NAVFAC FRCS A&A ACAS Scan Policy Settings List v1.2

Based on ACAS Best Practices Guide v5.3.1.1

**Policy settings must be configured in Tenable.sc or Nessus,
depending from where the scan is initiated.**

**These scan policy settings are intended to be used for NAVFAC FRCS A&A purposes only.
Follow local guidance for routine vulnerability scans.**

NAVFAC FRCS A&A ACAS Scan Policy Settings v1.2

Highlighed settings are deviations from DISA's Default Policy

Advanced Tab		Required Setting	Acceptable Deviation	Notes
General Settings	Enable safe checks	enabled		
	Stop scanning hosts that become unresponsive during the scan	enabled		
Performance Options	Slow down the scan when network congestion is detected	enabled		
	Use Linux kernel congestion detection	enabled		
	Network timeout (in seconds)	5	<60	
	Max simultaneous checks per host	5	<8	
	Max simultaneous hosts per scan	30	<60	
	Max number of concurrent TCP sessions per host	-		
	Max number of concurrent TCP sessions per scan	-		
Unix find command exclusions	Custom filepath	-		
	Custom filesystem	-		
Host Discovery Tab		**Required Setting**	**Acceptable Deviation**	**Notes**
	Ping the remote host	enabled		
General Settings	Test the local Nessus host	enabled		
	Use fast network discovery	enabled		
Ping Methods	ARP	disabled		
	TCP	enabled		
	Destination ports	21,22,23,25,53,80,111,123,135,139,443,445		
	ICMP	enabled		
	Assume ICMP unreachable from the gateway means the host is down	disabled		
	Maximum number of retries	2		
	UDP	disabled		
Fragile Devices	Scan Network Printers	enabled	disabled	Navy SCA requirement for A&A packages; deviation requires SAP update and FSCA approval.
	Scan Novell Netware hosts	enabled	disabled	
	Scan Operational Technology devices	enabled	disabled	
Wake-on-LAN	List of MAC addresses	-	site defined	
	Boot time wait (in minutes)	5	site defined	
Network Type	Network Type	Mixed		
Port Scanning Tab		**Required Setting**	**Acceptable Deviation**	**Notes**
Ports	Consider unscanned ports as closed	disabled		
	Port scan range:	all	0-65535	Navy SCA requirement for A&A packages.
Local Port Enumerators	SSH (netstat)	enabled		
	WMI (netstat)	enabled		
	SNMP	enabled		
	Only run network port scanners if local port enumeration failed	enabled		
	Verify open TCP ports found by local port enumerators	disabled		
Network Port Scanners	TCP	disabled	enabled	
	SYN	enabled		
	Override automatic firewall detection	Automatic (normal)		
	UDP	disabled	enabled	
Service Discovery Tab		**Required Setting**	**Acceptable Deviation**	**Notes**
General Settings	Probe all ports to find services	enabled		
	Search for SSL/TLS services	enabled		
	Search for SSL/TLS on	Known SSL ports		
	Identify certificates expiring within x days	60		
	Enumerate all SSL/TLS ciphers	enabled		
	Enable CRL checking (connects to the Internet)	disabled		
Assessment Tab		**Required Setting**	**Acceptable Deviation**	**Notes**
Accuracy	Override normal accuracy	Normal		
	Perform thorough tests	disabled		
Antivirus	Antivirus definition grace period (in days):	6		This is to stay consistent with STIG requirements.
SMTP	Third party domain	example.mil	site defined	
	From address	nobody@example.mi	site defined	
	To address	postmaster@[AUTO_REPLACED_IP]	site defined	
Brute Force Tab		**Required Setting**	**Acceptable Deviation**	**Notes**
General Settings	Only use credentials provided by the user	enabled		
Oracle Database	Test default accounts (slow)	disabled		

Hydra	Always enable Hydra (slow)	disabled		
	Logins file	-		
	Passwords file	-		
	Number of parallel tasks	16		
	Timeout (in seconds)	30		
	Try empty passwords	disabled		
	Try login as password	disabled		
	Stop brute forcing after the first success	disabled		
	Add accounts found by other plugins to the login file	disabled		
	PostgreSQL database name	-		
	SAP R3 Client ID (0 - 99)	-		
	Windows accounts to test	Local accounts		
	Interpret passwords as NTLM hashes	disabled		
	Cisco login password	-		
	Web page to brute force	-		
	HTTP proxy test website	-		
	LDAP DN	-		
Malware Tab		**Required Setting**	**Acceptable Deviation**	**Notes**
General Settings	Malware Scan	disabled		
General Settings	Disable DNS resolution	-		
Hash and Whitelist Files	Provide your own list of known bad MD5 hashes:	-		
	Provide your own list of known good MD5 hashes:	-		
	Hosts file whitelist	-		
File System Scanning	Scan file system	-		
Directories	Scan %Systemroot%	-		
	Scan %ProgramFiles%	-		
	Scan %ProgramFiles(x86)%	-		
	Scan %ProgramData%	-		
	Scan User Profiles	-		
	Custom Filescan Directories	-		
	Yara Rules Files	-		
SCADA Tab		**Required Setting**	**Acceptable Deviation**	**Notes**
Modbus/TCP Coil Access	Start at register	0		Tenable default settings.
	End at register	16		
ICCP/COTP TSAP Addressing Weakness	Start COTP TSAP	8		
	Stop COTP TSAP	8		
Web Application Tab		**Required Setting**	**Acceptable Deviation**	**Notes**
Web Application Settings	Scan web applications	disabled		
Windows Tab		**Required Setting**	**Acceptable Deviation**	**Notes**
General Settings	Request information about the SMB Domain	disabled		
User Enumeration Method	SAM Registry	enabled		
	ADSI Query	enabled		
	WMI Query	enabled		
	RID Brute Forcing	disabled		
Report Tab		**Required Setting**	**Acceptable Deviation**	**Notes**
Processing	Override normal verbosity	Normal		
	Show missing patches that have been superseded	enabled		
	Hide results from plugins initiated as a dependency	enabled		
Output	Designate hosts by their DNS name	disabled		
	Display hosts that respond to ping	enabled		
	Display unreachable hosts	disabled		
	Generate SCAP XML Results	disabled		
Authentication Tab		**Required Setting**	**Acceptable Deviation**	**Notes**
Authentication	Add Authentication Settings	-		
SNMP	UDP port	161		
	Additional UDP port #1	162		
	Additional UDP port #2	199		
	Additional UDP port #3	161		
SSH	known_hosts file	-	site defined	
	Preferred port	22	site defined	
	Client version	OpenSSH_5.0		
	Attempt least privilege	disabled		

Windows	Never send credentials in the clear	enabled		
	Do not use NTLMv1 authentication	enabled		
	Start the Remote Registry service during the scan	enabled		
	Enable administrative shares during the scan	enabled		
Plaintext Authentication	Perform patch audits over telnet	disabled		
	Perform patch audits over rsh	disabled		
	Perform patch audits over rexec	disabled		
HTTP	Login method	POST		
	Re-authenticate delay (seconds)	0		
	Follow 30x redirections (# of levels)	0		
	Invert authenticated regex	disabled		
	Use authenticated regex on HTTP headers	disabled		
	Case insensitive authenticated regex	disabled		
Compliance Tab		**Required Setting**	**Acceptable Deviation**	**Notes**
Compliance	Add Audit File	-		
Plugins Tab		**Required Setting**	**Acceptable Deviation**	**Notes**
Plugins	AIX Local Security Checks	enabled		
	Amazon Linux Local Security Checks	enabled		
	Backdoors	enabled		
	Brute force attacks	enabled		
	CentOS Local Security Checks	enabled		
	CGI abuses	enabled		
	CGI abuses : XSS	enabled		
	CISCO	enabled		
	Databases	enabled		
	Debian Local Security Checks	enabled		
	Default Unix Accounts	enabled		
	Denial of Service	enabled	disabled	Deviation requires SAP update and FSCA approval.
	DNS	enabled		
	F5 Networks Local Security Checks	enabled		
	Fedora Local Security Checks	enabled		
	Firewalls	enabled		
	FreeBSD Local Security Checks	enabled		
	FTP	enabled		
	Gain a shell remotely	enabled		
	General	enabled		
	Gentoo Local Security Checks	enabled		
	HP-UX Local Security Checks	enabled		
	Huawei Local Security Checks	enabled		
	Junos Local Security Checks	enabled		
	MacOS X Local Security Checks	enabled		
	Mandriva Local Security Checks	enabled		
	Misc.	enabled		
	Mobile Devices	enabled		
	Netware	enabled		
	NewStart CGSL Local Security Checks	enabled		
	Oracle Linux Local Security Checks	enabled		
	OracleVM Local Security Checks	enabled		
	Palo Alto Local Security Checks	enabled		
	Peer-To-Peer File Sharing	enabled		
	PhotonOS Local Security Checks	enabled		
	Policy Compliance	disabled	enabled	Not used for Navy A&A purposes.
	Red Hat Local Security Checks	enabled		
	RPC	enabled		
	SCADA	enabled		
	Scientific Linux Local Security Checks	enabled		
	Service detection	enabled		
	Settings	enabled		
	Slackware Local Security Checks	enabled		
	SMTP problems	enabled		
	SNMP	enabled		
	Solaris Local Security Checks	enabled		
	SuSE Local Security Checks	enabled		
	Ubuntu Local Security Checks	enabled		
	Virtuozzo Local	enabled		
	VMware ESX Local Security Checks	enabled		
	Web Servers	enabled		
	Windows	enabled		
	Windows : Microsoft Bulletins	enabled		
	Windows : User management	enabled		
	Plugin Families Not Listed Above	enabled		