Focus on CSIR

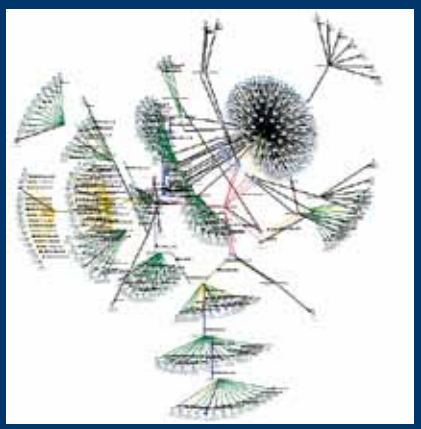
Red and Blue Teams

Security audits and penetration testing capabilities to identify weaknesses and exploits in systems and networks. Provision of risk assessments from operational, managerial and technical point of view. Assess the current security baseline and evaluate security levels.

Use security baseline for future audits and security assessments. Red and Blue Teams are beneficial in identifying critical issues in an organisation, as well as formulating a remedy strategy. Though the use of an independent party, system issues can be reported back to the relevant stakeholders.

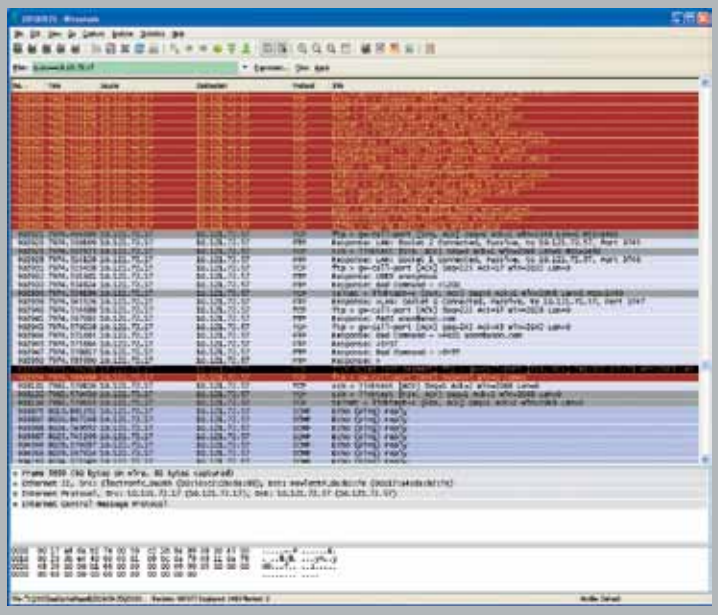
Capabilities

- Network Mapping
- Port Scanning
- Wireless Scanning
- Service Detection
- Vulnerability Testing
- Penetration Testing



CSIR

our future through science



```
[root@darkstar ~]#
[root@darkstar ~]# nmap -PN -sS  -O Scanme.Nmap.Org

Starting Nmap 5.21 ( http://nmap.org ) at 2010-04-01 11:19 IDT
Nmap scan report for Scanme.Nmap.Org (64.13.134.52)
Host is up (0.18s latency).
rDNS record for 64.13.134.52: scanme.nmap.org
Not shown: 993 filtered ports
PORT      STATE  SERVICE
25/tcp    closed smtp
53/tcp    open   domain
70/tcp    closed gopher
80/tcp    open   http
113/tcp   closed auth
8009/tcp  open   ajp13
31337/tcp closed Elite
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.15 - 2.6.26

OS detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 16.99 seconds
[root@darkstar ~]#
```

Scenario

A Red and Blue Team commences with a network scan to determine the critical devices. Thereafter vulnerability scans are run on the network to determine whether the systems have any security holes due to missing patches or system configurations. Simultaneously traffic capturing software collects packets which are inspected for anomalies.

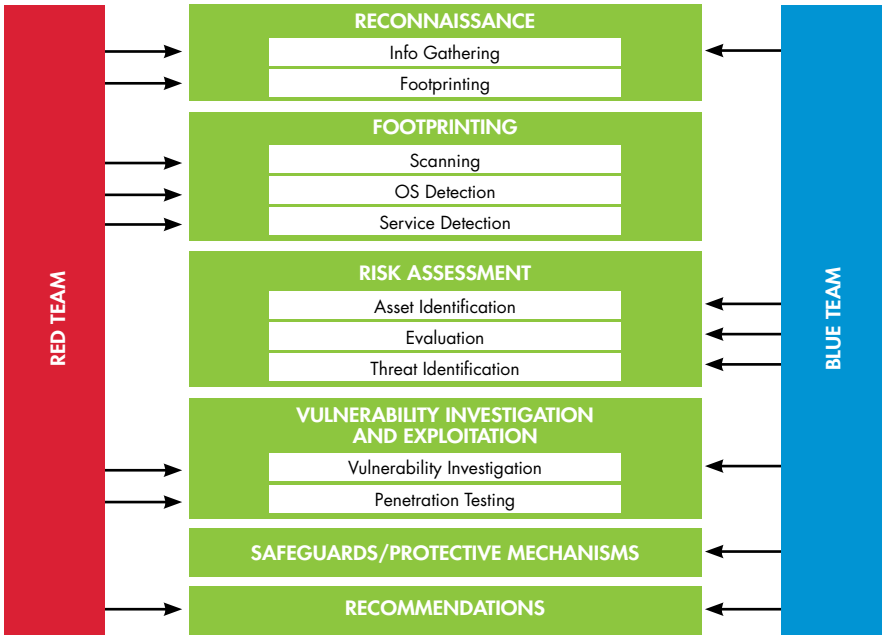
Vulnerabilities and anomalies are reported to relevant authorities in order to initiate remedial action. The impact of exploiting vulnerabilities are thus reported without jeopardizing the operation of the system.

Various tools can be used to carry out Red and Blue Teams. These include software for:

- Network
- Mapping
- Port scanning
- Wireless
- Scanning
- Traffic capture
- Network management and auditing

Several Red and Blue Team have been carried out in order to assess the security levels of operational and support systems.

Red and blue team methodology



Contact details:
Namosha Veerasamy
Tel: +27 12 841 2893
e-mail: nveerasamy@csir.co.za

www.csir.co.za