

Lipani Technologies LLC

SECURITY TRAINING WORKSHOP OUTLINE

2016 - 2017

Lipani Technologies LLC

**2149 Route 6
Hawley, Pa 18464
(570) 226-2301**

lipanisecurity.com

Defining Security
White Hat

1-1

Grey Hay	1-2
Black Hat	1-3
Hacker Groups	1-4
Hacktivism	1-5
Ethics	1-6
Certifications	1-7
Social Engineering	
Document Handling	2-1
Verification and Authorization Procedures	2-2
Password Handling	2-3
Phishing	2-4
Jump Drives / CD	2-5
Document Disposal	2-6
Shipping and Receiving	2-7
Corporate Directories	2-8
Malware Attack	2-9
Shoulder Surfing	2-10
Desk Checks	2-11
In-Person Attacks	2-12
Social Media	2-13
Footprinting	2-14
Scamming	2-15
Code for the Day	2-16
Authority	2-17
Establishing an Incident	2-18
Incident Response Team	2-19
Social Media	2-20
Data Collection	2-21
Physical Security	
Physical Media	3-1
Access control/intrusion/key and lock systems	3-2
Tailgating	3-3
Closed-circuit television and remote surveillance systems	3-4
Badges	3-5
Employee/Visitor security procedures and records	3-6
Alarm and fire detection systems	3-7
External service, vendor/contractor access, building maintenance procedures	3-8
Proprietary and intellectual property asset protection	3-9
Shipping and Receiving procedures	3-10
Record Storage procedures	3-11
Mantraps	3-12

Disaster Recovery

Hot Site	4-1
Warm Site	4-2
Cold Site	4-3
Backup MX	4-4
Online Backups	4-5
Off Site Backups	4-6
Onsite Backups	4-7
Network Attached Storage	4-8
Tape Backup	4-9
Storage Area Networks	4-10
Configuration and Daily Log Monitoring	4-11
Data Restoration and Testing	4-12
Disaster Recovery Plans	4-13
Disaster Recovery Testing	4-14
Disaster Recovery Simulations	4-15
Backup Switch & Firewall Configs	4-16

Employees

Disgruntled Employees	5-1
Mandatory Vacation	5-2
Background Checks	5-3
Fingerprinting	5-4
Identity Check	5-5
Credit Check	5-6
Driving Records Check	5-7
Criminal Records Check	5-8
References Check	5-9
Credentialing Check	5-10
Bonding	5-11
Security Awareness and Policy Adherence	5-12

Desktop Hardening

Check service pack levels	6-1
Check for missing security patches and install when required	6-2
Check for security alerts/vulnerabilities	6-3
Detect potential virus threats such as Trojans on servers and workstations	6-4
Updating Desktop Software	6-5
Detect unnecessary shared directories on your network	6-6
Check for unused user accounts and delete or disable	6-7
Check password policy and strength	6-8
Group Policy Evaluation	6-9

Network Assessment

Detect unnecessary open ports and protocols	7-1
Detect new security holes using scan comparisons	7-2
Make an inventory of your network	7-3
Disabling unused ports on switches	7-4
Segmenting Off Network	7-5
DMZ Configuration	7-6
Disable Modems / Network Boot	7-7
Spanning Tree Configuration	7-8
SNMP Configuration	7-9
Routing Configuration	7-10
Wireless Assessment	7-11
Intrusion Detection System	7-12
Network Monitoring	7-13
Multi-factor Authentication	7-14
VPN Solutions	7-15

Server Assessment

Certificate Assessment	8-1
Linux Servers Python / Apache	8-2
IIS Servers	8-3
Check Server Bindings	8-4
Decommission Unused Servers	8-5
Archiving Old Data	8-6
Removing Unused / Unneeded Software From Servers	8-7
Labing All Cabling and Servers	8-8
Documenting Servers Uses	8-9
Evaluating E-mail Servers	8-10
Verifying Internal and External DNS	8-11
Clearing Arp Tables	8-12
Routine Log Analyzation	8-13
IP Address and Port Databases	8-14
Spam Controls Review	8-15

Database Assessment

Database Input Validation	9-1
Cross scripting Check	9-2
XSS Check	9-3
Evaluate Patch Level and Infrastructure Setup and Design	9-4
Database Integrity Checks	9-5
Authentication Setup and Procedures	9-6
Analyzation Accounting, Financial, ERP, Customer and CRM Databases	9-9

Technology Department Procedures

Domain Registration	10-1
Change Control Procedures	10-2
Checks and Balances	10-3
Password and Documentation Storage and Access	10-4
Server Access For Techs / Engineers / Administrators / Programmers	10-5
Datacenter Access and Procedures	10-6
Air Condition / UPS / Generator Maintenance and Testing	10-6

Policies

Security Policies	11-1
Copyright Policies	11-2
Acceptable Use Policies	11-3
Password Policies	11-4
Hiring and Firing Policies	11-5
Third party service provider policies	11-6
Janitorial service, Security guard policies	11-7
Human Resources policies and procedures	11-8