Infopercept

INVINSENSE | RBAS

Setting the context

The cyber attacks have changed in method and execution and what we are seeing currently is that adversaries are using the combined might of the excessive processing power that is available and the human intelligence to inflict as much damage as possible.

These bots or automated scripts help them launch any sort of attack and explore the vulnerabilities within the network. Once the vulnerabilities are identified, then the attackers try exploiting those to inflict maximum damage

So, it can be briefly summarised that the cyberattacks of today is a combination of human effort as in sophisticated hackers and that of the excessive micro processing power that is derived from automated machines or bots / botnets. What we are trying to defend against is not just the unknown men alone; it is the combined might of man and machine.

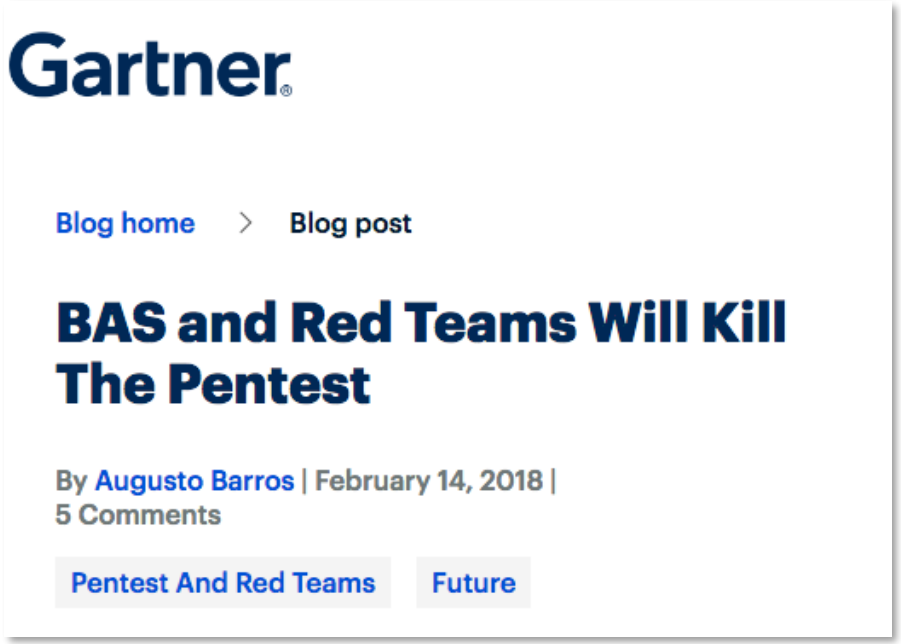
Considering the above scenario, it becomes imperative for us to address both these aspects of automation and determined hackers. An integrated approach of combining a Red Team and Breach & Attack Simulation is an approach that marries the human intelligence to artificial intelligence to put up the best fight against the cyber attacks.

Why Invinsense RBAS?

A Combined Red Team and Breach & Attack Simulation (BAS) Strategy is an exercise that focuses on defense, detection, and response capabilities to identify the gaps in your security monitoring, so you emerge prepared and empowered to take on attackers.
The most sophisticated Red Team combined with a State-of-the-Art 'Breach and Attack Simulation' Tool is a Military Grade Defense that will provide much-needed relief to management who has been caught in this battle to protect its most valuable assets.

- Our Red Team is as ruthless as Adversaries and focuses on the areas they would focus.
- Our Breach and Attack simulation will help your system and you to be always prepared for the actual cyberwar.

BAS and Red Teams Will Kill The Pentest


Gartner

Blog home > Blog post

BAS and Red Teams Will Kill The Pentest

By Augusto Barros | February 14, 2018 | 5 Comments

Pentest And Red Teams Future

Simple pentesting, for pure vulnerability finding goals and with no intent to replicate threat behavior, will vanish. This is different from the pentest that many people will prefer to call “red team exercises”, those very high-quality exercises where you really try to replicate the approach and methods of real threats.

https://blogs.gartner.com/augusto-barros/2018/02/14/bas-and-red-teams-will-kill-the-pentest/

BAS and Red Teams Will Kill The Pentest


Gartner

Blog home > Blog post

BAS and Red Teams Will Kill The Pentest

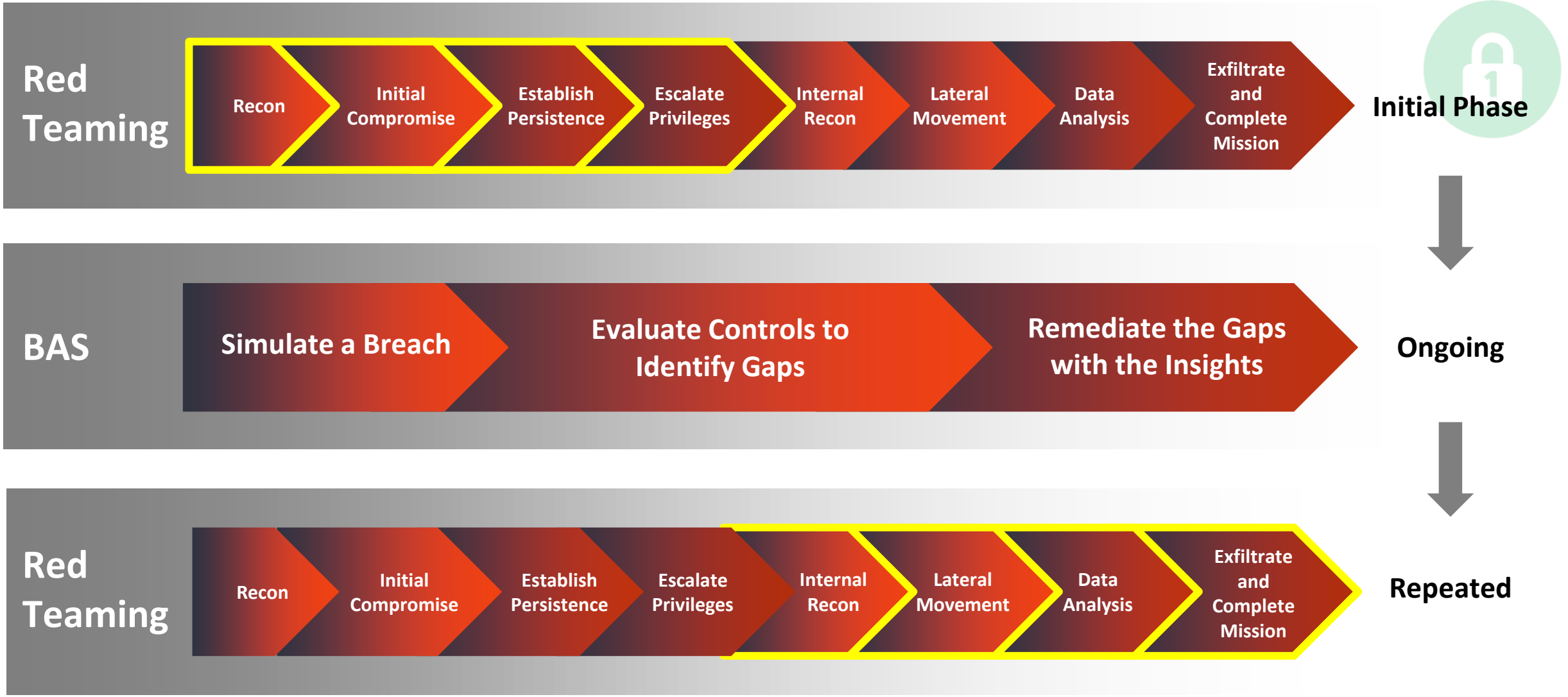
By Augusto Barros | February 14, 2018 | 5 Comments

Pentest And Red Teams | Future

BAS automates the simple pentest, performing the basic cycle of scan/exploit/repeat-until-everything-is-owned. If you have the ability to do that with a simple click of a button, why would you use a human to do that? The tool can ensure consistency, provide better reporting and do it faster. Not to mention requiring less skills (you don't even need to know how to use Metasploit!). So, with BAS, you either go for human tests because you want a red team, or you use the tool for the simple style of testing.

https://blogs.gartner.com/augusto-barros/2018/02/14/bas-and-red-teams-will-kill-the-pentest/

Invinsense RBAS - Approach



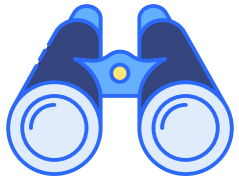
INVINSENSE

Invinsense RBAS – Red Teaming Approach

Approach
Kali Linux is an incredibly powerful tool for penetration testing that comes with over 600 security utilities, including such popular solutions as Wireshark, Nmap, Armitage, Aircrack, and Burp Suite.

KALI
BY OFFENSIVE SECURITY

Gathering Information



Analyzing Vulnerabilities

Traffic sniffing and spoofing

Stress Testing

INVINSENSE

Invinsense RBAS – Red Teaming Approach

Gathering information
▪ Amap ▪ DNSMap ▪ Network Mapper ▪ theHarvester ▪ Load Balancing Detector (lbd) ▪ Arp-scan ▪ SMBMap ▪ SSLsplit

Analyzing vulnerabilities
▪ APT2 ▪ BruteXSS ▪ Cisco Torch ▪ CrackMapExec ▪ jSQL Injection ▪ NoSQLMap ▪ SQLmap ▪ OpenVAS

Sniffing and spoofing traffic
▪ Arpspoof ▪ Burp Suite ▪ DNSChef ▪ OWASP Zed Attack Proxy ▪ MITMf ▪ Wireshark

Sniffing and spoofing traffic
▪ DHCPig ▪ FunkLoad ▪ MDK3 ▪ SlowHTTPTest ▪ T50

Invinsense RBAS – BAS

The relatively simple approach of the Breach and Attack Simulation exercise is mentioned below:

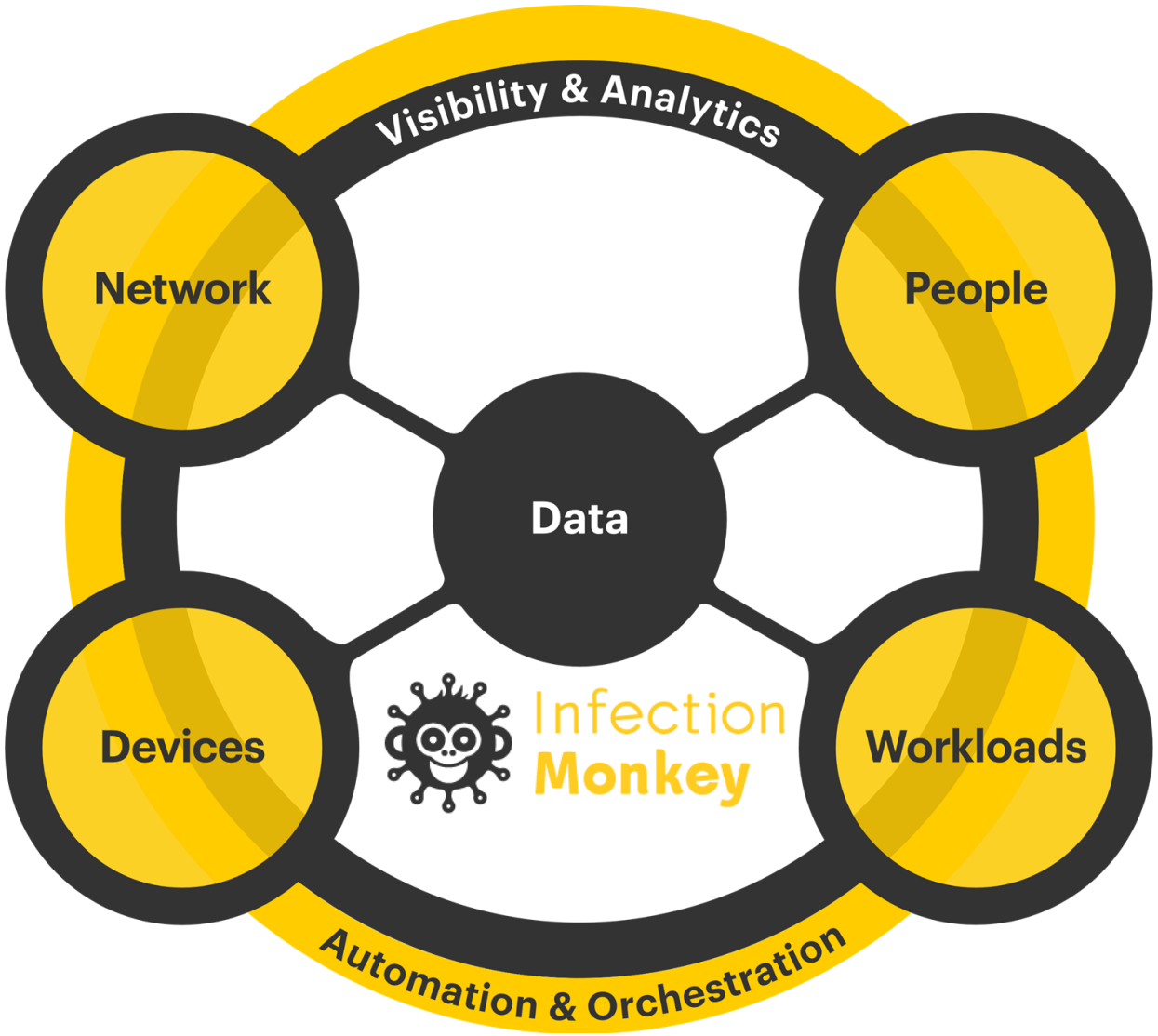
The Infection Monkey is a Breach and Attack Simulation (BAS) tool that assesses the resiliency of private and public cloud environments to post-breach attacks and lateral movement.

The Infection Monkey operates in much the same way a real attacker would - starting from a random location in the network and propagating from there, while looking for all possible paths of exploitation.

- Supports containers, public and private clouds
- Ongoing network-wide security testing
- Network map from the attacker's point of view
- Automatically Handles network regardless of size
- Simulates post breach lateral movement
- A comprehensive, detailed security findings

Infection Monkey

Invinsense RBAS – BAS Use Cases



Use Cases
▪ Test your network after every step you take toward a Zero Trust architecture. ▪ Identify the areas you need to focus on in your journey to Zero Trust. ▪ Verify your security tools meet Zero Trust requirements.

Invinsense RBAS – BAS Use Cases

Network Breach
Simulate an internal network breach and assess the potential impact.

Network Segmentation
Test network segmentation policies for apps that need ringfencing or tiers that require micro segmentation.

Credential Leak
Assess the impact of successful phishing attack, insider threat, or other form of credentials leak.

IDS/IPS Test
Test your network defense solutions.

Other
Tips and tricks about configuring monkey for your needs.

INVINSENSE

Infopercept

By accessing/ proceeding further with usage of this platform / tool / site /application, you agree with the Company's / Infopercept Consulting Pvt. Ltd.'s (ICPL) privacy policy and standard terms and conditions along with providing your consent to/for the same. For detailed understanding and review of privacy policy and standard terms and conditions. kindly visit www.infopercept.com or refer our privacy policy and standard terms and conditions.

INVINSENSE

Email
sos@infopercept.com

phone
+91 989 885 7117

website
www.infopercept.com