RED V BLUE

TSTC

ICT en Security Trainingen

DEFINITIONS

Ethical Hacking

Ethical hacking refers to the act of locating weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers.

Penetration Testing

The intention is to validate or test the security of any IT system, normally following a strict methodology agreed upon by both the penetration tester and the owner of the system.

Identifies both weaknesses and strengths in the system

Red Teaming

A red team test is a realistic, unannounced attack based on an agreed scenario that's executed by a group of friendly hackers—typically external security professionals. Unlike in a penetration test, the red team only needs to find one open door. Once inside, we, the red team, see how far we can navigate toward a target without being detected or blocked.

Blue Teaming

A group that defends an enterprise's information systems when mock attackers (i.e., the Red Team) attack, typically as part of an operational exercise conducted according to rules established and monitored by a neutral group (i.e., the White Team).

EXAMPLES

Client need: I have a new piece of software or hardware, or a new network connection. How do I know if it's created any new vulnerabilities?

- Test: Penetration test

Client need: There's a new cyber attack in the news. Could this happen to me?

- Test: Red team

Client need: Will my detection capabilities actually detect an intrusion?

- Test: Red team

Client need: My company needs evidence that it's compliant with specific regulations. How do I get this?

- Test: Depends on the regulation

https://www.strozfriedberg.com/blog/penetration-test-red-teaming-exercise-what-is-difference/

WHY RED / BLUE TEAMING?

‘We cannot solve our problems with the same thinking we used when we created them’.

- Albert Einstein

NATO red teaming handbook defines it as:

- “The art of applying independent structured critical thinking and culturally sensitized alternative thinking from a variety of perspectives, to challenge assumptions and fully explore alternative outcomes, in order to reduce risks and increase opportunities.”

THE FUNDAMENTALS

Red teaming should:

- identify strengths, weaknesses, opportunities and threats, hitherto unthought-of
- challenge assumptions
- propose alternative strategies
- test a plan in a simulated adversarial engagement
- ultimately lead to improved decision making and more effective outcomes

Red teaming is a complementary function:

- adding alternative thinking and an element of informed speculation to known or derived information sourced through the intelligence, operations and plans teams, or from independent research.

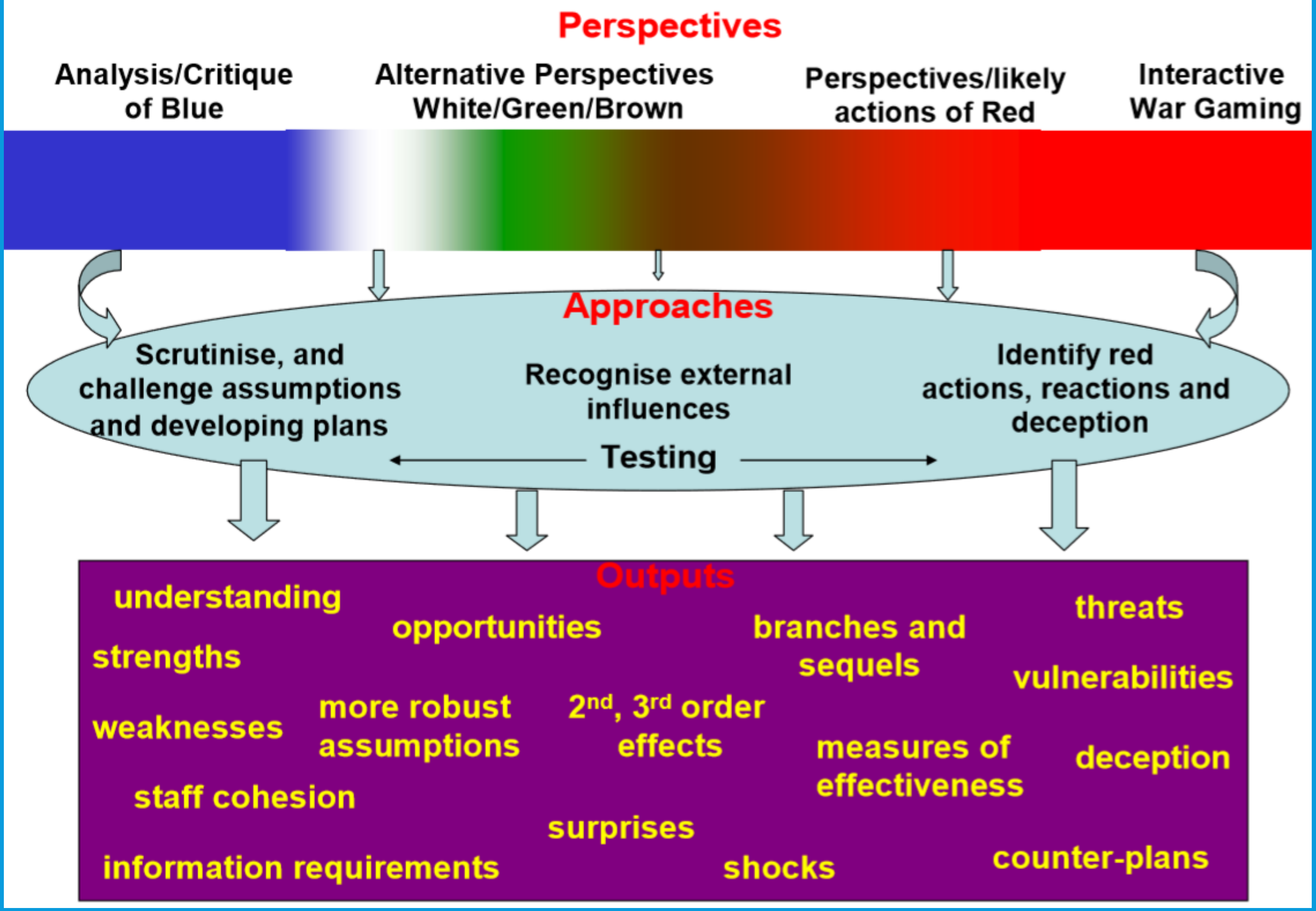
THE FUNDAMENTALS

Red teaming activities vary in purpose, scope and process according to the context and the product under consideration.

For example, red teams may be established to:

- Deliberately challenge own plans, programs and assumptions.
- Challenge or test a system, plan or perspective through the eyes of an adversary, outsider or competitor.
- Understand options available to adversaries by generating plausible hypotheses of adversary behavior and countering adversary deception.
- Better understand partners, local populations and other influential actors; activity which is often referred to as white, green or brown-teaming.
- Prepare an organization to deal with surprises, and strategic shocks.

White-teaming refers to organizers and facilitators, green-teaming to friendly actors, brown-teaming to actors that are neither supportive nor adversarial.



The left hand end of the spectrum illustrates the critical thinking function to mitigate against the comfort or complacency of accepted assumptions and solutions.

In this instance the red team should help to avoid group thinking and organizational bias, and should hedge against inexperience.

The function is often described as playing devil's advocate, or conducting prism or blue cell activity.

To the right hand end of the spectrum is the classic red cell function whereby the team acts as a surrogate adversary to propose opposing courses of action in order to help improve blue plans and decision making.

- The art of good red teaming is founded on the following high level principles:
  - Create the right conditions. Red teaming needs an open, learning culture, accepting of challenge and criticism.
  - Plan red teaming from the outset. It cannot work as an afterthought.
  - Support the red team. Its contribution should be valued and used to improve outcomes.
  - Provide clear objectives for the red and blue teams.
  - Fit the tool to the task. Assemble an appropriate red team and ensure individuals have the right skills and experience to do the job.
  - Ensure that the red team works with the blue not against them, but that the red team approach is critical and appropriately adversarial.
  - Focus on key issues. Red teaming should contribute quality thinking rather than quantity.
  - Poorly conducted red teaming is pointless, may be misleading and engender false confidence.

- 'No plan survives first contact with the enemy.'
    - Attributed to Helmuth von Moltke the Elder.
  - Red teaming may help to anticipate and mitigate that effect.

TSTC RED V BLUE
BASIC OBJECTIVES!

- Blue Team Testing the ability of the team members to:
  - find systems that have been compromised
  - find vulnerabilities and patch them
  - see new adversarial attacks on the fly
  - collaborate and report findings
- Red Team Testing the ability of the team members to:
  - use a standard pen testing methodology
  - find vulnerabilities
  - exploit vulnerabilities
  - maintain control and access to the systems that have been compromised
  - be stealthy
  - report the results accurately

TSTC RED V BLUE
RULE OF ENGAGEMENT!

- **Objective:**
  - Set defenses in the Blue portion of the Scenario.
  - Place your team name in both flag.txt files during the Red portion of the Scenario. If possible, sever access to your systems from other teams if they are connected.
- **Rules:**
  - At the beginning, everyone will have approximately 30 minutes to review Proximo and Gracchus for vulnerabilities and change passwords for the known accounts only!
  - No hacking of the administrator or root accounts are allowed.
  - Once the Blue team portion starts: *****NOTE: You cannot disable any services, they can only be patched*****
  - During the Red Team exercise, you are not allowed to use automated hacking features that try everything under the sun.

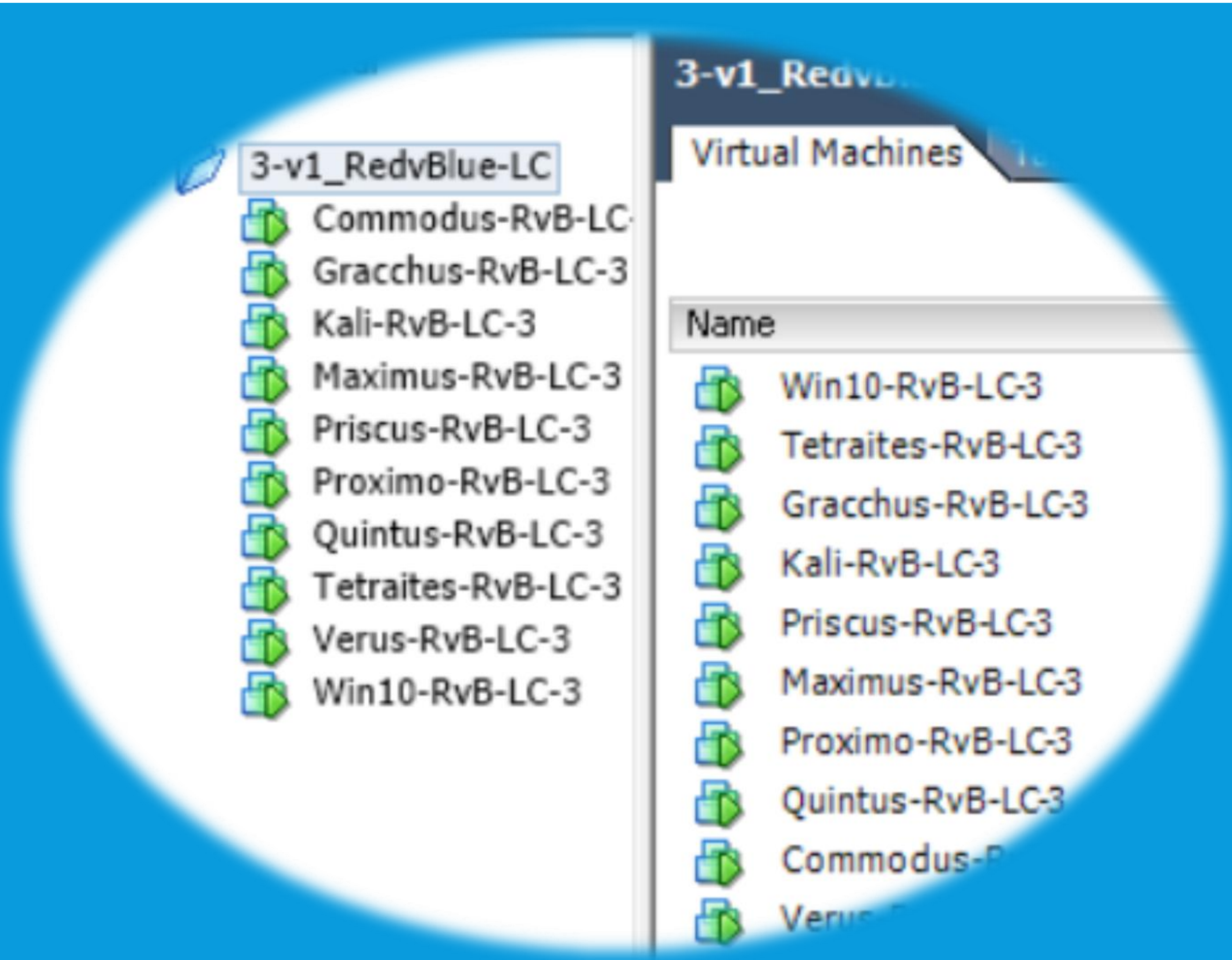
TSTC RED V BLUE
RULE OF ENGAGEMENT!

- **Rules:**
  - No ping of death or any DoS attacks!
  - You are authorized to change the credentials to your systems for user "**playerone**" during this time and provide the password to each team member and the facilitator.
  - You are authorized to change the credentials for the root account during this time and provide the password to each team member and the facilitator.
  - You cannot change the password for the facilitators account.
    - Hacking this account will disqualify the team.
  - *****NOTE: If credentials are changed after the start of the Red Team portion, the team member will be disqualified*****

SCORING!

- Points awarded per team!
- Blue Team points for the following(Proof must be reported):
  - Number of vulnerabilities patched or worked around (Compensating Controls)
  - Number of prevented exploits (This one is hard to prove)
  - Number of sessions severed
  - Number of exploits found or seen on the network or system
- Red Team points for the following (Proof must be reported):
  - Number of systems with team name in flag.txt
  - Number of successful hacks per system
  - Length of time a connection is established

INDIVIDUAL STUDENT VIEW



3-v1_RedvBlue-LC

Commodus-RvB-LC-

Gracchus-RvB-LC-3

Kali-RvB-LC-3

Maximus-RvB-LC-3

Priscus-RvB-LC-3

Proximo-RvB-LC-3

Quintus-RvB-LC-3

Tetraites-RvB-LC-3

Verus-RvB-LC-3

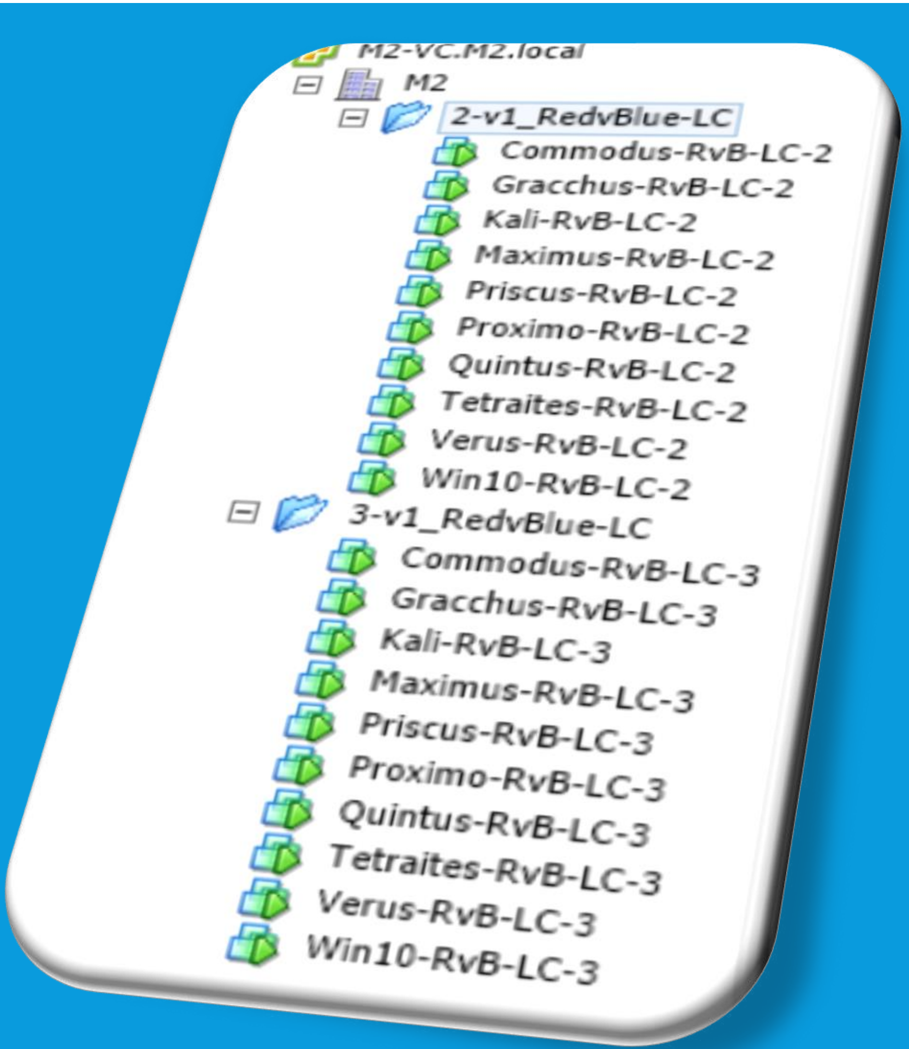
Win10-RvB-LC-3

3-v1_Redv

Virtual Machines

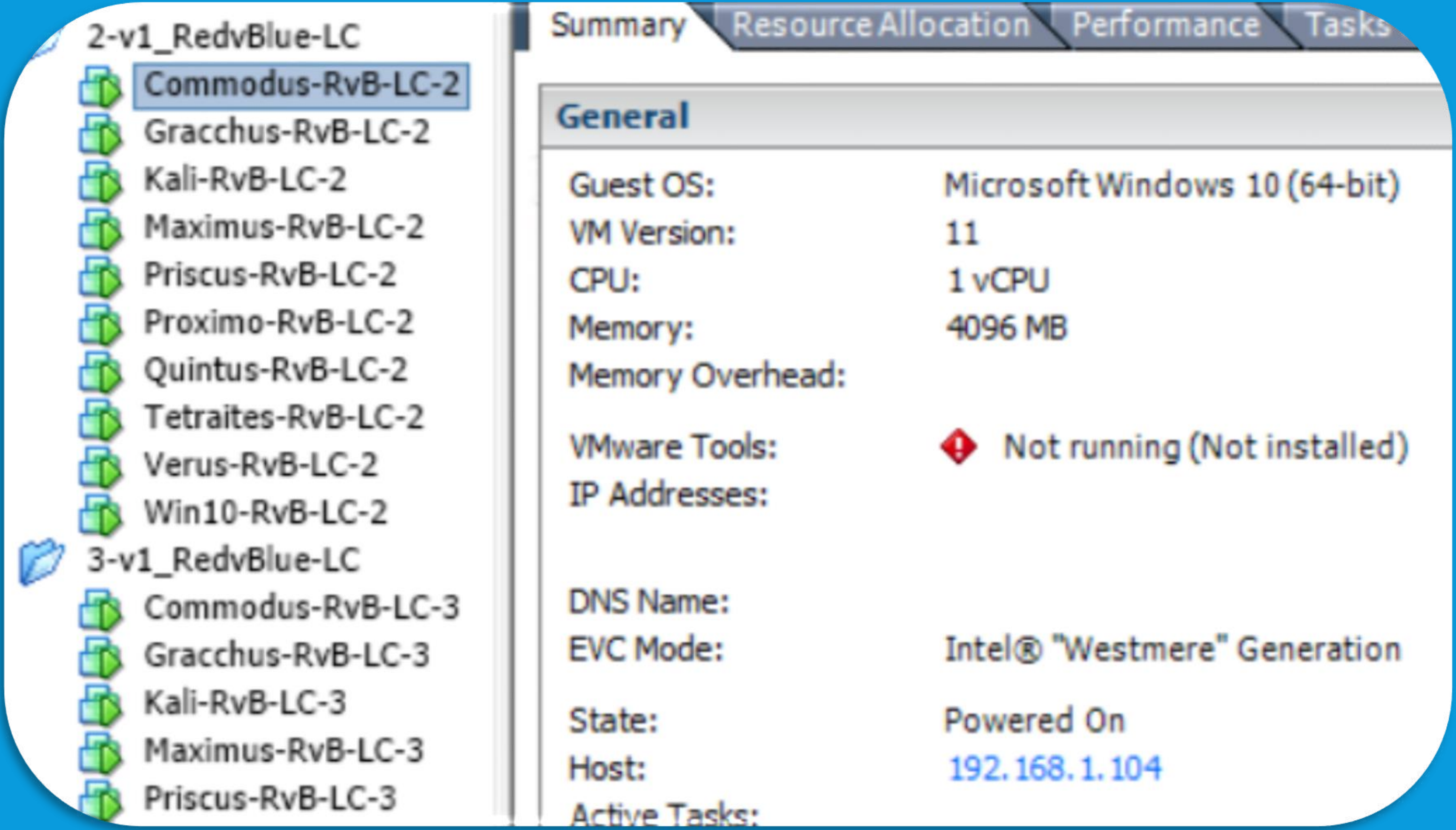
Name
Win10-RvB-LC-3
Tetraites-RvB-LC-3
Gracchus-RvB-LC-3
Kali-RvB-LC-3
Priscus-RvB-LC-3
Maximus-RvB-LC-3
Proximo-RvB-LC-3
Quintus-RvB-LC-3
Commodus-R
Veru

INSTRUCTOR/MEDIATOR VIEW



```
M2-VC.M2.local
  ⊟ M2
    ⊟ 2-v1_RedvBlue-LC
        Commodus-RvB-LC-2
        Gracchus-RvB-LC-2
        Kali-RvB-LC-2
        Maximus-RvB-LC-2
        Priscus-RvB-LC-2
        Proximo-RvB-LC-2
        Quintus-RvB-LC-2
        Tetraites-RvB-LC-2
        Verus-RvB-LC-2
        Win10-RvB-LC-2
    ⊟ 3-v1_RedvBlue-LC
        Commodus-RvB-LC-3
        Gracchus-RvB-LC-3
        Kali-RvB-LC-3
        Maximus-RvB-LC-3
        Priscus-RvB-LC-3
        Proximo-RvB-LC-3
        Quintus-RvB-LC-3
        Tetraites-RvB-LC-3
        Verus-RvB-LC-3
        Win10-RvB-LC-3
```

A WINDOWS SYSTEM



General

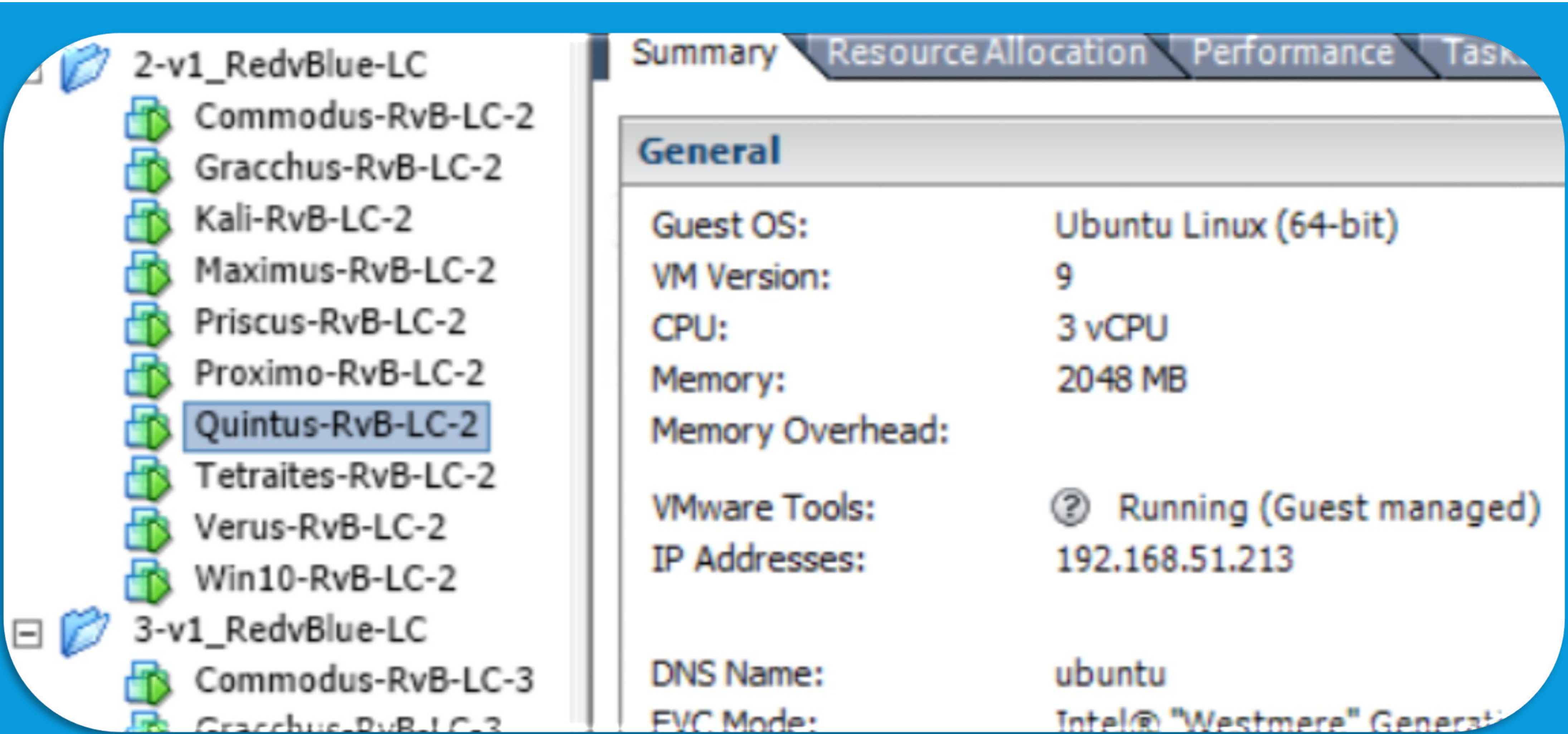
Guest OS: Microsoft Windows 10 (64-bit)
VM Version: 11
CPU: 1 vCPU
Memory: 4096 MB
Memory Overhead:

VMware Tools: Not running (Not installed)
IP Addresses:

DNS Name:
EVC Mode: Intel® "Westmere" Generation

State: Powered On
Host: 192.168.1.104
Active Tasks:

A LINUX SYSTEM



2-v1_RedvBlue-LC
- Commodus-RvB-LC-2
- Gracchus-RvB-LC-2
- Kali-RvB-LC-2
- Maximus-RvB-LC-2
- Priscus-RvB-LC-2
- Proximo-RvB-LC-2
- Quintus-RvB-LC-2
- Tetraites-RvB-LC-2
- Verus-RvB-LC-2
- Win10-RvB-LC-2

3-v1_RedvBlue-LC
- Commodus-RvB-LC-3
- Gracchus-RvB-LC-3

General

Guest OS: Ubuntu Linux (64-bit)
VM Version: 9
CPU: 3 vCPU
Memory: 2048 MB
Memory Overhead:

VMware Tools: Running (Guest managed)
IP Addresses: 192.168.51.213

DNS Name: ubuntu
EVC Mode: Intel® "Westmere" Generati

MOST IMPORTANT!!!

- Hands on!
- Real world collaboration!
- Diverse Perspectives! (Different Companies/Different Ideas)
- Variations on the Fly!
- Controlled Environment ?

- Despite its many advantages, red teaming is not a silver bullet. As one would expect, the credibility of the output hinges on the quality and experience of the team, the team's approach and toolset, the quality of the leadership and the overall context of the effort.

CONTINUING EDUCATION

- Any Security Certification under the sun!
- Any Security Training a company could ever need! Including customized trainings!
- Red v Blue – customized options available
- Come visit us at booth 01.B094
- Questions?

TSTC

ICT en Security Trainingen