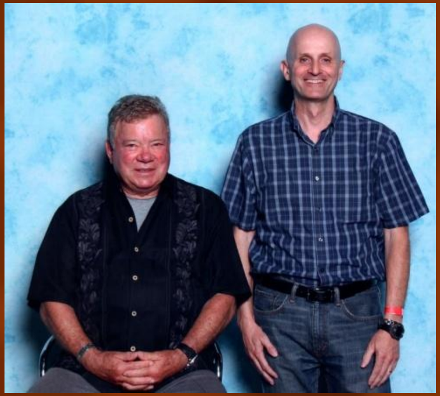
ShellCon 2019
RaiseMe

Pivot to a
Career in Cybersecurity

John Sicklick, CISSP

So Let’s Talk About Me…

- 30+ years of experience in the aerospace industry
- Worked as a software developer, systems administrator, systems integrator, and systems security engineer
- Retired Commander, U.S. Navy Reserves
- Certifications: GSLC, GXPN, GWAPT, GCIH, GCFE, GPEN, and CISSP
- Penetration Testing & Ethical Hacking certificate from SANS Technology Institute
- Adjunct Faculty at Long Beach City College
- Currently a graduate student in the SANS Technology Institute (MS in Information Security Engineering)



Topics

- Define Cybersecurity
- Define Pivoting
- Demand for Cybersecurity Professionals
- Cybersecurity Fields & Careers
- Technical, Physical, and Administrative Controls
- You May Already Be Involved in Cybersecurity
- Training Resources
- Certifications
- Networking
- Professional Reading
- Resumes & Applicant Tracking Systems

What is Cybersecurity?

- *Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries.“*
  Gartner “Definition: Cybersecurity”, 07 June 2013

- *"Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.“*
  Merriam-Webster
  https://www.merriam-webster.com/dictionary/cybersecurity

What is Pivoting?

- Pivoting is the exclusive method of using an instance also known by ‘foothold’ to be able to “move” from place to place inside the compromised network. It uses the first compromised system foothold to allow us to compromise other devices and servers that are otherwise inaccessible directly. https://resources.infosecinstitute.com/pivoting-exploit-system-another-network/

Demand for Cybersecurity Professionals

- Demand for Cybersecurity Talent Soars, Study Finds
  - 25 percent gap between demands for cyber talent and qualified workforce
  - Predicts a shortfall of 3.5 million cybersecurity professionals by 2021
  - Using existing talent
  - Closing the gap with "new collar workers"

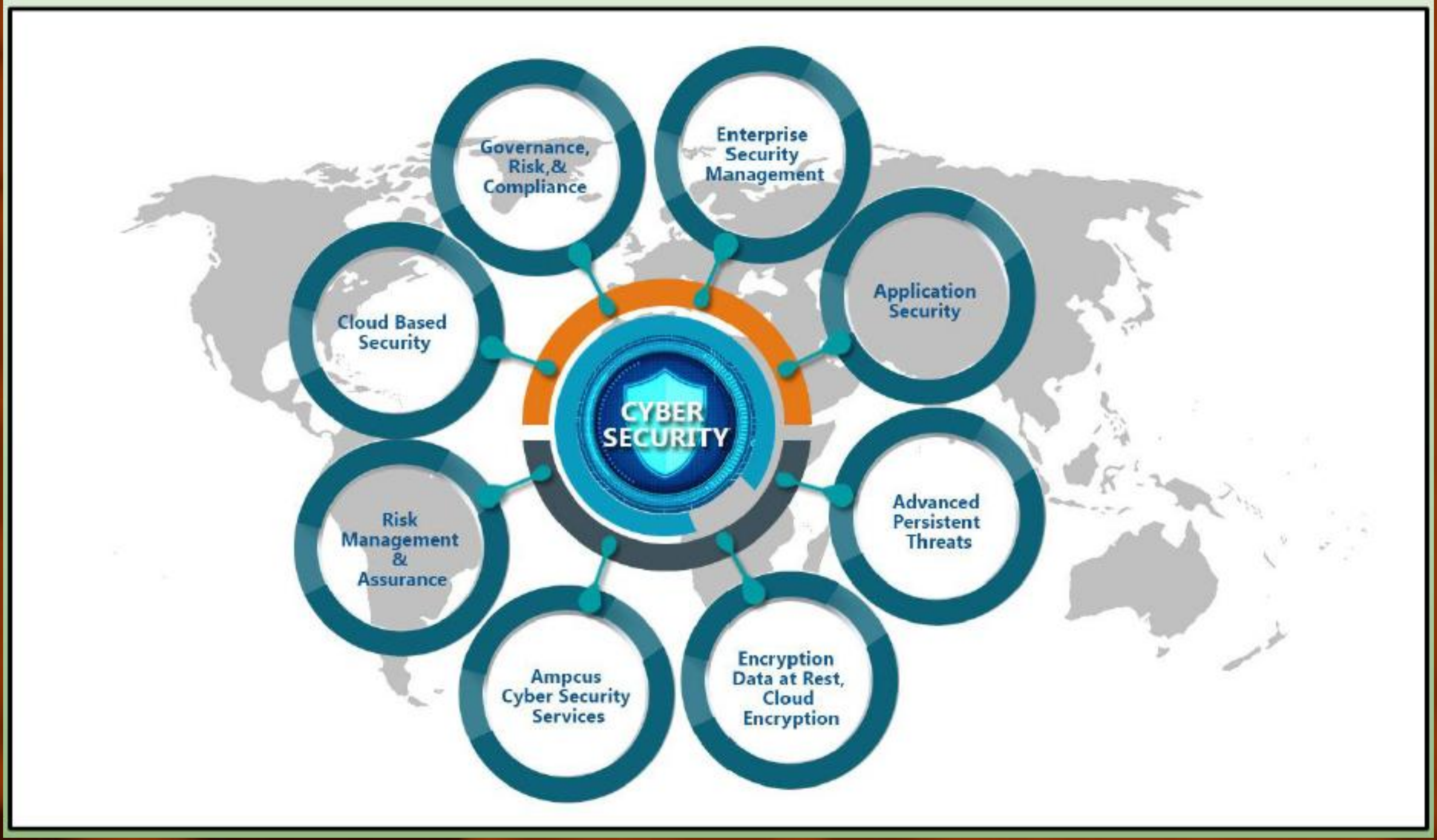
  https://securityintelligence.com/news/demand-for-cybersecurity-talent-soars-study-finds/

- Demand for Cybersecurity Jobs Doubles Over Five Years, But Talent Gap Remains https://www.prnewswire.com/news-releases/demand-for-cybersecurity-jobs-doubles-over-five-years-but-talent-gap-remains-300874877.html

- The 10 highest-paying cybersecurity jobs

  https://www.techrepublic.com/article/the-10-highest-paying-cybersecurity-jobs/

Cybersecurity Fields


CYBER SECURITY
Governance, Risk,& Compliance
Enterprise Security Management
Application Security
Advanced Persistent Threats
Encryption Data at Rest, Cloud Encryption
Ampcus Cyber Security Services
Risk Management & Assurance
Cloud Based Security

Careers in Cybersecurity

- Security Analyst
- Security Architect
- Security Software Developer
- Security Systems Engineer
- Security Administrator
- Security Consultant
- Forensics Examiner
- Penetration Tester
- Cryptographer
- Cryptanalyst
- Information System Security Manager
- Sales
- Quality Assurance
- Law
- Insurance

References:

“Learn How to Become”
https://www.learnhowtobecome.org/computer-careers/cyber-security/
“Cyber Security Jobs: Opportunities for Non-Technical Professionals”
https://onlinedegrees.sandiego.edu/non-technical-cyber-security-jobs/
“Getting Started in Cybersecurity with a Non-Technical Background”
https://www.sans.org/security-awareness-training/blog/getting-started-cybersecurity-non-technical-background

Technical, Administrative, and Physical Controls

- Technical - Hardware or Software Solutions
  - Firewalls
  - Intrusion Detection or Prevention Systems (IDS / IPS)
  - Biometric Authentication
  - Permissions
  - Auditing
- Administrative – implemented with policies and procedures
  - Fulfill legal requirements
    - Customer Privacy
  - Password Policy
    - Length, Complexity, Frequency of Change
  - User Agreement
- Physical – protect assets from both hackers and traditional threats https://www.asisonline.org
  - Guards
  - Locks
  - Cameras
  - Fire Protection

Oriyano, S. (2014) *Hacker Techniques, Tools, and Incident Handling,* 2nd Edition, Burlington, MA: Jones & Bartlett Learning

You May Already be Involved in Cybersecurity!

- Most computer vulnerabilities can be traced to:
  - Poorly implemented software
    - Failure to sanitize inputs
  - Incorrectly administered systems
    - Failure to disable inactive user accounts
  - Poorly designed systems
    - Meltdown and Spectre
  - Poor “cyber hygiene”
    - Lack of patch updates

If your job involves designing or administering information systems or developing software, you are effectively supporting cybersecurity efforts.

Cybersecurity Training

- College Degree versus Technical Certification
- Many, but not all, positions require a four year degree
- However, an additional degree may not be the best route to transition to cybersecurity
  - Depends on your original degree
  - Video: Success in the New Economy https://vimeo.com/67277269
- National Centers of Academic Excellence in Cyber Defense 2-Year Education (CAE-2Y) https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm#C
- There are three community colleges in Southern California with this designation
  - Coastline, Cypress, and Long Beach City College
- There are also four 4-year colleges in the area with the CAE designation
  - Cal Poly Pomona, CSUSB, UCI , Webster University
- Many positions also require specific certifications
  - e.g. Personnel administering DoD systems require the CompTIA Security+ certification at a minimum

Technical training & certifications can provide you with the needed skills faster

Training Resources for Veterans

- FedVTE
  The Federal Virtual Training Environment (FedVTE) provides free online cybersecurity training to U.S. government employees, Federal contractors, and veterans.
  https://fedvte.usalearning.gov/

- Splunk Pledge (Veterans and other groups)
  https://workplus.splunk.com/

- AWS Educate (Veterans)
  https://aws.amazon.com/education/awseducate/veterans/

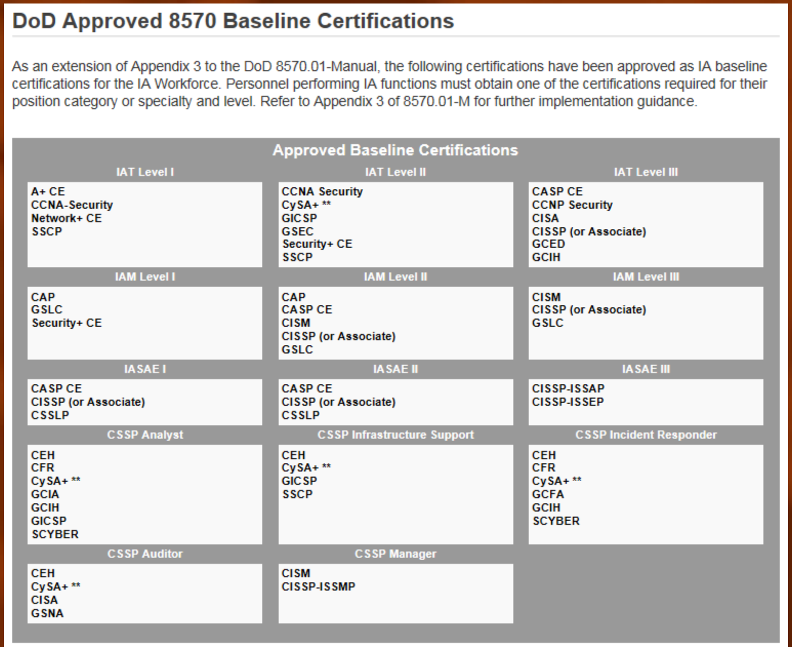
- LinkedIn for Veterans
  - Free one year Premium Careers subscription, including access to LinkedIn Learning
    https://www.linkedin.com/help/linkedin/answer/14803/linkedin-for-veterans-free-premium-career-subscription-and-eligibility?lang=en

Cybersecurity Certifications

- Purpose is to demonstrate a minimum set of skills
- Many positions also require specific certifications
  - e.g. Personnel administering DoD systems require at a minimum the CompTIA Security+ certification
- Search career websites for the certifications
  - Dice
  - Indeed
  - Monster

Cyber Workforce Management Program

- Cyber Workforce Management Program
  DoDD 8140.01 & DoD 8570.01-m for DoD related programs
- Applies to DoD and Contractors
- Positions dictate which certifications are required
  https://public.cyber.mil/cwmp/dod-approved-8570-baseline-certifications/
  https://public.cyber.mil/cwmp/



DoD Approved 8570 Baseline Certifications

As an extension of Appendix 3 to the DoD 8570.01-Manual, the following certifications have been approved as IA baseline certifications for the IA Workforce. Personnel performing IA functions must obtain one of the certifications required for their position category or specialty and level. Refer to Appendix 3 of 8570.01-M for further implementation guidance.

Approved Baseline Certifications

IAT Level I	**IAT Level II**	**IAT Level III**
A+ CE CCNA-Security Network+ CE SSCP	CCNA Security CySA+ ** GICSP GSEC Security+ CE SSCP	CASP CE CCNP Security CISA CISSP (or Associate) GCED GCIH
IAM Level I	**IAM Level II**	**IAM Level III**
CAP GSLC Security+ CE	CAP CASP CE CISM CISSP (or Associate) GSLC	CISM CISSP (or Associate) GSLC
IASAE I	**IASAE II**	**IASAE III**
CASP CE CISSP (or Associate) CSSLP	CASP CE CISSP (or Associate) CSSLP	CISSP-ISSAP CISSP-ISSEP
CSSP Analyst	**CSSP Infrastructure Support**	**CSSP Incident Responder**
CEH CFR CySA+ ** GCIA GCIH GICSP SCYBER	CEH CySA+ ** GICSP SSCP	CEH CFR CySA+ ** GCFA GCIH SCYBER
CSSP Auditor	**CSSP Manager**	
CEH CySA+ ** CISA GSNA	CISM CISSP-ISSMP	

CompTIA Certifications

- Security+
- Network+
- Cybersecurity Analyst (CySA+)
- Advanced Security Practitioner
- Pentest
- Linux+
- Cloud+

https://certification.comptia.org/certifications
https://www.businessnewsdaily.com/10718-comptia-certification-guide.html

Note: Many of these certifications can be obtained at low cost through your local community college

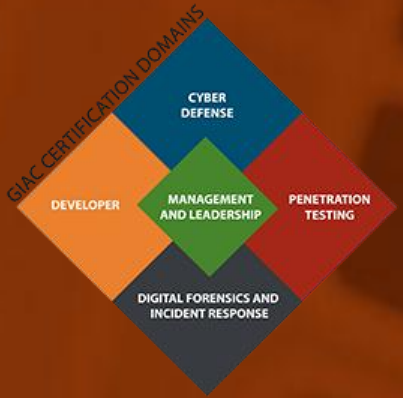
International Information Systems Security Certification Consortium (ISC2)

- Certified Information Systems Security Professional (CISSP)
  - One of the most widely recognized cybersecurity certifications
  - Tests security-related managerial skills
    - Usually more concerned with policies and procedures
  - Requires that you demonstrate five years of professional experience
    - Reduced to 4 years if you have a Bachelor’s degree
    - Can receive the CISSA if you pass the CISSP exam but do not have sufficient experience
- Certified Secure Software Lifecycle Professional (CSSLP)
- Several other certifications also offered
- Web site:
  - https://www.isc2.org/
  - https://www.isc2.org/credentials/default.aspx

SANS Institute

- Highly technical and hands-on training
  - Learn today and apply tomorrow philosophy
- SysAdmin, Audit, Network, Security (SANS) Institute
  - Offers training and over 20 certifications through Global Information Assurance Certification (GIAC) http://www.giac.org/certifications/get-certified/roadmap
  - Also offers Master’s Degrees and Certificates in Cyber Security http://www.sans.edu/
- Top 20 Critical Controls
  - One of the most popular SANS Institute documents
  - Details most common network exploits
  - Suggests ways of correcting vulnerabilities

    http://www.sans.org/security-resources/


GIAC CERTIFICATION DOMAINS
CYBER DEFENSE
DEVELOPER
MANAGEMENT AND LEADERSHIP
PENETRATION TESTING
DIGITAL FORENSICS AND INCIDENT RESPONSE

- Join the SANS.org community to subscribe to NewsBites & receive free posters https://www.sans.org/account/create

SANS CyberTalent Immersion Academies

- An intensive, accelerated training program that provides SANS world class training and GIAC certifications to quickly and effectively launch careers in cybersecurity
- 100% scholarship-based and no cost to participants
- **VetSuccess** - open to transitioning veterans and those transitioned in the last five years and not currently working in cybersecurity in a civilian role.
- **Women's Academy** - this Academy is open to career-changers and college seniors with a background in IT, but not currently working in cybersecurity roles.
- **Cyber Workforce Academy** - these Academies are made possible by grants, sponsors and organizations looking to hire cybersecurity talent or help advance the field by bringing in new talent. Academy eligibility requirements and curricula will be based on the specific focus and needs of the sponsors.
- **Diversity Cyber Academy** - SANS and International Consortium of Minority Cybersecurity Professionals (ICMCP) are partnering to create the SANS - ICMCP: Diversity Cyber Academy - DCA, combining efforts to increase the career opportunities for minorities and women in the cybersecurity field.

https://www.sans.org/cybertalent/seekers

EC-Council

- International Council of Electronic Commerce Consultants (EC-Council)

- Organization’s most recognized certification is the Certified Ethical Hacker (CEH)
  - Current certification is CEH v10
  - Based on 20 domains (subject areas)

- Also offers other certifications
  - Forensic Investigator, Application Security Engineer

- BS and MS in Cyber Security

https://www.eccouncil.org/

Offensive Security

- Creators of Kali Linux
- Penetration Testing and IT Security Training & Certifications
- Offensive Security Certified Professional (OSCP)
- Offensive Security Certified Expert (OSCE)
- Offensive Security Certified Web Expert (OSWE)
- Offensive Security Certified Exploitation Expert (OSEE)
- Offensive Security Certified Wireless Professional (OSWP)

https://www.offensive-security.com/

Employer Training & Collaboration Resources

- If you are currently employed, utilize available educational benefits and training resources.
  - Not just educational reimbursement programs
  - Some companies offer access to resources such as lynda.com or degreed.com
- Collaborate – many companies have an internal version of LinkedIn
  - Post your skills internally
  - Join groups that are related to cybersecurity
- Find the cybersecurity personnel at your employer and ask them for advice
  - They’re typically really friendly people!

Pivot to a cyber security position with your current employer

Other Training Resources

- LinkedIn Learning (formerly Lynda.com)
  - Paid subscription https://www.linkedin.com/learning/
  - How to Access LinkedIn Learning for free through public libraries
  - Possibly available through your school
- Cybrary - Free cybersecurity and IT training https://www.cybrary.it/
- Splunk Pledge (Veterans and other groups) https://workplus.splunk.com/
- Public Libraries
  - LinkedIn Learning
  - Access to online books

For the more “experienced” workers among us…

- Stop throwing away those letters from AARP!

- How Older Workers Can Learn New Job Skills
  https://www.aarp.org/work/job-search/info-2018/work-skills-resume-fd.html

- Learn@50+
  https://learn.aarp.org/

- Poor Training, Lack of Skills Leave Older Workers Behind: Study
  https://insights.dice.com/2019/07/02/skills-older-tech-professionals/

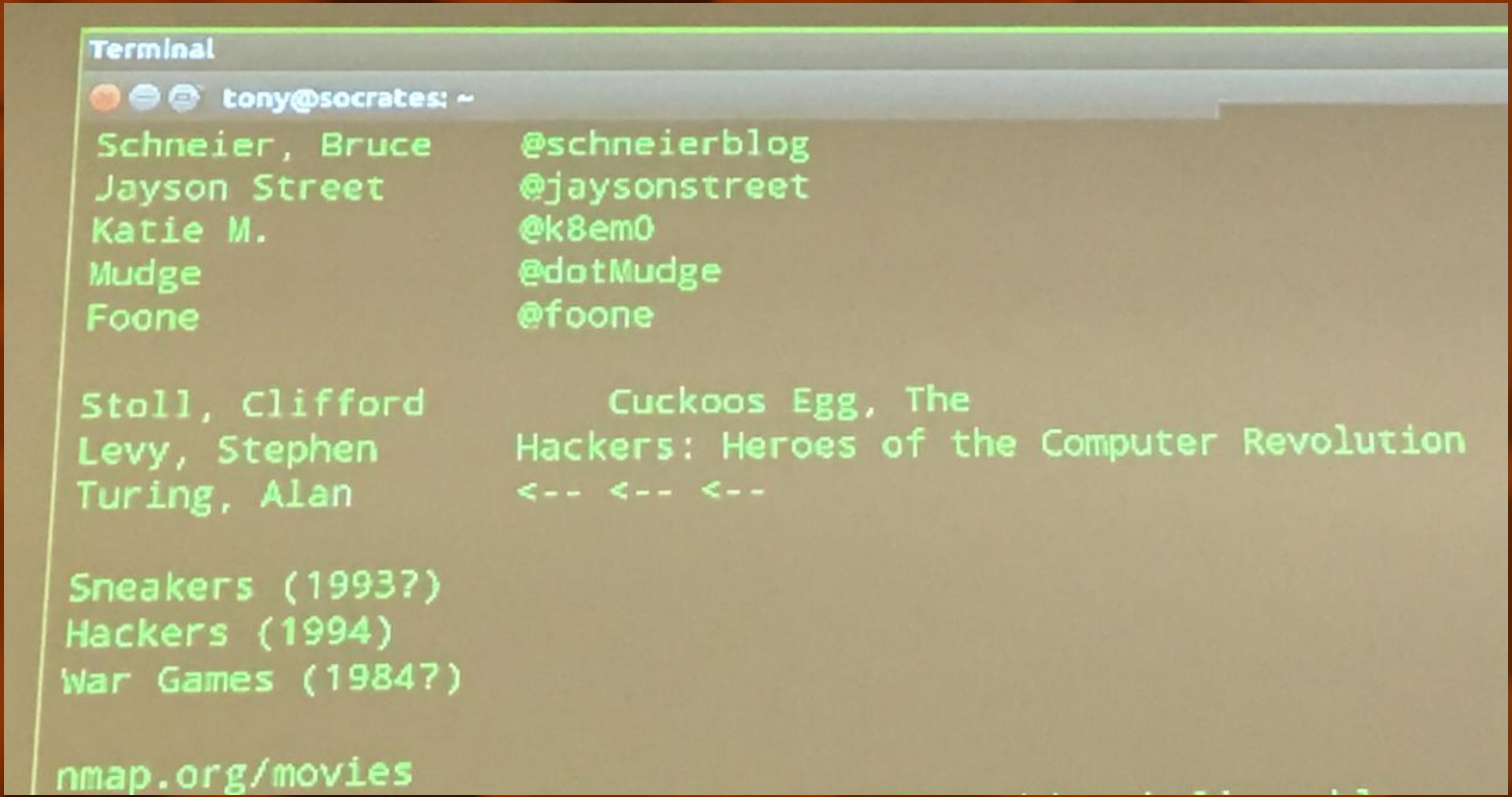
Networking

- **Invest in & market yourself**
  - Information System Security Association (ISSA) https://www.issa.org
  - Open Web Application Security Project (OWASP) https://www.owasp.org
  - Women's Society of Cyberjutsu (WSC) https://womenscyberjutsu.org/
  - Women in Cyber Security https://www.wicys.org/
  - Reverse Shell Corporation https://www.revshellcorp.org/
  - Null Space Labs https://032.la/
  - Search for local groups on http://meetup.com
    - LETHAL, Null Space Labs
- Attend conferences
  - DEF CON https://defcon.org
  - BSides http://www.securitybsides.com
  - Grace Hopper Celebration https://ghc.anitab.org/
  - ShellCon https://shellcon.io
  - LayerOne https://www.layerone.org/
  - AppSec California https://2020.appseccalifornia.org/

Professional Reading & Podcasts

- 7 Must-Read Blogs for Information Security Professionals (Capella University) https://www.capella.edu/blogs/cublog/top-blogs-for-infosec-professionals/
- The Top Cyber Security Blogs and Websites of 2019 https://onlinedegrees.sandiego.edu/top-cyber-security-blogs-websites/
- SANS Internet Storm Center https://isc.sans.edu/
- SANS Newsbites https://www.sans.org/newsletters/newsbites/
- DoD Cyber Exchange – Public https://public.cyber.mil/

Twitter, Read, and Watch



```
Schneier, Bruce       @schneierblog
Jayson Street         @jaysonstreet
Katie M.              @k8em0
Mudge                 @dotMudge
Foone                 @foone

Stoll, Clifford           Cuckoos Egg, The
Levy, Stephen         Hackers: Heroes of the Computer Revolution
Turing, Alan          <-- <-- <--

Sneakers (1993?)
Hackers (1994)
War Games (1984?)

nmap.org/movies
```

A Quick Word on Resumes and Applicant Tracking Systems

- Resumes
  - An art form
  - Everyone who reviews your resume will have a different opinion
  - You should always have one ready
  - Update it on a regular basis
- You should maintain your resume in two different formats*
  *John's opinion
  - Human readable for individuals and smaller companies
  - Longer, more detailed resume for larger companies which utilize…
- Applicant Tracking Systems
  - Resume is scanned and placed in a database
  - Interviewers rarely see your original resume
  - Database is searched on key words to find qualified applicants
- Use a website such as Jobscan (www.jobscan.co) to evaluate your resume against a position description
  - You will be surprised how poorly your resume scores
  - Plural forms of words is a common problem (e.g. firewalls vs firewall)

Questions or Comments?

- Contact Information for John Sicklick
  - Email: john@sicklick.name
  - LinkedIn: https://www.linkedin.com/in/johnsicklick/
  - Twitter: @cdrcybr

ShellCon 2019
RaiseMe

Pivot to a
Career in Cybersecurity

John Sicklick, CISSP

Download the Slides

- https://tinyurl.com/y53gml8q