

Physical Pen Testing for Fun and Profit

And An Introduction to Terremark's Secure Information Services Group

Pete Nicoletti

VP Security Engineering, Secure Information Services

B E Y O N D A V A I L A B I L I T Y



Meet your Presenter: Pete Nicoletti

- VP: Secure Information Services
- CISSP, CISA, FCSNE, CCNE
- VP FBI Infragard
- President S. Florida Information Systems Security Administrators (ISSA)
- Member: ISACA, Miami Electronic Crimes Task Force, Anti-Phishing Working Group, Computer Security Institute, Honey-net Alliance, IEEE



Steps To A Successful Pen Test

- Skill and Reputation Building
- The Lead
- The Call
- The Background Check
- The Meeting
- The Objective and the bonus

Steps To A Successful Pen Test

- The Proposal
- The Tweaks
- The Agreement
- Get out of Jail Free
- The Police
- The Plan
- Intel, Intel, Intel
- Review the plan

Steps To A Successful Pen Test

- Dry walk through
- Communications Plan
- Plan Execution
- Go/no go Points agreed on
- Look outs
- Drop off
- Tools

Steps To A Successful Pen Test

- Door Attacks
- Stealth vs evidence
- Insertion of Back door
- Insertion of KB Logger
- Muster and recap
- Task Division
- Morning Status and phase planning

Steps To A Successful Pen Test

- Removal
- Network Ownage
- Report writing
- Peer review
- Presentation and remediation Drama
- Offer next project now during max trust
- Followup
- Deletion or storage of Case Files

Steps To A Successful Pen Test

- Methodology and Resources
 - OSSTMM
 - You tube
 - Security Equipment Manufacturer Sites

Security Services

Security Issues are Driving Many Market Decisions

- Most organizations today cannot function without their information technology systems
- Information today has tangible value
 - Identity Theft
 - Virtual Bank Theft
 - Military and Intellectual Property Secrets
- New and pending legislation attempting to force organizations to secure their infrastructure and the data they possess.
- Vertical Market-specific compliance requirements (PCI, HIPAA, etc.)

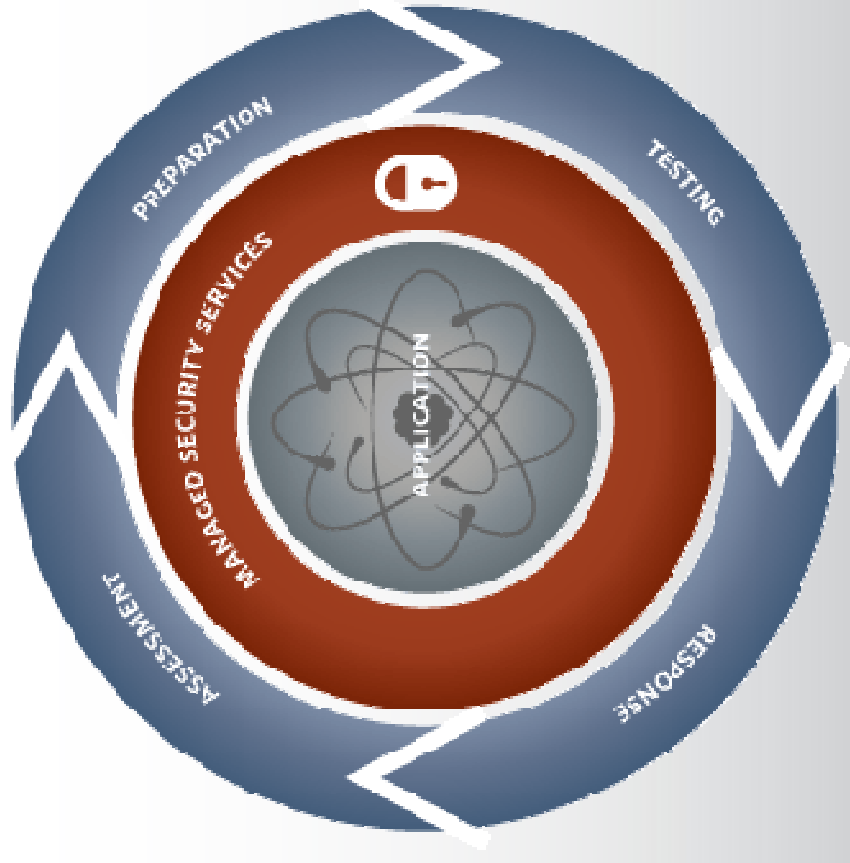
Security Services

Terremark's Secure Information Services Group

- Our purpose is to provide services to help our customers design, build, and manage secure computing environments
- We work with customers both in and outside of our facilities. In other words, we can help get in with that customer who doesn't yet need hosting or colo services!
- Very experienced and certified team

Security Services

- **Team Certifications**
 - Certified Information System Security Professional (CISSP)
 - SANS Global Information Assurance Certification (GIAC)
- **Professional Services**
 - Incident Response & Forensics
 - Incident Preparation
 - Vulnerability Assessments
 - Penetration Testing
 - Custom Security Architecture Design
- **Managed Services**
 - Managed firewalls
 - Intrusion Detection/Prevention Services
 - Log Management/Analysis
 - Anomaly Detection Services



Security Services

Incident Response and Forensics

- When an organization experiences an information system security breach, they almost always want a third party to investigate
- This is one of the fastest growing parts of our professional services business and is often the first time a customer works with Terremark
- We help the organization understand how they were compromised, how to fix the vulnerability, and assist with disclosure or other regulatory issues

Security Services

Incident Preparation

- We often find that organizations who experience a breach are missing crucial elements in the ability to respond and investigate
- Customers engage us to help harden and prepare their environments so as to be “incident ready”
- We prepare a customer by looking at their policies, procedures, system logging levels, security of those logs, and so on
- We also help organizations practice incident response by running simulated attacks and score their response

Security Services

Vulnerability and Penetration Testing Services

- Vulnerability Assessments and Penetration Tests are related but serve different purposes. Vulnerability Assessments evaluate systems, applications, and processes for known vulnerabilities using a combination of automated and manual tools and techniques
- Penetration Tests often follow a Vulnerability Assessment, attempting to use any identified vulnerabilities to compromise a system or network; essentially proof that a vulnerability can actually be used to breach an organization's security

Security Services

Custom Security Architecture Design

- Many organizations, especially small and medium enterprises, do not have dedicated security staff and need assistance to design systems that can defend against many of the emerging threats
- We help with the design and deployment of intrusion detection/prevention systems, log aggregation and security event management systems, system hardening procedures, e-commerce and banking system design and review, and wireless networks

Security Services

Managed Security Services

- Given the sophisticated nature of online threats today, we must go beyond simply offering managed firewalls and Intrusion Detection/Prevention Systems
- By gathering information from numerous sources in the environment, we can use this “data fusion” approach to identify security problems that do not show up in traditional approaches.

Security Services

Log Aggregation and Analysis

- **Aggregating and securely storing log data from disparate devices and systems providing:**
 - Regulatory Compliance by securely logging audit data from all systems across an enterprise
 - Long-term data retention and instant accessibility of archived logs
 - A mechanism for storing forensically sound log data for use in future investigations
- **Collecting security related logs from various sources to build real-time intelligence about an organization's assets through:**
 - Normalization and correlation of events across disparate devices to help minimize false positives and reduce incident response times
 - Analysis and visualization tools for identifying incidents in real-time and drilling down into packet payload data
 - Reporting and ticketing on security related information to identify potential issues worth investigating and communicating to all parties overall security incident status

Security Services

Anomaly Detection

- **Observing network activities that deviate significantly from the established normal usage indicating that something is suspicious:**
 - Predictive, learning-based technology that will identify attacks that are overlooked by normal signature-based Intrusion Detection Systems
 - Identification of static network traffic anomalies such as IP protocol and network security violations or Denial of Service attacks
 - Identification of dynamic network traffic statistics such as threshold based anomalies, service based bandwidth utilization and traffic shaper tools

Security Services- Case Study

- Fortune 1000 customer engaged us to perform a comprehensive corporate vulnerability assessment with the objective of ascertaining the vulnerability of their stored customer credit card information.
 - Ultimately, we were successful in compromising not only their stored credit card information but also fully compromising their core mainframe application and other business-critical applications.
 - This assessment allowed them to strengthen their network and systems in advance of their recent purchase by larger organization.
- Due to our success we closed a portfolio of security services valued at over \$1.2 million (3-year total contract value) consisting of managed security services (\$17,000/month), professional services, and hardware/software.
- Client has also informed us they will be putting much of their current outsourced/hosted infrastructure at another large IT infrastructure outsourcer out to bid and we are already a front runner due to our Infinistructure platform and our proven migration capabilities.

Services that can be delivered with various configurations of our 'SOC in a Box' Concept:

- Firewall Hardware and Managed Firewall Services
- Log aggregation
- Log Analysis
- Network Forensics
- Network and Host Scanning
- Application Level Scanning
- Intrusion Prevention and Managed Intrusion Prevention Services
- Content Filtering
- Malware Investigations
- Out of Band Management and Access
- NetFlow Aggregation and Analysis
- 24 hour Turnaround from request to insertion available worldwide
- 24/7/365 Intensive Security Monitoring, Forensics, Analysis Available

Security Services - 'SOC in a Box' Case Study

- A large health care provider was being blackmailed by a group of rogue employees
- During our investigation and remediation of this incident, it became apparent the customer's ability to monitor their security posture was non-existent
- We proposed deploying a set of shippable racks loaded with pre-configured security gear such as:
 - Intrusion Prevention Systems
 - Network Traffic Baselining Systems
 - Log and Event Aggregation Systems
 - Network Forensics Systems
- We stood the array up in one day and were providing them actionable data by the next morning including identifying a massive data leak (HIPAA violation waiting to happen) as well as a number of compromised systems

Thank You For Your Time!

When in Doubt:

