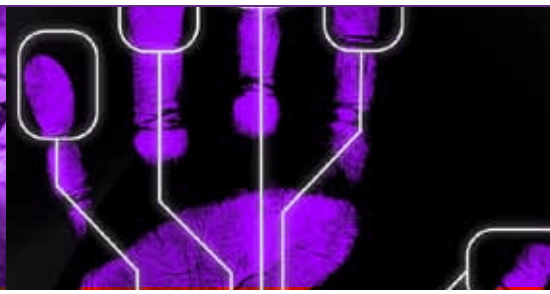
Specialized Security Services, Inc.

REDUCE RISK WITH CONFIDENCE



s3security.com

Security Professional Services

S3 offers security services through its Security Professional Services (SPS) group, the security-consulting arm of S3. S3's Security Professional Services (SPS) group combines the most advanced information security expertise in the industry with straightforward methodology to offer a sound security strategy that carefully balances critical operational requirements with vital information security needs.

S3 consultants have a proven record of success and an intimate understanding of the latest security technologies and vulnerabilities. S3 has successfully completed security assessments and provided incident response for hundreds of organizations, including global Fortune 1000 corporations, mid-size organizations, and Financial Institutions.

S3 uses both proprietary and publicly available resources to expose information security vulnerabilities. With customized monitoring and analysis tools, our information security consultants are able to identify malicious activities and security vulnerabilities that are often overlooked.

Each relationship begins with a careful assessment of the client's unique business practices and thorough mapping of the organization's IT infrastructure. After identifying the client's core business needs, S3 develops a customized information security solution that combines expert consulting with product and service recommendations.

S3's Security Professional Services group operates on the premise that information security solutions must be based on a client's fundamental business models and processes. Working closely with client staff, members of the SPS team identify both high-level strategic threats and specific technical vulnerabilities and suggest practical, business-friendly solutions to mitigate risk.

Critical Security Assessments (CSA)

S3 Security Assessments include a broad range of methods and techniques, including vulnerability and risk assessment, cooperative security reviews and actual penetration to demonstrate the potential risks represented by identified vulnerabilities. Each assessment or penetration test is designed to accomplish specific goals, however, in general, each assessment determines whether:

- Critical components work together
- Mechanisms for redundant protection are in place
- Implemented perimeter security is adequate
- An optimal defense in-depth strategy exists
- Effective policy exists and is enforced
- Reporting and response mechanisms are effective, and
- Residual vulnerabilities and other critical issues have been addressed

Solutions Tailored to Your Business' Specific Needs

Each assessment is designed to meet specific client requirements. A typical approach to assessing a network begins with a professional, controlled penetration and vulnerability assessment of the external network perimeter. This portion of the assessment evaluates the security posture of the network as it appears to an outsider. This is usually followed by an active vulnerability assessment and cooperative security review in which S3 Consultants work with the client's staff to determine the extent of potential impact of the access gained, as well as to identify internal vulnerabilities that may not be accessible from the Internet.

Cooperative Assessment

Once the penetration test and internal vulnerability assessment have been completed, the cooperative assessment provides the opportunity for S3 Engineers to identify policies and practices that have contributed to the technical vulnerabilities. It also permits us to become acquainted with the client's organizational structure and business processes, enabling a more accurate estimate of the level of risk represented by the identified vulnerabilities. The cooperative assessment familiarizes S3 Engineers with the client's business functions and requirements to allow the development of effective and practical countermeasures to mitigate risks.

Keeping Your Staff in the Loop

S3 Engineers work with the client representative to enable the client to remain in control of any test or assessment and to keep the client abreast of progress. In all efforts, the goal is to work with the client IT staff to identify vulnerabilities, assess the risk represented by those vulnerabilities, and develop a recommended course of action to eliminate existing vulnerabilities and modify policies and practices to prevent a recurrence of risk.

Internet Gateway Assessment Methodology

S3 divides the its standard security assessment into two phases: External Penetration Study, and an On-Site Cooperative Assessment.

External Penetration Study

S3 performs a penetration study against the Internet Gateway. This penetration study includes any routers, firewalls, and hosts that define the customer's gateway.

Though the specific tests vary, based on the topology and exposed systems making up a gateway network, the overall methodology applies to all assessed gateways:

Passive Information Gathering

Prior to the beginning of active penetration efforts, the S3 Test Team conducts an extensive research effort to gather information on the Client networks and components. The collection of publicly available information concerning a target network is a vital first step in a penetration effort. A wealth of information about any public network is available via a series of internetworking system services, as well as through use of information gathering tools. The types and importance of the information varies with each service and tool, but together this information can be used to identify potential vulnerabilities that may enable a successful penetration of the network perimeter.

Active Network & System Services Discovery

Physical network design and routing information can often be determined through use of IP scan tools as well as simple network management protocol (SNMP) queries of the routers. First, the team uses IP and/or UDP scanning tools to perform discovery of systems within the customer's gateway IP addresses. Each system that is discovered, is scanned for active network services, using a combination of public, commercial off the shelf and proprietary scanning tools. The choice of tool is determined by the size of the address block, but the results of the scanning tools are comparable for this purpose.

These scans show the common results of the set of hosts and services which are active on the target systems and the set of services which are permitted to pass through the firewall or router filters. In many cases, it also shows which services are being blocked by firewall or router filters.

Identifying Vulnerable Versions of Software

Many systems that have not been fastidiously updated are running vulnerable versions of software that provides network services. These outdated network services contain software bugs that enable the service to be manipulated into providing information or even providing unauthorized access to the system. Therefore, once all active hosts and services have been identified, S3 probes these services to identify their make and versions, and cross-references the active services against a database of potentially vulnerable services.

Anonymous Access

In addition to versions of software, simple misconfigurations and insecure use of certain protocols can permit the compromise of a system. Systems that might permit anonymous access are checked for anonymous read, and even more importantly, anonymous write access. If access is discovered, an Engineer checks the service to determine if access exists to directories that might be used to create unauthorized access, denial of service, or to plant malicious software. Services that commonly provide anonymous access include HTTP (web), FTP and TFTP (file transfer), and NFS and NetBIOS (network file sharing).

External Penetration Study

A number of services that rely on RPC protocols are vulnerable to attacks that exploit the RPC protocols or the services themselves. Systems that have active RPC services are checked for access controls, RPC protocol versions that are known to be vulnerable to spoofing, and trust relationships. In this way, recommendations are not only offered about the dangers of the general use of some of the more vulnerable of these services, but specific services that are vulnerable to known attacks in the active configurations and versions are listed in the vulnerabilities.

Penetration of Gateway Network

The actual penetration methodology is a three step, repetitive process that mirrors an effort by a knowledgeable, motivated hacker. The team must gain initial access to at least one system within the gateway network. Next, the team increases their access to gain administrative control of any compromised system. Finally, the team then may use the compromised system as a platform from which to repeat data gathering and penetration of other systems in the gateway, or sometimes even in the internal network, to determine if multiple vulnerabilities can be added together to compromise the internal network or other parts of the client's critical infrastructure.

Initial Penetration of Exposed Systems

Once the exposed vulnerabilities have been identified and mapped, the S3 Test Team attempts to gain access to exposed systems. The selection of specific exploits (attacks) to be used against a system is based on each system's operating system version and the services that are running on it. Since operating systems and services vary widely, exploiting them requires an in-depth knowledge of the potential security flaws of each operating system, as well as working configuration exploits of all common system services. S3 penetration methods have been developed from published exploits, security advisories, and from attacks that have been developed in-house. Due to the large number of potential exploits (attacks), it is impossible to describe each here. However, some of the more common system attacks are listed below:

- **File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP):** Misconfigured FTP and TFTP servers may provide attack opportunities, such as allowing file access attacks and exploiting the use of trust relationships. If present and improperly configured, TFTP can provide access to valid userids or to encrypted passwords.

- **Poorly Enforced Password Policy:** Some of the most exploitable vulnerabilities on many systems are the existence of default and poorly chosen user passwords. Either condition increases the potential of unauthorized access. Application and operating systems is probed to determine if default (out-of-the-box) passwords are used. Also, tools may be used to run brute force attacks from a dictionary of common passwords.

- **Network File System (NFS):** NFS attacks are usually file-based and work via remote file system mounts. This is typically used to access mail or to exploit trust relationships with rlogin, rsh, or rexec

- **Hypertext Transfer Protocol (HTTP):** Commonly known as web servers, these servers have become well known for misconfigurations of common graphic interface (CGI) scripts, as well as for bugs in the daemon software, which allow remote execution and file access.

- **X-Windows:** X-Windows is the method of used for graphic user interface (GUI) to Unix systems. Some default X-windows configurations can allow a third party to monitor the user's keystrokes, capture screen images, or even push input through the X-Terminal, as if the attacker were the authorized user.

- **Windows NT Default Registry:** The default registry configuration can allow anonymous access to the user names and shared directory names. This default configuration is intended to permit allocation of privileges between a trusted and untrusted NT domain, but can reveal enough information to permit a successful brute force or password guessing attack against selected accounts.

Administrative Control of Compromised Systems

Once a normal user shell account is achieved, the Test Team attempts to obtain administrative privilege, which is tantamount to having total system and application control (except perhaps to some databases). Many of the same exploits used to gain user-level access on a system can be used locally to gain root or administrator access. In addition, misconfigurations and software bugs may be used to obtain increased privileges.

Expanding The Scope of Access

Once administrative control of a system is obtained, that system then becomes a potential platform from which the team surveys and attacks other portions of the network that may not be directly reachable from the Internet. In this way, it is possible to expand the penetration of a single system into a much larger compromise. Some of the methods that are often used to expand the compromised access include the following:

- **Host and Port Scanning:** Once control of a system is achieved, network scanning tools are often used to determine if the compromised system has access to portions of the network that are shielded from direct Internet access by firewalls or router filters. In this way, the team looks for weaknesses in network topology and access controls to discover if external system vulnerabilities can be exploited to gain access to the internal network.
- **Network Packet "Sniffing":** Most multi-user systems are capable of being used to intercept data packets as they stream past the system on the network. Once the test team gains administrative control of a Unix or Windows NT system, which appears to have an important strategic location within the network, the team may attempt to use it to "sniff" network traffic to capture passwords for other systems, as well as identify strategic targets for additional penetration efforts.
- **Trust Relationships:** Some systems use defined trust relationships to bypass authentication. Once a "trusted" system is compromised, it is often possible to simply perform an rlogin, rsh or rexec to gain access to the "trusting" system.
- **Previous Attacks:** Most of the system penetration and shell access attacks can be issued from the compromised system to gain access to additional systems.

The ultimate goal is to determine if the identified external vulnerabilities can be leveraged into access of critical Client systems, or even the internal network.

Precautions Taken to Protect Client Systems & Data During Testing

Extensive effort is expended to ensure that data is not modified and that authorized user access to client systems and networks is not impeded. Denial of service attacks are not executed, but if denial of service vulnerabilities are identified, they are documented and recommendations are made to correct them. S3 maintains a test lab where attacks and exploit code are developed and tested. No attacks or other assessment tools are used on client systems without first being successfully tested. In addition, any vulnerabilities that are found during external testing that represent an immediate risk of compromise from the Internet are immediately brought to the attention of the Client Representative to prevent a continuation of risk.

On-Site Assessment: Interviews and Data Collection

S3 conducts interviews with the firewall and network managers/administrators to identify the purpose of the gateway and its intended functionality. This part of the task helps the security consultant determine what type of traffic the gateway must permit inbound, as well as outbound. From that information, the engineer begins to identify what types of rules to expect to see defined on the firewall.

Configuration Review of Network Protection Devices

Next, the consultant works with the firewall and network administrators to review the configurations of the firewall and supporting routers to determine if the intended controls are properly implemented and if those controls are adequate to reduce the risk of intrusion to the internal network to an acceptable level.

As a result of the effort described above, the assessment team is now familiar with the rule sets of any firewalls and routers that are used to protect the network and individual systems from intrusion. The assessment team works with the network administrators to identify systems that are accessible from the Internet and conduct system configuration reviews to identify system-level vulnerabilities that may be exploited from the Internet. During the configuration reviews, the S3 Security Engineer conducts interviews/discussions to identify any update and administration procedures that may create vulnerabilities

Cooperative System Reviews and Discussions

Next, the S3 team again meets with applicable administrators and network management staff to discuss potential vulnerabilities that have been identified and to perform a more in-depth review of selected network components and systems. The hands-on analysis of a representative selection of systems is focused to ensure that the technical implementations match the described configurations and to look for weaknesses in the security controls of each system.

This portion of the security assessment is accomplished in total cooperation with applicable network and system administrators, and is valuable in assessing vulnerability and exploitation repercussions from network compromise. Also during this process, S3 conducts discussions with network managers and system administrators to identify actual administration and configuration control practices. Variations from written or verbal guidance, as well as potential recommended corrective actions, are discussed.

In every case, the intent is to have S3 security experts work interactively with the client support staff to develop solutions cooperatively. In this way, recommendations better fits the Client network environment, there is less resistance to change for procedural changes, and the Client administrators gain the benefit of value-added technical security training.

Configuration Review of Network Protection Devices

Throughout the testing, S3 consultants document their actions in the form of notes, working papers, and data files. Immediately after the assessment effort, S3 formally documents the effort in the Internet Gateway Security Assessment Report.

The report identifies the systems being tested, describe the network protection scheme, list the active and accessible services on each system that was tested, and describe detailed, specific vulnerabilities for each applicable system. Each vulnerability is accompanied by a description of it's potential to impact the Client network or systems, as well as recommended actions to correct them. The report also documents any recommended modifications to gateway or external network topology or architecture and explains what it is desirable to make the change.

It is anticipated that most of these recommendations will be short term configuration changes and implementation projects necessary to mitigate the identified risks. However, where patterns of vulnerabilities indicate a potential weakness in practices, long-term procedural changes may also be offered to prevent the reoccurrence of vulnerabilities. The assessment is truly a snapshot in time. Therefore, in addition to the findings, recommendations and conclusions, S3 includes as much raw scan data as possible.

In addition, where possible, the assessment also describes any residual risks that cannot be corrected without large-scale effort, and discusses the effort that would be required, as well as alternative solutions, if applicable.

Report delivery is typically within two weeks of assessment completion.

Additional Security Professional Services Offerings

S3 offers a full suite of Security Professional Services to suit your needs. For additional information about S3's Security Professional Services, see the following documents:

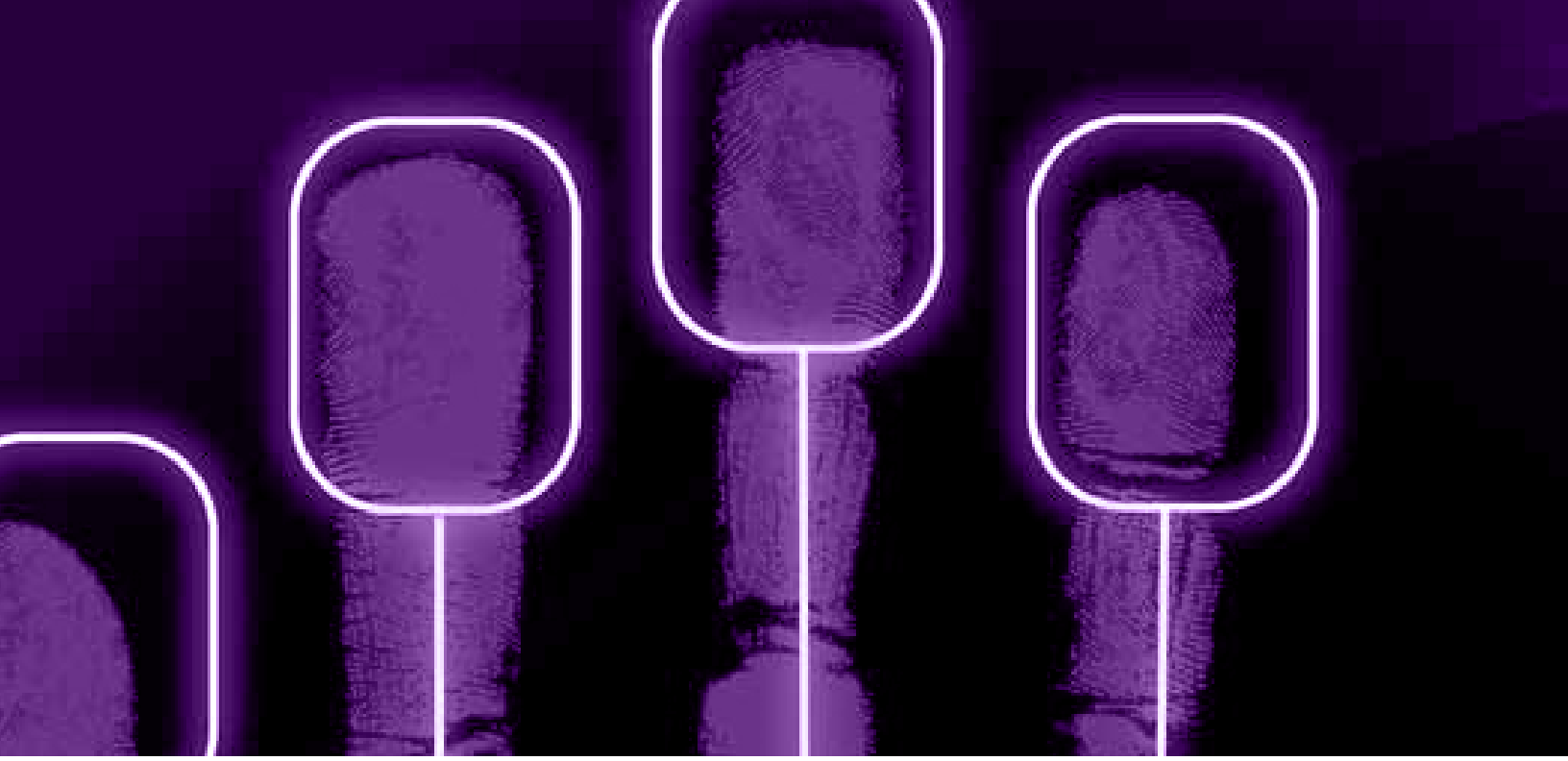
S3 Security Professional Services Technical Capabilities Overview

S3 Security Professional Services Incident Response & Forensics Methodology

S3 Security Professional Services Partners

Protect Your Network with S3 Security Professional Services CriticalSecurity Assessment

Protect Your Network with S3 Security Professional Services CriticalSecurity Assessment



Specialized Security Services, Inc.

s3security.com

info@s3security.com