SecurityGen

Telecom Security. Transcending Generations.

Telecom Network Security Assessment: Legacy versus BAS (Breach and Attack Simulation) security approach

Cyberattacks pose a clear and present danger to businesses large and small. And the telecom industry – with huge amount of sensitive customer data, and critical business nature – offers adversaries rich pickings. Threat landscape is always increasing as traditional telecom networks transform into smart, application and service-aware, high speed and low latency infrastructure, which adopts a lot of new technologies.

Suffice to say, a lot of mobiles networks remain extremely vulnerable to sophisticated attacks.

Telecom security leaders have predominantly used two means to assess the security of their core network and data systems: Penetration-testing, and Vulnerability scans. These techniques primarily help assess the health and strength of the security systems at large and have an important role to play. However, these approaches come with their own set of limitations.

The strength of a vulnerability scanner is its automated approach to security monitoring. On the flip side, this means it can only detect known/potential vulnerabilities, providing no information about context and real environment – leaving the main question unanswered – "is it exploitable or not?" Similarly, while Penetration testing offers a more customized and thorough examination: if it is possible to infiltrate into the system and introduce negative impact, its manual and cost-heavy approach leads to infrequent assessments. Not only does this limit the coverage, but it also adds to the cost overheads.

Given the ever-growing and complex nature of telco ecosystems, automated and continuous monitoring of systems is the need of the hour. Apart from validating the efficacy of the systems, a detailed prioritization and remediation guidance could be really helpful. It is essential to have an intelligent solution that helps classify business-critical systems, identify threats and further help prioritize them, based on set parameters, to ensure enhanced security.

This is precisely where BAS emerges as the perfect fit for telecoms. By simulating real-life attack scenarios, it helps validate the efficacy of your security systems while the automated format and remediation module helps save on the resource overheads and strengthen the security posture.

Let's look at how each of these systems work, and the limitations of each approach.

Vulnerability Scanner:

An automated tool scans the systems to detect known weaknesses within the environment. The idea is to discover vulnerabilities by running tools against a target system, application, or network, and generate a report listing these vulnerabilities.

Limitations:

1. It only lists the vulnerabilities based on knowledgebase, with no insights into the real risks posed to the business
2. It helps to collect data but doesn't provide analysis about how a particular vulnerability could be exploited
3. It can only detect known vulnerabilities, which leaves the whole zero-day vector open for exploitation
4. It may generate false-positive alerts, which then need to be assessed by the security teams
5. It continuously tests and detects the environment, but lacks scope and threat insights
6. It doesn't provide any context-aware remediation guidance
7. It can only notify about the presence of a vulnerability, but is not capable of checking for effects in case of an exploit
8. It Involves installation cost and requires skilled resources

Penetration-testing

A pen test is a semi-manual test conducted by a team of penetration testers, or ethical hackers, and is used to identify and verify networks and identify entry points and threats within an environment. During the pen testing exercise, the testing team carries out cyberattacks to assess the strength of your security system against potential vulnerabilities. Pen-testing also has its limitations.

Limitations:

1 Its restricted testing-time and environment limits the depth of analysis and attack techniques

2 It doesn't give a complete picture of your network perimeter

3 Infrequent assessments make the network vulnerable to attacks

4 It cannot provide continuous analysis due to the short-term nature of these testing services

5 It lacks the automated and constant monitoring approach

6 Its efficacy depends, largely, on the skill and experience of the pen testing team

7 Remediation advice depends on experts having related knowledge about the assessed system - It is easier to ruin something than to create

8 It is expensive since it is a niche area of operation

Breach and Attack Simulation (BAS)

The new entrant in the telecom industry stands out because it provides comprehensive security coverage by overcoming the limitations of the legacy testing approaches mentioned above (Pen-testing and Vulnerability scanners).
The BAS solution helps identify the landscape by collecting basic information about existing assets and vulnerabilities on network nodes. Then, by performing a simulation of real attack scenarios, it assesses whether the vulnerabilities are real and can be potentially exploited. Moreover, it generates an automated, easy-to-read security posture report at the end of each assessment, covering details of severity level, description of threats identified, and guidance on how to fix the threat/s.

Features:

1 Automated and continuous security validation mechanism

2 Simulates the techniques and tools used by adversaries

3 In-depth threat analysis of the network and the environment

4 Provides a complete picture of your permitter network

5 Offers proactive security coverage by identifying real threats to which any given organization is exposed, and calculates the potential for related damages

6 It notifies about a vulnerability and also lists the scoring/severity and remediation details

7 It reduces time from threat identification to remediation, thus ensuring a more robust security posture

8 The cloud-based model ensures low cost and a quick start

9 It doesn't require telecom specialists or an engineering team, thus helping reduce overhead costs

10 It is backed by a constantly updated knowledge base – which helps it efficiently address advanced threats

Comparison: BAS, Vulnerability Scanner, Penetration Test

	Intelligent Breach and Attack Simulation (BAS)	Vulnerability scanner	Penetration test
Low touch	✓	✖	✖
Automation	✓	partially	✖
Continuous detection	✓	✓	✖
Real attack scenarios	✓	✖	✓
Security improving progress tracking	✓	partially	partially
Risk exposure	✓	✖	✓
Prioritization	✓	partially	✓

	Intelligent Breach and Attack Simulation (BAS)	Vulnerability scanner	Penetration test
Minimized efforts required	✓	✗	partially
Savings on engineering resources	✓	partially	✗
Savings on time-to-action activities	✓	partially	✗
Stuff doesn't have to be deep security/telco expert	✓	✗	✗
Actionable remediation provided	✓	partially	✓
5G SA/NSA support	✓	partially	partially

Backed by a robust research-driven approach to cybersecurity and insights from over 300 telecom security assessments conducted by our core team of experts, SecurityGen has built the telecom industry's first BAS solution – ACE – Artificial Cybersecurity Expert platform.

To know how the ACE platform can help continuously assess and validate your network security posture against advanced threats and ensure proactive security coverage reach us at - contact@secgen.com

About SecurityGen

Founded in 2022, SecurityGen is a global firm focused on telecom security. We deliver a solid security foundation to drive secure telecom digital transformations and ensure next-gen enterprise intelligent connectivity. Our extensive product and service portfolio provides complete protection against existing and advanced telecom security threats.

Connect With Us

✉ **Email: contact@secgen.com**

🌐 **Website: www.secgen.com**

UK | Italy | Czech Republic | Brazil | Mexico
India | South Korea | Japan | Malaysia | UAE