PROTEUS|OCM
Technical Penetration Test Service Engagement – Final Report

In support of:

Wiresoft, Inc.

September 9, 2009: Version 1.0

www.proteus-ocm.net

1360 Eisenhower Blvd,Suite 204
Johnstown, PA 15904

Phone: 814.308-5048
Toll Free: 877.283.1501
Fax: 814.308-5048

Executive Summary

Wiresoft FIREGATE 100
Small Business Security Suite Appliance

This report provides summarized information about all the different hosts, users and vulnerabilities that were identified, targeted and exploited by PROTEUS|OCM during this penetration test.

This penetration test was conducted with the aim of discovering any technical vulnerabilities that may exist within the appliance. As such, client side (end-user) exploits were not executed against this system as a client exploit would be outside of the scope of this penetration test.

This penetration test targeted the internal and external interfaces of the FIREGATE 100 appliance. The system itself was void of any direct attack avenues due to technical vulnerabilities related to current configuration or third party software applications.

Business Requirement
Penetration testing is performed on enterprise applications by a third party to find vulnerabilities in the infrastructure or application so that they can be remediated before exploited by a third party. This can also be done on existing applications, typically on a yearly basis, to find out vulnerabilities so that they can be remediated.

For the purpose of this engagement, the penetration test was focused at discovering technical vulnerabilities which could have the potential of being exploited.

Caveat emptor
While PROTEUS|OCM strives to ensure that ever available vulnerability, new vulnerabilities are discovered daily and a technical penetration test is a form of a formalized audit procedure and methodology that attempts to validate hardware and software configurations and identify potential exploitable vulnerabilities. *It is a snapshot of the current build version of a system at a point in time.*

Summary of Exploits

Total number of vulnerabilities successfully exploited:	0
Total number of unique vulnerabilities successfully exploited:	0
Total number of compromised hosts:	0
Total number of unique network vulnerabilities successfully exploited:	0

Engagement Summary
The technical penetration test is a method for identify vulnerabilities within a system and exploiting such vulnerabilities to attain privileges not previously authorized. For this engagement, the technical penetration consisted of two focal point areas, 1) network services and 2) application services. These areas often lead to a successful compromise. At the conclusion of this engagement, PROTEUS|OCM was unable to successfully compromise the system.

About PROTEUS|OCM

PROTEUS OCM LLC is a Service Disabled Veteran Owned Small Business (SDVOSB) which specializes in the Governance, Risk Management, and Compliance of Information Technology. Our services range from assessment of the organizational risk exposure, the correction of existing security problems, to the design and implementation of secure information technology frameworks.

PROTEUS|OCM's personnel have been committed to delivering and providing Information Security Consultation Services that address the information security needs of many corporations and government organizations throughout the United States. Some of our clients require protection of their information assets from unauthorized access in order to comply with industry and governmental regulations while others strive to enhance their security posture. Additionally our personnel are well versed in and provide a wide spectrum of information security services relating to IT Governance, Risk management and Compliance.

PROTEUS|OCM's information security consulting services provide our clients with comprehensive, complete and informative assessments as to their security posture. This allows the organization to make informed decisions about how to best prioritize vulnerabilities, plan remediation efforts, optimize existing security posture, and make informed decisions regarding future security efforts and initiatives. As a result, we are able to secure their information assets and ensure compliance in the most efficient and cost-effective way possible. PROTEUS|OCM has been essential in helping them achieve their goals.

PROTEUS|OCM is a privately held company and is based in Johnstown, Pennsylvania. In addition to providing private sector solutions for business, PROTEUS|OCM also provides continuous consulting services to various U.S. federal and state government agencies, and Fortune 500 companies in addition to small-to-medium sized organizations. Our consultants have held successful engagements with commercial organizations such as Nationwide Financial Services, State Farm Bank and JP Morgan Chase in addition to federal and state government engagements with the U.S. Bureau of Industry and Security, U.S. Department of Energy, Department of the Navy, the United States Marine Corps, Federal Bureau of Investigation, State of Michigan (State Bureau of Investigation), State of Iowa (Iowa Workforce Development), and State of Oregon (Department of Transportation).

PROTEUS|OCM works closely with various domestic and international CERT authorities and intelligence communities to establish on-going security threat mitigation, as well as maintaining industry certification and relationships with such bodies as the Payment Card Industry Security Standards Council, Carnegie Mellon Software Engineering Institute, National Security Agency, Information Systems Security Association, Information Systems Audit and Control Association, National Institute Standards and Technology and International Information Systems Security Certification Consortium.

Appliance Environment, Configuration & Implementation

Testing was carried out in a live test environment. The appliance was configured for use within a SMB setting with primary administration and management being performed via the web management portal by an IT Generalist.

The appliance was inserted and implemented as a perimeter unified threat management (UTM) appliance (see figure 1) that sat between the demarcation (screening) router and the internal switch. The environment consisted of a logical network consisting of multiple personal computer systems, running various Windows based operating systems as well as a cluster of servers used in routine operations.

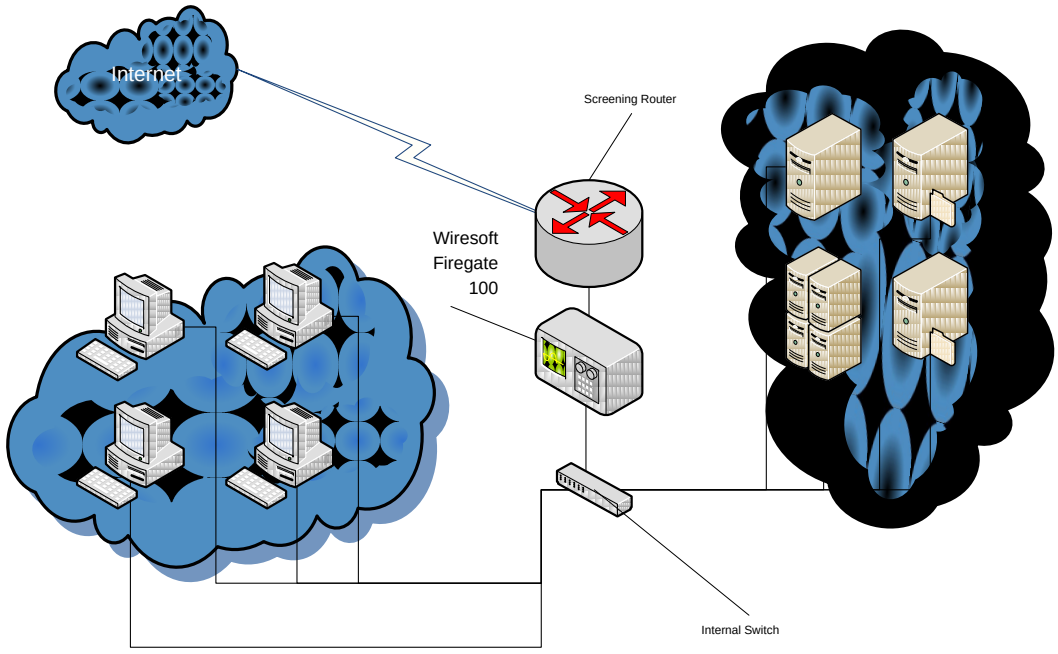


Figure 1

Penetration Test – Network

Targets

- Network Services

Attack Vector

- External (Internet)
- Internal (end-user)

Exploits Attempted

- 200+ unique remote exploits attempted

Findings

- No exploitable vulnerabilities discovered at this time

Penetration Test – Application

Targets

- Web Management Portal

Attack Vector

- Internal (end-user)

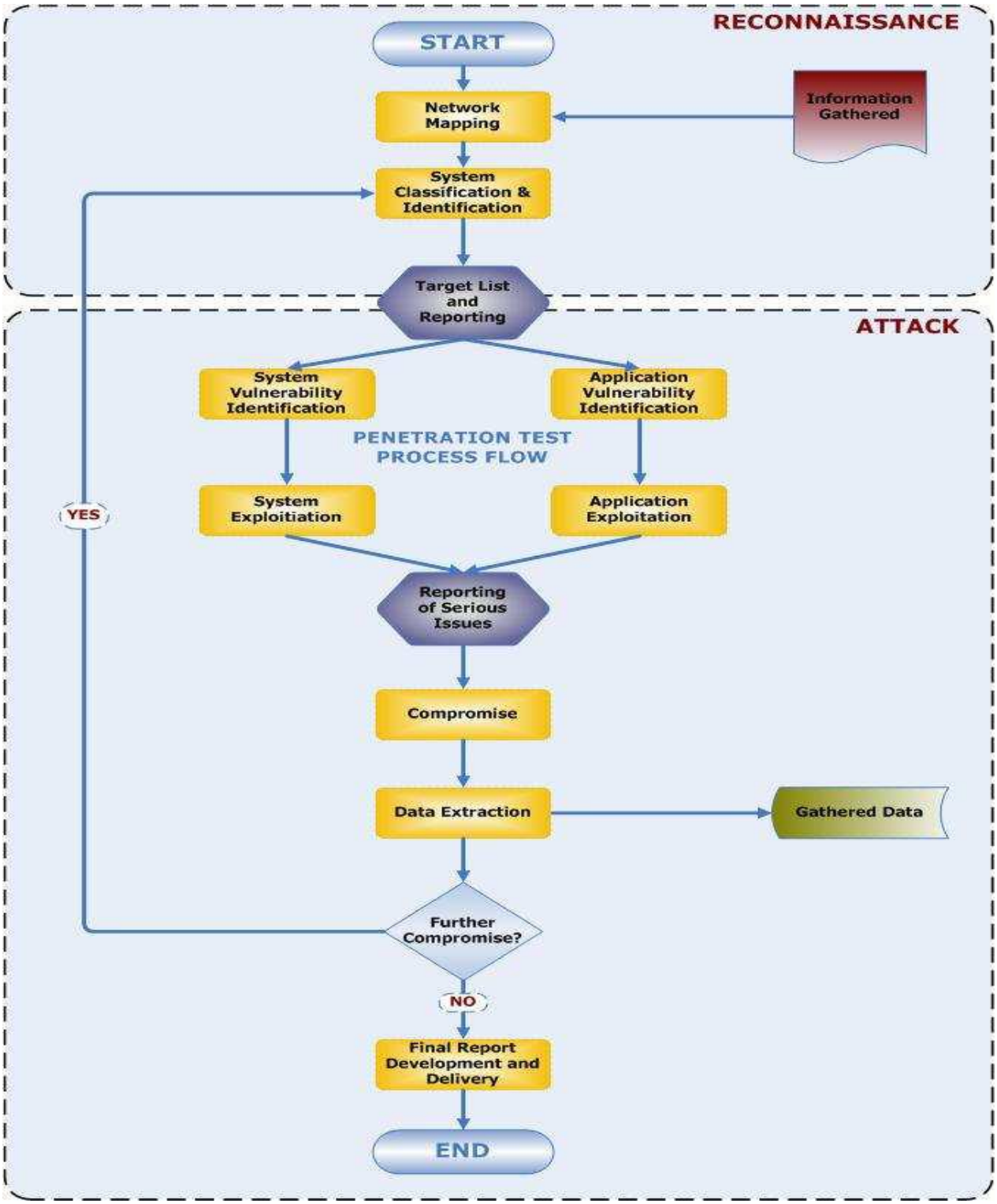
Exploits Attempted

- Input Validation
- Buffer Overflow
- Cross Site Scripting
- URL Manipulation
- SQL Injection
- Hidden Variable Manipulation
- Cookie Modification

Findings

- No exploitable vulnerabilities discovered at this time.

PROTEUS|OCM Penetration Testing Methodology



System Identification & Classification

The network map would not be very useful if the systems located on the network were not identified and classified. Another probe is performed of the systems identified, this time using TCP finger printing, service fingerprinting, and various methods to identify and classify systems and services. The data gathered is used to classify the systems by function. Data gathered about the system helps to determine the classification For example, a system running a particular version of the Apache Web Server as well as BEA Web logic is most likely a web application server. After each system is classified the network map is updated to reflect each system's functionality and operation system. Before the next testing steps begin, PROTEUS|OCM will debrief the client's key security contacts on specific system findings and intended target list to be used in the attack phase.

System Vulnerability Identification

Each host and all associated listening service to be targeted for the test is probed, singularly and in tandem with the other hosts to locate potential vulnerabilities. Using a large working knowledge of exploit techniques, public information, and results of private vulnerability research, the PROTEUS|OCM consultants catalog all the potential attack vectors that might be exploitable. PROTEUS|OCM consultants devise several attack strategies and commence to exploitation.

System Vulnerability Exploitation

If the plan of attack devised in the previous step includes any techniques that may impact production systems and infrastructure, the client is first advised of the possible system downtime that may arise. At this point it is up the client to decide whether or not to proceed with the exploitation. As a rule, any potential vulnerability found is manually investigated, researched, and an attempt is made to exploit. Exceptions to this rule are techniques that will cause a denial of service (DoS) or harm the data on the target system. PROTEUS|OCM will only attempt to exploit a Denial of Service, or alter data on a target if specifically instructed by the client in writing. In exploiting vulnerability, PROTEUS|OCM has will make an attempt to either gain unauthorized access to the target system, or extract sensitive data from it. An exploit is considered successful if we were able to achieve either of these objectives. As successful exploitation leads PROTEUS|OCM to systems compromise, PROTEUS|OCM consultants will report the breach to the client's key security personnel immediately.

Application Architecture Identification

Using the classifications previously established, PROTEUS|OCM will use tools and manual intervention to identify the specific applications running on each of the systems. When an application server is identified, other systems will be identified within an application server group. This grouping will help identify potential flaws in application trust relationships. This information is vital to the successful identification of application vulnerabilities. In addition to identifying purposeful applications, PROTEUS|OCM will attempt to discover Trojans and Backdoors that may be present in the environment.

Application Exploitation

Before any application exploitation occurs, PROTEUS|OCM will debrief the client's key security contacts on the application architectures identified. PROTEUS|OCM will explain the plan of attack for each system and which techniques will be used. At this point, the client will sign off on application exploitation. If the system is a production system, the client will be advised of the possible system downtime that may arise. At this point it is up the client to decide whether or not to proceed with the exploitation. Each system will be attacked with many different types of application vulnerability testing techniques.

These tests include but are not limited to:

- Input Validation
- Buffer Overflow
- Cross Site Scripting
- URL Manipulation
- SQL Injection
- Hidden Variable Manipulation
- Cookie Modification

System Compromise

As systems are compromised, the client's key security contacts will be notified. At this time, the client contacts are given the opportunity to decide if the particular system should undergo additional tests. If they decide to have PROTEUS|OCM continue, additional techniques will be used to further penetrate the target system and the environment as a whole. This can include password cracking tools, a network sniffer, remote management tools, etc. Successful execution establishes a launch point for additional attacks against the environment.

Data Extraction

Each system that is compromised will be examined for the existence of critical data and files. If PROTEUS|OCM finds such data to be accessible, a sample of this data will be downloaded from the system and securely stored by PROTEUS|OCM until the presentation of deliverables.

PROTEUS|OCM Penetration Testing Team

Dr. Alexander Ganzy, PhD, CSSLP, CGEIT, NSA-IAM/IEM, CSOXP, CICMP, CITGP, CITRP. CITCP
Dr. Ganzy currently serves as co-founder and principal emeritus of PROTEUS|OCM. He develops and applies advanced cyber intelligence methods, theories, and research techniques in the investigation of system threats. Dr Ganzy is a leader in OSINT, ELINT, and Cyber related intelligence activities and has led global teams to develop and implement detailed plans which cover the full life cycle of security.
Edward B. McCabe, CGEIT, CISM

Mr. McCabe is an information security professional with over 18 years consulting experience with Fortune 100 companies such as Nationwide and State Farm in addition to various state and federal organizations including the U.S. Department of Defense. Mr. McCabe has presented to numerous organizations and conferences on issues such as Social Engineering, Internal IT Audit Practice Development, Enterprise Risk Management, and Adopting Information Security into the Business Corporate Culture.

Mr. McCabe currently serves as a Director on the Security MBA in Columbus, Ohio, is an active speaker and presenter on Information Security Management, Governance, and Compliance for the commercial and government sectors.

Charles Burke, CISSP, CSSLP, SCJP, SCJA, CWIP

Charles Burke is an experienced information security professional with over 19 years of success leading traditional engagements with security organizations including IBM Internet Security Systems, Home Depot and iSI. Mr. Burke has served as the Managing Principal for iSI (InfoSec Integrators Inc.) Security Practice leading a management team that has served companies such as Kellog Global IT, The Home Depot, Aviva USA, Publix, and Marriott.

For several years Mr. Burke worked in R&D for IBM Internet Security Systems developing security management applications for the security industry and Fortune 10 clients. In addition to PCI compliance engagements and security assessments, Mr. Burke's most recent work has been in the areas of Enterprise Security Architecture and Application Security working with clients to incorporate security into their existing SDLC. Mr. Burke is known for his effectiveness in developing security assessment programs for Fortune 100 clients that include high capacity infrastructure, processes, metrics, and reporting.

Mr. Burke also founded the Atlanta chapter of the Open Web Application Security Project (OWASP) and remains involved in the groups activies as a chapter lead. Mr. Burke has also created several security applications for iSI including CodeSpect for secure code reviews and PIIFinder for data discovery. Mr. Burke has received his B.S. in Computer Science with minors in Military Science and Mathematics from Georgia Southwestern State University and a M.S. in Management from Troy University.

William “Bill” Stonner III, CISSP
A seasoned security engineer, Mr. Stonner has a strong IT background that he started in while supporting OSU as a Systems Operator before being sought after by such companies as Sun Microsystems, Microsolved and Information Control Corporation.
Mr. Stonner has successfully executed penetration engagements for clients in various industries to include clients within the financial sector, public and privately held corporations, state agencies and medical institutions.

Signature Page

PROTEUS|OCM

Technical Penetration Test Service Engagement – Final Report

Agreed to by:
Wiresoft, Inc
5710 Wooster Pike, Suite 210
Cincinnati, Ohio, 45227

By _____
Authorized signature

Name (type or print):
Tom Schram
CEO
Wiresoft, Inc

Agreed to by:
PROTEUS|OCM
1360 Eisenhower Blvd, Suite 204
Johnstown, Pennsylvania 15904 United States

By /EBM//ORIGINAL SIGNED
Authorized sigature

Name (type or print):
EDWARD MCCABE
DIRECTOR, GRC SERVICES
PROTEUS|OCM LLC