IP Network Security Assessment

Sun Microsystems©, one of the greatest and most innovative technology companies had a motto: “The Network is the computer”. The phrase was first coined in 1984 by John Gage, the 21st employee of Sun Microsystems, where he was credited with building Sun’s vision around “The Network is the Computer.” and now is a trademark of Cloudflare©, one of the biggest companies providing content delivery network and DDoS mitigation services. This really says it all about the importance of Network Security in our current interconnected world. But when it comes to talking about Network Security, everybody thinks of firewalls or penetration testing to check their current status, ignoring what really happens inside the companies networks and delegating everything to a device that only protects from the outside world. Ironic, isn’t it? Ransomwares, data theft and security breaches are so much in the news everyday that aren’t even so much “news”, it’s routine. **Until you are impacted directly.**

What is an IP Network Security Assessment and why is different from a Penetration Testing ?

A common penetration testing or so called “Security Assessment” usually includes only analysis of system vulnerabilities and their possibility to be exploited by an attacker. It’s basically a snapshot of possible attack surfaces at a given moment in time. This could also include network devices firmwares and system patches as well, and depending on the capabilities of the “white hat” (and the cost of the assessment), it could really show interesting things and ways to fix them. Shortly, it’s basically a snapshot of your security situation at a certain time. Which is probably subject to change in time, and quite quickly, because technologies changes and evolve.

An IP Network Security Assessment is quite different. It doesn’t aim to check the vulnerabilities on your system (that’s what the penetration testing does), but tries to let you understand how your network infrastructure is used by your users and internal systems to find patterns and signs of possible compromise. Too often internal network security is underestimated and most (if not all) network security is delegated to the boundary firewall. There could be an IDS/IPS in most security aware scenarios, but over the time it struggles keeping on with bandwidth usage. Also, SIEMs failed to deliver, since companies rarely have the resources available to check all the logs and there is literally an ocean of data to search into. That’s where a bird’s eye point of view helps you to find the right things to check.

Introducing Fl0wer

That's why a tool like Fl0wer can really help your network team to accelerate Security Team response time to current and future threats. Making use of most used and consolidated flow technologies (Netflow, IPfix, sFlow) and OLAP data storage, it can really identify quickly what's happening on your internal network. Fl0wer can be feeded with data provided by a huge list of devices (a short and incomplete list can be found at http://downloads.fl0wer.me/Fl0werDeviceMatrix.pdf)
It can help you to quickly identify IOCs (Indicators of Compromise) like:

- TOR connections
- P2P connections
- possible Covert Channels
- vertical scans on a host (like a target to compromise)
- horizontal scans for a service (like a worm, a malware or a ransomware)
- policy violations for internal core services like NTP, DNS, BGP, SNMP, VPN, SDN, etc.
- connections to bogon networks or blacklisted IPs on the Internet
- out of matrix traffic
- cryptocurrencies related traffic
- social network traffic inside your datacenter
- probably unwanted traffic

IP Network Security Assessment Service

The IP Network security assessment service conceptually works more or less like a penetration testing, giving you a snapshot of a week (or more) of traffic of your internal network, to understand what's really happening by using the Fl0wer tool. All data is captured from your internal network configuring properly your network devices (or temporarily providing dedicated network taps if configurations can't be touched) and stored for further analysis and reporting. At the end of the observation period, a report is generated and all data gathered is delivered as CSV (Comma Separated Value) files for most flexibility and further analysis.

What is needed ?

Fl0wer powered network security assessments don't really need so much information. A pre-configuration meeting will point-out:

- a global network topology map
- all internal networks (IPv4/IPv6) including names, netmasks and security zones
- all internal policy set official "resources" (DNS, NTP, BGP, VPN concentrators and tunnels, etc.)
- considerations about special traffic to be classified in specific ways
- network observation points using Flow protocols (Netflow V1,V5,V9,IPFix, sFlow)

Fl0wer then is licensed and delivered in a VM (Virtual Machine) to be hosted on a customer Hypervisor on-premise (or on rented physical hardware if needed) and network devices configured to export flow data to Fl0wer (or rented network taps installed if needed). A two days checking to verify proper configuration of the analysis infrastructure is performed, then the observation period starts.

At the end of the observation period, the report is delivered and discussed with the customer network team, checking out findings and outcome of the Fl0wer report and reasoning on possible solutions.

For further information: https://fl0wer.me – info@fl0wer.me