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've 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

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

~~Crowdsourced 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~~

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

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?

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)

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

James Bower

Pentesting is dead: adapt or demise

Engaged threat

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

pentest return on investment?
(physical report x 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

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