Gov-X Innovation Challenge 2021

OFFENSIVE SECURITY

Martin Potgieter & Benedikt Boehm

Martin Potgieter

Technical Director

Background:

- Techie at heart
- Co-founder of Nclose
- Almost 20 years of Cyber Security Exp
- Running Nview MDR and Security Assessment

Benedikt Boehm

Penetration Tester

Background:

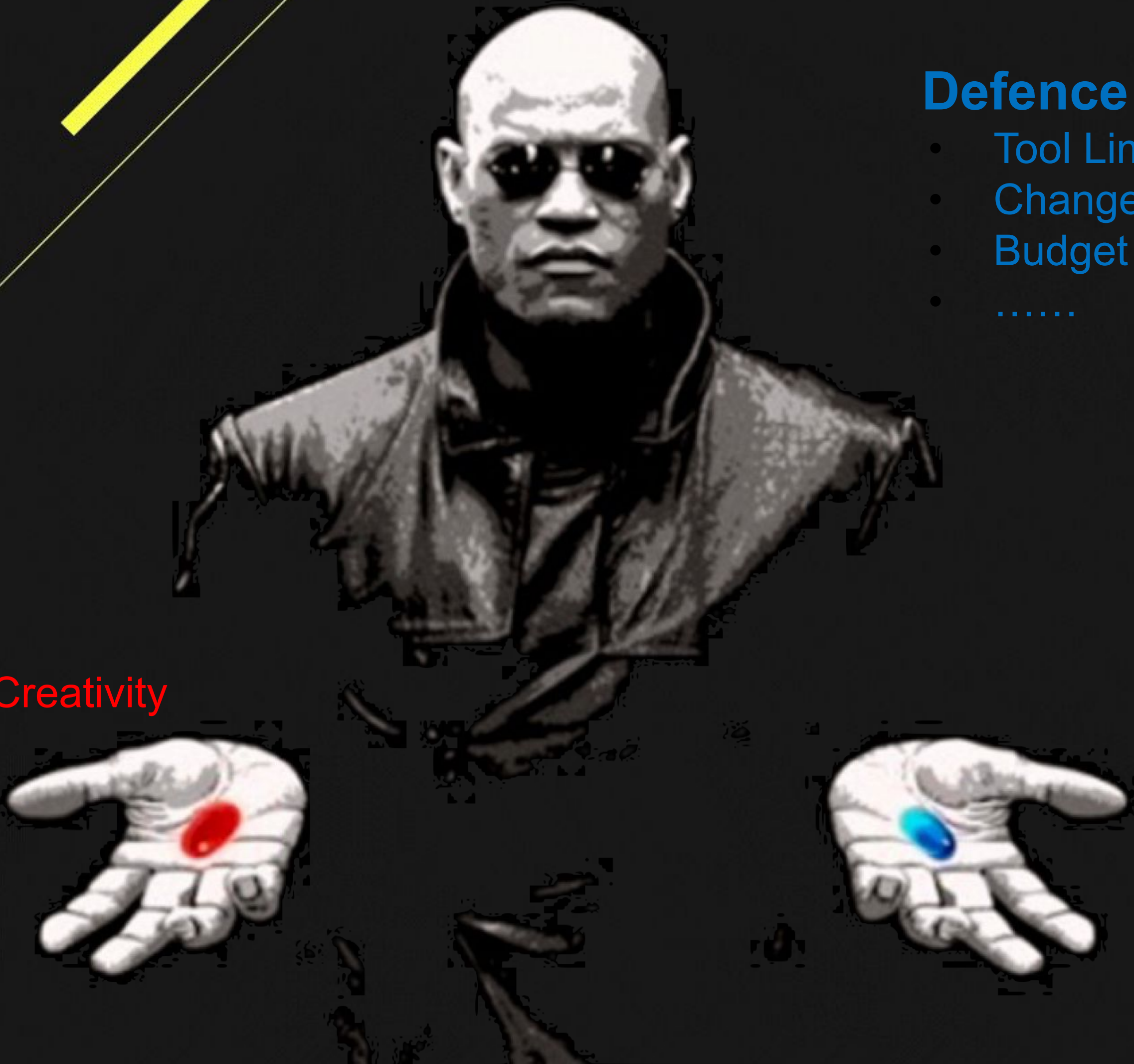
MSc in Computer Security @ University of Kent, UK

Performing cyber security assessments at Nclose since 2019

Offensive Security?

Simulating the methods, tactics, techniques and using tools of real world adversaries in an attempt to identify weaknesses within an system. The ultimate goal being to proactively mitigate the identified weaknesses

**https://danielmiessler.com/study/security-assessment-types/



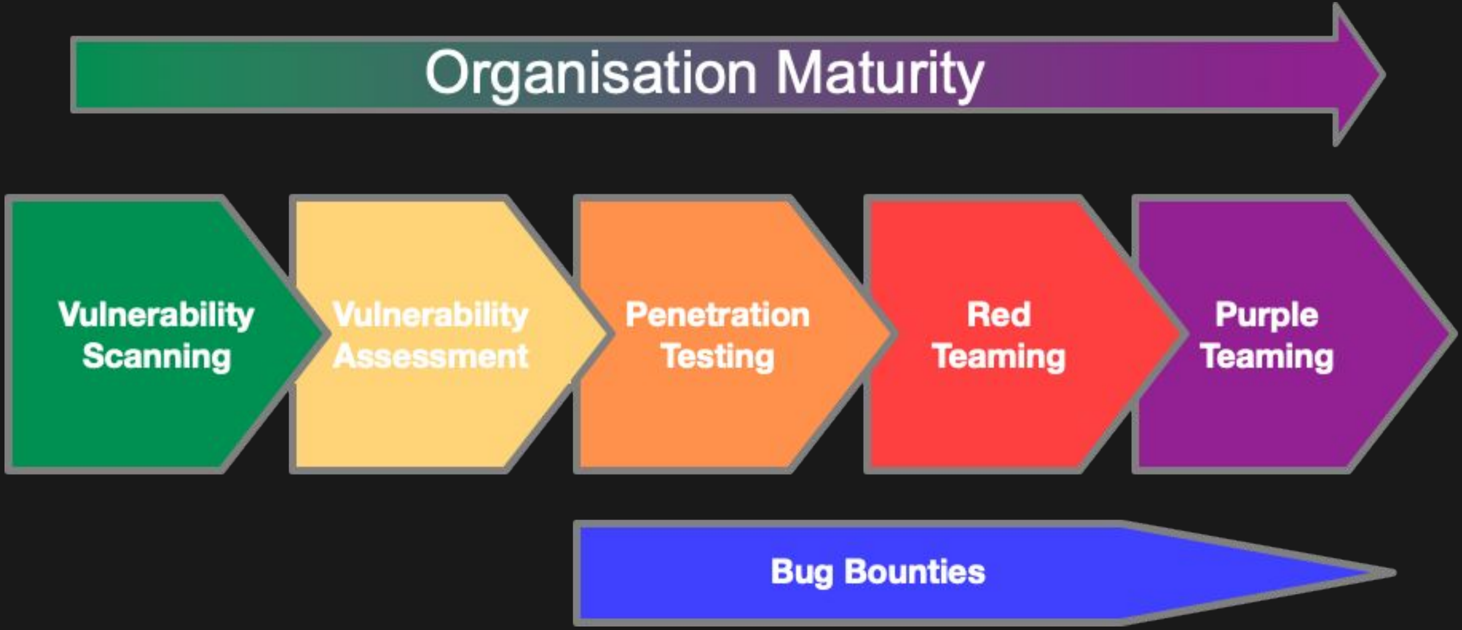
Defence

- Tool Limitations
- Change Control
- Budget Approval
- ……

Offence

- Complete Creativity
- No Rules
- Sneaky
- ……

Maturity of Offensive Practices



**https://danielmiessler.com/study/security-assessment-types/

ZA's Rich Cyber Offensive History

sensepost

thinkst
applied research
http://thinkst.com

TheGrugq

Evolving from Offence to Defence

There is a history of offensive researchers moving to defence.

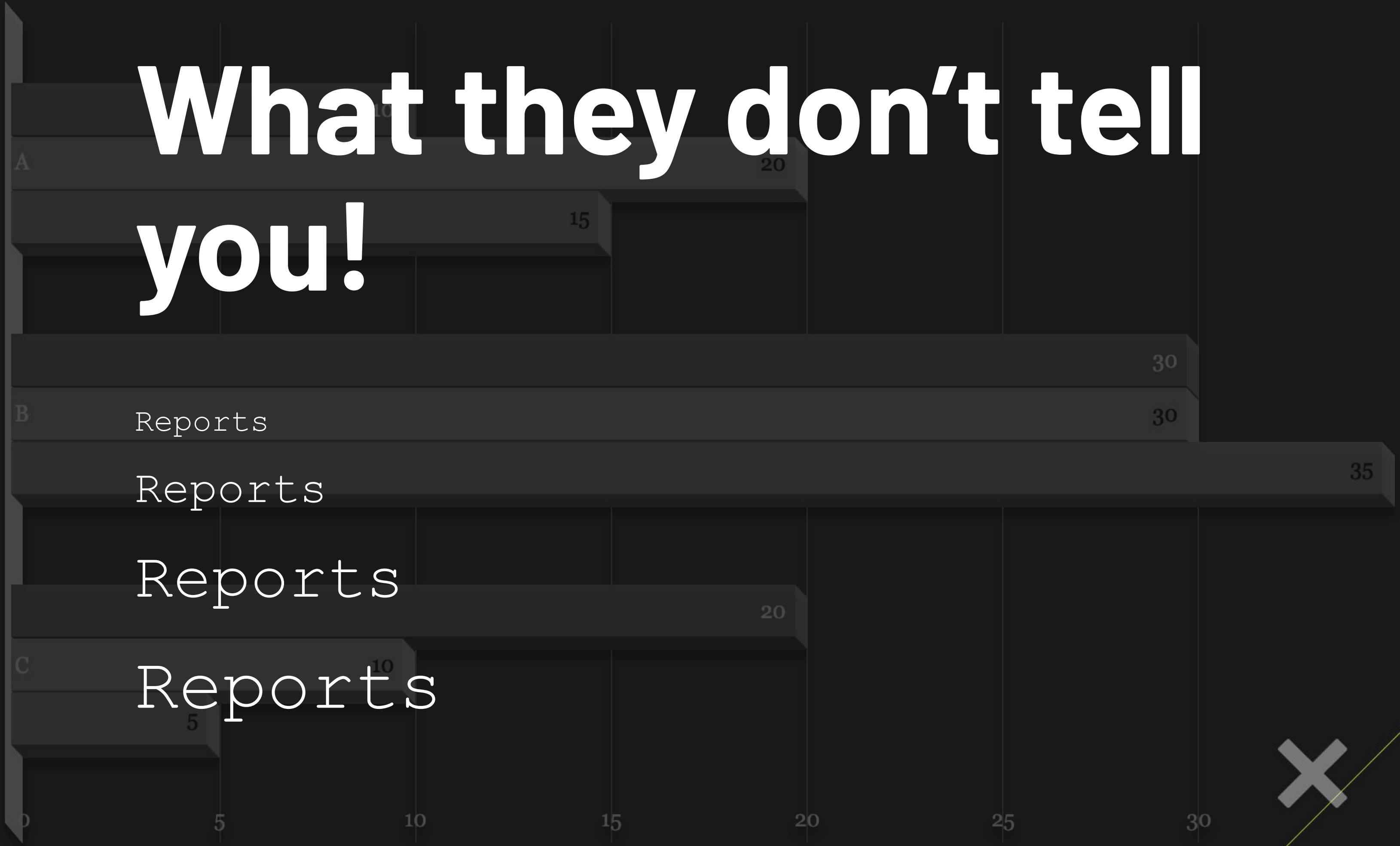
- Offence practices have their ceiling if you have morals.
- Defence has become more creative and interesting.

- Defence is more challenging.

What do I study?

- PenTest+ -> basics
- CEH -> basics
- Offensive Security (OSCP) -> You know what you are doing
- University Degree -> you need to write reports
- Dev experience -> Great for web application testing
- Broad IT experience -> Cyber Security Touches on anything

What they don’t tell you!



Reports

Reports

Reports

Reports

Walkthrough of a Typical Engagement

The following slides will cover a common engagement knows a ‘Vulnerability Assessment’

Aim of a Vulnerability Assessment

- Provide the client with a prioritized list of cyber security related issues that were discovered
- Be able to demonstrate and explain the danger of each finding to the client
- Help the client remediate the issues identified

High Level View of a Vulnerability Assessment

- Receiving a scope from a particular client
- Passive and Active Intelligence Gathering
- Vulnerability Analysis
- Performing POC (proof of concept) attacks. Knows a ‘exploitation’
- Reporting

Gathering a Scope from the Client

What we need from a client to perform the assessment

- List of all targets that need to be assessed (typically via a list of IP addresses or domain names)
- Client deadlines that need to be considered
- Any other special requirements that the client might have

passive intelligence gathering

Any type of activity that reveals useful information but does not raise any flags for the target.

- Employee names from Linkedin
- Subdomains names via research tools such as ‘dnsdumpster’
- Careers pages
- Search of leaked credentials
- Many more

active intelligence gathering

Reveals information about the target by probing it directly. Typical activities include:

- Port scans
- Host identification on a specific network range
- SSL cipher suite enumeration
- Brute force subdomain enumeration
- Many more

Vulnerability Analysis

Once all services of a target have been identified, we start looking into each service and try to discover issues that may impact the security of the system

Vulnerability analysis typically starts with the use or automatated vulnerability scans and ends in manual analysis

Automated Vulnerability Analysis

Use of tools that perform functions such as

- Lookup discovered services in exploit databases
- Sending a series special inputs to a service in order to achieve direct access to a database
- Sending a series of unexpected inputs to a service in order to obtain debugging information

Examples of tools

- General (infrastructure type) Scanners
  - Nessus
  - OpenVAS
- Specialized Scanners for specific services
  - Nikto
  - Burp Suite

Manual Vulnerability Analysis

Manual vulnerability analysis is important in order to verify vulnerabilities that were reported during automated scans as well as increase the thoroughness of a vulnerability assessment by crafting probes that are specific to the target and would not be covered by an automated tool

Examples of tools

- Netcat (manual networking tool that allows for interaction with any type of networked service)
- Burp Suite (toolkit for http(s) services with manual and automatic testing functions)

Exploitation

Verifying the existence of security issues by running exploits in a responsible manner.

Successful exploitation will have a significant impact on the severity of a finding

Examples

- Successfully manage to store a script on a website that can negatively affect other users (known as cross site scripting).
- Successfully Uploading a file to a web server that will cause a arbitrary operation to be run on the host machine (knows as remote code execution).

Reporting & Remediation

- Report containing a summary of the engagement and a detailed list of all discovered vulnerabilities is handed to the client
- A debrief session is scheduled with the client to discuss all issues in person or via web conference
- A remediation test is scheduled in order to ensure that the clients vulnerabilities have in fact been remediated

Are there Other Forms of Security Assessments?

- Social Engineering Assessments (e.g. phishing)
- Wireless Security Assessments
- Password Strength Audits
- Penetration Test

THANK YOU!

Any questions?

You can contact us via martin@nclose.com
and benedikt@nclose.com