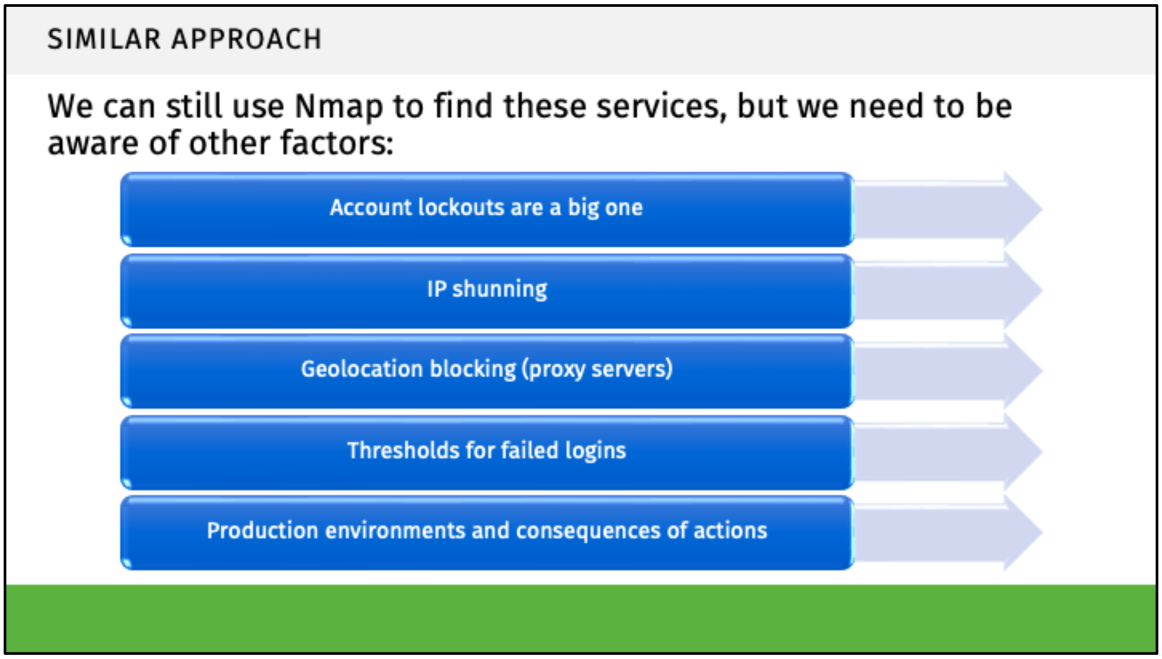
- Confirm valid users
- Confirm password complexity
- Tune our input to only make use of custom wordlists
- Incorporate multithreading or disparate servers



OTHER SERVICES

There are also other services to take into consideration:

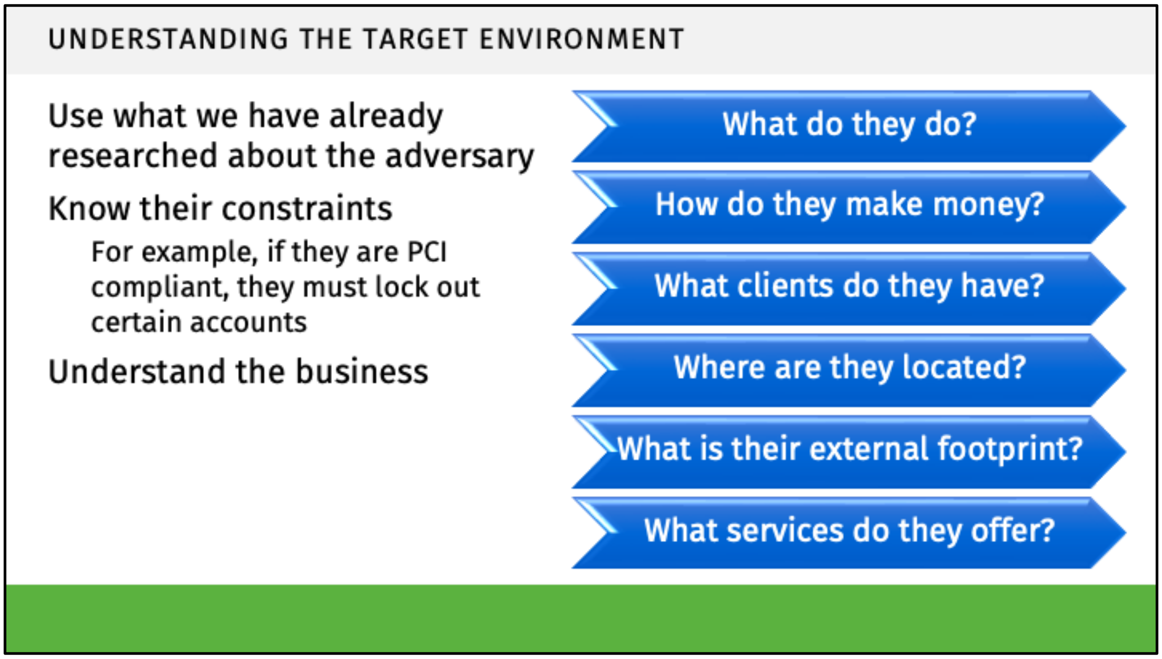
- SSH
- RDP – remote desktop (mostly Windows machines)
- SMB (should never be open to the web… but it is occasionally)
- Telnet
- FTP/SFTP/FTPS
- SQL
- And the most common one of all, Web (HTTP and the various implementations of authentication)



SIMILAR APPROACH

We can still use Nmap to find these services, but we need to be aware of other factors:

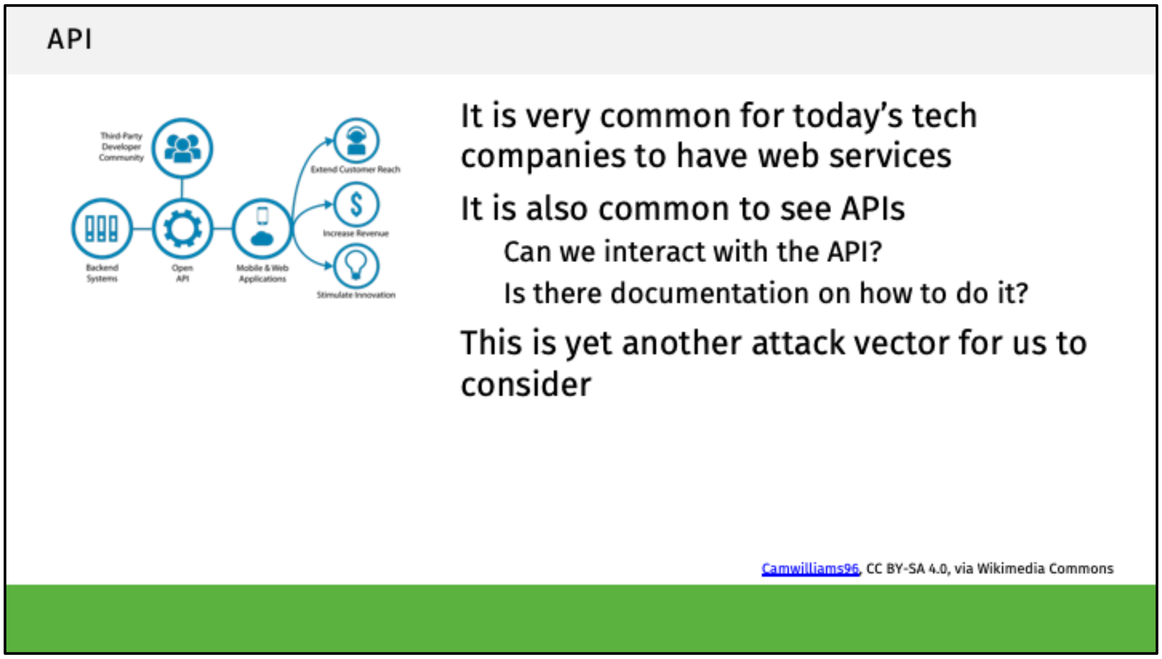
- Account lockouts are a big one
- IP shunning
- Geolocation blocking (proxy servers)
- Thresholds for failed logins
- Production environments and consequences of actions



UNDERSTANDING THE TARGET ENVIRONMENT

- Use what we have already researched about the adversary
- Know their constraints
  - For example, if they are PCI compliant, they must lock out certain accounts
- Understand the business

- What do they do?
- How do they make money?
- What clients do they have?
- Where are they located?
- What is their external footprint?
- What services do they offer?



API

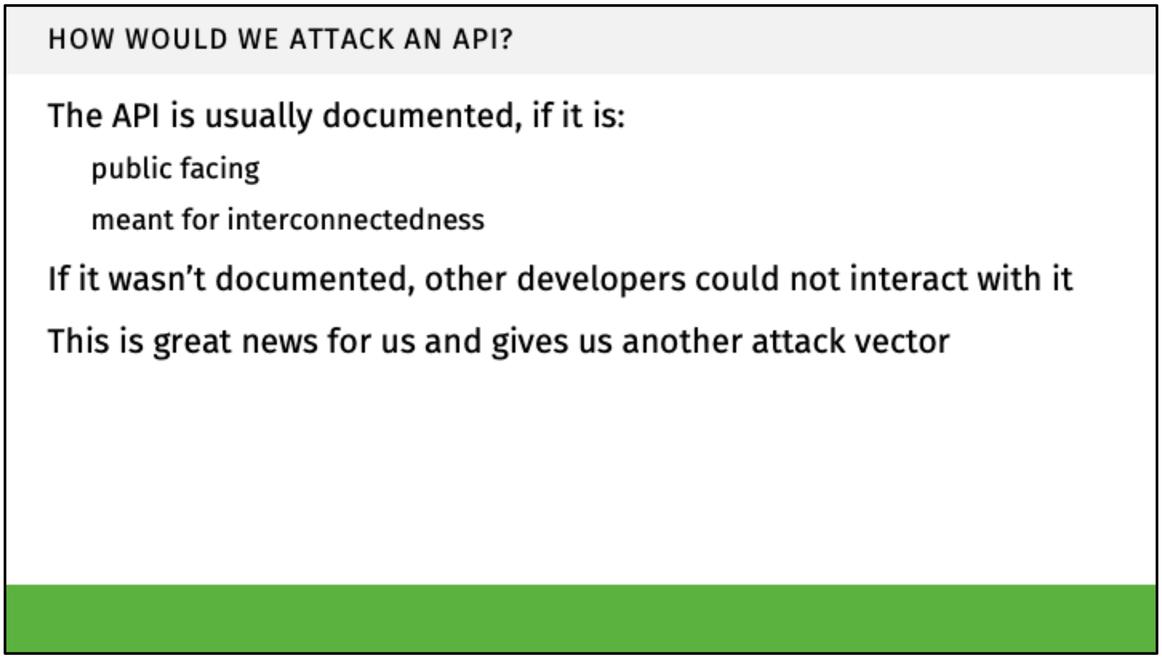
It is very common for today's tech companies to have web services

It is also common to see APIs

- Can we interact with the API?
- Is there documentation on how to do it?

This is yet another attack vector for us to consider

Camwilliams96, CC BY-SA 4.0, via Wikimedia Commons



HOW WOULD WE ATTACK AN API?

The API is usually documented, if it is:

- public facing
- meant for interconnectedness

If it wasn't documented, other developers could not interact with it

This is great news for us and gives us another attack vector