WTF is Purple Team?!

$ whoami

v1n1v131r4.com

Agenda

- Who is Red Team?
- Who is Blue Team?
- So, who is Purple Team?
- Scenarios

Who is “Red Team”

Red Team

- Penetration tester

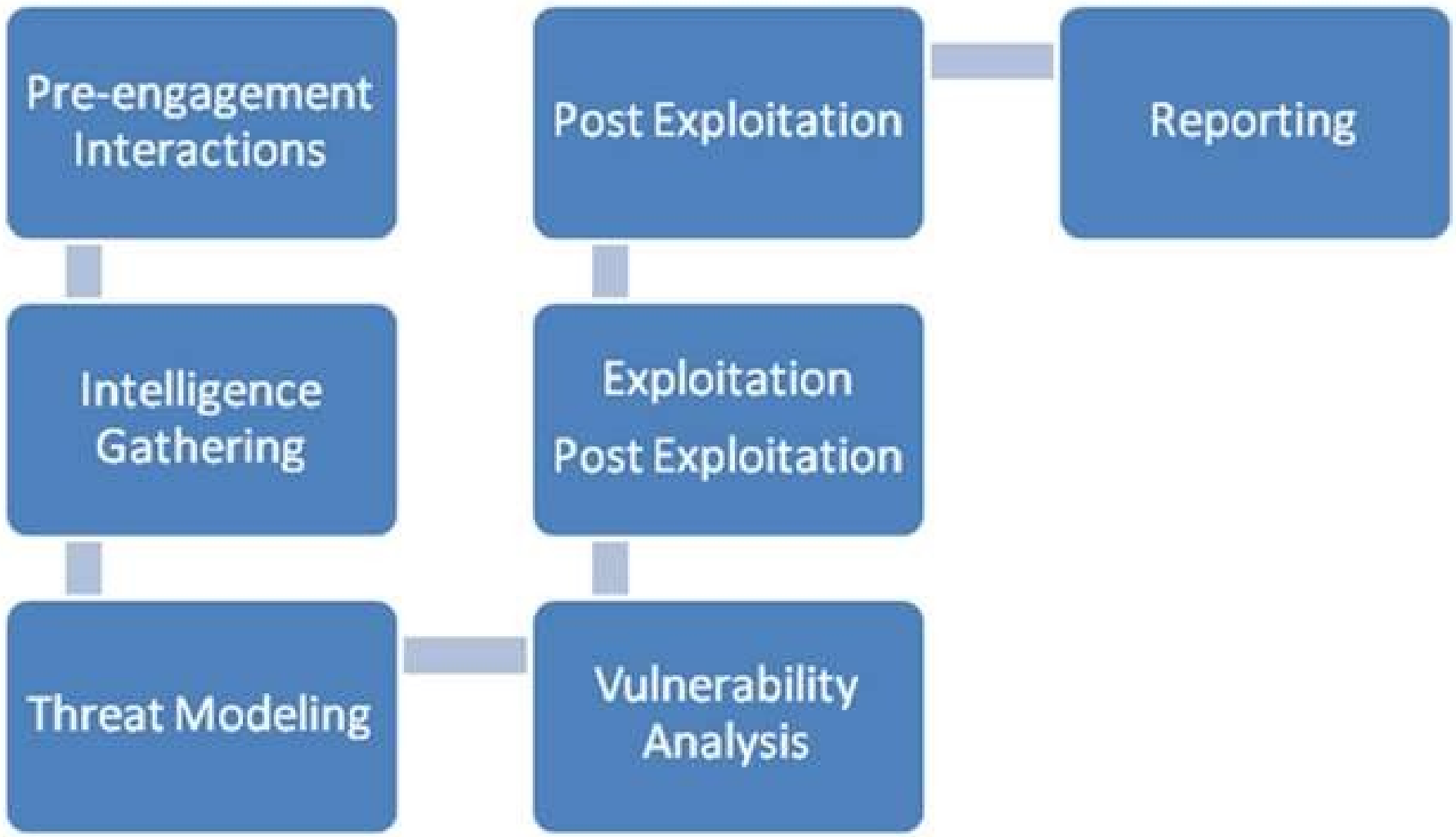
- Try to find vulnerabilities of any surface with Tactics, Techniques and Procedures (TTPs).

- Test with or without notifying to Blue Team.

- Test security detection and response capabilities to improve security.

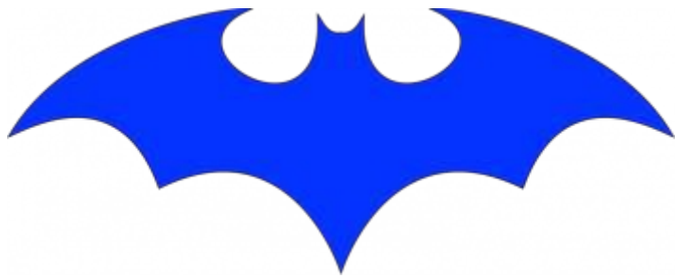
Red Team

- Vulnerability Scanning
- Social Engineering
- OSINT (Open Source Intelligence)



Reference:: http://resources.infosecinstitute.com/penetration-testing-methodologies-and-standards/

Who is “Blue Team”

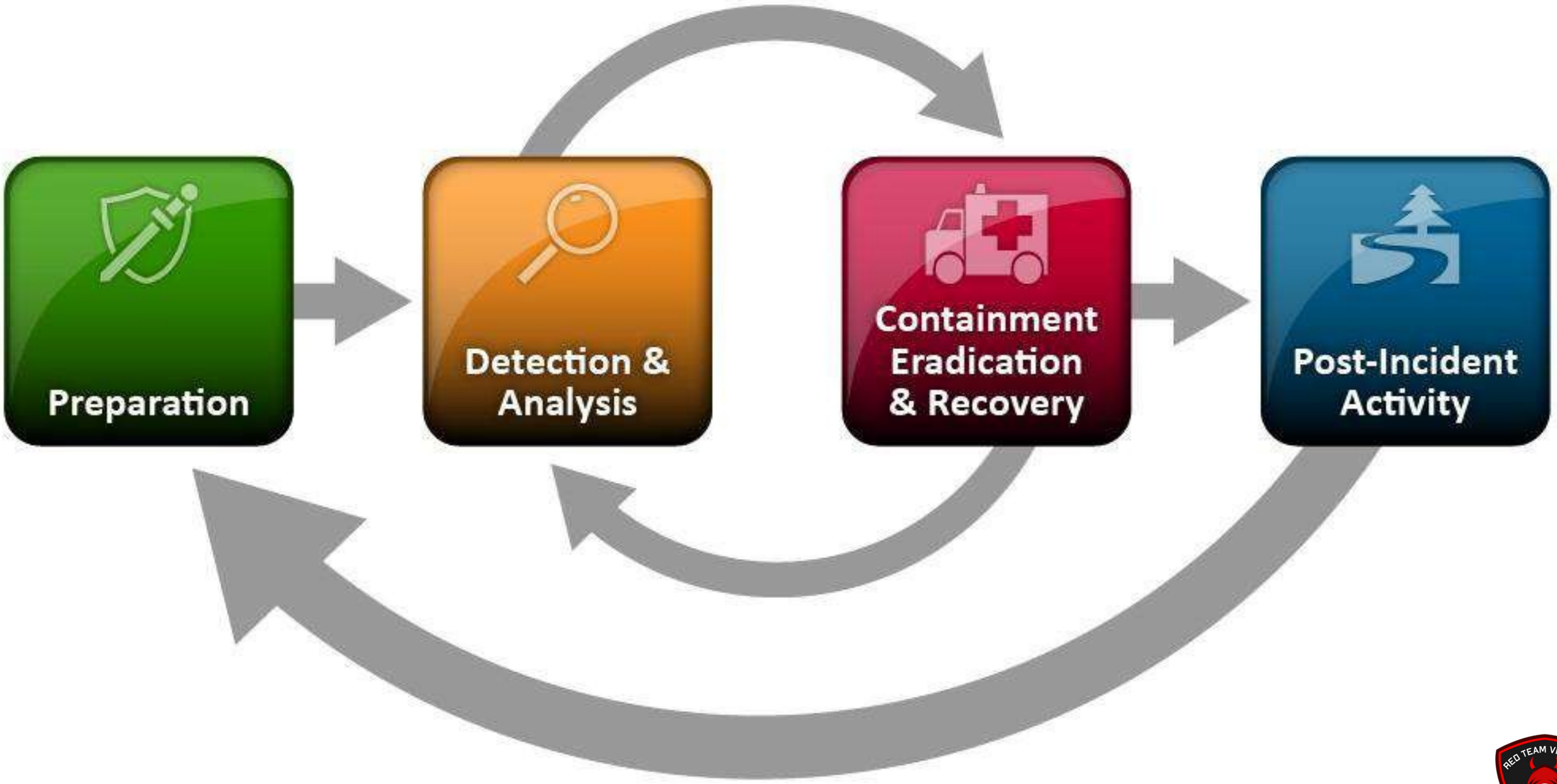


Blue Team

- SOC, Incident Response Team, Security Analysis, etc.
- Detection of attack and penetration testing
- Response of attack and penetration testing
- Recovery from data leakage, tampering or compromise
- Correct evidence left by attacker or penetration tester
- Prevention and better detection of future attacks

Blue Team

- Threat Intelligence
- Malware and Exploit - Reverse Engineering
- Digital Forensics
- Security Monitoring



Reference:: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Basically in many company

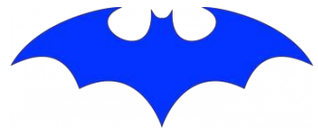
-  and  often separate the job and keep fighting each other.

- Feedback loops consist of reports being tossed over the wall if shared at all

- Emphasis is given on remediation of vulnerabilities rather than prevention and detection growth

Misleading from the top view

- Attack
- Scary report = Well done.
- Can bypass = Well done.



- Defend
- Server work fine = Well done.
- Detect and Response = Well done.
- No alert or less alert = Well done.

So, who is “Purple Team”

Purple Team

- Combine the skillset. Fulfill the gaps
- Change mind set of Red Team and Blue Team
- No alerts doesn’t mean no incident
- Scary report must have full disclosure.
- Goal of the both teams are “Improving the security of the organization”

Scenario #1

- Red Team: Can pwnage internal pc and use the pc to espionage data from another servers.
- Blue Team: Alert when Red Team do some suspicious behavior in internal network.
- Purple Team: Alert and discuss with Red Team. What they miss and what shall do next?
- Result: Coverage of Incident Response Breach Scenario

Scenario #2

- Blue Team: Monitor psexec usage and get the Red Team to test. Or it have any psexec alternative to monitor. (Event ID: 7045)

- Red Team: Find another way to run psexec alternative. (winexe, msf psexec, impacket, etc)

- Result: Blue Team get the goal.Red Team have sharpen the skill.

Scenario #3

- Blue Team: Want to detect and block ransomware
- Red Team: Test it with the brand new ransomware(created by team)
- Result: Blue Team can test the security product and got the real one. Red Team get the new surface to test.

Scenario #4

- Blue Team: Want to block all powershell command (group policy, AppLocker, etc.)
- Red Team: Test and tried to find the way to bypass (MSBuildShell, Unmanaged Powershell, etc.)
- Result: Blue Team can block powershell and similar things. Red Team have sharpen the skill.

Scenario #5

- Blue Team normally use 10 minutes to detect “Suspicious event”. How can detect and response in 1 minute.
- Red Team show what “Suspicious event” looks like.
- Result: Better monitoring and response plans.

Question?

Reference

- https://danielmiessler.com/study/red-blue-purple-teams/#gs.null
- https://www.rsaconference.com/writable/presentations/file_upload/air-w02-the-rise-of-the-purple-team.pdf
- http://carnal0wnage.attackresearch.com/2016/03/more-on-purple-teaming.html
- http://tacticaledge.co/presos/Jorge%20Orchilles%20-%20Purple%20Team%20-%20Evolving%20Red%20vs%20Blue%20-%20Tactical%20Edge.pdf
- http://www.slideshare.net/chrisgates/purple-teaming-the-cyber-kill-chain-practical-exercises-for-everyone-sector-2016