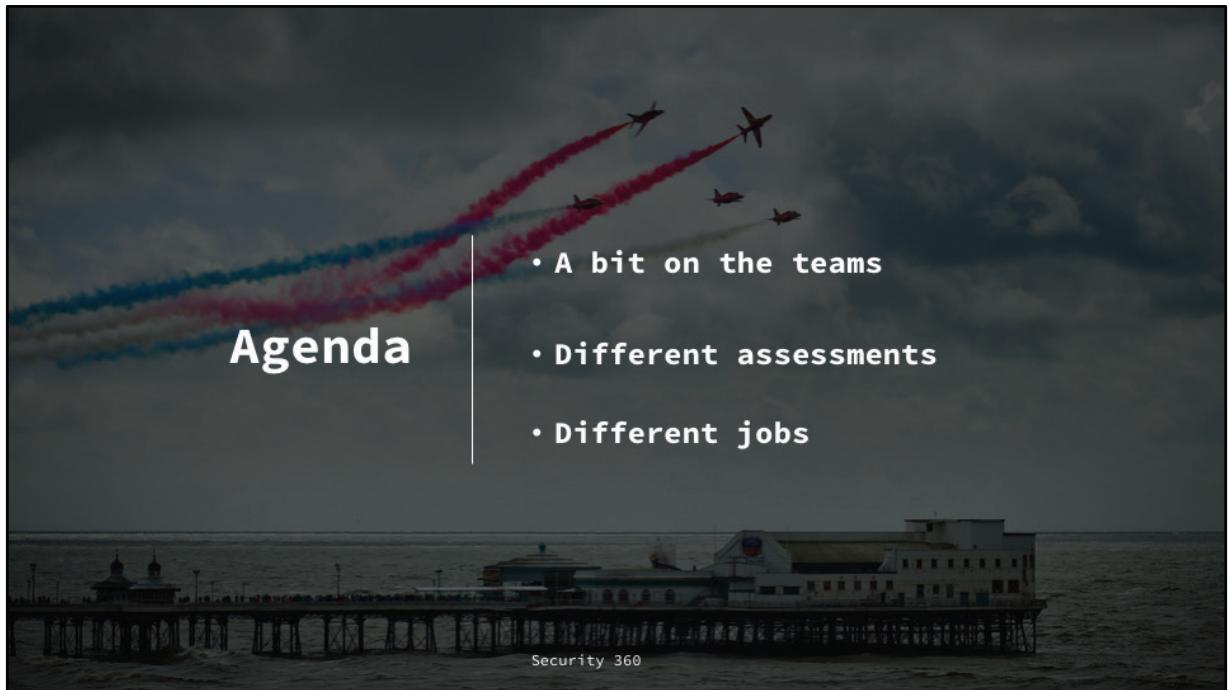


Red, Blue & Purple

Responsibilities & Jobs



"Red Arrow display team" by [KevHaworthPhotography](#) is licensed under [CC BY-NC 2.0](#)

The Teams

- Red
 - Hired in to simulate a malicious attack on an organisation's infrastructure (consultants)
 - Large organisations likely have red experts on staff
- Blue
 - Employed to defend organisation critical infrastructure
 - Full-time employment with the organisation

Security 360

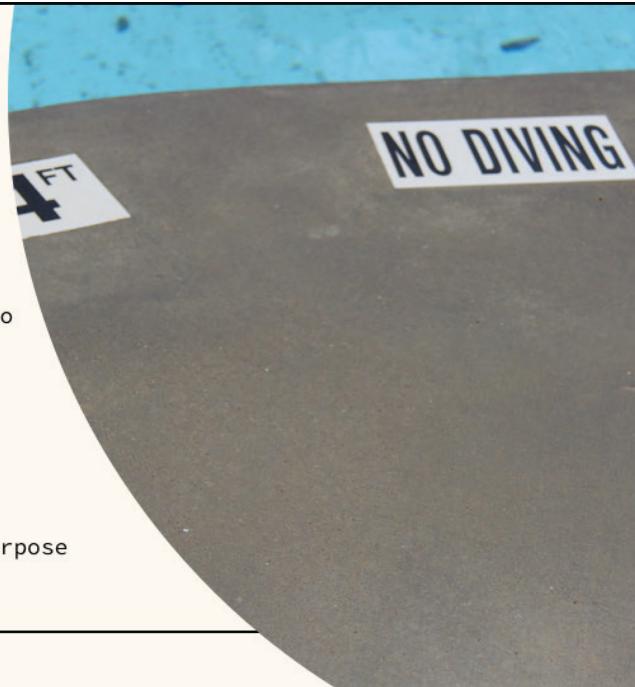


"Goal Posts" by [KTDEE....](#) is licensed under [CC BY-NC-ND 2.0](#)

Common Assessments

- Vulnerability Scanning
 - The basic assessment, requires no expert knowledge
 - Penetration Test
 - A manual black- or grey-box test
 - Red Team Engagement
 - Black-box. Has a much broader purpose
-

Security 360



["IMG_8439"](#) by [sdauchert](#) is licensed under [CC BY-NC 2.0](#)

Vulnerability Scanning

- An assessment, usually automated by software
 - Find common vulnerabilities, not organisation-specific
 - Can be run by blue teams, red teams or non-experts



White-box/Authorised Vulnerability Scan

- Run locally or over the network, has admin rights



Grey-box Vulnerability Scan

- Run over the network, given some knowledge of network



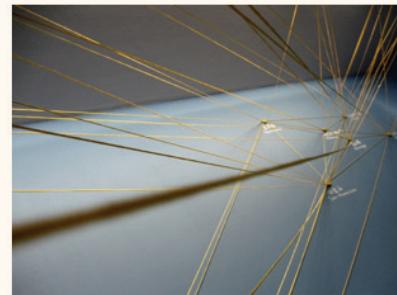
Black-box/Manual Vulnerability Scan

- Run over the network with no special knowledge

Security 360

Penetration Testing

- A manual assessment
- Carried out by a red team
 - Mimics common network attacks
 - Targeted at the organisation
- Different levels of focus
 - Can be black-box for general testing
 - Or grey-box for testing specific parts of the network
 - Organisation might reveal IP ranges/ports



Security 360

"Network" by [Jennifer Stylls](#) is licensed under [CC BY-NC-ND 2.0](#)

Red Team Engagement

- A mission
- Double-blind
 - opposing blue team is unaware
- Includes a vulnerability scan
 - manual or automated
- Includes a penetration test
 - Realistic techniques
- Breaches of physical security
- Social engineering
- Impact analysis



Security 360

["Monkey Checkers: Red"](#) by [iamhenry](#) is licensed under [CC BY-NC-ND 2.0](#)

Physical Security

- Physical Pen Testing - it's a thing!
- Many techniques threaten physical security
 - Lockpicking
 - Copying RFID cards, key fobs
 - Theft
- Social engineering can help!
 - Cause a server outage, be the engineer
 - Sit beside victim in a cafe



Security 360

"Today I taught lock picking 101 at @techsmith. What'd you do today at work? #lockpick #geek #nerd" by betsyweber is licensed under CC BY 2.0

Social Engineering

- Phishing & Spear-Phishing
- Pineapple WiFi
- Remember Koppix?
 - USB-bootable security distro
 - Boot-to-Kali & steal hashes manually



Security 360

"Supervisor with tablet PC at construction site" by [Engineering at Cambridge](#) is
licensed under [CC BY-NC-ND 2.0](#)

Social Engineering Hardware

- Rubber Ducky
 - Keyboard emulation, auto keystroke injection in a USB
- Bash Bunny
 - Scripted recon, opening shells, cred sniffing in a USB
- LAN Turtle, Packet Squirrel
 - Scripted MitM, packet sniffing in a USB



Security 360

" by [李伯舜](#) is licensed under [CC BY-NC-ND 2.0](#)

impact site on Earth!

Guided Rim Tours • Gift & Rock Shop
Interactive Discovery Center

MeteorCrater
EXPERIENCE THE IMPACT!

Impact Analysis

- What is the potential harm
 - Denied service?
 - Corrupted data?
 - Stolen PII?
 - Personally Identifiable Information
 - Stolen IP?
 - Intellectual Property
 - Defacement?

Adult missions
with this ad*

Security 360 100-289-5898 • MeteorCrater.com

WILLIAMS SEDONA

*Offer good with purchase of admission ticket. Discount good for two consecutive admissions. Offer expires 03/31/2017. KEY0217

"*Meteor crater*" by [MarkGregory007](#) is licensed under [CC BY-NC-SA 2.0](#)

Red Team Ideas

- Get permission
- Be adversarial (*real threat*)
- Report thoroughly
- Provide alternative analysis
 - Ideas, attacks, techniques not previously considered
- Provide an attack model (Advanced Persistent Threat)
 - Long-lasting, covert attack or data extraction

Security 360



<https://www.slideshare.net/TobyKohlenberg/red-teaming-probably-isnt-for-you-81283357>
"[26/365] The Pioneers" by SortOfNatural is licensed under CC BY-NC 2.0

There's a NIST for that...

- NIST SP800-115
 - Technical Guide to InfoSec Testing & Assessment
- Four steps
 - Plan (& report)
 - Discover
 - Attack
 - Gain Access
 - Escalate Privileges
 - Browse (& re-discover)
 - Install tools
 - Report



Security 360

"070218D Informática al peso" by [juanignaciosl](#) is licensed under [CC BY-NC-ND 2.0](#)
<https://csrc.nist.gov/publications/detail/sp/800-115/final>

NIST Vulnerability Categories

- Misconfigurations (as in OWASP)
 - Poorly implemented security controls / practices
 - Kernel Flaws
 - Weaknesses in the core of the OS itself
 - Buffer Overflows
 - Input does not fit in the allocated memory.
 - Malicious code passed in & executed
 - Smashing the Stack for Fun & Profit
-

Security 360

http://www-inst.eecs.berkeley.edu/~cs161/fa08/papers/stack_smashing.pdf

More Vulnerable Categories

- Poor Input Validation (injection in OWASP)
 - Attacks such as SQL-injection
- Symbolic Links
 - "shortcuts" while maintaining (elevated) permissions
- Race Conditions
 - Executing malicious code in parallel with privileged calls can give privileges to the malicious code

Security 360

Red Team HQ

- Large organisations have in-house red teams
- Small & medium organisations use security firms & consultancies specialising in red teaming
- An organisation must have a strong blue team in place first, otherwise the work of the red team is wasted



Security 360

["Sure Does Feel Like It"](#) by [Amarand Agasi](#) is licensed under [CC BY-NC-SA 2.0](#)

Blue Team HQ

- Called the Security Operations Centre (**soc**)
 - On payroll - so they get an office
 - The SOC uses a SIEM
 - Security Information and Event Management system
 - A single interface which aggregates logs, alerts and monitoring from IDS/IPS/Firewall/System/etc...
 - OWASP is working on a framework which defines some responsibilities & roles
-

Security 360

[https://www.owasp.org/index.php/OWASP_Security_Operations_Center_\(SOC\)_Framework_Project](https://www.owasp.org/index.php/OWASP_Security_Operations_Center_(SOC)_Framework_Project)

OWASP SOC Framework

- Processes
 - Monitoring & Detection
 - Incident Response
 - Threat (Vulnerability) Hunting
 - Quality Assurance (Learning)
- Roles
 - SOC Analyst - monitor SIEM logs/alerts & raise tickets
 - SOC Engineer/Expert - configure SIEM & other components
 - SOC Incident Handler
 - SOC Manager



Security 360

"Sub Control Station At The Submarine Force Library & Museum" by [Islbrian](#) is licensed under [CC BY-NC-SA 2.0](#)

Red teams have all the fun

- A blue team equivalent of pen tests and red team engagements?
(not quite)
- But honeypots!

Security 360



["clown"](#) by [I woz ere](#) is licensed under [CC BY-ND 2.0](#)

Honeypots

- Kind of like a penetration test in reverse
 - Intentionally weak/vulnerable servers
 - **Not** obviously so, attacker cannot tell
 - Isolated, no danger to critical infrastructure
 - With specific activity tracking scripts
 - Verbose logging / monitoring
-

Security 360

Honeypot Goals

- See attempted passwords
- Follow attempted techniques
- See tools used
- Discover geolocation by IP
- Distract from critical infrastructure



Fingerprinting, or, building an attack signature

Security 360

"Hunny" by Thomas Hawk is licensed under CC BY-NC 2.0

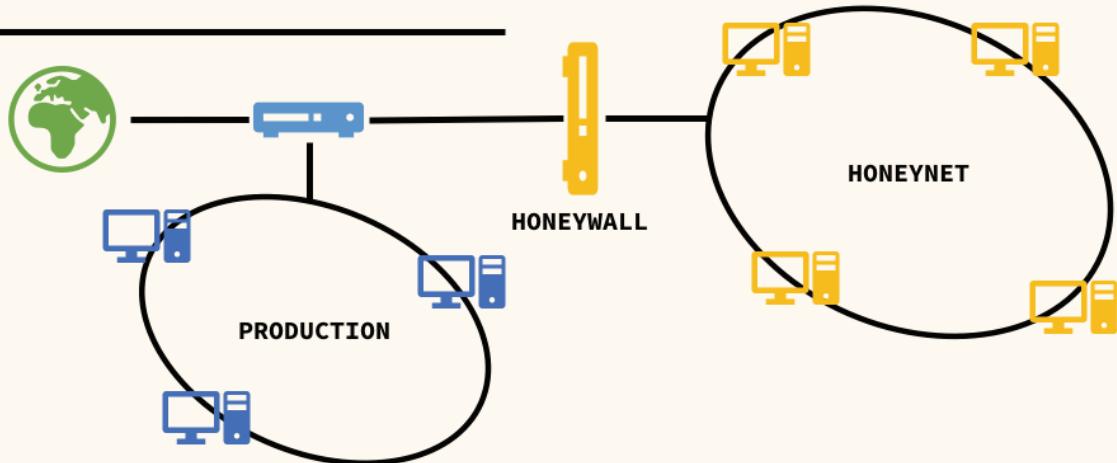
Honeynets

- A collection of honeypots, imitating a network
- Goals
 - Discover lateral movement across the honeynet
 - Discover probing techniques
 - Discover vulnerabilities
 - Discover lower layer OSI attacks
- Separated from real network by a **honeywall**
 - **Captures** data passing in & out of honeynet, covertly
 - **Controls** data passing in & out, for protection
 - **Analyses** data for the blue team

Security 360

<https://distrowatch.com/table.php?distribution=honeywall>

Honey Architecture



Job Titles

- Job titles in security (and IT in general) are easily thrown around and used quite loosely

50 Cybersecurity Titles That Every Job Seeker Should Know About



A special resource for cybercrime fighters and wannabes

- [Steve Morgan](#)

Northport, N.Y. — Feb. 1, 2019

There will be [3.5 million unfilled cybersecurity jobs by 2021](#) — enough to fill 50 NFL stadiums — according to Cybersecurity Ventures.

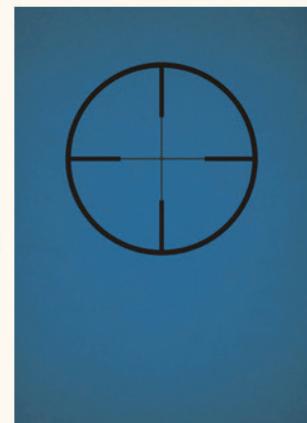


Security 360

<https://cybersecurityventures.com/50-cybersecurity-titles-that-every-job-seeker-should-know-about/>

A few ideas for a blue team

- Analyst
- Incident Responder
- Malware Analyst
- Security Engineer
- Threat Intelligence R&D (think Symantec)
- ADMIN {
 - Policy & Governance
 - Identity & Access Management
 - Secure Development



Security 360

<https://tisiphone.net/2015/11/08/starting-an-infosec-career-the-megamix-chapters-4-5/>

"Posters" by Guðný Pálsdóttir is licensed under [CC BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/)

A few less for a red team

-
- Penetration Tester
 - Physical Pen Tester
 - Vulnerability Researcher



Less positions

More demand because red teams are "cool"
Experience needed

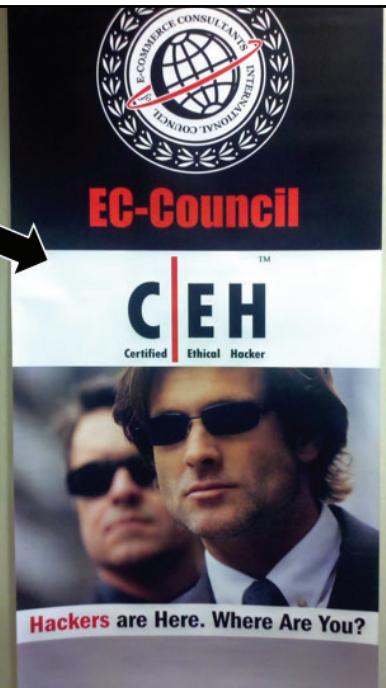
Security 360

"Red Fleet Trucks" by InertiaCreeps is licensed under CC BY-NC 2.0

Certifications

- CompTIA path
 - The entry-level creds
- (ISC)² path
 - The pro creds
- OffSec path
 - Pen test bragging rights

Not highly regarded in industry



Security 360

"Certified Ethical Hacker" by pchow98 is licensed under CC BY-NC-ND 2.0



CompTIA Pathway

- Computing Technology Industry Association
- Start with CompTIA Security+
- Then specialise:
 - CompTIA CySA+
 - Defence - a blue team cred
 - CompTIA PenTest+
 - Offence - a red team cred

Security 360



(ISC)² Pathway

- International Information System Security Certification Consortium
- Enter with CISSP (min. 5 year paid work in 2 security streams)
- Specialise with
 - Information Systems Security **Architecture** Professional
 - CISSP-ISSAP
 - Information Systems Security **Engineering** Professional
 - CISSP-ISSEP
 - Information Systems Security **Management** Professional
 - CISSP-ISSMP
 - Certified **Cloud** Security Professional

Security 360



OffSec Pathway

- From Offensive Security, creators of Kali
- Start with the OSCP
- Specialise with:
 - Offensive Security Certified Expert (OSCE)
 - Level up
 - Offensive Security Web Expert (OSWE)
 - WebAppSec
 - Offensive Security Exploitation Expert (OSSE)
 - Windows Exploits

Security 360