Building an Information Security Program (Starting Five Resources)

Policies and Procedures

- Policy Template Resources
  - PCI Policy Portal (https://pcipolicyportal.com) ($)
  - Instant Security Policy (https://www.instantsecuritypolicy.com) ($)
  - SANS (https://www.sans.org/security-resources/policies/) (Free)
- Hardening Guide Resources
  - Center for Internet Security (https://www.cisecurity.org/cis-benchmarks/) 140+ Configuration Guidelines (Free)
  - NIST National Checklist Program (https://nvd.nist.gov/ncp/repository) (Free)

Segmentation

- PCI SSC's Guidance for PCI DSS Scoping and Segmentation (https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1_1.pdf)
- Cisco Framework to Protect Data Through Segmentation (https://www.cisco.com/c/en/us/about/security-center/framework-segmentation.html)

Remote Access

- PCI SSC's Multi-Factor Authentication Information Supplement (https://www.pcisecuritystandards.org/pdfs/Multi-Factor-Authentication-Guidance-v1.pdf)

Visibility

- Document Key Systems/Applications (Sample Table)

Name	Hostname	IP	Key Apps/Data	OS	Type	Location	Security Overlays
IVR Server	IVR.ACME.COOP	10.10.10.20	IVR	SUSE 11	Virtual	VLAN 43	AV, SYSLOG, MW
File Server	F.ACME.COOP	10.10.10.21	CC Data, HR	Server 2016	Physical	VLAN 44	SYSLOG

- Document Security Overlays (Logging) (Sample Table)

Name	Hostname	IP	Domain	Location	Log Retention	Alerts	Description
FirewallX	FORT.ACME.COOP	10.10.10.1	Perimeter Ctrl	Edge	Unknown	Unknown	Perimeter Firewall
AntiVirusY	SIEM.ACME.COOP	10.10.10.30	Anti-Virus	VLAN 43	90 Days	No	Central AV Log Server

- Examples of Key Events to Log CIS 7.1 Controls
  - 4.8 Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.
  - 4.9 Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.
  - 7.9 Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.

- 8.6 Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.
- 8.7 Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.
- 8.8 Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.

- Examples of Key Events to Log PCI DSS 3.2.1 Controls
  - 10.2.2 Verify all actions taken by any individual with root or administrative privileges are logged
  - 10.2.3 Verify access to all audit trails is logged
  - 10.2.4 Verify invalid logical access attempts are logged
  - 10.2.5.c Verify all changes, additions, or deletions to any account with root or administrative privileges are logged.
  - 10.2.7 Verify creation and deletion of system level objects are logged.
- Logging Basics
  - Record at least the following for each log:
    - User Identification
    - Type of Event
    - Date and Time
    - Success or Failure Indication
    - Source of Event
    - Identity of Affected Data, System Component or Resource
  - Using time-synchronization technology, synchronize all critical system clocks and times.

Routine Audits

- Example CIS 7.1 Controls (https://www.cisecurity.org/cybersecurity-best-practices/)
  - 3.1 Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.
  - 6.7 On a regular basis, review logs to identify anomalies or abnormal events.
  - 19.7 Plan and conduct routine incident response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real-world threats.
  - 20.3 Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.

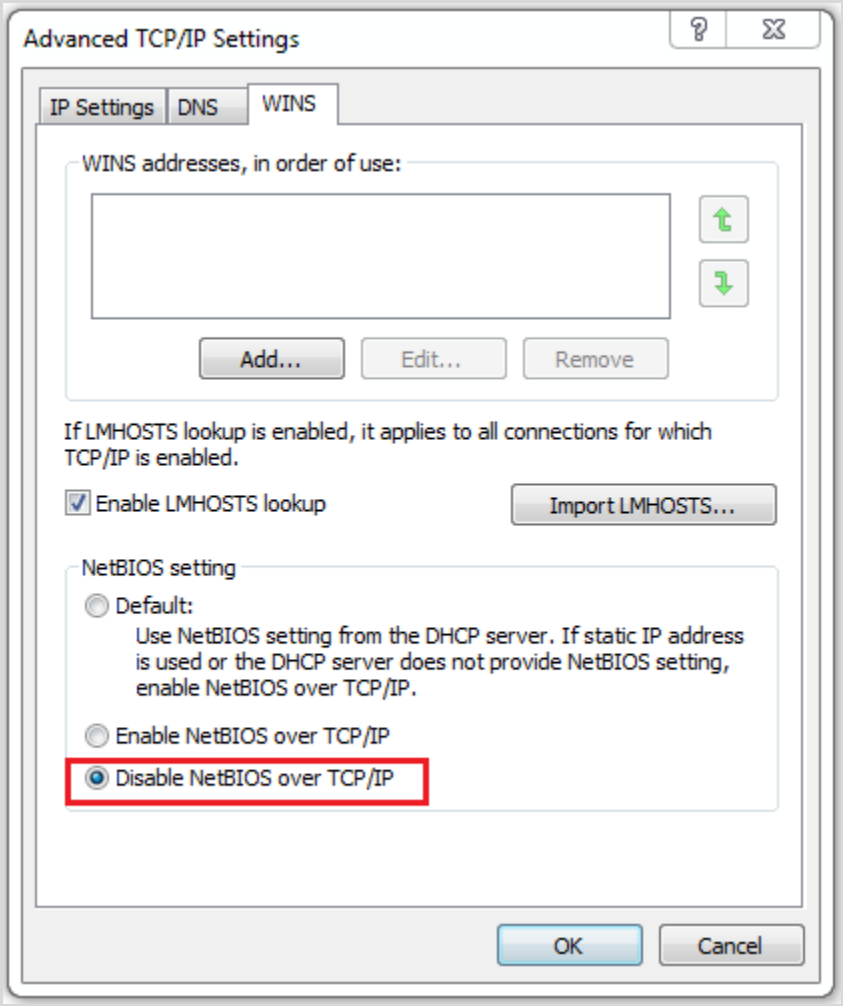
- Example PCI DSS 3.2.1 Controls (https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf)
  - 1.1.7: Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.

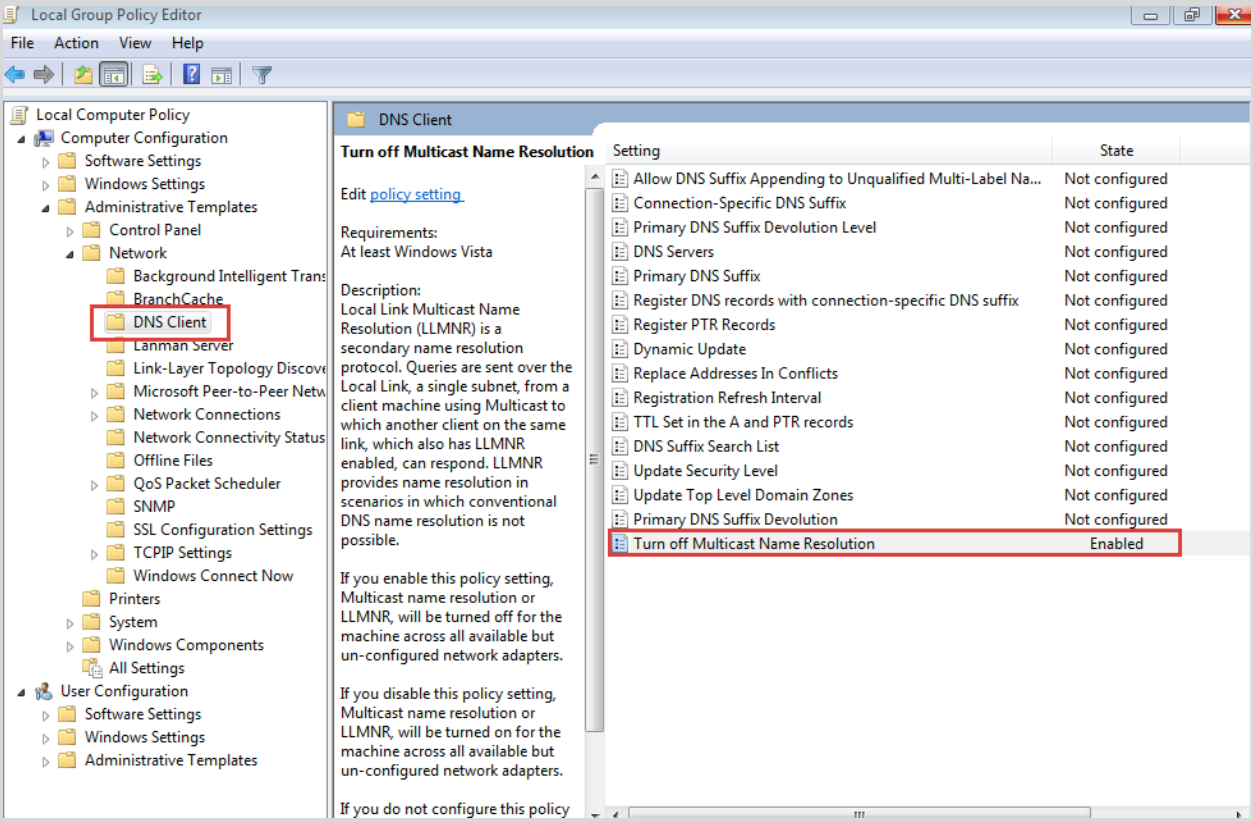
- 11.1.c Execute wireless scans at least quarterly for all system components and facilities (if wireless scanning is used to detect and test for unauthorized/authorized wireless).
- 11.2.1 Perform quarterly internal vulnerability scans.
- 11.2.2 Perform quarterly external vulnerability scans.
- 11.3.1 Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).
- 11.3.2 Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

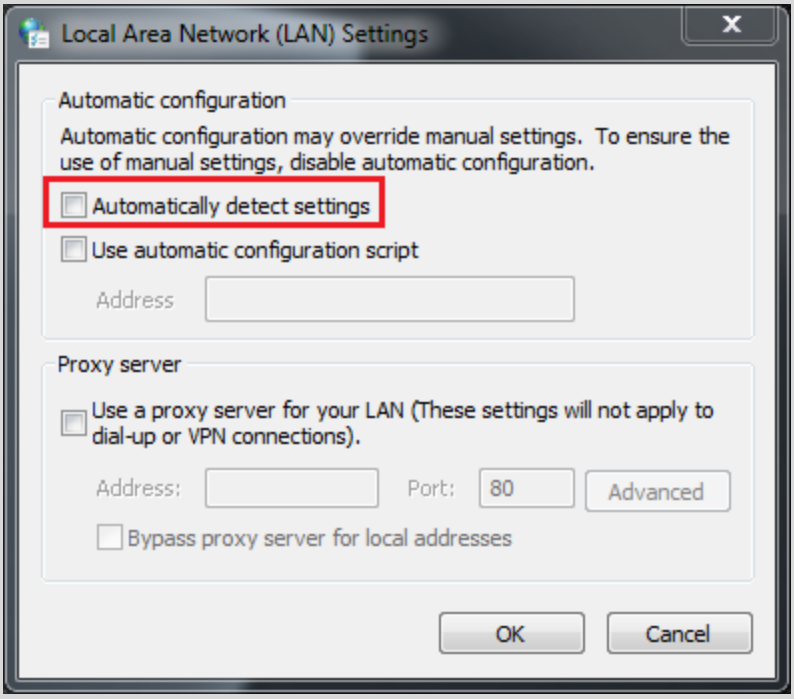
Tools Featured in the Presentation

- USB Rubber Ducky Running Custom Code (Policy and Procedures Demo)
  - Used to show how a USB mimicking a HID keyboard can be used in an attack to harvest system information and email to an external recipient.
  - https://shop.hak5.org/collections/physical-access/products/usb-rubber-ducky-deluxe
- HCXTOOLS, WIFITE2 Tools (Segmentation Demo)
  - Pairwise Master Key Attack (PMKID) demonstrated using the following tools:
    - HCXTOOLS – Set of tools to convert packets from captures for use within John the Ripper. https://github.com/ZerBea/hcxtools
    - WIFEFITE2 – Python script for auditing wireless networks. https://github.com/derv82/wifite2
- Social-Engineer Toolkit (SET) (Remote Access Demo)
  - Used to clone a sample login page
  - https://github.com/trustedsec/social-engineer-toolkit
- Canary Tokens (Visibility Demo)
  - Used to add code to a sensitive document that beaconed back when opened (honeypot, tripwire)
  - https://thinkst.com/products.html, https://blog.thinkst.com/p/canarytokensorg-quick-free-detection.html
- Have I Been Pwned (Routine Audits Demo)
  - Used to identify accounts involved in a breach/paste
  - https://haveibeenpwned.com

Concerning the poisoning settings that need to be changed, you will need to turn off LLMNR, which can be accomplished through GPO, disable NetBIOS over TCP/IP, and Microsoft WPAD. See the attached images below. NetBIOS can be disabled by clicking your Network card > Properties > IPv4 > Advanced > WINS and then under "NetBIOS setting" select Disable NetBIOS over TCP/IP. WPAD disable is located in your LAN settings general. Please let me know if you have any questions!




Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Network
Background Intelligent Trans
BranchCache
DNS Client
Lanman Server
Link-Layer Topology Discove
Microsoft Peer-to-Peer Netw
Network Connections
Network Connectivity Status
Offline Files
QoS Packet Scheduler
SNMP
SSL Configuration Settings
TCPIP Settings
Windows Connect Now
Printers
System
Windows Components
All Settings
User Configuration
Software Settings
Windows Settings
Administrative Templates
DNS Client
Turn off Multicast Name Resolution
Edit policy setting
Requirements:
At least Windows Vista
Description:
Local Link Multicast Name Resolution (LLMNR) is a secondary name resolution protocol. Queries are sent over the Local Link, a single subnet, from a client machine using Multicast to which another client on the same link, which also has LLMNR enabled, can respond. LLMNR provides name resolution in scenarios in which conventional DNS name resolution is not possible.
If you enable this policy setting, Multicast name resolution or LLMNR, will be turned off for the machine across all available but un-configured network adapters.
If you disable this policy setting, Multicast name resolution or LLMNR, will be turned on for the machine across all available but un-configured network adapters.
If you do not configure this policy
Setting
State
Allow DNS Suffix Appending to Unqualified Multi-Label Na... Not configured
Connection-Specific DNS Suffix Not configured
Primary DNS Suffix Devolution Level Not configured
DNS Servers Not configured
Primary DNS Suffix Not configured
Register DNS records with connection-specific DNS suffix Not configured
Register PTR Records Not configured
Dynamic Update Not configured
Replace Addresses In Conflicts Not configured
Registration Refresh Interval Not configured
TTL Set in the A and PTR records Not configured
DNS Suffix Search List Not configured
Update Security Level Not configured
Update Top Level Domain Zones Not configured
Primary DNS Suffix Devolution Not configured
Turn off Multicast Name Resolution Enabled


Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address:
Port: 80
Advanced
Bypass proxy server for local addresses
OK
Cancel

WE WANT TO BE YOUR TRUSTED SECURITY PARTNER

ContextualSecurity

Kevin Thomas
QSA CISSP CISA CRISC GWAPT GCFA
Co-Founder and Principal Consultant
Contextual Security Solutions
e: kevin.thomas@contextsec.com
p: 844.526.6732 x 701
m: 865.898.1362
w: http://contextualsecurity.com

Slade Griffin
Director of Security Assessments
Contextual Security Solutions
e: Slade.Griffin@contextsec.com
p: 844.526.6732 x703
m: 865.360.7699
w: http://contextualsecurity.com