Know Your Threat Actor

Liam Glanfield

nccgroup

About Me

- 10+ Years Experience in IT Support.
- 3 ½ Years Working in Cyber Security.
- Specialising in Microsoft Technology Attack and Defense.
- Managed Red Team Operations.
- Conducted Physical Security Assessments.
- Primary Contact for DC441392.

@OneLogicalMyth

OneLogicalMyth

@DC441392

nccgroup

MITRE ATT&CK Framework

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

Allows an organisation to better understand what adversaries are doing.

Covers three tactics:

- PRE-ATT&CK.
- Enterprise.
- Mobile.

https://attack.mitre.org

nccgroup

Red Team vs Blue Team

Red Team – Simulate Attacks

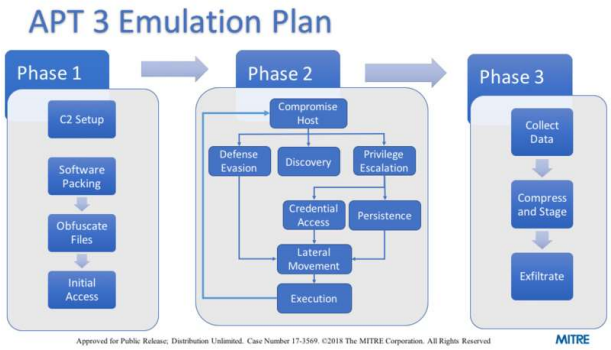
A red team challenges an organisation to improve its effectiveness by assuming an adversarial role or point of view. By assessing your cyber preventative controls, staff security awareness and challenging your Blue Team's detection and response processes.

Blue Team – Defend Attacks

A blue team is a group of individuals who perform an analysis of information systems to ensure security, identify security flaws, verify the effectiveness of each security measure, and to make certain all security measures will continue to be effective after implementation

nccgroup

Example Red Team Workflow



nccgroup

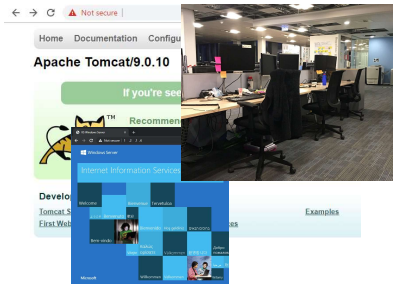
Open-source Intelligence (OSINT)

- Social Media.
- Search Engines.
- DNS Brute Forcing.
- Shodan.
- Password Dumps.
- Default Passwords.
- Document Properties.
- Certificates.

nccgroup

OSINT Example

- ServiceNow.
- Fiserv Aperio.
- Splunk.
- ID Badge Format.
- Applications Hosted on Windows.
- Shodan Search.
- Identified Contracted Firm to help Cloud Migration to AWS.

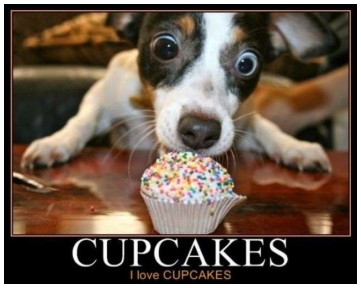


nccgroup

Social Engineering

- Phishing/Smishing/Vishing.
- Pretexting.
- Quid Pro Quo.
- Baiting.
- Tailgating.
- Warshipping.

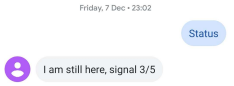
https://www.social-engineer.com



nccgroup

Drop boxes

- Raspberry Pi with 4G Dongle.
- SMS Control Capability.
- Securely Granted Access to Target Network.
- Discrete Enough to Lay Hidden for Several Months.



https://github.com/OneLogicalMyth/Huawei-SMS

nccgroup

Threat Actors

Types

- Activist.
- Competitor.
- Organised Crime Groups.
- Hacker.
- Insider (accidental/disgruntled).
- Nation-state.
- Sensationalist.

Sophistication

- None.
- Minimal.
- Intermediate.
- Advanced.
- Expert.
- Innovator.
- Strategic.

https://www.ncsc.gov.uk/blog-post/rating-hackers-rating-defences

nccgroup

Persistence

- Scheduled Tasks.
- WMI Subscriptions.
- Windows Startup Folder.
- Registry Run Key.
- Process Resource Hooking.
- Stolen Plaintext Credentials.
- KBTGT Account Hash.

http://www.fuzzysecurity.com/tutorials/19.html

nccgroup

Logging Made Easy (LME)

- A logging system that just about any organisation could manage
- Monitor software patch levels on enrolled devices
- Shows where administrative commands are being run on enrolled devices
- See which users are using which machine
- NCSC worked with the NCC Group to develop LME

https://www.ncsc.gov.uk/blog-post/logging-made-easy
https://github.com/ukncsc/lme

nccgroup

Five things to think about

- Network.
- Auditing and Logging.
- Password and Account Policies.
- Role-based Access Control (RBAC).
- Patch Management including 3rd Party Software.

nccgroup

Final Thought

The Only Thing Necessary for Evil to Triumph is for Good Men to do Nothing

Edmund Burke

nccgroup