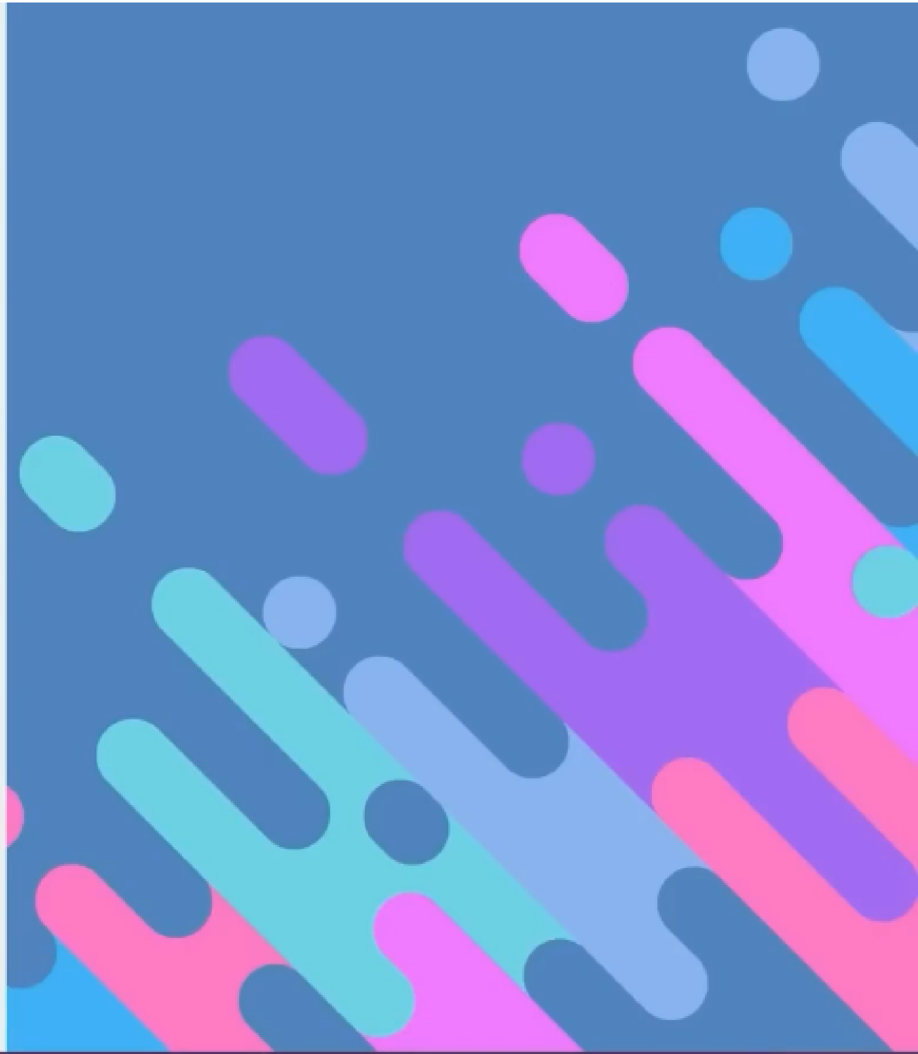
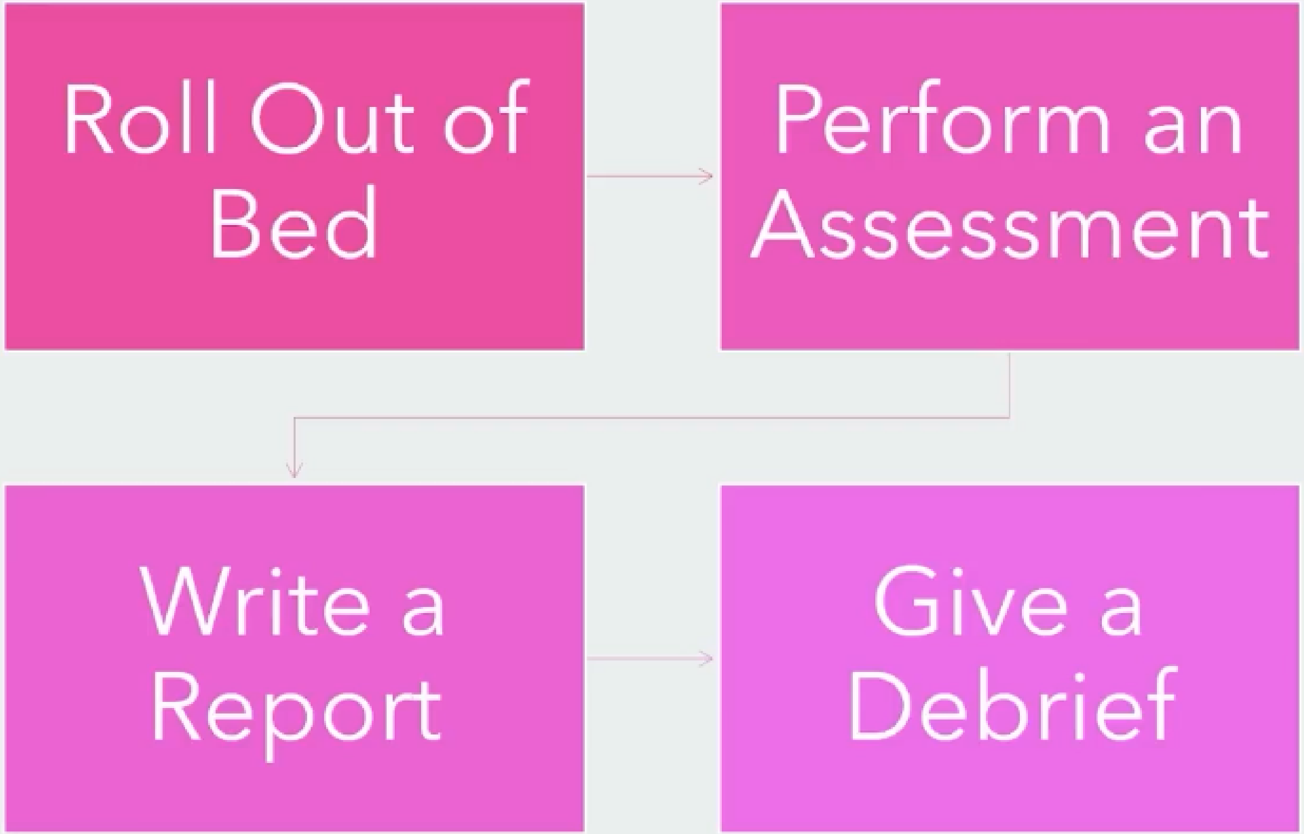
A Day in the Life of an Ethical Hacker

2022 Edition



A Pentester’s Day to Day



Roll Out of Bed

Perform an Assessment

Write a Report

Give a Debrief

Assessment: External Network Pentest

Assessing an organization’s security from the outside looking in

Methodology focuses heavily on Open-Source Intelligence (OSINT) Gathering

Typically lasts 32-40 hours with another 8-16 for report writing

Assessment: Internal Network Pentest

- Assessing an organization’s security from inside of the network

- Methodology focuses heavily on Active Directory attacks

- Typically lasts 32-40 hours with another 8-16 for report writing

Assessment: Web Application Pentest

- Assessing an organization's web application security
- Methodology focuses heavily on web-based attacks and the OWASP testing guidelines
- Typically lasts 32-40 hours with another 8-16 for report writing

Assessment: Wireless Pentest

- Assessing an organization's wireless network security
- Methodology depends on wireless type being used (guest vs WPA2-PSK vs WPA2 Enterprise)
- Typically lasts 4-8 hours per SSID with another 2-4 for report writing

Assessment: Physical Pentest & Social Engineering

- Assessing an organization's physical security and/or end-user training
- Methodology depends on task and goals
- Typically lasts 16-40 hours with another 4-8 for report writing

Other Assessments

- Mobile Penetration Testing
- IoT Penetration Testing
- Red Team Engagements
- Purple Team Engagements
- Plus more

Report Writing

A report is typically delivered within a week after the engagement ends

Report should highlight both non-technical (executive) and technical findings

Recommendations for remediation should be clear to both executives and technical staff

Debrief

A debrief walks through your report findings. This can be with technical and non-technical staff present.

It gives an opportunity for the client to ask questions and address any concerns before a final report is released.