Secure Network Assurance Program

part of our Cyber Alliance Program (CAP)

Services Primer

Penetration testing remains one of the best tools to strengthen your security defenses and prove the effectiveness of your security program. If that's true, why do it once a year?

Stay Compliant and Secure All Year Long

Why do a Penetration Test?

A penetration test (pentest) is a controlled simulated attack carried out by a third-party security expert, using the same techniques that a hacker would use. It is considered by the security community to be among the best investments you can make in your overall security program. Part of the reason is that pentests address many different needs, such as compliance requirements and customer demands. Most importantly, a pentest guides your security efforts.

Haven't I heard of this somewhere?

You may hear of two different approaches to doing more frequent penetration testing:

- **Bug Bounties -** many large organizations have moved to continuous pentesting thru bug-bounty programs where contracted "ethical" hackers run penetration testing constantly. These cost hundreds of thousands of dollars a year, and require a dedicated team to watch the unknown bounty hunters. Plus, you can't ask questions because it's a constant stream of different contract hackers.
- **Pentest-as-a-Service** – the unfortunately named "PTaaS" has only worked with software developers who want to test code as part of their development lifecycle. Testing is completely automated and resembles a scan. It's all managed through a dashboard with little to no access to any security professionals.

You need something better…and we have it!

Our **Secure Network Assurance Program** blends more frequent testing with control and an appropriate budget.

Secure Network Assurance Program

Security Pursuit has developed the Secure Network Assurance Program (SNAP) to balance your need for more frequent testing, the need to schedule those tests at convenient times, and the need to work within a reasonable budget for a small to mid-sized organization.

Our Approach

SNAP is part of our Cyber Alliance Program and is designed to handle a critical need completely. All elements of penetration testing are considered:

- Network Penetration Testing (external and internal)
- Wireless Penetration Testing
- Vulnerability Scanning (external and internal)
- Social Engineering
- Red Team Test
- Custom Reporting

These services are provided at a pre-determined frequency that meets your exact needs. In addition, for software developers we provide a Secure Application Assurance Program. Elements of that program can be combined with SNAP to create a truly custom penetration testing program.

WHY DO THIS?

Annual testing is inadequate. Yet the alternatives are not designed for most organizations. Our Secure Network Access Program is sized just right for you with the following critical features:

- **Testing at a frequency that meets your needs**
- **Work directly with our security team**
- **Scheduling and contracting is greatly simplified**
- **Reporting is highly tuned for all your audiences**
- **Balance that serves your budget**
- **Flexibility to change when needed**

EXAMPLES: SECURE NETWORK ASSURANCE PROGRAM (SNAP)

The following are examples of how we may build your Secure Network Assurance Program:

	Small Business	Mid-Sized	Larger Business
Number of Employees	Less than 100	100 – 500	500+
Appropriate for…	**Local services** law firms, clinics, consultants, services	**Higher Risk** Software, financial, mfr, larger B2B	**Enterprises** International, large brands
External Network Penetration Testing	1 per year	2 per year	4 per year
Internal Network Penetration Testing	1 per year	1 per year	2 per year
Wireless Penetration Testing	1 per year	1 per year	2 per year
External Vulnerability Scanning	Quarterly	Quarterly	Monthly
Internal Vulnerability Scanning	2 per year	Quarterly	Quarterly
Social Engineering	2 per year	4 per year	Monthly
Custom Reporting	As Needed		

Elements of Penetration Testing

The following services are considered in every SNAP program. A custom combination of these will be used for your specific needs.

External Network Penetration Testing

The external network penetration test identifies public-facing vulnerabilities that could be exploited by an attacker to gain access to private systems/data from the Internet. The assessment begins with a thorough analysis of the entity's public Internet and Darknet exposure; searches are conducted that discover employee information (names, titles, email addresses, passwords, etc.) which could be used to aid in an attack. Hostnames, IP addresses, websites, and exposed ports/services are also enumerated.

Once the discovery phase is completed, vulnerabilities are identified and analyzed, and manual exploitation attempts are performed. Key web applications discovered are assessed for most common vulnerabilities. If access is achieved, the assessor demonstrates the level of risk as is permitted by pre-defined rules of engagement.

Internal Network Penetration Testing

Penetration testing of an entity's internal, or "private side" network is a critical, yet oftentimes overlooked aspect of cybersecurity due diligence. It is ill-advised to conclude assets residing on the internal network are protected because the perimeter is secure. The objective of this assessment is to evaluate the internal network's risk exposure to insider threats, computers infected by sophisticated malware, or a malicious intruder who has gained access inside the network perimeter.

The testing begins by placing the assessor's system onto a segment of the target network. Network eavesdropping is conducted to intercept sensitive data broadcasting over the network. Automated vulnerability scans are then performed, followed by manual exploitation attempts against susceptible assets. Common services with remote login functions such as SMB, RDP, FTP, Telnet, SSH, SNMP, HTTP and HTTPS are checked for weak account passwords. The assessment will identify and provide remediation guidance for vulnerabilities such as: remote code execution, man-in-the-middle attacks, privilege escalation, weak configurations, missing host and application patches, and the use of insecure services/protocols. If access is achieved, the assessor demonstrates risk as is permitted by pre-defined rules of engagement.

Wireless Network Penetration Testing

The wireless network penetration test achieves two objectives; First, efforts are made to identify any possible "rogue" WiFi access points that could be connected to the private LAN. A comprehensive survey of the physical location is performed to detect all broadcasting and hidden wireless networks in close proximity. The full inventory of access points found are provided to IT staff for review.

Next, efforts to exploit and access the managed wifi in scope are performed by attempting to compromise a shared wireless password, using brute force techniques, or by tricking users of mobile devices (laptops, phones, tablets, etc.) into joining a wireless network controlled by the assessor. This last item is achieved by configuring

an “Evil Twin” access point that closely resembles the legitimate managed network. When a device attempts to connect to the Evil Twin network, the password provided will be captured and used by the assessor to join the legitimate network. Once access is achieved, the assessor demonstrates risk as is permitted by pre-defined rules of engagement.

Quarterly External and Internal Vulnerability Scan

Vulnerability scanning helps identify vulnerable services and misconfigurations which could allow unauthorized access into your organization’s network. We utilize the latest tools and industry best-practices for vulnerability scanning to identify the weaknesses in your internal and external network environments, delivering a report which clearly defines priorities for remediation activities.

Depending on the level of program, Security Pursuit may validate vulnerabilities with penetration testing. These are provided according to mutually agreed rules of engagement.

Social Engineering

With all of the best technical controls in place, hackers continue to gain unauthorized access into networks through social engineering. The social engineering attacks attempt to trick employees into disclosing sensitive information such as login credentials or bank account numbers. There are many options to consider, such as:

- **Email Phishing:** In this assessment, Security Pursuit will attempt to convince employees to disclose sensitive information through use of an email solicitation. The assessment begins by harvesting client employee email addresses from a variety up public information sources. If an insufficient number of email addresses are discoverable, or the client prefers, they may opt to augment the final email address list used in the campaign. With input provided by the client, the consultant will construct an email that visually resembles that of an internal email broadcast, or one that is likely to deceive target recipients into believing it is legitimate. Embedded within this email will be a link to a web site hosted and controlled by Security Pursuit but made to look and feel like one belonging to the client or a trusted third party.

- **Pretext Phone Calling:** Pretext phone calling is a method of social engineering where an attacker calls employees on the phone, and attempts to gather sensitive information by deceiving the employee into thinking that the attacker is a legitimate company representative who can be trusted. For this assessment, Security Pursuit will focus on obtaining the usernames/passwords of employees.

- **Physical Security Assessment:** In this assessment, Security Pursuit surveys and collects information on the client facility security controls then carries out derived methods of attacks at the location with the objective of gaining physical access to restricted areas. If physical access is achieved, the assessor will next attempt to gain access to sensitive information either by way of network access, or hard copy documentation left unsecured. Tests may include: door locking controls, tailgating of employees through secured doorways, LAN jack access and network visibility, USB flash drive drops, and the accessing of unattended computer systems.

Red Team Test

A Red Team test simulates a targeted attack against your business by a real-world adversary with limited constraints on our penetration testing team. It is achieved by providing the consultant:

- Objective: A set of target data that is critical to the business (Ex. Intellectual property, customer database, financial data, etc.)
- A set amount of man hours and timeframe to complete (Ex: 160 man hours used between September 1 and November 1)
- Rules of engagement (Ex. Targeting board members prohibited, No denial of service attacks against critical production servers, etc.)

The consultant team then has this time to use any and all attack vectors within the defined rules of engagement to attempt to gain access to the protected data set or reach the defined mission objective. A Red Team engagement exercises not only your technical defenses, but the detection and response capabilities of your in-house IT personnel or outsourced security monitoring service.

Custom Reporting

Penetration testing centers on two critical needs. First, your security team needs to understand real vulnerabilities and how they may be exploited and result in a compromise. This report provides details on the vulnerability, how it was exploited, whether it was successful, and details on how to remediate. Second, your penetration test must provide assurance to a variety of stakeholders. This includes owners, board of directors, customers, insurance companies, partners and more.

These are two very different reports! That's why Security Pursuit works to understand your external reporting requirements so that we can provide you with all the reports you need. Common reports include:

- **Board of Director and Stakeholder Reports** – these are used to provide assurance that the security team is addressing the unique risks of the organization. They may also be used to secure budget for new projects. Your pentest must be written for this purpose
- **Customer Reports** – these are used to provide assurance and confidence in prospects and customers. When written properly, they may also be used against your competitors. Current reports with a marketing feel serve your prospects and clients best.
- **Partner Reports** – your insurance company, bank or other critical partners may want assurances through a penetration test. These usually need to address specific concerns of the partner, so they need to be written carefully.

Security Pursuit is committed to helping you get the most leverage you can from our Secure Network Assurance Program. Everytime we provide updates, whether they are penetration tests or scans, your reports are updates as required. This provides a long term return on your penetration testing investment.

Let's Begin Building Your Secure Network Assurance Program today.

Appendix: Our Penetration Testing Methodology

Security Pursuit penetration testing methodologies follow accepted industry standards and best practices. Penetration test engagements are conducted in seven distinct phases as follows:

Discovery	Reconnaissance	An attack surface of the target is created by using automated and manual techniques. This phase helps determine the host operating systems, web pages, exposed ports and services, network segmentation, and other details that will be used in subsequent phases of testing.
	Vulnerability Identification	Automated scanning and manual techniques are used to identify vulnerabilities for the systems in scope. Each host is checked using industry recognized vulnerability scanning tools. Moreover, any mis-configurations that could potentially lead to a compromise are identified.
Analysis	Develop Attack Plans	The findings from the Discovery phase are analyzed to formulate a series of attack scenarios giving the consultant the best opportunities to achieve the end objectives of the project.
Exploitation	Perform Attacks	Manually attempt to compromise assets in scope. Privilege escalation methods and pivot attacks are often employed on compromised systems to attempt further access to additional systems and data.
	Demonstrate Access	Capture screenshots and/or sensitive data which clearly demonstrate the access achieved and the business impact.
Reporting	Report Creation	Exploited critical and high risk vulnerabilities are prioritized for detailed reporting purposes, while all findings identified as medium, low, informational, and false positives are captured in summary format.
	Knowledge Transfer	Security Pursuit provides a verbal debriefing for each project performed. This gives stakeholders an opportunity for Q&A for the purposes of clarifying findings, methods used, risk ratings, and recommended remediation action items.