Security Best Practice

Presented by

Muhibbul Muktadir Tanim
mmtanim@gmail.com

✓Hardening Practice

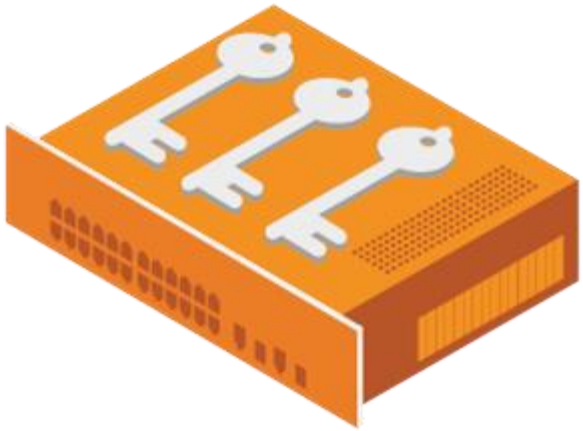
for

Server | **Unix / Linux** | **Windows** | **Storage**

✓Cyber Awareness & take away

✓Management Checklist

Hardening Server



✓ Architecture should be Separate zone

✓ Should have N+1 node level redundancy

✓ Individual node redundancy in: physical RAM, HDD, NIC etc.

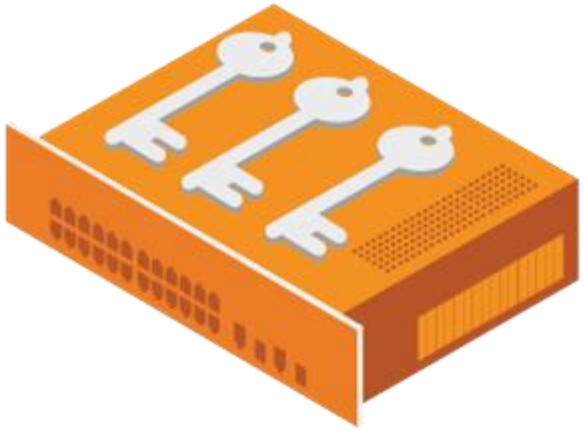
✓ Power supply units, HDDs, removable media devices should be Hot swappable.

✓ Each node must have at least one non built-in NIC. Even number of NICs in all nodes required.

✓ Server rack with redundant PDUs and redundant Power connectors.

✓ All the nodes should have their firmware (BIOS, Management Port, Storage Controllers, Switch Controllers) upgraded.

Hardening Server (cont..)



- ✓ Hardware should be within EOL (End of Life)
- ✓ Hardware or server must be mounted on rack properly.
- ✓ Sever Rack grounding must be done properly.
- ✓ The Racks should be stabilized before power cables are connected.
- ✓ Proper cable managing and tagging for serviceability must be done.
- ✓ All the nodes should be accessible via management ports.
- ✓ Rack system’s doors should be possible to lock.

Hardening Storage

✓ The storage system must have redundant controllers.

✓ Controllers must have web based secure interface.

✓ The firmware Upgrade should be possible without downtime.

✓ Hot plug expansion and replacement of redundant controllers, fans, power supplies, and I/O modules for simple, fast installation and maintenance is required.

✓ Each controller with minimum 2 GB cache. Cache memory battery should stable.

✓ The cache memory should have protection with backup.

✓ Redundant san switches have same configuration.

Hardening Storage

- ✓ The storage system must support standard RAID systems.
- ✓ The storage must support SNMP monitoring.
- ✓ Must be within HLD / LLD.
- ✓ San switch & storage will be connected with separate power source.
- ✓ Storage, san switch management IP will be in different IP block.
- ✓ Storage system must have successful cache dumping capability in case of power failure.
- ✓ Storage system must have at least 2 hot spare disc.

Hardening OS [Unix / Linux]

✓ User Accounts without password should not exist.

✓ Inactive User accounts (i.e. uucp, smtp, listen, nobody, ftp) should be deleted.

✓ Direct root-login shell should be only allowed from the system consol.

✓ Root login should only allowed from an authenticated user account with proper logging records.

✓ Auto logout after 5 min if not attended or inactive.

✓ Must comply Password Policy

Hardening OS [Unix / Linux] cont..

✓ Minimize Packages to Minimize Vulnerability

✓ Disable unnecessary network services

✓ Always keep system updated with latest releases patches, security fixes and kernel when it's available.

✓ To lock a user using cron, simply add user names in cron.deny and to allow a user to run cron add in cron.allow file. If you would like to disable all users from using cron, add the 'ALL' line to cron.deny file.

✓ Disable USB stick to Detect. Create a file '/etc/modprobe.d/no-usb' and adding below line will not detect USB storage.

✓ Disable Ctrl+Alt+Delete in Inittab

Hardening OS [Unix / Linux] cont..

✓ Monitor User activities with ‘psacct’ and ‘acct’ command.

✓ Ignore icmp or broadcast request

✓ Configure Iptables and TCPWrappers for Unix

✓ Delete X Windows

✓ Hardening Kernel configuration parameters i.e /etc/sysctl.conf

✓ Separate disk partitions should be practiced

✓ Identify world writable files (+w) and unnecessary SUID , SGID binaries that can be ignored

Hardening OS [Windows]

✓ HDD RAID

✓ Minimum 50GB for OS Drive

✓ Application is recommended to be installed other than system drive, but if any specific requirement arises then it can be installed on Operating System drive.

✓ Database is recommended to be installed other than the Operating System drive.

✓ Server should be joined to the domain. This will ensure the server manageability and maintain server corporate baseline standards.

✓ Server has to be updated with latest Service Packs and Patches before going to the production environment.

Hardening OS [Windows]

✓Local Guest account should be disabled

✓Local Administrator account name should be renamed

✓Server Firewall has to be turned on and only necessary ports will be opened for Home and Public Network. Firewall may be turned off for the Domain network based on the requirement.

✓Server default Terminal Service will be enabled which enables two concurrent remote sessions to the server.

✓Server Telnet Service will be disabled by default.

✓Last logged on Username will not be shown during the user log on.
✓Interactive logon: Message text for users attempting to logon
✓Interactive logon: Message title for users attempting to log on

Hardening OS [Windows]

✓Approved Windows Patch Management policy has to be followed to maintain the consistency and integrity of the server operation in future.

✓ Server must be installed with Antivirus solution.

✓Server built in Local Administrator account will be retained and handed over proper Administration team.

Cyber Awareness

What is Cyber Security

cybersecurity = security of cyberspace

What is Cyber Security

cybersecurity = security of cyberspace

information systems and networks

What is Cyber Security

cybersecurity = security of information systems and networks

What is Cyber Security

cybersecurity = security of information systems and networks

+ with the goal of protecting operations and assets

What is Cyber Security

cybersecurity = security of information systems and networks with the goal of protecting operations and assets

What is Cyber Security

cybersecurity = security of information systems and networks with the goal of protecting operations and assets

security in the face of attacks, accidents and failures

What is Cyber Security

cybersecurity = security of information systems and networks in the face of attacks, accidents and failures with the goal of protecting operations and assets

What is Cyber Security

cybersecurity = security of information systems and networks in the face of attacks, accidents and failures with the goal of protecting operations and assets

availability, integrity and Confidentiality

What is Cyber Security

cybersecurity = availability, integrity and Confidentiality of information systems and networks in the face of attacks, accidents and failures with the goal of protecting operations and assets

(Still a work in progress.)

What is Cyber Crime

- **Cybercrime**, is any **crime** that involves a **computer** and a network. The **computer** may have been used in the commission of a **crime**, or it may be the target

- The former descriptions were "**computer crime**", "**computer-related crime**" or "**crime by computer**". With the pervasion of digital technology, some new terms like "high-technology" or "information-age" crime were added to the definition. Also, Internet brought other new terms, like "cybercrime" and "net" crime.

Cyber Crime includes

- Illegal Access
- Illegal Interception
- System Interference
- Data Interference
- Misuse of devices
- Fraud

TIPS

- ✓ **Is That App Giving Away Your Privacy?**
- ✓ **Have A Backup Plan**
- ✓ **Configure Your Computer Securely**
- ✓ **Keep Software and Operating Systems Updated**
- ✓ **Use Strong Passwords**
- ✓ **Be Cautious About Links and Attachments**
- ✓ **Protect Your Personal Information**
- ✓ **Review Your Financial Statements Regularly**

Management Checklist

Update antivirus software. Automate updates if possible	Daily
Update spyware software	Daily
Update operating system and software	On a regular schedule, as patches are released.
Back up files	Daily
Perform incremental back ups	Daily
Perform full back up	Weekly
Conduct security review	Anually
Establish and review inventory (hardware / software)	Anually/As acquired
Change staff access control	As needed and when job function changes
Draft non-disclosure agreements	Start of agreements
Review policies	Annually
Revise policies	As needed
Notify users of alerts / advisories	Daily or as needed
Vulnerability Testing / Penetration Testing	Annually
Risk Assessment	Annually

THANK YOU