

hackthebox.au

Curtis Koenig

Leadership is for everyone

any great or inspiring leader sets out
to do something unrealistic

leadership is taking action & helping
your people

must be a good communicator & tailor
the communication to your audience

active listening: repeating what you
heard

express, address, resolve conflict
basic conflict management

good leaders are good self assessors
what do you need to start doing?
" " stop doing?
" " continue doing?

Aldous Huxley + Mike Wallace

1. The first step is to identify the problem.

2. The second step is to define the problem.

3. The third step is to analyze the problem.

4. The fourth step is to develop a solution.

5. The fifth step is to implement the solution.

6. The sixth step is to evaluate the solution.

7. The seventh step is to monitor the solution.

8. The eighth step is to report the results.

9. The ninth step is to conclude the project.

10. The tenth step is to reflect on the project.

James Powell

Overkill, the home edition

dia (linux diagram tool that's free)

always have a way in

make one change at a time

document your network

when something doesn't work, check
DNS and/or network segments

10-10-1955

10-10-1955

10-10-1955

10-10-1955

10-10-1955

10-10-1955

10-10-1955

10-10-1955

~~outsourced~~ disaster response
The state of the insanity

cyber crimes aren't much different
than 10 years ago

opened link or attachment in email

defense ~~is~~ mostly reactive but missing
detection

zero day attacks are extremely rare
(handful in 10 years)

nobody expects to be targeted or a
victim

The FBI cannot get your stuff back
or put people in jail... bad actors are
usually overseas

APT = average phishing technique

Know your network

Run AppLocker in audit mode to see
what runs on a client

look for forwarding rules in email
(bad guys do this)

confirm financial transactions by
phone, not email

disable Powershell

client isolation

most threats are external, not internal

Better OSINT for better social engineering
phishing: not just for pentesters

①

advancedpersistentsecurity.com

social engineering = people hacking
6 principles of persuasion

- ① reciprocity
- ② commitment & consistency
- ③ social ~~proof~~ proof ("everyone's doing it")
- ④ likability
- ⑤ authority
- ⑥ scarcity (urgency)

OSINT is publicly-available info

resume is a great way to gather data
on a company (if Joe Know works at
Company X and uses C#...))

bars, malls, restaurants good places to
gather info

take your time with OSINT

1. The first part of the paper is devoted to the study of the properties of the function $f(x)$ defined on the interval $[0, 1]$.

2. In the second part, we consider the case when the function $f(x)$ is continuous on the interval $[0, 1]$.

3. The third part of the paper is devoted to the study of the properties of the function $f(x)$ defined on the interval $[0, 1]$.

4. In the fourth part, we consider the case when the function $f(x)$ is continuous on the interval $[0, 1]$.

5. The fifth part of the paper is devoted to the study of the properties of the function $f(x)$ defined on the interval $[0, 1]$.

6. In the sixth part, we consider the case when the function $f(x)$ is continuous on the interval $[0, 1]$.

7. The seventh part of the paper is devoted to the study of the properties of the function $f(x)$ defined on the interval $[0, 1]$.

8. In the eighth part, we consider the case when the function $f(x)$ is continuous on the interval $[0, 1]$.

DNC hacked data in the hands
of a trained intelligence professional

there is a lot of breached data
out there

can I collect enough of it to get
leverage over someone?

1. The first step in the process of
learning is to identify the problem.

2. The second step is to gather information
about the problem.

3. The third step is to analyze the information
and develop a plan of action.

Ways we do security wrong & how to fix it

people issues (skilled people are overused)
technology issues
process issues

promotion thru attrition: poor performers move up because good people burn out & quit

lack of quality metrics
spend more on tools than training your people

○ automate before your process is mature

process & procedure are modified based on mistakes of a single person (overly-complex processes)

pair new hire w/ most skilled person

integrate the tools you have (so you can get info easier from combined tool output)

1. The first step in the process of the scientific method is to ask a question.

2. The second step is to do background research to find out what is already known about the topic.

3. The third step is to form a hypothesis, which is a prediction about the outcome of the experiment.

4. The fourth step is to design and conduct the experiment to test the hypothesis.

5. The fifth step is to analyze the data and draw conclusions from the results.

6. The sixth step is to communicate the results of the experiment to others.

7. The seventh step is to repeat the experiment to verify the results.

8. The eighth step is to apply the results of the experiment to real-world situations.

Bob
Wheeler

bwheeler@cybersecjobs.com

Job hunting tips

education on bottom, if you have experience

remove any references or "references on request"

put experience & skills on top but keep it to the top 1/3
describe how you use tools

interview tips

keep it real

focus on the job

ask questions (come prepared w/some)

follow up (thank you email)

you should interview the interviewer

tell them you want the job

"is there something in my resume that needs clarification?"

build & maintain your network while employed

1. The first step in the process of the scientific method is to ask a question.

Page 1
Date: / /

2. The second step is to do background research.

3. The third step is to form a hypothesis.

4. The fourth step is to test the hypothesis by conducting an experiment.

5. The fifth step is to analyze the data and draw a conclusion.

6. The sixth step is to communicate the results of the experiment.

7. The seventh step is to repeat the experiment to verify the results.

8. The eighth step is to publish the results of the experiment.

9. The ninth step is to use the results of the experiment to answer the question.

James Bower

Pentesting in dead: adapt or demise

Engaged threat

defining pentest isn't easy
how much human work makes a pentest?

pentest return on investment?
(physical report \times perceived value)

CSO "Pentest is dead"

- No clear, accepted definition
- market maturity, saturation & aftermath
 - led to "click the button" to get a pentest
- what am I going to get?
- should I spend \$100 or \$10,000?
- what does this look like?
- why buy what I can't fix?

Pentester perspective

- conflicted interest "how much human work?"
- pricing model?
 - what do you do for what price?
(e.g. extra \$ for fuzzing)
- razor thin profit margins

Page 10 of 10

1. The first part of the document is a list of the

main points of the document.

2. The second part of the document is a list of the

main points of the document.

3. The third part of the document is a list of the

main points of the document.

4. The fourth part of the document is a list of the

main points of the document.

5. The fifth part of the document is a list of the

main points of the document.

6. The sixth part of the document is a list of the

main points of the document.

7. The seventh part of the document is a list of the

main points of the document.

8. The eighth part of the document is a list of the

main points of the document.

9. The ninth part of the document is a list of the

main points of the document.

10. The tenth part of the document is a list of the

main points of the document.

Passive network assessments

get permission to test in writing
from someone w/ authority

common OSINT results: network topology,
insider threats, 3rd party data leaks

cross-correlate tools like Burp & ZAP

always put documentation in layman's
terms & technical speak

make a wireless heatmap (where is signal
strong & weak?)

most people don't know the devices on
their network

- network printers are a juicy target

check warranties & licenses on devices
and software

check spacing, power & cooling on
where devices live

no direct attacks

Chlorophyll content index

1.0 - 1.5 (low) 1.6 - 2.0 (medium) 2.1 - 2.5 (high)

2.6 - 3.0 (very high) 3.1 - 3.5 (extremely high)

3.6 - 4.0 (very high) 4.1 - 4.5 (extremely high)

4.6 - 5.0 (very high) 5.1 - 5.5 (extremely high)

5.6 - 6.0 (very high) 6.1 - 6.5 (extremely high)

6.6 - 7.0 (very high) 7.1 - 7.5 (extremely high)

7.6 - 8.0 (very high) 8.1 - 8.5 (extremely high)

8.6 - 9.0 (very high) 9.1 - 9.5 (extremely high)

9.6 - 10.0 (very high) 10.1 - 10.5 (extremely high)

10.6 - 11.0 (very high) 11.1 - 11.5 (extremely high)