Cisco Layer 2 & Layer 3 Security Hardening Checklist

نسخه اجرایی برای پروژه‌های عملیاتی

- Backupاز Running Configuration
- Backupاز Startup Configuration
- ثبت نسخهIOS
- ثبت مدل تجهیزات
- ثبتIP Management
- ثبت VLANها
- ثبتInterface ها
- تغییر Hostname
- تنظیم Domain Name
- ایجادLocal User
- فعال کردنEnable Secret
- فعال کردنPassword Encryption
- تنظیمBanner
- SSH
- غیرفعال کردنTelnet
- فعال کردنAAA
- اتصال بهRADIUS / اتصال به+TACACS
- حذف SNMP v1
- حذف SNMP v2
- استفاده از SNMPv3
- تعریف ACL برای SNMP
- تعریف NTP
- احراز هویت NTP
- تعریف Syslog Server
- ارسال Log به یک SIEM مانند (Splunk / Wazuh /.....)
- Port Security برای تمام Access Portها فعال شود
- BPDU Guard فعال روی Access Port

- PortFast فعال روی Access Port
- Root Guard فعال روی Uplinkهای Access
- UDLD فعال روی لینک‌های فیبر
- DHCP Snooping
- Trust فقط روی Uplink
- Dynamic ARP Inspection
- IP Source Guard
- Storm Control (Unknown Unicast / Multicast / Broadcast)
- Disable Unused Ports
- تغییرNative VLAN
- DTP غیرفعال
- حذف VLAN1 از کاربران
- Management VLAN جدا
- Voice VLAN جدا
- Server VLAN جدا
- Client VLAN جدا
- Guest VLAN جدا
- Printer VLAN جدا
- CCTV VLAN جدا
- IoT VLAN جدا
- Routingغیرفعال کردن پروتکل‌های بلااستفاده
- OSPF (Passive Interface / Authentication)
- EIGRP (Authentication)
- Static Route (فقط مسیرهای موردنیاز)
- ICMP محدودسازی (Directed Broadcast)
- Anti Spoofing
- Proxy ARP
- Source Route
- Redirect
- ICMP Redirect
- CoPP

- Rate Limit
- غیرفعال کردن موارد غیرضروری (HTTP / HTTPS / CDP / ....)
- HSRP
- VRRP
- EtherChannel
- Archive Config
- گزارش Hardening انجام‌شده
- گزارش تست امنیت (Verification)

Hossein Malekzadeh

HOSSEIN MALEKZADEH

HOSSEIN MALEKZADEH HM HOSSEIN MALEKZADEH