STEALTH
ISS GROUP®

VULNERABILITY SCANNING & PENETRATION TESTING

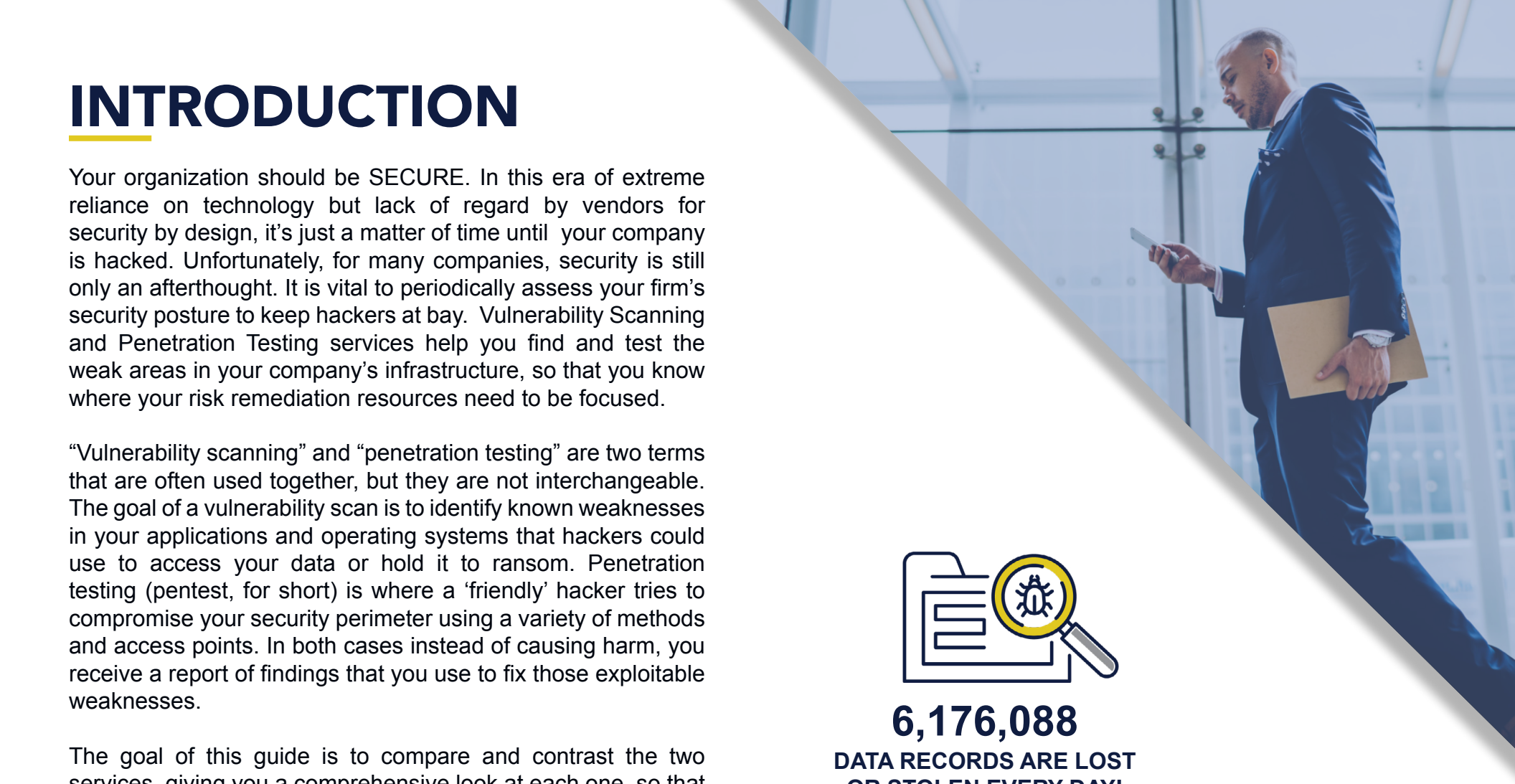
Table of **CONTENTS**

INTRODUCTION

Your organization should be SECURE. In this era of extreme reliance on technology but lack of regard by vendors for security by design, it's just a matter of time until your company is hacked. Unfortunately, for many companies, security is still only an afterthought. It is vital to periodically assess your firm's security posture to keep hackers at bay. Vulnerability Scanning and Penetration Testing services help you find and test the weak areas in your company's infrastructure, so that you know where your risk remediation resources need to be focused.

"Vulnerability scanning" and "penetration testing" are two terms that are often used together, but they are not interchangeable. The goal of a vulnerability scan is to identify known weaknesses in your applications and operating systems that hackers could use to access your data or hold it to ransom. Penetration testing (pentest, for short) is where a 'friendly' hacker tries to compromise your security perimeter using a variety of methods and access points. In both cases instead of causing harm, you receive a report of findings that you use to fix those exploitable weaknesses.

The goal of this guide is to compare and contrast the two services, giving you a comprehensive look at each one, so that you can have confidence when choosing the right partner for securing your company from hackers.



6,176,088

DATA RECORDS ARE LOST OR STOLEN EVERY DAY!

-Breach Level Index

YOUR **VALUE**

Performing regular vulnerability scans and penetration tests is essential to being proactive with your overall security strategy. Vulnerability scans provide answers regarding how strong your security posture is, while giving you actionable recommendations for improvement. They allow you to:

- Remain compliant while strengthening your environment
- Show your security team where attacks might come from
- Identify vulnerabilities you did not know existed
- Prioritize your vulnerabilities by risk
- Identify the various security controls that you need to implement
- Gain confidence and even enhance performance of your technologies
- Aid education decisions regarding your security team for more effective control
- Align your business to industry standards and best practices
- Strengthen your customer loyalty and trust

VULNERABILITY SCANNING

A **vulnerability scan** is an essential component in your effective information security program and can provide you with a wealth of valuable information about your level of exposure to threats. It is the process of recognizing, identifying, and prioritizing vulnerabilities in computer systems, applications, and network infrastructures. This scan points out the vulnerabilities in your network, but it does not exploit them. It provides your organization with the necessary intel to understand the threats within your business processing environment and act proactively to remediate them.

The Causes of Vulnerabilities

No business is completely safe from an attack. There are many ways that your company can be (or may be already) vulnerable to risks.

DESIGN AND DEVELOPMENT ERRORS

The design of your hardware and software can often include bugs. Hackers could access your data via these bugs. If your system is improperly configured, or not regularly patched, then you are effectively providing an open door to hackers..

HUMAN ERROR

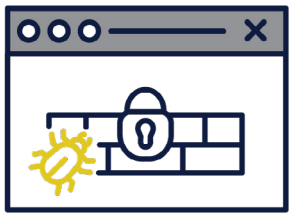
Your people are your first line of defense. Unfortunately, many are not educated in the area of cybersecurity best practices. From password management, improper document storage and phishing, the employees in your workplace can easily be the cause of security breaches.

CONNECTIVITY

If your system is connected to an unsecured network (open connections), then it is in the reach of hackers. Many companies allow their employees to BYOD (Bring Your Own Devices), which often leads to open channels for cyber attackers to gain access.

LACK OF PATCHING

Your organization may struggle to keep up with and manage the process of applying software updates. Detecting and prioritizing and getting vulnerabilities solved seems to be the most significant thing an organization can do to prevent getting breached. However, more than half organizations that suffered a data breach in the past two years cite as the culprit a known vulnerability for which they had not yet patched.



The Types of Vulnerabilities

Our vulnerability scanning tools complete an automated discovery of all the assets within your enterprise, identifying any vulnerabilities and ranking them by risk and priority.

EXTERNAL

We remotely probe for and find any externally-facing holes in your firewalls.

INTERNAL

Testing is typically performed from a number of internal network access points, representing each logical and physical network segment. For example, this may include tiers and DMZs within the network architecture, the corporate network, or partner company (3rd party) connections.

APPLICATION SECURITY

Our testing is designed to identify and assess threats to the organization through bespoke, proprietary applications, or systems. These applications may provide interactive access to potentially sensitive materials. It is vital that they be assessed to ensure that, first, the application doesn't expose the underlying servers and software to attack; and second, that a malicious user cannot access, modify, or destroy data or services within the system. Even within a well-deployed and secured infrastructure, a weak application can expose the organization's "crown jewels" to unacceptable risk.

WIRELESS/REMOTE ACCESS (RAS) SECURITY

We address the security risks associated with an increasingly mobile workforce. Telecommuting, broadband, streaming Internet access, 802.1X wireless networking, and a plethora of emerging remote access technologies have greatly increased the exposure of companies by extending the traditional perimeter ever further. It is vital that the architecture, design, and deployment of such solutions is secure and sound, to ensure the associated risks are managed effectively.

TELEPHONY SECURITY

We address security concerns relating to corporate voice technologies. This includes abuse of PBXs by outsiders to route calls at the target's expense, mailbox deployment and security, voice over IP (VoIP) integration, unauthorized modem use, and associated risks.

Our Methodology

Stealth-ISS Group® Inc. ensures that each level of your organization's information processing infrastructure meets customer and regulatory-driven information security objectives and requirements. We use state-of-the art tools, seasoned IT and security professionals, and industry security best practices to create a detailed analysis that identifies areas of all possible risks and recommended remediation efforts. Our scanning services range from enterprise-wide evaluations to individual program and code reviews.
Our vulnerability scanning follows this standard process:

DISCOVERY PHASE

We work with system and application owners to identify appropriate scanning methods. Discovery is also used to conduct asset identification, checking against existing databases to identify potential rogue devices and validating proper commissioning and decommissioning activities.

ANALYSIS PHASE

Our Cyber Security Engineers perform automated scanning, manual testing, and analysis for identifying and validating vulnerabilities. We interface and coordinate with your business to conduct operational network and OS vulnerability evaluations to analyze the environment and its state of security readiness.

MITIGATION PHASE

Vulnerabilities require mitigation within 90 days or sooner if risk classification is critical and applies to a Highly Valuable Asset (HVA). Our engineers leverage ticketing mechanisms and follow Change Management processes and procedures for requesting configuration changes, upgrade/patching, disabling or coding changes. We verify corrections through retesting and provide artifact details with recommendations for closure. As needed, we submit a request for exception for instances where there is no means for mitigation and propose workarounds or mitigating controls to minimize the risk until remediation is possible. We review submitted artifacts for corrections, requests for exception, and close submissions.

Your Benefits

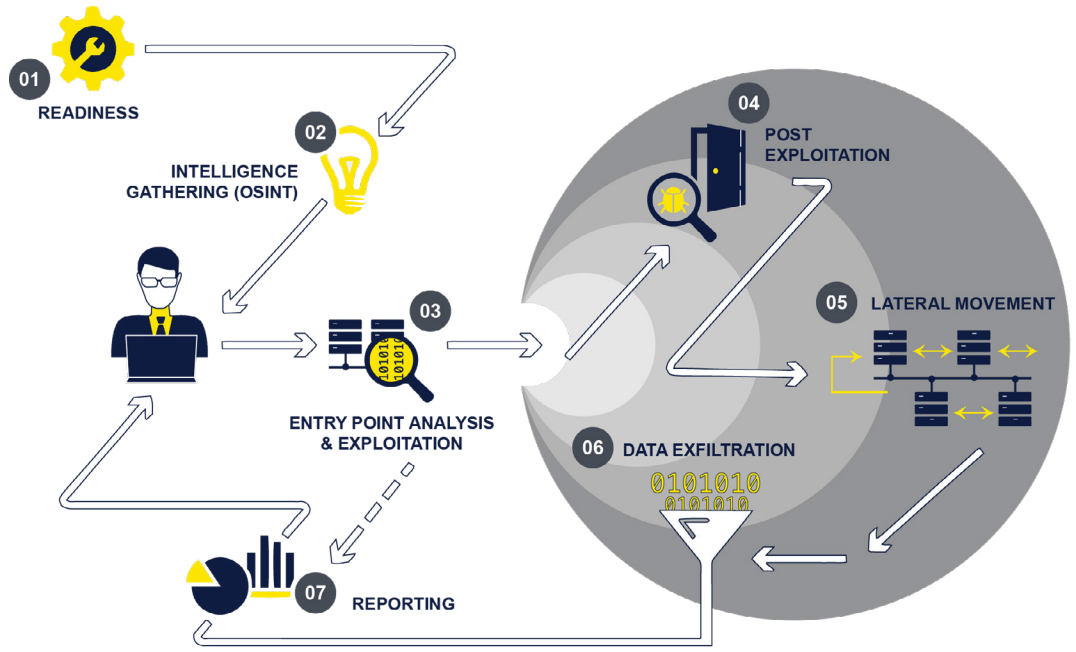
If you don't have a good handle on your security posture, or need help ranking your risks, a vulnerability scan is great place to start. Why?

- Identifying your vulnerabilities provides a **better understanding of your company's security posture**.
- Knowing your vulnerabilities helps your company **maintain compliance**.
- Organizing your inventory of devices in the enterprise leads to more **proactive planning** of upgrades and future assessments.
- **Defining the level of risk** existent on the network enables you to focus remediation efforts on the most vulnerable areas.
- Identifying risks helps **optimize your security investments**.

PENETRATION TESTING

Penetration testing is a time-constrained and authorized attempt to breach the architecture of a system using attacker techniques. This form of testing relates the most accurate and comprehensive view of an organization's information security stance, as it evaluates an entire system, exploiting vulnerabilities to determine precisely how an unauthorized user can get control of valuable information assets.

The form of such a test depends greatly on the client's own situation. Tests can range from a brief overview of the security of an existing infrastructure, to an extensive simulated break-in with the goal of obtaining specific information. Only a comprehensive penetration test can determine the real risk to network resources, thereby making it possible to immediately prioritize corrective measures, and to set the overall direction for an organization's security strategy.



(Application) Penetration Test:

01 02 03 04 05 06 07

Ethical Hacking & APT Test:

01 02 03 04 05 06 07

Custom Test:

01 02 03 04 05 06 07

APPROACH

Test type:
White box, black box, grey box

Attack vector:
External, internal, combined (APT)

Techniques:
Hacking, code review, reverse engineering, exploiting

What a Pen Test Reveals

- If an installed security system is inadequate and can be bypassed, and if or how the system reacts to attack.
- Which information can be obtained from outside the network.
- The security of an environment and its resistance to a certain level of attack.
- The possibility of system break-ins using available or existing knowledge and which information becomes accessible, if a breach occurs.
- Security problems caused by some inconsistency between organizational elements. Complex interactions are sometimes difficult to apprehend during an audit which focus individually on architecture, IP filtering, operating systems, web servers, or applications.

Types of Pen Tests

INTERNAL & EXTERNAL NETWORK PENETRATION TESTING

Network Penetration Testing is typically the most traditional approach for companies to test their cyber security posture. This testing is focused on the servers, infrastructure, and the underlying software comprising the target. Network Penetration Testing typically involves a comprehensive analysis of publicly available information about the target, a network enumeration phase where target hosts are identified and analyzed, and analysis of the behavior of security devices such as screening routers and firewalls. Vulnerabilities within the target hosts are identified, verified, and the implications assessed.

MOBILE APP PENETRATION TESTING

Mobile app penetration testing reveals vulnerabilities in the cyber security posture of a mobile application. We emulate an attack specifically targeting a custom mobile application (iOS and/or Android) and aim to enumerate all vulnerabilities ranging from binary compile issues and improper sensitive data storage to application-based issues such as username enumeration or injection.

WIRELESS NETWORK PENETRATION TESTING

This penetration test attempts to exploit the devices and infrastructure within the wireless network for vulnerabilities. Most commonly the pentester will try and exploit wireless encryption protocols, network traffic, unauthorized hotspots and access points, address spoofing, poorly used passwords, DoS attacks, web server misconfigurations, exposure of sensitive data, malware on your server and more. It is not uncommon for hackers to use unsecured wireless networks to gain entry into your organization.

WEB APPLICATION TESTING

This is another common type of pen test where our ethical hacker searches for the vulnerabilities in your web server applications. This test goes further to identify the vulnerabilities within said business applications. The typical applications that the hacker is trying to exploit include web applications, APIs, Frameworks, Systems, Connections, SAP, and mobile applications.

SOCIAL ENGINEERING TESTING

People are the forefront of your company's security. Social engineering is a way to see if a threat actor can infiltrate your company's environment. Our ethical hackers use techniques like phishing campaigns, taking on the identity of fellow employees or vendors, pre-texting, dumpster diving, eavesdropping. This type of test is helpful in telling you where the 'people' vulnerabilities are within your company.

CLOUD, OT & IOT TESTING

The public cloud and IoT devices are becoming more increasingly used by business. Security protocols are playing catch-up. It is important to be aware that these forward-looking technologies are more vulnerable to attacks. Businesses like yours are gaining competitive advantage by integrating IoT devices and migrating their operations to the cloud. It is important while making these business changes that you're maintaining a watchful eye on the data transmission/collection and related back-end services. Every new endpoint or asset you connect to your network potentially adds another attack vector.

How Pen Tests are Performed

BLACK BOX

In this method of penetration testing, our professional penetration testers have no prior information about your network. This approach simulates a real-world attack. As our attacker researches your network, we identify and document the best way to compromise your network.

WHITE BOX

Our professional hacker receives all information about your network. This is an important technique to identify how an attack would be carried out by a user with admin rights. This method can also determine any faults in your network that can be compromised in other ways.

RED TEAM VS. BLUE TEAM

This technique is to prove the effectiveness of your Security Operation Center (SOC). In this scenario, a team of attackers (red team) will attempt to attack your company while the company's SOC (blue team) responds.

Our Methodology

We provide quality services/products and management oversight of all processes by utilizing seasoned project management consultants, including support personnel, to meet objectives and deadlines of each project. Our penetration testing follows this industry standard process:

SCOPING

The purpose of this initial phase is to define the scope and objective of the penetration test, as well as the parties involved, and agree on Rules of Engagement

RECONNAISSANCE (PASSIVE & ACTIVE)

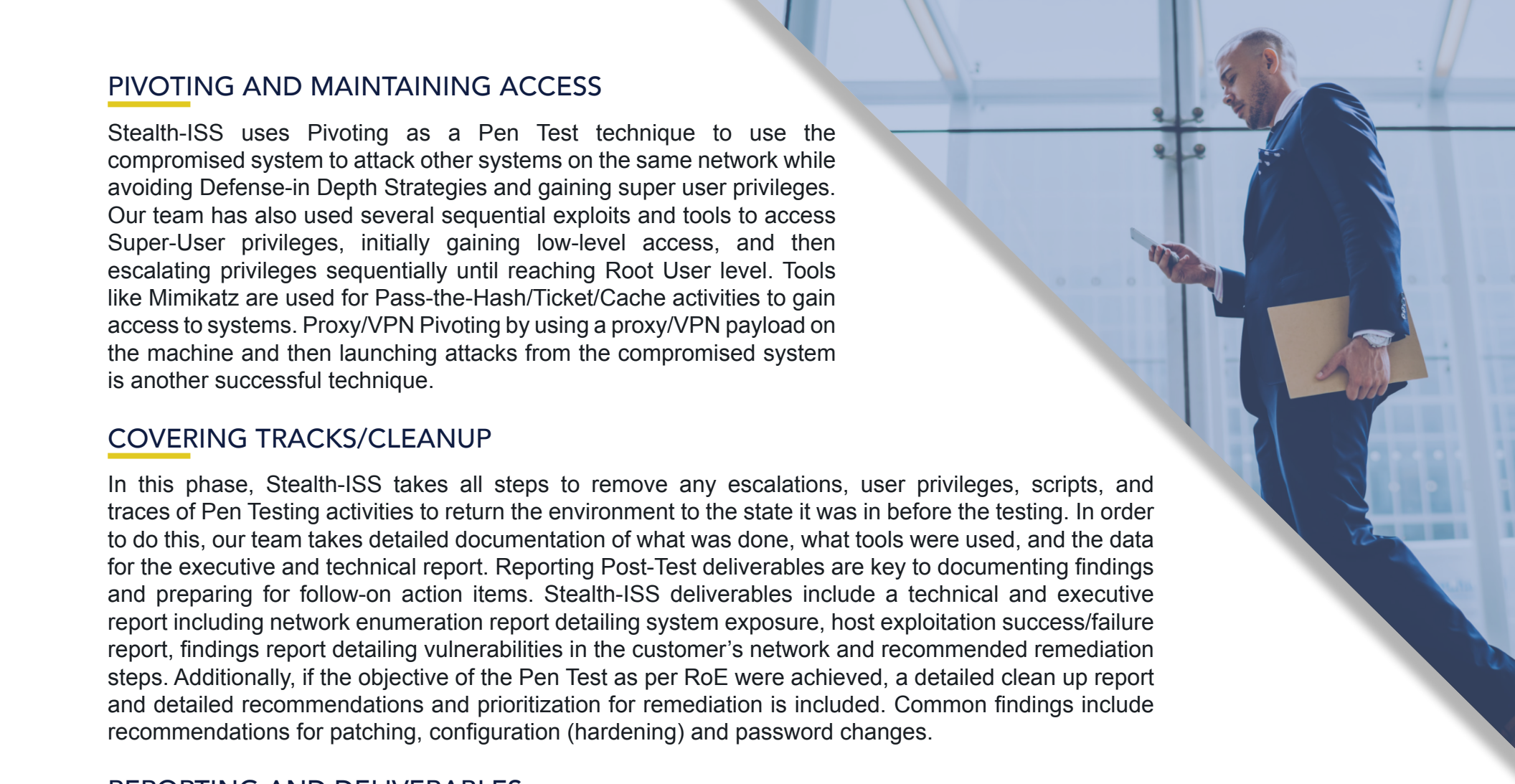
We gain information about targeted computers and networks passively, without actively engaging with the systems. Our methods of passive reconnaissance include: Gathering initial information (e.g. WHOIS, nslookup, SamSpade), determining network ranges and identifying active machines, discovering open ports and fingerprinting the operating systems, mapping the network and uncovering services on ports.

SCANNING AND ENUMERATION

Stealth-ISS conducts scans to detect live systems (network ping sweeps), and what services and versions the applications are running. This allows us to identify which asset is the best to attack to gain access into the network. Port Scanning is first used to identify the vulnerabilities in the services listing on a port within the network. During this process, we identify the host, operating systems involved, firewalls, Intrusion Detection Systems, servers/services, perimeter devices, routing and poorly protected resource shares using active connections to other systems. During the enumeration phase, we use techniques to obtain Active Directory information, discover NetBIOS enumerations, perform DNS queries, and establish null sessions and connections to assets.

EXPLOITATION

Operating exclusively within the defined scope of properly authorized exercises, Stealth-ISS uses a variety of techniques to exploit vulnerabilities, taking advantage of a vulnerability to test a threat ability to gain control of a system, and allow Privilege Escalation. The standard exploit tactics used by Stealth-ISS include Web application, network, memory-based attacks, Wi-Fi, Zero-Day and physical exploitations as well as social engineering. Each pen test has a different and customized exploitation approach based on technology used or tailored exploits (e.g. using existing and public exploits for specific OS). Exploits against client applications require some interaction with the user and so these may be used in combination with the social engineering method. The most common tools by Stealth-ISS are Meterpreter (interactive shell to execute code), Metasploit (payload input) and Cobalt Strike.



PIVOTING AND MAINTAINING ACCESS

Stealth-ISS uses Pivoting as a Pen Test technique to use the compromised system to attack other systems on the same network while avoiding Defense-in Depth Strategies and gaining super user privileges. Our team has also used several sequential exploits and tools to access Super-User privileges, initially gaining low-level access, and then escalating privileges sequentially until reaching Root User level. Tools like Mimikatz are used for Pass-the-Hash/Ticket/Cache activities to gain access to systems. Proxy/VPN Pivoting by using a proxy/VPN payload on the machine and then launching attacks from the compromised system is another successful technique.

COVERING TRACKS/CLEANUP

In this phase, Stealth-ISS takes all steps to remove any escalations, user privileges, scripts, and traces of Pen Testing activities to return the environment to the state it was in before the testing. In order to do this, our team takes detailed documentation of what was done, what tools were used, and the data for the executive and technical report. Reporting Post-Test deliverables are key to documenting findings and preparing for follow-on action items. Stealth-ISS deliverables include a technical and executive report including network enumeration report detailing system exposure, host exploitation success/failure report, findings report detailing vulnerabilities in the customer's network and recommended remediation steps. Additionally, if the objective of the Pen Test as per RoE were achieved, a detailed clean up report and detailed recommendations and prioritization for remediation is included. Common findings include recommendations for patching, configuration (hardening) and password changes.

REPORTING AND DELIVERABLES

This is the last but equally important phase after all vulnerability scanning and penetration activities have been completed. After completion of each assessment (internal, external, web, and social engineering), the following reports are delivered to key stakeholders in no later than 5 days: Security Assessment Report - Executive Summary Report - Risk Matrix - Proof of Concept/Engagement Logs - Proposed Mitigations and Workaround.

A draft report is provided and discussed, with a final report produced after key stakeholder feedback is received. The report includes all documentation of what was performed, exploits identified and executed, remediation recommendations and other relevant data required based on the outcome and in adherence to the client requirements.

Your Benefits

There are several reasons why organizations choose to perform a penetration test; they range from technical to organizational but the most common are:

- To **identify** the threats facing your organization's information assets.
- To **quantify your information risk** and provide adequate information security expenditure.
- To **reduce your security costs** and provide a better return on IT Security Investment (ROI).
- To help your company **meet compliance regulations**.
- To **adopt best practices** by conforming to legal and industry regulations.
- To **maximize efficiency** by pointing your teams into the right direction.
- To **show nontechnical peers** how/why money is being spent.
- To **know the financial impact** of the vulnerabilities exposed.
- To **see the potential business operational impacts** of successful attacks.

Our Tools

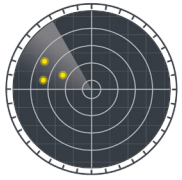
Our certified Pen Testers use the NIST SP 800-115 Penetration Testing Methodology and relevant processes to perform the testing, document the results, and provide an executive as well as technical report, along with recommended actions to mitigate any findings. Stealth-ISS uses a variety of COTS/GOTS tools for Vulnerability scanning and Penetration Testing, including Browser Exploitation Framework (BeEF), Core Impact, w3af, Kali Linux suite, Canvas, Burp Suite, Metasploit, Wireshark, Cain & Able, ZAP, Retina, Maltego, AngryIP, SamSpade, shodan, DNSDumpster, scans.io, nikto, gophish, and netcraft. The tool kit we use in these activities are usually full penetration test OS distributions such as Kali Linux, BackBox, Parrot Security and Pentoo which include the tools used such as Metasploit, Neosploit and multiple tools to map network traffic flows (TCP/ IP, DHCP, DNS) and conduct exploits based on buffer overflow mobile code, cross-site scripting, PL/SQL and injections, race conditions, covert channel, replay, return-oriented attacks, and malicious code.

WHY **STEALTH-ISS**

Stealth-ISS Internal and External Penetration services include Network Mapping, Vulnerability Scanning, Phishing Assessments, Wireless Assessments, Web Application Assessments, OS Security Assessments (OSSA), and Database Assessments. Where applicable – especially for in-house developed applications – we perform automated and manual application code analysis and code review by following the OWASP framework during the entire Software Development Life Cycle. This dramatically increases the probability that any security issues are identified as soon as possible while minimizing risk in production.

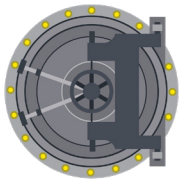
Stealth-ISS has extensive experience conducting vulnerability analysis and penetration testing, including development of processes and procedures for integration with clients' tool sets to quickly isolate vulnerabilities posing the greatest risks to applications and the infrastructure.

Stealth-ISS has extensive experience in implementing, operating, and customizing different vulnerability scanning tools such as Nessus, Qualys, OpenVAS, Network Mapper (Nmap), Syhunt, BeyondTrust. Reports are delivered using built-in functionalities of the respective tools and custom scripting to allow for unique scanning capabilities and identifying threats for custom-built applications or zero-day vulnerabilities. Our processes and procedures quickly isolate root cause vulnerability findings and adhere to Continuous Monitoring constructs compliant with reporting requirements.



GET SHARP.

GET SERIOUS.



GET SAFE.

GUARANTEED RESULTS

Stealth-ISS doesn't just test. We negotiate test priorities and goals with you, and we guarantee to meet those goals. You do receive the testing and test results that we claim.

CONFIDENTIALITY

We preserve and protect the information we develop and gain during testing from disclosure to any other parties. A non-disclosure agreement is signed with customers prior to testing. We do not use any external consultants or hackers for this service.

QUALIFICATIONS

Our security personnel have strong technical credentials, with the latest training in their field, and they hold the highest levels of accreditation such as OSCP, CEH, CISA, CISSP, CCSP, and other.

METHODOLOGY

Not only do we use the latest technology, but we also use high-level methodology that follows standards such as MSTG, PTES and OWASP. Also, we perform all security audits and penetration tests according to national and international security and IT standards such as NIST 800-115, ISO 27001/2, PCI DSS, and others.

SECURITY POLICY

We ask to review the customer's security policy to help us understand prevailing security standards, practices, procedures, and potential weaknesses.

TECHNOLOGY

We use latest commercial technology for penetration tests with daily updates as well as opensource software and the knowhow of our security consultants. In order to ensure the quality and outcome of the test, we also perform manual checks on latest vulnerabilities. The technology we use during testing is being used by institutions such as Department of State, Department of Defense, Bank of America, Citibank, Hewlett Packard, Rolls Royce, Price Waterhouse Coopers, British Airways, and many other globally-recognized brands.

REPORTING RESULTS

A written report is provided, containing manager level overview, summary of the issues identified sorted by severity, and technical details of each issue complete with outline-associated recommendations. Also included is a full listing of the actual tests results, and notes on the scope and limitations of tests. We will also provide the customers with copies of all logs, reports, and other raw data collected during the testing process.

PROJECTS

Our security staff has performed vulnerability and penetration testing for mid-size and large corporations as well as governmental institutions throughout Europe, international organizations and NATO member states and institutions.

CUSTOMER COOPERATION

Our vulnerability scan and penetration test projects are always designed in collaboration with the client.

ABOUT STEALTH-ISS GROUP

Stealth-ISS Group® Inc. (est. 2002) act as your extended IT, cyber security, risk and compliance team and provide strategic guidance, engineering and audit services, along with technical remediation and security operations. We pride ourselves on the quality and professionalism of our workforce, collaborative relationships with our clients, and our ability to bring you innovative, customized but affordable vendor-neutral solutions based on your immediate needs while aligning with your business strategy and operations. We add massive value and save you money on staffing a permanent security organization.

We are a Woman Owned, Service-Disabled Veteran Owned Small Business (SDVO) passionate about protecting companies and agencies from all facets of cyber-crime, protecting your people and company data, reducing your information and financial losses, and protecting your reputation. We are one of only a few WOSB, SDVO companies in the US with all HACS SINs.

CONTACT US

+1 (866) 500-0751

610 E Zack Street
Suite 110-4165
Tampa, FL 33602

FOLLOW US

/stealth-issgroup
@stealth_iss
@stealthiss

STEALTH
ISS GROUP®