Cape Town Testing

Security Testing from an attacker's perspective!

June 2017

What is this all about then?

- Whoami?
  - @pragmaticswan
  - Where my perspective comes from
  - What I am not
- What are we hoping to achieve tonight
  - What do attackers look for?
  - An attackers mind set
- How do I win a prize?
  - Can I win if I don’t have a laptop?

Keys Explained

Mr. Hackerman

Mr. Tester

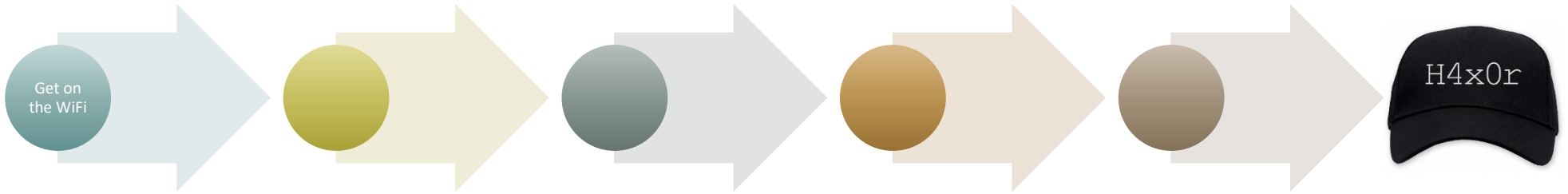
The one rule

End of the challenge

Get on the WiFi

Hey there, I am doing some recon. Do you have any information that I might find interesting?

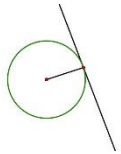
What information am I exposing that you might find useful?



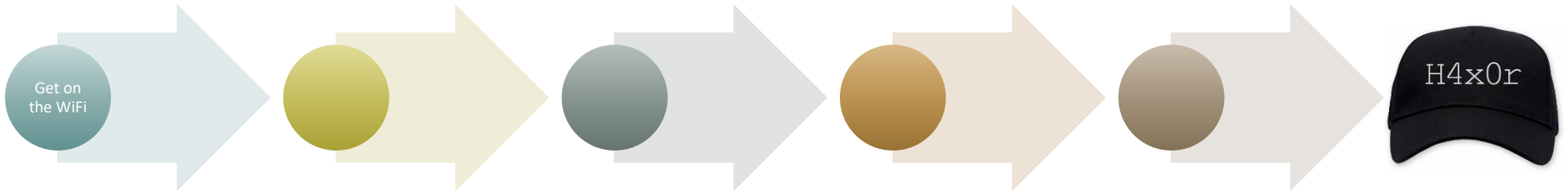
Get on the WiFi

- TESTING -

- Look to see if there are any known weaknesses (framework or technology)
- Test to see if there are verbose error messages
- Testing that exceptions logged.
- Brute force protection testing? Velocity testing?
- What other information could you be over sharing? E.g. code comments?



What is fuzzing?

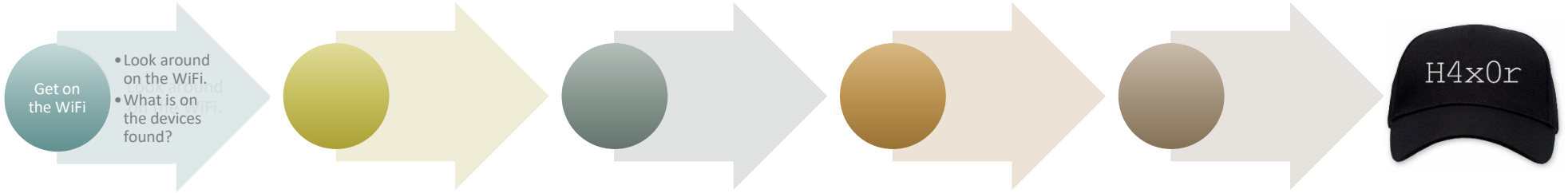


Get on the WiFi

- Look around on the WiFi.
- What is on the devices found?

Nice WiFi dude, is there anything interesting on this WiFi for me to "explore"?

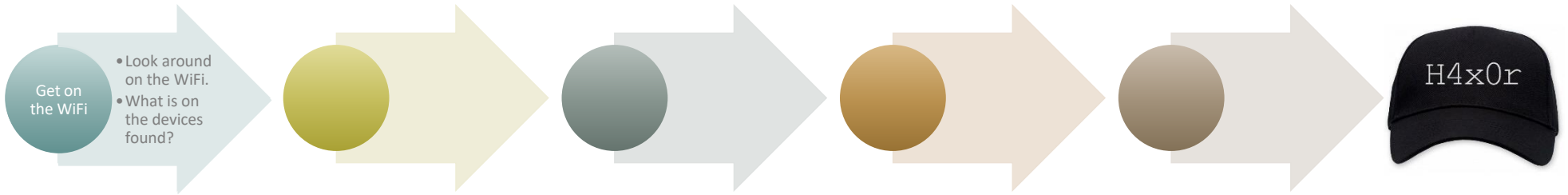
What connected systems would be at risk if the first layer of protection is compromised?



Get on the WiFi

- TESTING -

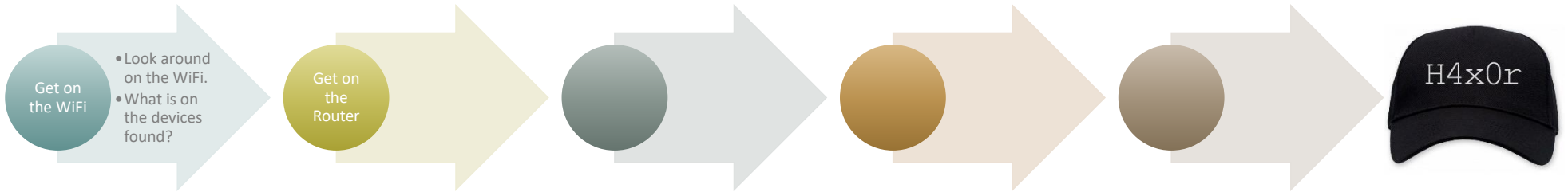
- Unit testing is great, but don't forget connected systems.
  - Internal APIs, back end servers?
- Consider different perspectives when testing, e.g. are there other plausible scenarios I should consider?
- What about the network stack, are there possible additional services exposed?
- Is your database access only to your instance / data?



Get on the Router

I have found an admin login. Can I attack the authentication or authorization for this system?

Have I made some basic mistakes, that are easy to test for?

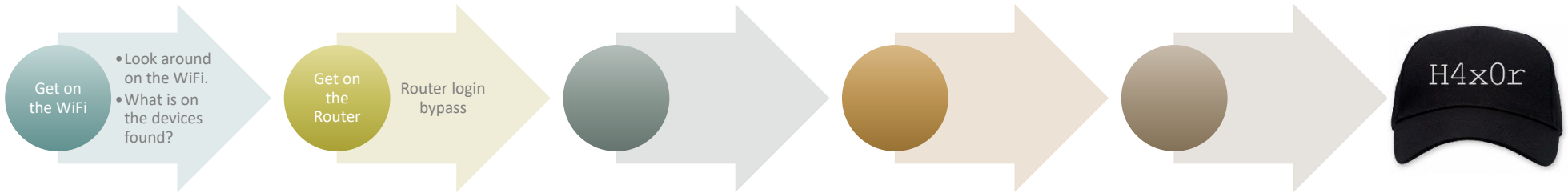


Get on the Router

Router login bypass

- TESTING -

- Have I done basic checks for common issues like the OWASP top?
  - Static code analysis?
- Are there any exposed administration interfaces?
- Am I checking all input and output in my application against types and black/whitelist?
- Never trust client side validation of data, always check server side.
  - Client side is for performance, server side is for security.



- SQL Injection -

How does SQL Injection work?

Common vulnerable login query

```
SELECT * FROM users
WHERE login = 'victor'
AND password = '123'
```

(If it returns something then login!)

ASP/MS SQL Server login syntax

```
var sql = "SELECT * FROM users
WHERE login = '" + formusr +
"' AND password = '" + formpwd + "'";
```

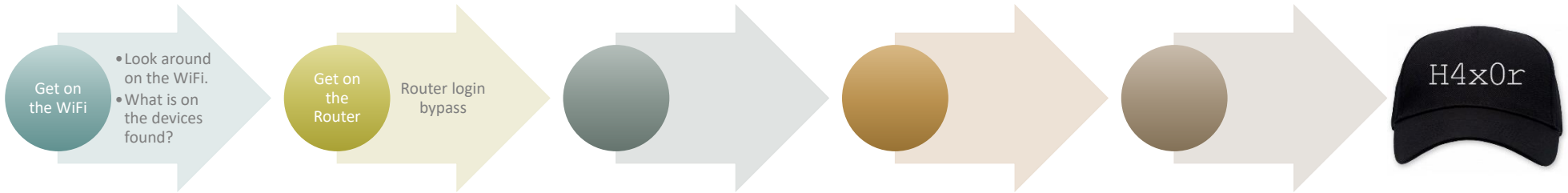

Injecting through Strings

formusr = **' or 1=1 – –**

formpwd = anything

Final query would look like this:

```
SELECT * FROM users
WHERE username = '' or 1=1
– – AND password = 'anything'
```

Get the admin password

Has this guy stored his secrets securely?

Where and how are I storing my secrets?

Get on the WiFi
- Look around on the WiFi.
- What is on the devices found?

Get on the Router — Router login bypass

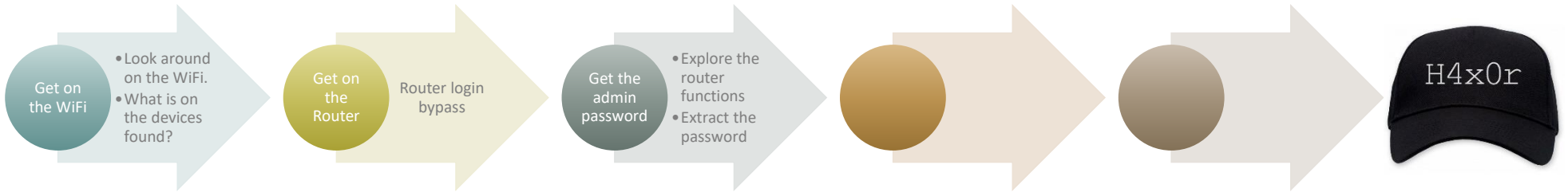
Get the admin password

Get the admin password

- Explore the router functions
- Extract the password

- TESTING -

- **Where are your secrets stored?**
- **Who can access your secrets?**
- **How are your secrets stored / are they strongly encrypted?**
- **Encryption should not be reversible, predictable or brute-forcible e.g. cookies or tokens**



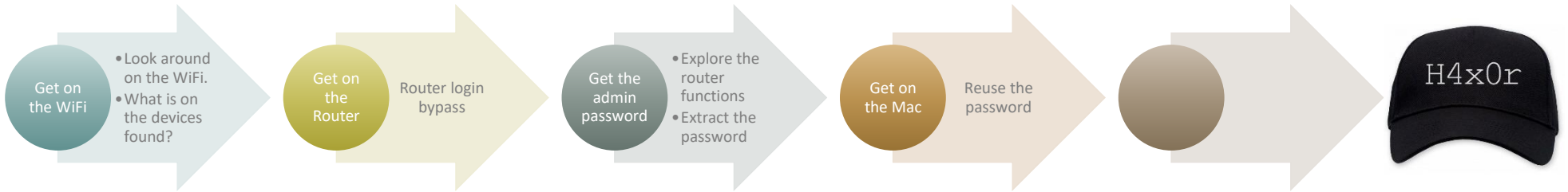

STOP

Get on the Mac

Reuse the password

Is this guy using the same credentials everywhere?

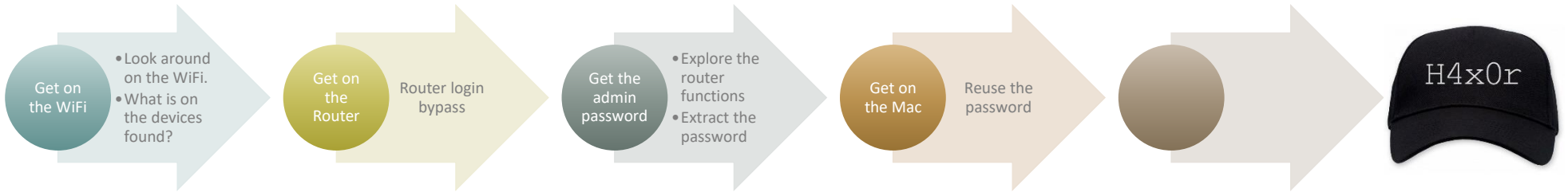
Will the compromise of one system, give an attacker access to other/all systems?



Get on the Mac

- TESTING -

- Unit testing is great, but don't forget connected systems.
  - Internal APIs, back end servers?
- Consider different perspectives when testing, e.g. are there other plausible scenarios I should consider?
- What about the network stack, are there possible additional services exposed?
- Is your database access only to your instance / data?



Unlock the Mac

Is this guy using the same credentials everywhere?

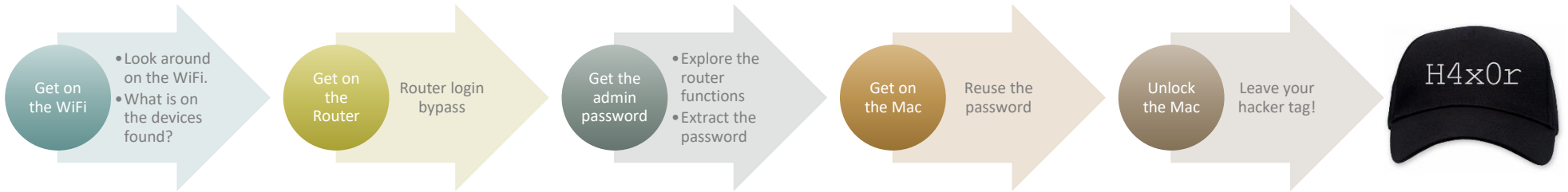
Will the compromise of one system, give an attacker access to other/all systems?

- **Get on the WiFi**
  - Look around on the WiFi.
  - What is on the devices found?
- **Get on the Router** — Router login bypass
- **Get the admin password**
  - Explore the router functions
  - Extract the password
- **Get on the Mac** — Reuse the password
- **Unlock the Mac** — Leave your hacker tag!

Unlock the Mac

- TESTING -

- Positive and negative testing matters
- Test authorisation e.g. can one user access another user's stuff?
  - can a normal user access an admin user's stuff?



The end

Questions?