Simple Approach to Access Control: Port Control and MAC Filtering

William Knaffl

April 2017

GIAC GCFE, GCIA, GCIA, GCPM, GSEC, GCCC

Objective

- Background: The Attack/Failure
- Immediate Action
- Long Term Solution
  - MAC Filter/Security
  - Auditing

Lab Access Control Failures

- Remote Access Trojan
- Personal laptop of employee
- Unauthorized/Unprotected Wireless
- Uncontrolled movement of equipment
- Unmanaged hub

Primary Failure –

Control 1: Inventory of Authorized Devices

Immediate Triage

- Shut down
- Assets removed from network
- Lab operations halted
- Downtime to multiple programs

Long Term Requirements

- No replacement of existing hardware
- Allow DHCP due to migrating equipment
- Automated processes to turn off ports on unauthorized activity
- Notifications when port status is changed
- Open source directives

Discovery Effort

- Interview Lab Manager and Program operations teams
- Understand movement of hardware and software
- Determine overall objectives and current procedures

Lab Operations

- Discovery
  - We knew as much as they did
- Operationally – "Wild West"
- Network was considered "off net"
  - Long forgotten lab area
- Outcome – Streamlined and documented process/procedure

Hardware Control Failure

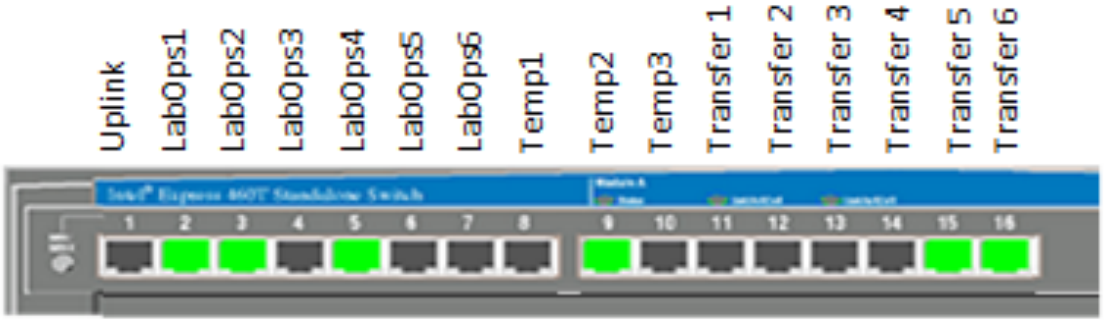
- Firewall in place but misconfigured
- Switch in place –
  - On a shelf over an employees desk
- Multiple Hub/switch(es) used to expand connectivity
- Servers that had been decommissioned

Hardware

- Intel EtherExpress 460t
  - Not in current budget plan
  - Not standard equipment any longer
  - Supported both MAC filtering and Port Security operations
  - No direct alerting, but supported SNMP
- Wireless and unauthorized devices removed

Port Security/MAC Filter

- Nonstandard Hardware (Intel vs Cisco)
- Allowing DHCP reduced downtime



- 2-7 – Long Term - Pseudo Perm
- 8-10 – Temp MAC Filter Alone
- 11-16 – Port Security

Automated Response

- Constrained by Cost and nonstandard hardware
  - OpenSource/batch processing
- Required some management from IT
- Metrics gathered from tickets/requests

Software Monitoring

- Corporate standards do not apply
  - Current tool suite cannot cross platform
- Intel software tools
- Process owned by Lab Management
- SNMP
  - Open Source

SNMP

- SNMP TrapWalker - **Capture**
  - BTT Software
- SNMPGet - **Query**
  - Sourceforge

Enabled	Disabled	Unplugged
<intel>.6.17.3.1.1.3.<port>=2	<intel>.6.17.3.1.1.3.<port>=3	<intel>.6.17.3.1.1.3.<port>=3
<intel>.6.17.3.1.1.4.<port>=5	<intel>.6.17.3.1.1.4.<port>=5	<intel>.6.17.3.1.1.4.<port>=2
<intel>.6.17.3.1.1.5.<port>=3	<intel>.6.17.3.1.1.5.<port>=3	<intel>.6.17.3.1.1.5.<port>=4

Script Output

- Batch File process
- Creates a TXT file with simple data
- Queries the switch, pulls in the appropriate data
  - Compares to known values
  - Exports

Summary

- Failure – Lack of physical control
  - MAC and Port Security
- Monitoring was not present
  - Batch File processing
- Streamlined operation
  - Reduced risk to programs using lab