Orange Cyberdefense

SensePost assessments

Internal Infrastructure

Key benefits

Qualified real-world testing
Using a strict methodology, a thorough understanding of vulnerabilities from an attacker's perspective, using both authenticated and unauthenticated perspectives, provides thoughtful insights into an organisations internal network thread landscape.

Reduced risk:
Comprehensive reviews increase the chance of finding any security issues before a malicious actor does. Internal infrastructure assessments can easily be tailored to focus on mission-critical networks underpinning the business function of an organisation.

Systematic approach:
We follow industry recommended practises to allow for consistently reproducible results as well as custom experience-led activities to demonstrate real world risk.

Service description

The heart of any organisation is undoubtedly its internal network and related services. Internal network assessments are often recommended following an external network assessment as a defence in depth approach. This however does not dilute its importance, but rather aims to balance the security posture of both networks.

The idea behind a defence in depth approach is that should any single control fail (be it from an external perspective, or any host internally) along the route to a target, another control could help mitigate, prevent or alert that an attacker is on the network. More often than not, organisations have a good external security posture but a weak internal posture. An analogy of a hard-external shell but squishy internals is often used to describe this. An internal network assessment aims to balance this, providing a realistic perspective of the current security posture should the external permitter be compromised.

Internal assessments are typically conducted onsite, scoped as a sample set of IT infrastructure and applications based on a detailed methodology aligned with best practices (such as OWASP, CREST, and MITRE). The assessment includes detailed penetration testing, exploitation of vulnerabilities, privilege escalation and pivoting in the target network. When scoped with specific targets in mind, those would be what drives the aforementioned phases. Our ethical hackers make extensive use of both open source and self-developed tooling and often develop custom tooling when required.

Internal assessments can also be performed remotely, often to simulate a compromised perimeter. Consider a successful phishing attack scenario resulting in the execution of a malicious payload providing remote network access to an attacker. A valuable exercise the SensePost team can perform is to craft a payload within the organisation's confines and start the assessment assuming the payload was successfully executed; a common consequence of a successful phishing attack. This provides an in depth look at the extent of damage an attacker could achieve after gaining remote access to the internal network while also providing defending teams with a scenario to perform threat hunting.

The SensePost team has a specific methodology when it comes to wireless networks, checking that the intended network segregation is affective and that authentication requirements and its implementation is secure. Wi-Fi networks have the potential to cause more damage than traditional wired networks part given that one only has to be in range of the target network vs. being physically present at a network point.

Internal networks take on many shapes and often include a myriad of different technologies. These include serverless environments, hybrid cloud-based networks, containerised environments using Docker orchestration layers like Kubernetes. Irrespective the technologies used on an internal network, assessment efforts will typically focus on attacking the in-scope surface area, performing network and service enumeration using scanning techniques, perform vulnerability analysis against all identified hosts and finally exploit issues to demonstrate risk.
This is one of the most important assessment types and goes a long way in supporting the decision-making capabilities of the security team.

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As a leading go-to security provider, we strive to protect freedom and build a safer digital society.

We are threat research, intelligence-driven, offering unparalleled access to current and emerging threats. With a 25+ year track record in information security, 250+ researchers & analysts and 16 SOCs distributed across the world and sales and services support in 160 countries, we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

We are proud of our high-end security research unit, thanks to which we publish regularly white papers, articles and tools on cybersecurity which are widely recognised and used throughout the industry and featured at industry conferences including, Infosec, Manchester DTX, RSA, BlackHat and DefCon.

SensePost is an ethical hacking team of Orange Cyberdefense, offering offensive security consulting services and trainings. With a 20-year track record, SensePost is seen as trusted advisors who deliver insight, information and systems to enable our customers to make informed decisions about information security that support their business performance.

With team members that include some of the world's most preeminent cybersecurity experts, SensePost has helped governments and blue-chip companies both review and protect their information security and stay ahead of evolving threats. They are also a prolific publisher of leading research articles and tools on cybersecurity which are widely recognised and used throughout the industry and feature regularly at industry conferences including Black Hat and DefCon.

Key service components

For the internal network:
- Perform a full network survey to determine attack surface
- Full network enumeration using scanning techniques
- Perform a vulnerability analysis assessment against all identified hosts
- Exploitation of issues after vulnerability verification

For Wi-Fi networks:
- Discovery of wireless networks / Access Points
- Review of network encryption (WPA/WPA2 etc.)
- Checking for wireless "bleed" whereby Wireless networks are available beyond the office boundary
- Wireless device configurations