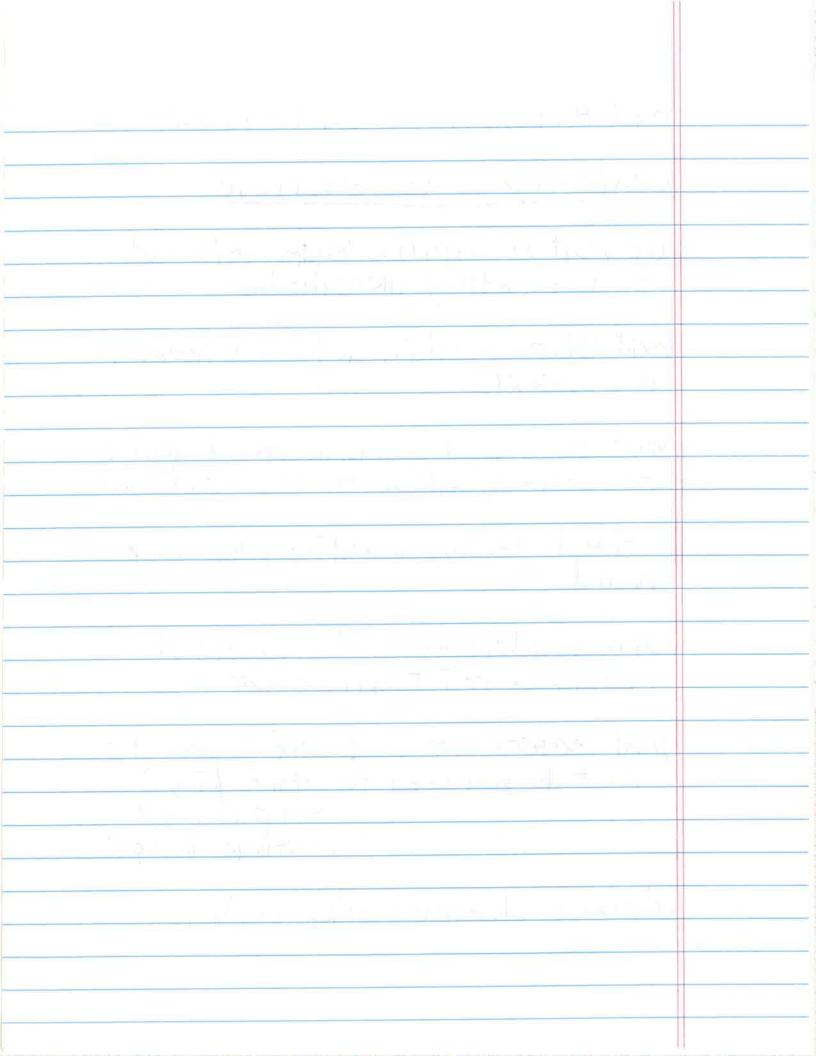
hackthebox, au curtis Koenig Leadership is for everyone any great or inspiring leader sets out to do something unrealistic leadership is taking action + helping must be a good communicator & tailor the communication to your audience active listening: repeating what your express, address, resolve conflict basic conflict management good leaders are good self assessors what do you need to start doing?

" stop doing?
" continue doing? Aldons Huxley+ Nike Wallace



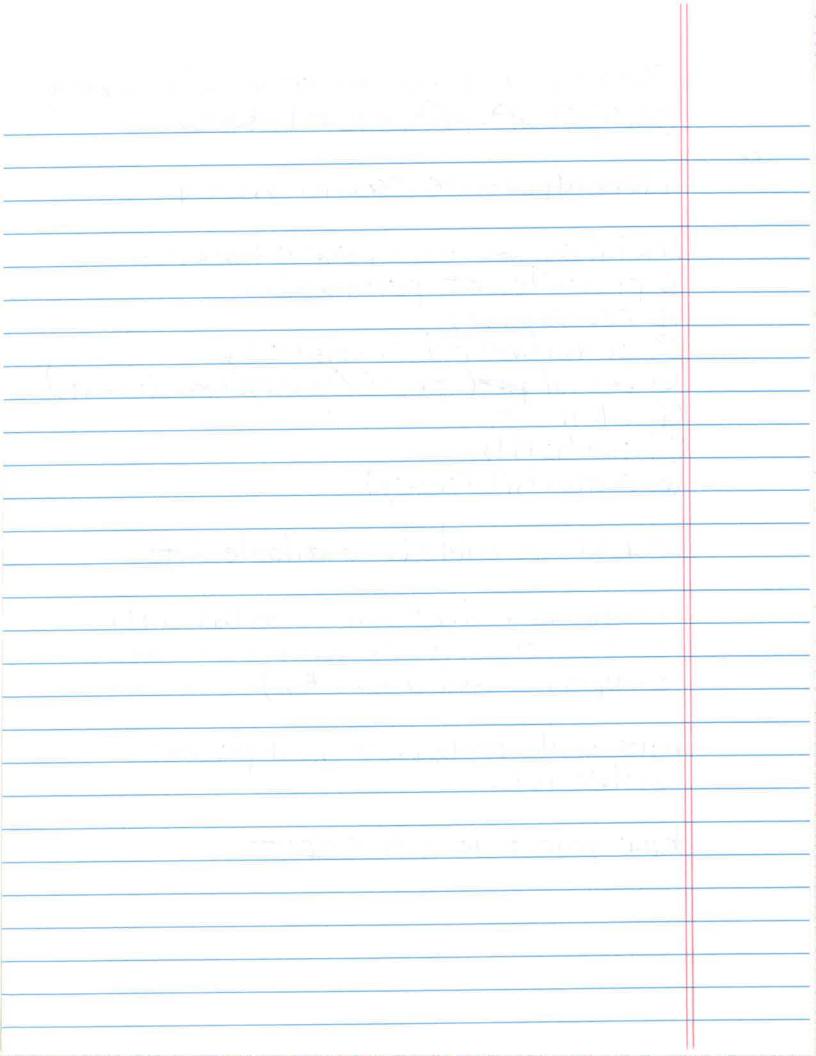
James Powell Overkill, the home edition dia (linux diagram tool that's free) always have a way in make one change at a time document your network when something doesn't work, check DNS and/or network segments

Suit to Tours and the suit say of	
man be the Testeron	

The state of the insquity Cyber crimes gren't much different than 10 years ago opened link or attachment in email defence he mostly reactive but missing detection zero day attacks are extremely rare (handful in 18 years) Nobody expects to be targeted or a The FBI cannot get your stuff back or put people in jail ... bad actors are usually overseas APT = average phishing technique KNOW YOUT NETWORK Run Applocker in audit mode to see what runs on a client

IDMATNI TON, IDMATXS STD STDSTAT Noitplasi tusila 11596 POWETShell Soufin Financial transactions by (214) ob syup bod) TIPMS NI SOLM

Better OSINT for better social engineering advanced persistent security. com social engineering = people hacking 6 principles of persuasion 1) reciprocity
2) commitment of consistency
3) social prof proof ("everyone's doing it")
4) likability 2 authority 6) scarcity (urgency) OSINT is publicly-available info on a company (if Joe know works at Company X and uses C#...) bars, malls, restaurants good places to 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?

And the state of t	
9791 F 120	
	=

Ways we do security wrong + how to People issues (skilled people are overysed) technology issues process issues promotion thry attrition: poor performers move up because good people burn out 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)

The remaining the state of the second	
The state of the s	
A ASSESS OF THE CONTRACT OF TH	

bwheeler@cybersecjobs.com Bob Wheeler Job hunting tips education on bottom, if you have experience remove any references or "references Put experience of skills on top byt keep it to the top is 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 darification?" build & maintain your network while employed

	H H
	Report !
and the second s	
The state of the s	
37 - AH H - H - H - H	
THE RESERVE THE PROPERTY OF TH	
That where a line with the South and	

James Bower Pentesting in dead: adapt or demise Engaged threat defining pertest isn't easy how much human work makes a pertest? pentest return on investment? (physical report x perceived value) LSO "Pentest 15 dead" - No dear, accepted definition - Market naturity, saturation of afternath - led to "click the button" to get a - What am I going to get? - Should I spend \$199 or \$10,000? - what does this look like? - why buy what I can't fix? Pentester perspective -conflicted interest "how much - pricing model? -what do you do for what price? (e.g. extra & for fuzzing) - razor thin profit margins

water that the same and the	
The state of the s	
The state of the s	
September 1985 Septem	
Y 1 2 10 1 1 1 1 1 1 2 10 2 10 2 10 2 10	
pour and the results of the first of the com-	

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 of 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

stance published market
VEGGARAN SANTAN
to the first and the state of the same to the second of
and the company of the section of th
Tradit of State (State)
1 - 13 - 13 - 13 - 13 - 13 - 13 - 13 -
and the field
the state of the same of the s
a same as a second of the contract per payer
Struct to be to
34.1.1. 36.3. 15.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1