MINISTRY OF SECURITY

Network Security Checklist

MINISTRY OF SECURITY

Firewalls

SLNo	Guidance	Compliance
1	Update the router to the latest firmware version.	
2	Enable stateful packet inspection (SPI).	
3	Disable ping (ICMP) response on WAN port.	
4	Disable UPnP (universal plug-and-play).	
5	Disable IDENT (port 113).	
6	Disable remote management of the router.	
7	Change the default administrator password.	
8	The settings for a firewall policy should be as specific as possible. Do not use 0.0.0.0 as an address.	
9	Check for incoming/outgoing traffic security policy	
10	Check for firewall firmware / OS updates	
11	Allow only HTTPS access to the GUI and SSH access to the CLI	
12	Re-direct HTTP GUI logins to HTTPS	
13	Change the HTTPS and SSH admin access ports to non-standard ports	
14	Restrict logins from trusted hosts	
15	Set up two-factor authentication for administrators	
16	Create multiple administrator accounts	
17	Modify administrator account lockout duration and threshold values	
18	Check if all management access from the Internet is turned off, if it does not have a clear business need. At most, HTTPS and PING should	

	be enabled.	
19	Ensure that your SNMP settings are using SNMPv3 with encryption and configure your UTM profiles	
20	All firewall policies should be reviewed every 3 months to verify the business purpose	

Routers

SLNo	Guidance	Compliance
1	Do not use Default password for your router	
2	Check if the router block access to a modem by IP address	
3	Ensure that router admin gets an alert when a new device joins the network	
4	Most routers let you disable UPnP on the LAN side	
5	Enable port forwarding and IP filtering for your router	
LOCAL ADMINISTRATION		
6	Check if the router supports HTTPs, in some routers it is disabled by default	
7	If HTTPS is supported, can admin access be limited exclusively to HTTPS?	
8	Check if the TCP/IP port used for the web interface can be changed	
9	To really prevent local admin access, limit the LAN IP address to a single IP address that is both outside the DHCP range and not normally assigned.	
10	Check if the admin access can be limited to Ethernet only	
11	Check if the router access can be restricted by SSID and/or by VLAN	
12	The router should not allow multiple computers to logon at the same	

	time using the same userid	
13	Check if there is some type of lockout after too many failed attempts to login to the web interface	
REMOTE ADMINISTRATION		
14	Make sure the remote administration settings are turned off by default	
15	Check if the port number can be changed remotely	
16	If you forget to logout from the router, eventually your session should time out, and, you should be able to set the time limit, the shorter, the more secure	
ROUTER FIREWALL		
17	**Inbound WAN:** What ports are open on the WAN/Internet side? The most secure answer is none and you should expect any router not provided by an ISP to have no open ports on the Internet side. One exception is old school Remote Administration, which requires an open port. Every open port on the WAN side needs to be accounted for, especially if the router was provided by an ISP; they often leave themselves a back door. The Test your Router page links to many websites that offer firewall tests. That said, none of them will scan all 65,535 TCP ports or all 65,535 UDP ports. The best time to test this is before placing a new router into service.	
18	**Inbound LAN:** What ports are open on the LAN side? Expect port 53 to be open for DNS (probably UDP, maybe TCP). If the router has a web interface, then that requires an open port. The classic/standard utility for testing the LAN side firewall is nmap. As with the WAN side, every port that is open needs to be accounted for.	
19	**Outbound:** Can the router create outgoing firewall rules? There are	

	all sorts of attacks that can be blocked with outgoing firewall rules. Generally, consumer routers do not offer outbound firewall rules while business class routers do. In addition to blocking, it would be nice if the blocks were logged for auditing purposes. Note however, that devices connected to Tor or a VPN will not obey the outbound firewall rules.	

Switches

SLNo	Guidance	Compliance
1	Check if the latest firmware is used.	
2	Check the switch's user guide's for security features and see if the required ones have been implemented properly.	
3	Create an Enable Secret Password Encrypt Passwords on the device	
4	Use an external AAA server for User Authentication	
5	Create separate local accounts for User Authentication Configure Maximum Failed Authentication Attempts	
6	Restrict Management Access to the devices to specific IPs only	
7	Enable Logging for monitoring, incident response and auditing. You can enable logging to an internal buffer of the device or to an external Log server.	
8	Enable Network Time Protocol (NTP) - You must have accurate and uniform clock settings on all network devices in order for log data to be stamped with the correct time and timezone.This will help tremendously in incident handling and proper log monitoring and correlation.	
9	Use Secure Management Protocols if possible	

10	Restrict and Secure SNMP Access	

Linux Servers

SLNo	Guidance	Compliance
1	Update your package list and upgrade your OS	
2	Remove unnecessary packages	
3	Detect weak passwords with John the Ripper	
4	Verify no accounts have empty passwords	
5	Set password rules	
6	Set password expiration in login.defs	
7	Disable USB devices (for headless servers)	
8	Check which services are started at boot time	
9	Detect all world-writable files	
10	Configure iptables to block common attacks	
11	Set GRUB boot loader password	
12	Disable interactive hotkey startup at boot	
13	Enable audited to check for read/write events	
14	Secure any Apache servers	
15	Install and configure UFW	
16	Configure SSH securely	
17	Disable telnet	
18	Configure sysctl securely	
19	Lock user accounts after failed attempts with Fail2Ban	
20	Configure root user timeout	
21	Check for hidden open ports with netstat	

22	Set root permissions for core system files	
23	Scan for rootkits	
24	Check that shut down mode is enabled for sensitive event log alerts	
25	Check that all event log data is being securely backed up	
26	Evaluate event log monitoring process	
27	Keep watch for any users logging on under suspicious circumstances	
28	Check remote access logs regularly	
29	In case of remote access activity: Make sure that the suspicious activity is flagged and documented	
30	Make sure that the Suspected account privileges temporarily frozen	
31	Evaluate server configuration control process	
32	Update service packs and patches for software	
33	Check event log monitoring is properly configured:	
34	Check that all user account logins are being recorded	
35	Check that all system configuration changes are being recorded	
36	Make sure that there is a process in place for changing system configurations	
37	Ensure start-up processes are configured correctly	
38	Remove unnecessary startup processes	
39	Ensure regular users cannot change system startup configuration	
40	Remove unused software and services	
41	Run a full system anti-virus scan	
42	Review your server firewall security settings and make sure everything is properly configured	
43	Disable or remove all user accounts that haven't been active in the last 3 months	

44	Make sure that membership to both the admin and superadmin group is restricted to as few users as possible without causing any problems	

Windows Servers

SLNo	Guidance	Compliance
1	Install the latest service packs and hotfixes from Microsoft.	
2	Enable automatic notification of patch availability.	
3	Set minimum password length.	
4	Enable password complexity requirements.	
5	Do not store passwords using reversible encryption. (Default)	
6	Configure account lockout policy.	
7	Restrict the ability to access this computer from the network to Administrators and Authenticated Users.	
8	Do not grant any users the 'act as part of the operating system' right. (Default)	
9	Restrict local logon access to Administrators.	
10	Deny guest accounts the ability to logon as a service, batch job, locally or via RDP	
11	Place the warning banner in the Message Text for users attempting to log on.	
12	Disallow users from creating and logging in with Microsoft accounts.	
13	Disable the guest account. (Default)	
14	Require Ctrl+Alt+Del for interactive logins. (Default)	
15	Configure machine inactivity limit to protect idle interactive sessions.	

16	Configure Microsoft Network Client to always digitally sign communications.	
17	Configure Microsoft Network Client to digitally sign communications if server agrees. (Default)	
18	Disable the sending of unencrypted passwords to third party SMB servers.	
19	Configure Microsoft Network Server to always digitally sign communications.	
20	Configure Microsoft Network Server to digitally sign communications if client agrees.	
21	Disable anonymous SID/Name translation. (Default)	
22	Do not allow anonymous enumeration of SAM accounts. (Default)	
23	Do not allow anonymous enumeration of SAM accounts and shares.	
24	Do not allow everyone permissions to apply to anonymous users. (Default)	
25	Do not allow any named pipes to be accessed anonymously.	
26	Restrict anonymous access to named pipes and shares. (Default)	
27	Do not allow any shares to be accessed anonymously.	
28	Require the "Classic" sharing and security model for local accounts. (Default)	
29	Allow Local System to use computer identity for NTLM.	
30	Disable Local System NULL session fallback.	
31	Configure allowable encryption types for Kerberos.	
32	Do not store LAN Manager hash values.	
33	Set LAN Manager authentication level to only allow NTLMv2 and refuse LM and NTLM.	

34	Enable the Windows Firewall in all profiles (domain, private, public). (Default)	
35	Configure the Windows Firewall in all profiles to block inbound traffic by default. (Default)	
36	Configure Windows Firewall to restrict remote access services (VNC, RDP, etc.) to authorized organisation-only networks .	
37	Configure Windows Firewall to restrict remote access services (VNC, RDP, etc.) to the organization VPN.	
38	Digitally encrypt or sign secure channel data (always). (Default)	
39	Configure machine inactivity limit to protect idle interactive sessions.	
40	Require strong (Windows 2000 or later) session keys.	
41	Configure the number of previous logons to cache.	
42	Configure Account Logon audit policy.	
43	Configure Account Management audit policy.	
44	Configure Logon/Logoff audit policy.	
	Configure Policy Change audit policy & Privilege Use audit policy.	
39	Configure Event Log retention method and size.	
40	Configure log shipping (e.g. to Splunk).	
41	Disable or uninstall unused services.	
42	Configure user rights to be as secure as possible: Follow the Principle of Least Privilege	
43	Ensure all volumes are using the NTFS file system.	
44	Configure file system as well as registry permissions.	
39	Disallow remote registry access if not required.	
40	Set the system date/time and configure it to synchronize against Organization time servers.	
41	Install and enable anti-spyware and antivirus software.	

42	Configure anti-virus software to update daily.	
43	Configure anti-spyware software to update daily.	
44	Provide secure storage for Confidential (category-I) Data as required. Security can be provided by means such as, but not limited to, encryption, access controls, file system audits, physically securing the storage media, or any combination thereof as deemed appropriate.	
39	Install software to check the integrity of critical operating system files.	
40	If RDP is utilized, set RDP connection encryption level to high.	

Reference: SANS & NIST & CIS Benchmarks

MINISTRY OF SECURITY

Did you like our checklist ?

We have many more to offer !

Follow us on