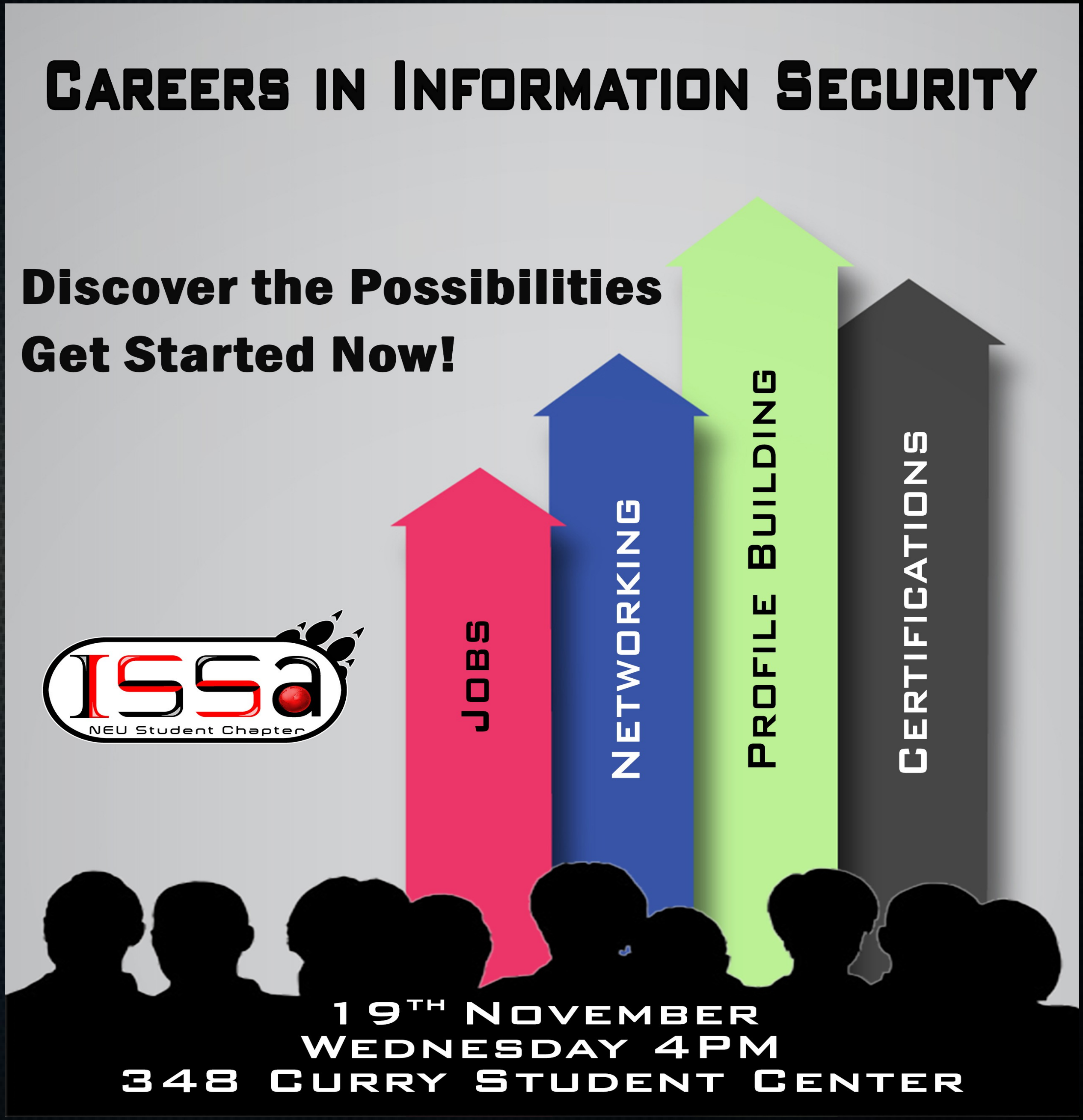
Careers in Infosec!



Careers in Information Security

Discover the Possibilities

Get Started Now!

19th November
Wednesday 4PM
348 Curry Student Center

Agenda

- Holistic view of Infosec Jobs
- Infosec Domains
- Various Jobs and required Skills
- Egg and Chicken problem
- Breaking the ice
- Profile Building
- Q & A Session
- Discussion Panel with Co-op and Intern Students

About Me

- N00b/beginner
- /usr/name: Uday Seelamantula
- /usr/occupation: Masters Student
- /usr/mail: uday@ccs.neu.edu, udaybhaskar.it@gmail.com , seelamantula.u@husky.neu.edu
- /usr/twitter: @Uday_infosec
- /usr/LinkedIn: http://www.linkedin.com/in/udayseelamantula
- /usr/Git: https://github.com/stmh-infosec
- /usr/site: http://stmh-infosec.github.io/

Disclaimer

[1] The information and opinions expressed in this talk are neither the opions of the presenters (and not constitute policy, positions or opinions of previous organizations the presenter worked at) nor that of Northeastern University.

[2] Any demos and case studies discussed in the talk are only for educational purposes, presenter will not be held responsible for any misuse of this data.

Two Tracks

- Management
  - Your job role is limited to your company and a few company clients
  - High/Medium level of expertise
  - Sort of relaxed environment
  - Not much of client interactions
  - Not much of travelling required
  - Learning Curve – Medium (but you would become expert in what you do on daily basis)
  - You are well aquainted with the organizational security posture and needs
  - Job role may be to moniter, administor and audit internal security

- Consulting
  - You do projects from multiple companies. (Mostly Short term)
  - High level of expertise
  - Different projects with different architectures and requirements
  - Rich client Interaction
  - You travel a lot...visit more places.
  - Learning Curve – Fast and High
  - You get to know what the industry needs
  - Job role mostly includes auditing, recommendations, implementations

- Management

Goldman Sachs

Fidelity INVESTMENTS®

amazon

ebay™

Akamai

Bank of America

citi

YAHOO!

Google

EMC² ® where information lives®

And there are many cats on the wall.

- Consulting

cigital

RAPID7

Security Innovation

KPMG

EY Building a better working world

GOTHAM DIGITAL • SCIENCE

CISCO™

Deloitte.

FireEye™

WhiteHat SECURITY

Domains in Infosec

- IT Security Management
- Risk And Compliance
- NOC, Sys Admins, Security Archi
- SOC, Intrusion Detection
- Incident Response
- Digital Forensic Investigation
- Penetration Testing And Vulnerability Assessments
- Software Development (Normal S/W or Tool Developments)

IT Security Management

- **Job Roles**: CISO, Cybersecurity manager/officer, Security director, Security Analyst
- **What they do ?**: Management of people, processes, and technologies is critical for maintaining proactive enterprise situational awareness and for the ongoing success of continuous monitoring efforts.
- **Required Skill Set**:
  - Team Management skills
  - Communication skills
  - Implementaion Skills
  - Awareness of Internal Audits
  - Risk analysis Management
  - Awareness of Compliance
  - Awareness of VA/PT, SIEM and security tools
  - Project Management Skills
  - Awareness of Incident and responce Management

Risk And Compliance

- **Job Roles**: Auditor, Compliance Officer, Risk Analyst, Security Compliance Consultant, QSA (Qualified Security Assesser), BSI Consultant, BCP & DR Consultant.
- **What they do ?**: These experts assess and report risk to the organization by measuring compliance with policies, procedures and standards.
- **Required Skill Set**:
  - Experience in implementation of ISO 27001
  - Experience in conducting Risk Assessment and Information Security Audits
  - Experience in documenting policies and procedures
  - Good knowledge of various compliance standards and frameworks like PCI DSS,ISO 20000 SSAE 16, COBiT 5 , BCMS
  - Implementation experience in the above would be an added advantage
  - Excellent communication, documentation & interpersonal skills

NOC, Sys Admins, Security Archi

- **Job Roles :** System/IT administrator, Security administrator, Security architect/engineer.
- **What They Do? :** A Network Operations Center is a center where IT professionals supervise, monitor and maintain the enterprise network. The network operations center is the focal point for network troubleshooting, software distribution and updating, router and system management, performance monitoring and coordination with affiliated networks.
- **Required Skill Set :**
  - Experience with switching and internet routing technologies.Strong network diagnostic skills.
  - Experience configuring internet applications such as Apache, Exim, BIND.
  - Experience of network monitoring tools and protocols (MRTG, RRD, NAGIOS, SNMP).
  - Experience of scripting (Perl, Bash) and other web application languages (SQL,PHP).
  - Experience of analysing system and network performance using monitoring and graphical data.
  - Experience of diagnosing network and service issues, following them through to resolution.
  - Keen to be involved in a wide variety of ISP services.

SOC, Intrusion Detection

- **Job Roles :** Intrusion detection analyst, Security operations center analyst/engineer, CERT member, Cyber threat analyst.
- **What they do ? :** SOC analysts are responsible for enterprise situational awareness and continuous monitoring, including monitoring traffic, blocking unwanted traffic from and to the Internet, and detecting any type of attack.
- **Required Skill Set :**
  - knowledge & Hands on experience of implementation and management of IDS/IPS, Firewall, VPN, and other security products.
  - Experience on Security Information Event Management (SIEM) tools, Creating advance co-relation rules .
  - Administration of SIEM.
  - System hardening.
  - Vulnerability Assessment
  - Should have expertise on TCP/IP network traffic and event log analysis.
  - Knowledge & Hands on experience of Arcsight, NetIQ Sentinel or any SIEM tool.
  - Knowledge of ITIL disciplines such as Incident , Problem and Change Management.

Incident Response

- **Job Roles :** Security analyst/engineer, SOC analyst, Cyber threat analyst, CERT member, Malware analyst
- **What they do ? :** When the security of a system or network has been compromised, the incident responder is the first-line defense during the breach.
- **Required Skill set :**
  - Using ENCASE and FTK forensic-analysis tools for analysis of Security Incidents
  - Security Incident (hacks, illegal network penetration, website defacements, etc.) forensic analysis
  - Malware Analysis
  - Threat & Vulnerability Management
  - Business Impact Analysis
  - Data Integrity/Recovery
  - System Audit & Correlation
  - Contingency Planning
  - Risk Assessment

Digital Forensic Investigation

- **Job Roles :** Forensic Investigator, Forensic Analyst and Consultant
- **What they do ? :** These guys are experts in collecting evedience, analysing them and report or identify the attack and the agent who had initiated the attack.
- **Required Skill set :**
  - Experience with common computer forensics tools such as Encase, FTK, The Sleuth Kit, Volatility, etc.
  - Knowledge of Python, C/C++ and/or Java.
  - Deep understanding of the current threat landscape including common attack types and malware capabilities.
  - Strong understanding of Unix and Windows security.
  - Good communication Skills

Development – Secure Development

- **Job Roles:** Developer, Software Architect, QA tester, Development Manager
- **What they do ?: The security-savvy software developer leads all developers in the creation of secure software, implementing secure programming techniques that are free from logical design and technical implementation flaws.**
- **Required Skill Set :**
  - Should be good at Java, J2EE or .net technologies.
  - Good at JQuery, JavaScript, JS Toolkits, AngularJS, Node.js, XML, HTML, CSS, JavaScript Library, AJAX, Webservices, JSON, Restful Services.
  - Experience with Linux.
  - Working on MVC.
  - Knowledge of framework like Hibernate, Spring, Struts.
  - Good SQL knowledge using Oracle and MY SQL Server.
  - Good understanding of secure software development life cycle processes.
  - Knowledge of Security Flaws and its Resolution as listed in sites like OWASP, SANS etc.

Development – Security Tools and Products

- **Job Roles:** Developer, Software Architect, QA tester, Development Manager
- **What they do?: These developers are good at developing security related products. Products like log management tools, SIEM tools, Firewalls, Vulnerability Scanners etc.**
- **Required Skill Set:**
  - Should be good at Java, J2EE or .net technologies.
  - Good at JQuery, JavaScript, JS Toolkits, AngularJS, Node.js, XML, HTML, CSS, JavaScript Library, AJAX, Webservices, JSON, Restful Services.
  - Experience with Linux.
  - Working on MVC.
  - Knowledge of framework like Hibernate, Spring, Struts.
  - Good SQL knowledge using Oracle and MY SQL Server.
  - Good understanding of secure software development life cycle processes.
  - Knowledge of Security Flaws and its Resolution as listed in sites like OWASP, SANS etc.

Pentesting And Vulnerability Assessments

- **Job Roles/Titles:** Penetration Tester, Vulnerability Assessor, Ethical Hacker, Red/Blue team member, Cyberspace Engineer
- **What They Do ?:** These guys are experts in Network Pentesting, Web Application Pentesting, Mobile Applications and Device Security, Wireless Pentesting, Security Code Reviews, Secure Network Architecture Reviews, Exploit Research, Reverse Engineering, Vulnerability Assessments, Configuration Audits etc.
- **Required Skill Set:**
  - Familiarity with software security weakness, vulnerability and secure code review a plus.
  - Familiarity with software attack and exploitation techniques.
  - Familiarity with at least one from each

    1. low level s/w programming language.
    2. Web App programming language.
    3. Database programmming
    4. Systems and Applications programming.

Everybody wants experience....if they don't give me a job, how will I gain experience

So, how should I get around this problem....?

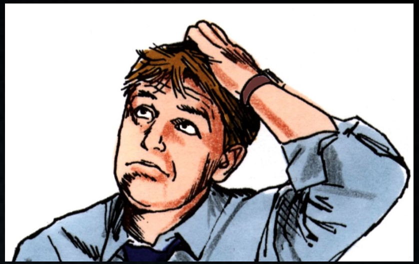
Build your profile!

Build your profile!

Build your profile!

Infosec industry looks for talent and there are many instances where experience is side tracked.

But how? How can I build a good, strong profile?



Course in Information Assurance/ Information Security / Cyber Security	✓
Publish Articles and Research Papers	✓
Work under a research professor who is working on a security topic of your interest	✓
Ensure to meet the skill set required for the jobs you wish to join	✓
Keeping improving your skill stack	✓
Networking , Conferences and communities	✓

Get Involved in ongoing Security Projects	✓
Start participating in CTFs, Wargames, CCDC	✓
Start coding scripts, tools and frameworks	✓
Bug Bounty and hall of fames	✓
Certifications	✓
LinkedIn, Twitter, Blogs and GIT (Showcasing is as important as you do your counterparts)	✓

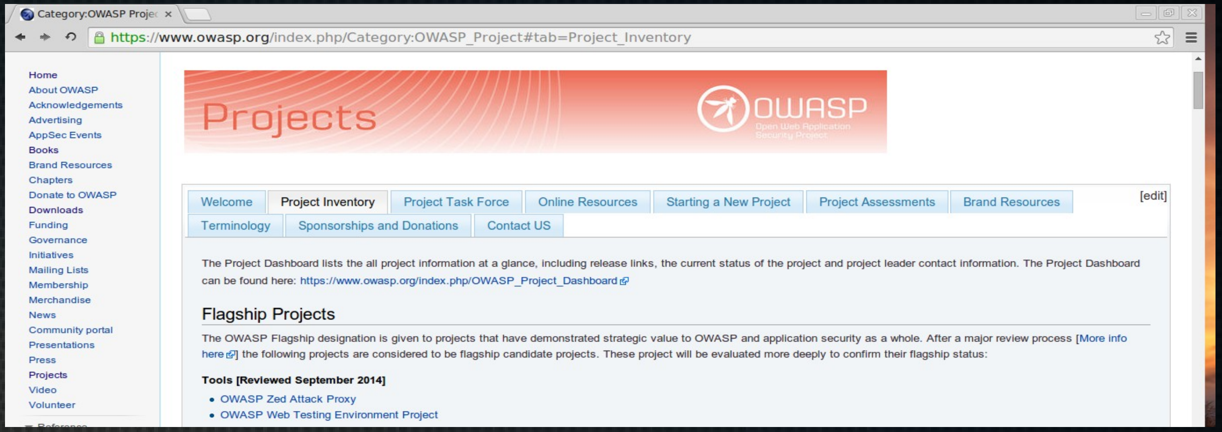
Networking , Conferences and communities

- Infosec nerds and passionates are friendly to approach and are very helpful in guideing you.
- You get to meet a lot of industry security guys.
- Rich presentation contents, a lot to learn (somethings may even compel you to think further)
- Job Fairs and you get to directly talk to the team head or members who head the security devisions.
- It would work out best if you are on the presenters side rather than the audience side.

black hat
DEFCON
BSIDES St John's
OWASP Open Web Application Security Project
OWASP FOUNDATION PRESENTS APPSEC USA
NUCON
HITB
SHMOOCON

Get Involved in ongoing Security Projects

- OWASP Projects
- Metasploit Contributions
- Linux Contributions
- Snort Contributions
- WASC Contributions
- Honeynet
- Almost every opensource security tool has some kind of contributions



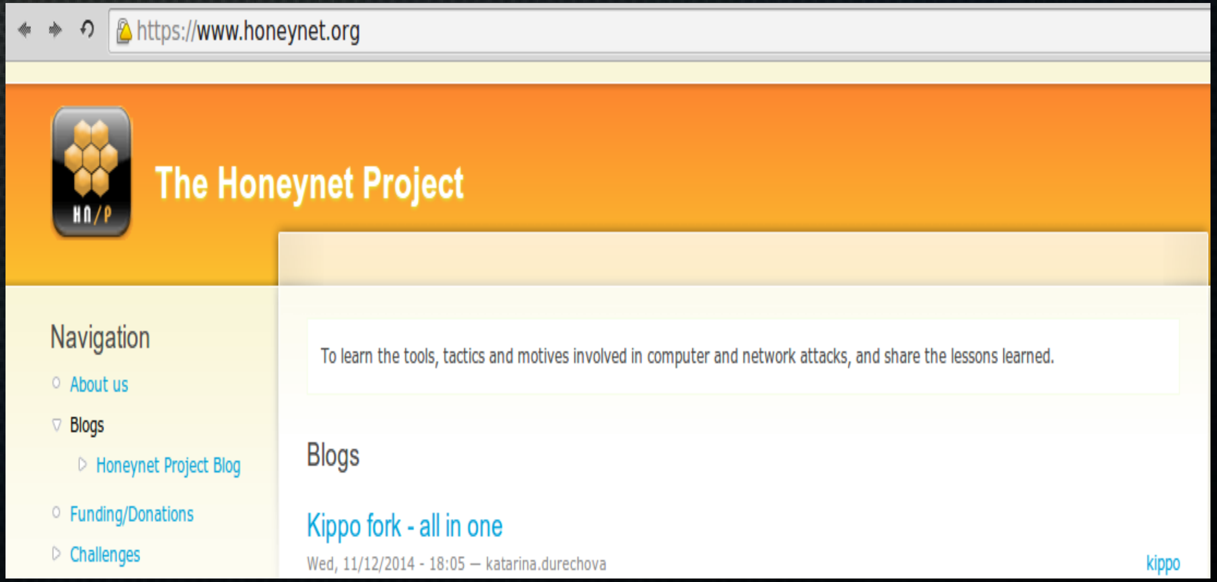
The Project Dashboard lists the all project information at a glance, including release links, the current status of the project and project leader contact information. The Project Dashboard can be found here: https://www.owasp.org/index.php/OWASP_Project_Dashboard

Flagship Projects

The OWASP Flagship designation is given to projects that have demonstrated strategic value to OWASP and application security as a whole. After a major review process [More info here] the following projects are considered to be flagship candidate projects. These project will be evaluated more deeply to confirm their flagship status:

Tools [Reviewed September 2014]

- OWASP Zed Attack Proxy
- OWASP Web Testing Environment Project



To learn the tools, tactics and motives involved in computer and network attacks, and share the lessons learned.

Blogs

Kippo fork - all in one

Wed, 11/12/2014 - 18:05 — katarina.durechova

kippo

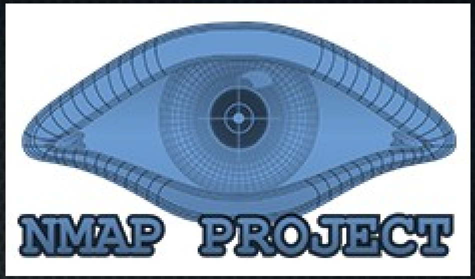
Start participating in CTFs, Wargames, CCDC

- **CTFs** – Capture The Flag
- **Wargames**
- **CCDC** - Collegiate Cyber Defense Competition
- Challenging Tasks and great way to learn things in a fast paced environment
- https://ctftime.org/ :The best way to keep a track of ongoing CTFs
- **Most of the challenging pentest interviews have a few hands-on challenges to solve, playing these kind of stuff comes handy**

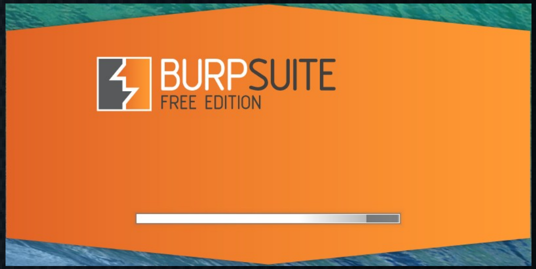
Off The Shelf websites having Security Challenges:

- Webgoat
- DVWA
- HacMe Bank(McAfee)
- HackThisSite.org
- Overthewires.com
- Hackinglab.org
- Enigmagroup.or**g**
- The list goes on and on...:)

Start coding scripts, tools and freameworks



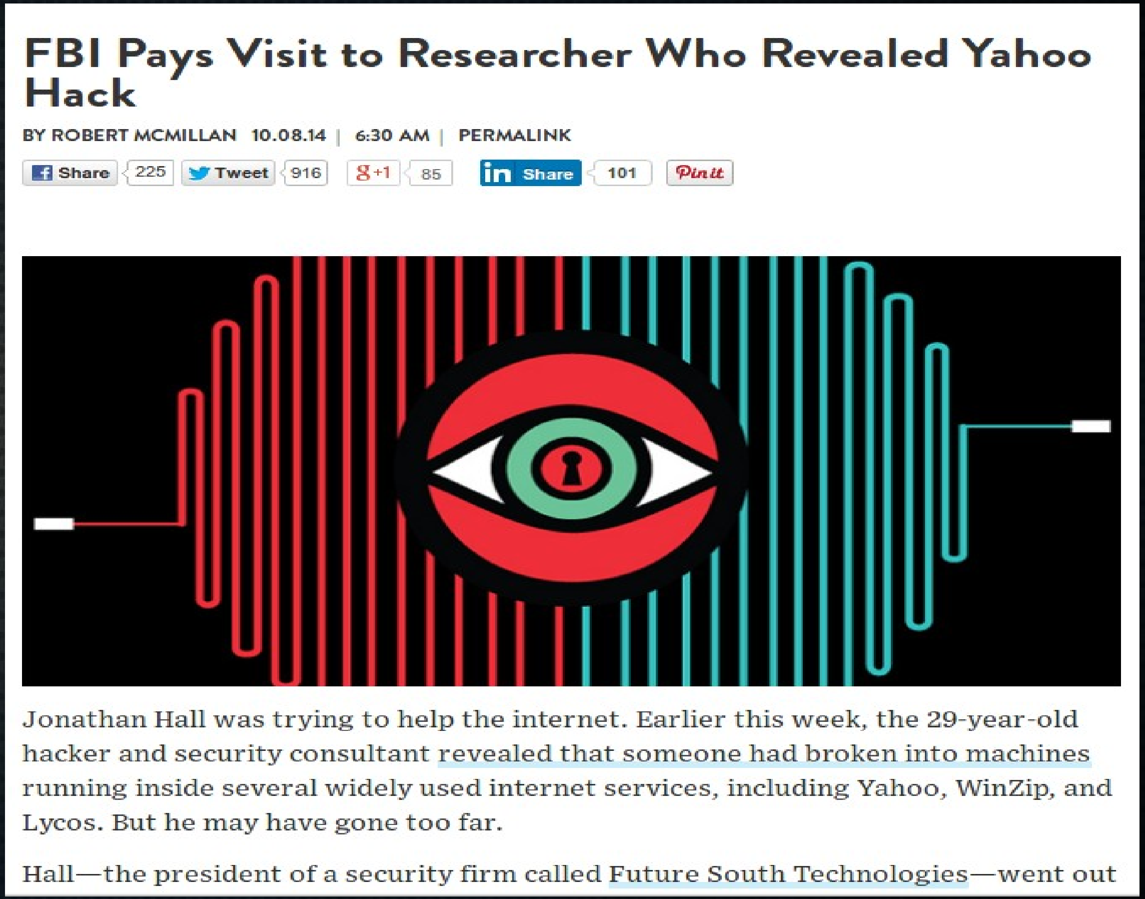
- Start with small automation scripts.
- Nmap NSC scripts
- Burp Suite extensions
- Static Analysis scripts
- Pentesting or analysis tools



- Build vulnerable applications (learn to code applications, identify loopholes and know how to write secure code)
- Regex and N/W programming
- **One of the best tricks to impress your leads at work: automate, automate and automate...;)**

Bug Bounty and hall of fames

- Get paid for finding bugs in applications.
- Get your name published among the "Hall Of Fame(white hats)" pages on companies websites.
- Include these in your resume to make it stand out from the rest.
- Cons:
  - Do not do any crap with the stuff which is out of scope.
  - Pay specific attention to scope and don't test for things randomly on the web, this may land you in jail. Better be aware of things.



FBI Pays Visit to Researcher Who Revealed Yahoo Hack

BY ROBERT MCMILLAN 10.08.14 | 6:30 AM | PERMALINK

Jonathan Hall was trying to help the internet. Earlier this week, the 29-year-old hacker and security consultant revealed that someone had broken into machines running inside several widely used internet services, including Yahoo, WinZip, and Lycos. But he may have gone too far.

Hall—the president of a security firm called Future South Technologies—went out

Certifications

CISSP - Certified Information Systems Security Professional
SSCP - Systems Security Certified Practitioner
CAP - Certified Authorization Professional
CSSLP - Certified Secure Software Lifecycle Professional
CCFPSM - Certified Cyber Forensics Professional
HCISPP - HealthCare Information Security and Privacy Practitioner

OSCP,OSWP,OSCE,OSEE,OSWE

ISO 27001 Lead Auditor

CEH - Certified Ethical Hacker
ECSA - EC Certified Security Analyst
CHFI – Computer Hacking Forensic Investigator

GSEC,GCIH,GCIA,GPEN,GWAPT,GPPA,GCWN,GISF,GAWN,GCED,GCUX,GXPN,GMOB,GICSP,GCCC

LinkedIn, Twitter, Blogs and GIT

- Having done most of the above is not all said and done, you need to showcase your skills, contributions, enthusiasm and promptness
- Use **GIT** to showcase your code
- Keep **blogging** your interests in the field of information security, at the same time keep reading blogs of indusrty security professionals...who knows... you may land up writing a paper as an extension of those thoughts.
- **Twitter** has become a knowledge base for infosec professionals these days, anyone come with new stuff, they "Tweet"
- **LinkedIn**: A best way to showcase your profile to industry experts, people get calls and job invitations through linkedIn

Finally!!!

Interview Tips:

- Keep you default question stack ready.
  - Risk, Vulnerability, Exploit, CIA etc.
  - N/W port numbers, Ping stuff, Pentesting phases
  - S/W vulnerabilities
  - Web basics, xss, sqli and csrf
  - Basic Linux commands
  - Examples, Testing scenarios and processes.
  - Growth Mind Set
  - Analytical Skills, thought process and reasoning. (Back your answers with concepts and reasoning)
  - Don't keep your answers defenitive...provide your approach of thinking
  - Showcase interest and enthusiasm

- Learn it, Master it and give back to the community.

You see...you forget

You do...you remember

You practice...you master

Its Video Time

Questions?

Let's get the panel discussion on :)

Thank you!