YOU CAN'T SECURE WHAT YOU ARE NOT AWARE OF

coupa

IMeMyself

- I am Pramod Rana, working as a senior security engineer in coupa Spend Smarter.
- Responsible for security functions in Agile methodology like penetration testing, threat modeling and cloud security assessment
- Love to understand new security trends and how to practically implement them.
- A security engineer by profession, a coder by hobby, a runner by passion
- BlackHatEurope2018 | BlackHatUSA2019 | Defcon27 | BlackHatEurope2019 | OWASP Pune Chapter Leader | OSCP

Scenario

1. You are a pen-tester and have a Hack-Me-If-You-Can black-box engagement.
   - Identified a vulnerable machine in network -> Able to compromise the host with custom exploit -> Obtained the password hashes -> Replicated your compromise in network using pass-the-hash.
   - Awesome scenario for pen-testers, right?
2. You are a security engineer and your job is to reduce the risk pertaining to your network, continuously.
   - Easy enough to approach, right?
   - Perform host enumeration scan -> Run vulnerability scan -> Triage the vulnerabilities -> Devise the remediation plan -> Revalidation -> Done

But…

1. Customer responds that impacted machine is a ‘test’ machine, which we were not aware of and we can simply decommission it. You are expected to exploit a ’actual’ target.
2. You are doing these activities on daily basis and then you became aware (from unintended resources) that one of ‘unknown’ server is running with default tomcat credentials facing internet.

And now imagine these scenarios in cloud environment. Remember CICD.

Challenges

1. It is a daunting task to have a ‘true’ understanding of a widespread network.
2. In a mid to large level organisation’s network having a network architecture diagram doesn’t provide the complete understanding and manual verification is a nightmare
    - **Static** document & difficult to update
    - Based on **understanding** of architect(s)
3. We need to have a complete picture of all the systems which are connected to your network, irrespective of their type, function, technology etc.

Proposed Solution

1. Accurate
2. Dynamic
3. Easy–to-use

Omniscient – Lets Map Your Network

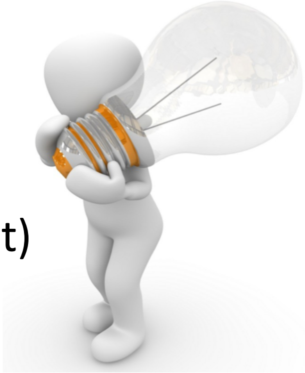
#WhyOmniscient

Network architecture diagram is obsolete to represent today’s ‘***highly dynamic***’ networks and manual verification is a nightmare.

No understanding of ***‘true’*** state of network.

#WhatOmniscient

Omniscient provides an easy-to-use interface to ***‘visualize’*** the network with zero manual error, leveraging graph theory, network commands (**SEED** host) & cloud APIs



Key Features

- Bulk load of CMDB file & perform several on-demand network activities; and collate the results within a single project
- Project management -> Ability to create & manage projects
- Cloud (AWS) support
- Enumeration of identified systems
- Ability to analyse 'interesting' network only
- Continuous monitoring
- Segregation of backend activities and UI
- Docker installation for Linux

Live Demo

Known for “not working”.

So I hacked it – recorded when working :)

Questions??

https://github.com/varchashva/LetsMapYourNetwork

@IAmVarchashva

YouTube https://www.youtube.com/channel/UC77eNGlIzjGL0fgx3i6Hcyw

varchashva@gmail.com
rana.miet@gmail.com