



13-14 November
The Royale Chulan, Kuala Lumpur



"SECURING CYBERSPACE FOR ECONOMIC GROWTH"

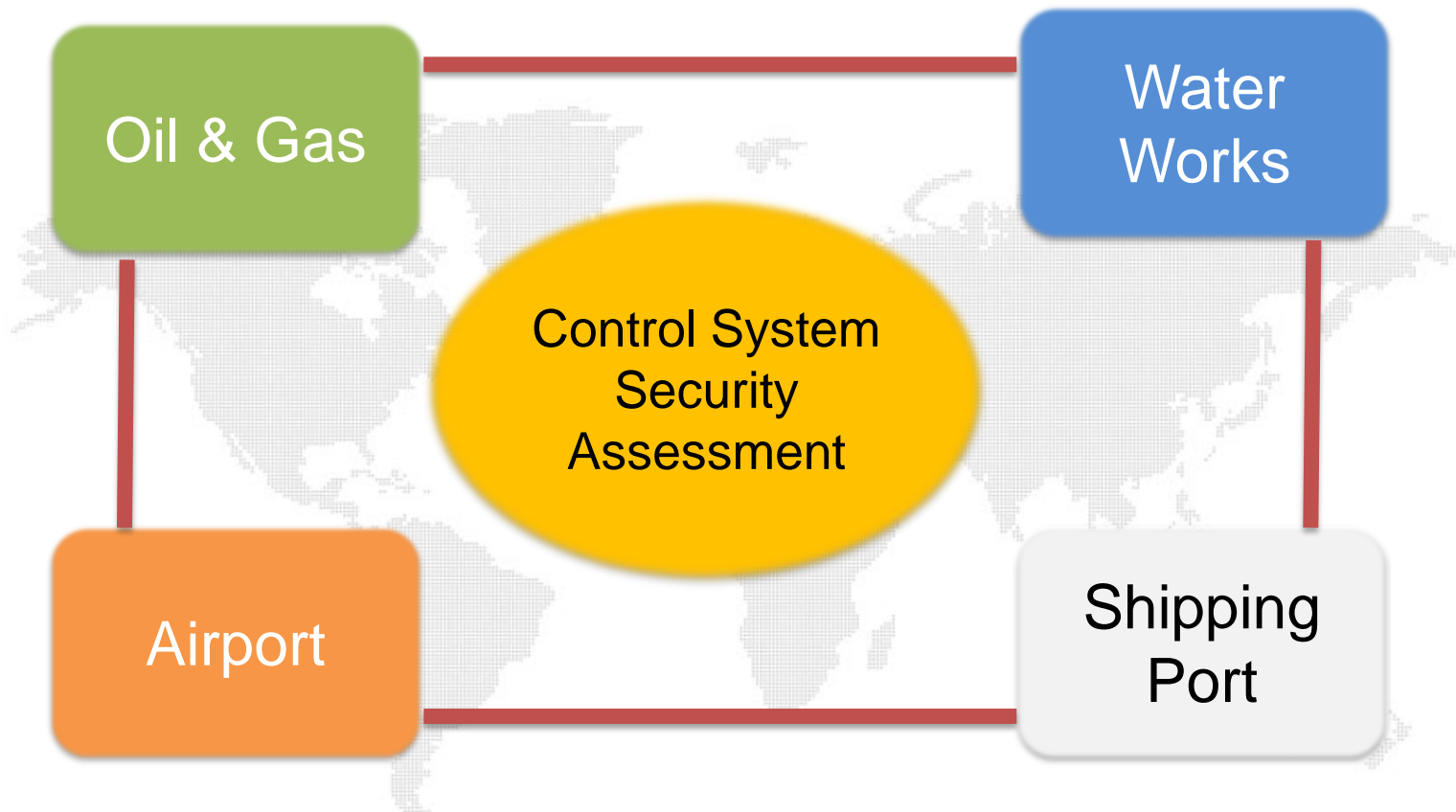
www.csm-ace.my

Top 5 SCADA Security Vulnerabilities

Muhammad Reza Shariff

14 November 2013

Our Experience 2013





SCADA Security Policy Issues

Lack of Enforcement



Applying Corporate IT Policy



No or Incomplete SCADA Security
Policy





Password Issues

Default Password



No Access Control List



All for One



PI C Web Enabled - Password

The screenshot shows a web browser window displaying the TSX ETY410 Web Server interface. The browser's address bar shows the URL "http://192.168.1.100:8080/". The page has a blue header with the "Telemecanique" logo and the title "TSX ETY410 Web Server". Below the header, there are navigation tabs: "Home", "Documentation", "Monitoring", "Control", "Diagnostics", "Maintenance", and "Setup". The "Security" section is active, showing "HTTP access rights" and "Data Editor Write Password" settings. The "HTTP access rights" section includes fields for "Username", "New password", and "Confirm password", with a "Change Password" button below. The "Data Editor Write Password" section includes fields for "Data Editor Write password", "New write password", and "Confirm write password", with a "Change Write Password" button below. The footer of the page states "Copyright © 2000-2006, Schneider Automation SAS. All rights reserved."

TSX ETY410 Web Server

Home Documentation Monitoring Control Diagnostics Maintenance Setup

Security

HTTP access rights

Username:

New password:

Confirm password:

Change Password

Data Editor Write Password

Data Editor Write password:

New write password:

Confirm write password:

Change Write Password

Copyright © 2000-2006, Schneider Automation SAS. All rights reserved.

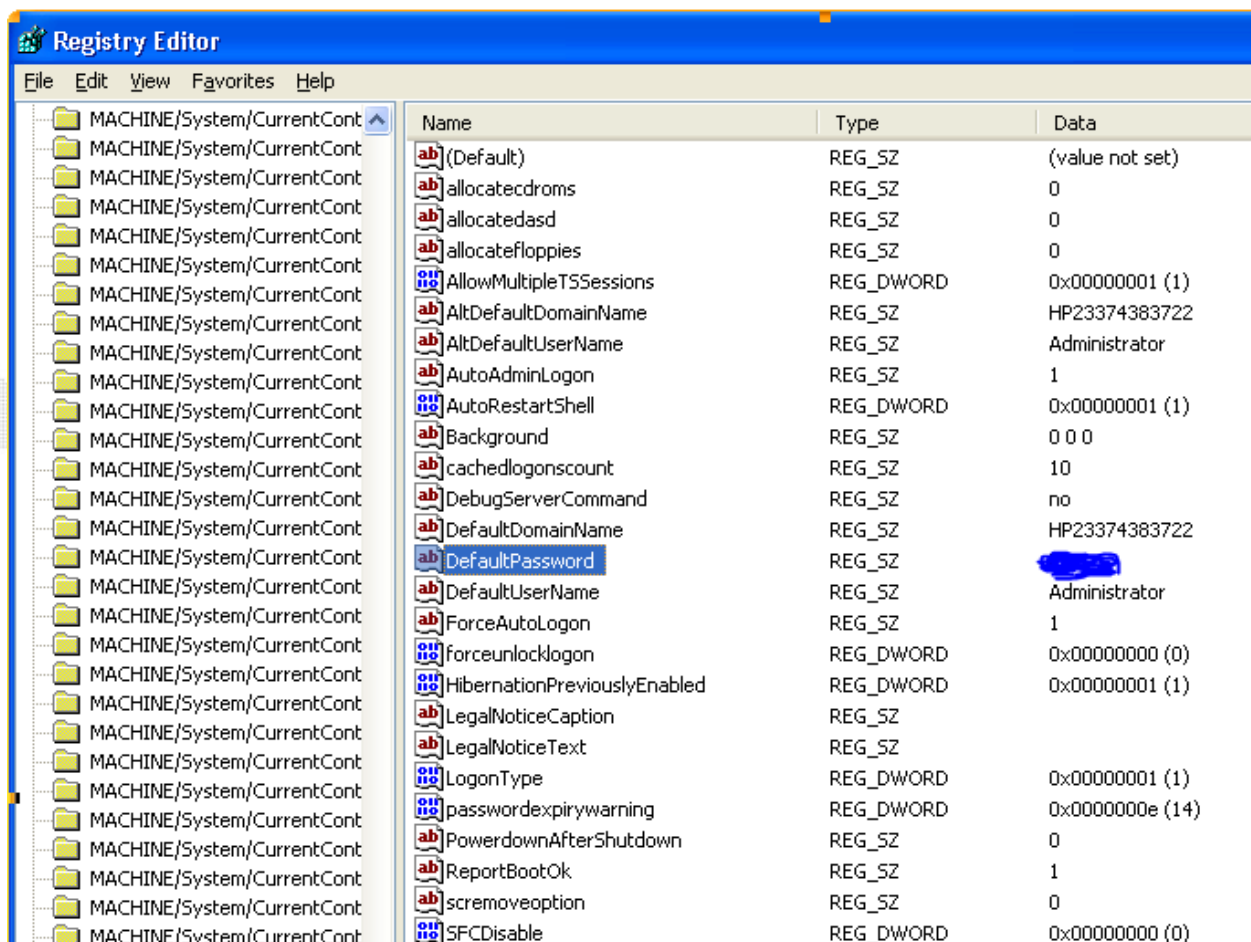
Annuaire.XML for Topkapi

```

- <OPERATOR Tag="1">
  <Name>[REDACTED]</Name>
  <Password>1A3668B60F34C6E56122FBD53948FF24</Password>
  <Phone/>
  <Renv/>
  <Radio/>
  <Email/>
  <Account>local</Account>
  <RequestLDAP/>
  <Sheet_Init/>
  <Files/>
  <Permission_local>False</Permission_local>
  <Visu>7</Visu>
  <Type_Astr>Minitel</Type_Astr>
  <Code_Astr>1</Code_Astr>
  <Category>Z</Category>
  <Code>8</Code>
</OPERATOR>
- <OPERATOR Tag="1">
  <Name>[REDACTED]</Name>
  <Password>3C305017D846712D6748CE000E4527E8</Password>
  <Phone/>
  <Renv/>
  <Radio/>
  <Email/>
  <Account>local</Account>
  <RequestLDAP/>
  <Sheet_Init/>
  <Files/>
  <Permission_local>False</Permission_local>
  <Visu>7</Visu>
  <Type_Astr>Minitel</Type_Astr>

```


Hardcoded Password in the Registry



The screenshot shows the Windows Registry Editor with the following structure in the left pane: `MACHINE\System\CurrentControlSet\Local Settings\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\Password`. The right pane displays a list of registry values.

Name	Type	Data
(Default)	REG_SZ	(value not set)
allocatecdroms	REG_SZ	0
allocatedasd	REG_SZ	0
allocatefloppies	REG_SZ	0
AllowMultipleTSSessions	REG_DWORD	0x00000001 (1)
AltDefaultDomainName	REG_SZ	HP23374383722
AltDefaultUserName	REG_SZ	Administrator
AutoAdminLogon	REG_SZ	1
AutoRestartShell	REG_DWORD	0x00000001 (1)
Background	REG_SZ	0 0 0
cachedlogonscount	REG_SZ	10
DebugServerCommand	REG_SZ	no
DefaultDomainName	REG_SZ	HP23374383722
DefaultPassword	REG_SZ	[REDACTED]
DefaultUserName	REG_SZ	Administrator
ForceAutoLogon	REG_SZ	1
forceunlocklogon	REG_DWORD	0x00000000 (0)
HibernationPreviouslyEnabled	REG_DWORD	0x00000001 (1)
LegalNoticeCaption	REG_SZ	
LegalNoticeText	REG_SZ	
LogonType	REG_DWORD	0x00000001 (1)
passwordexpirywarning	REG_DWORD	0x0000000e (14)
PowerdownAfterShutdown	REG_SZ	0
ReportBootOk	REG_SZ	1
scremoveoption	REG_SZ	0
SFCDisable	REG_DWORD	0x00000000 (0)



Network Architecture and Design

Active Ports Available



Web Enabled RTU and PLC



No Segregation of Network



Coils Read & Write

ModScan32 - [ModSca1]

File Connection Setup View Window Help

011 16 10 0X 32 32 64 64

Address: Device Id: Number of Polls: 7
 Length: MODBUS Point Type: Valid Slave Responses: 7

00001:	<0>	00017:	<0>	00033:	<0>	00049:	<0>	00065:	<0>	00081:	<0>	00097:	<0>
00002:	<0>	00018:	<1>	00034:	<0>	00050:	<0>	00066:	<0>	00082:	<0>	00098:	<0>
00003:	<0>	00019:	<0>	00035:	<0>	00051:	<0>	00067:	<0>	00083:	<0>	00099:	<0>
00004:	<0>	00020:	<0>	00036:	<0>	00052:	<0>	00068:	<0>	00084:	<0>	00100:	<0>
00005:	<1>	00021:	<0>	00037:	<0>	00053:	<0>	00069:	<0>	00085:	<0>		
00006:	<0>	00022:	<1>	00038:	<0>	00054:	<0>	00070:	<0>	00086:	<0>		
00007:	<0>	00023:	<1>	00039:	<0>	00055:	<0>	00071:	<0>	00087:	<0>		
00008:	<0>	00024:	<0>	00040:	<0>	00056:	<0>	00072:	<0>	00088:	<0>		
00009:	<0>	00025:	<1>	00041:	<0>	00057:	<0>	00073:	<0>	00089:	<0>		
00010:	<1>	00026:	<0>	00042:	<0>	00058:	<0>	00074:	<0>	00090:	<0>		
00011:	<1>	00027:	<1>	00043:	<0>	00059:	<0>	00075:	<0>	00091:	<0>		
00012:	<1>	00028:	<0>	00044:	<0>	00060:	<0>	00076:	<0>	00092:	<0>		
00013:	<0>	00029:	<0>	00045:	<0>	00061:	<0>	00077:	<0>	00093:	<0>		
00014:	<0>	00030:	<0>	00046:	<0>	00062:	<0>	00078:	<0>	00094:	<0>		
00015:	<0>	00031:	<0>	00047:	<0>	00063:	<0>	00079:	<0>	00095:	<0>		
00016:	<1>	00032:	<0>	00048:	<0>	00064:	<0>	00080:	<0>	00096:	<0>		

For Help, press F1

Polls: 7 Resps: 7



Antivirus Issues

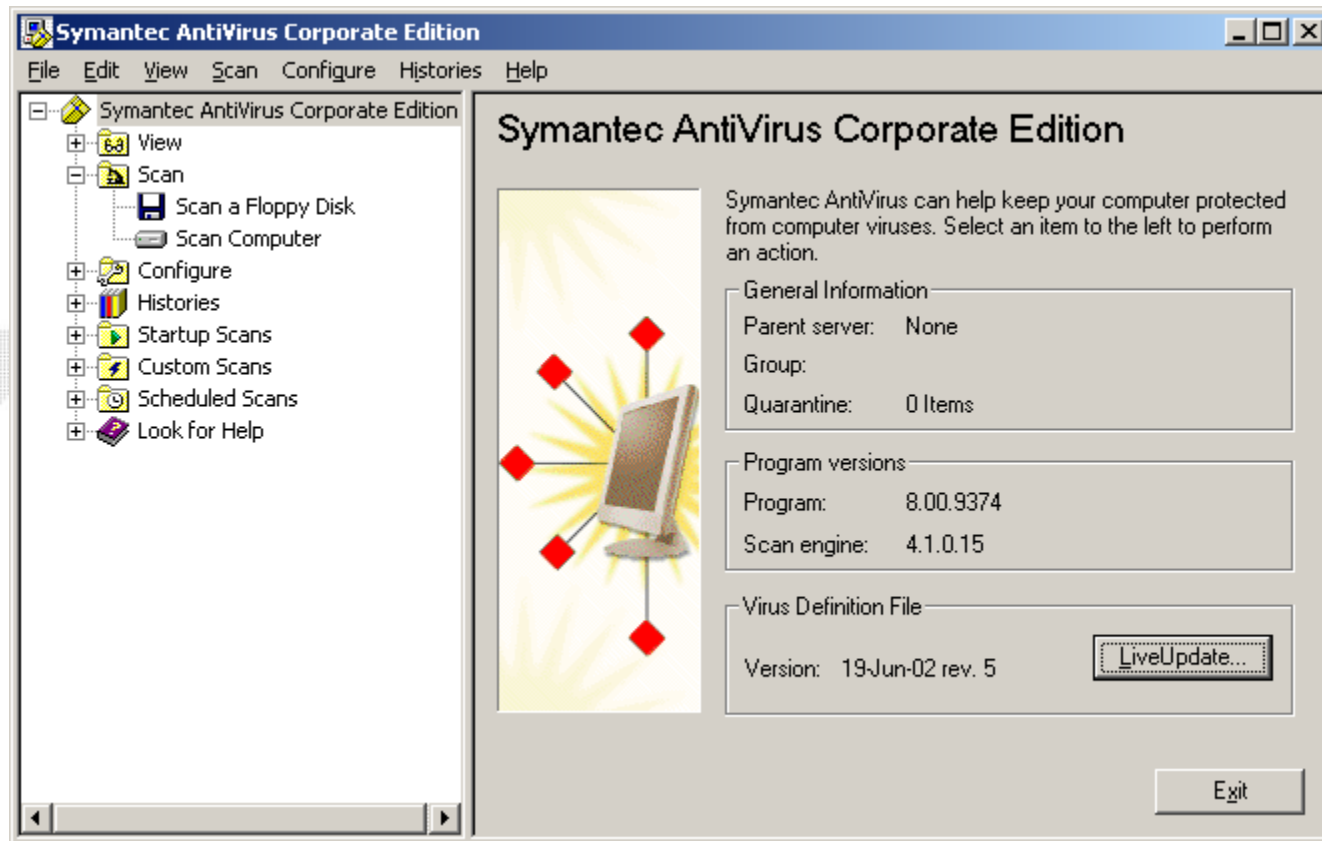
Missing AV or Updates

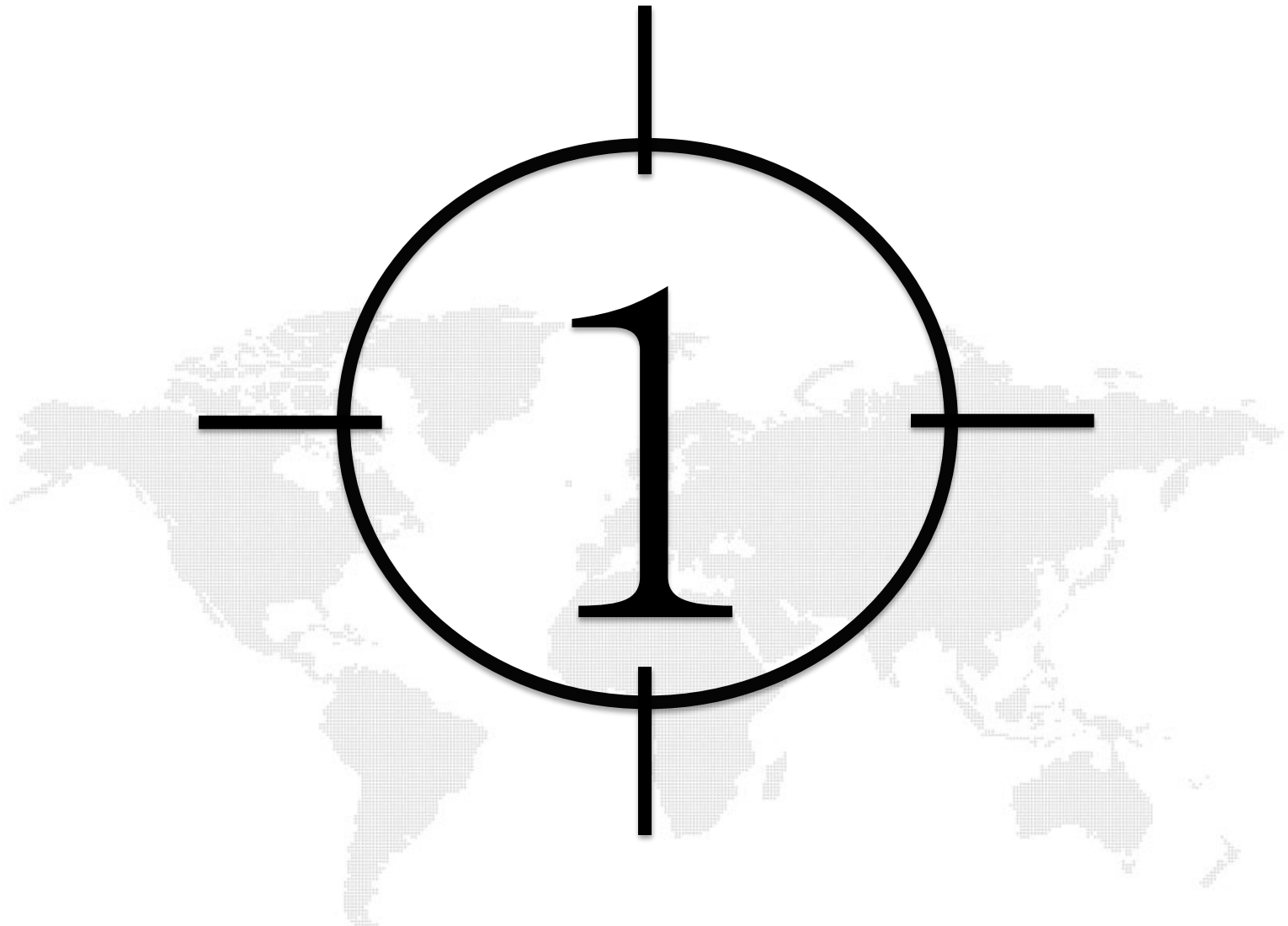
Fear of System Disruption

False Sense of Security – Closed
Network



Antivirus Issues





Operating System & Applications

Obsolete OS, Missing Patches &
Services Packs

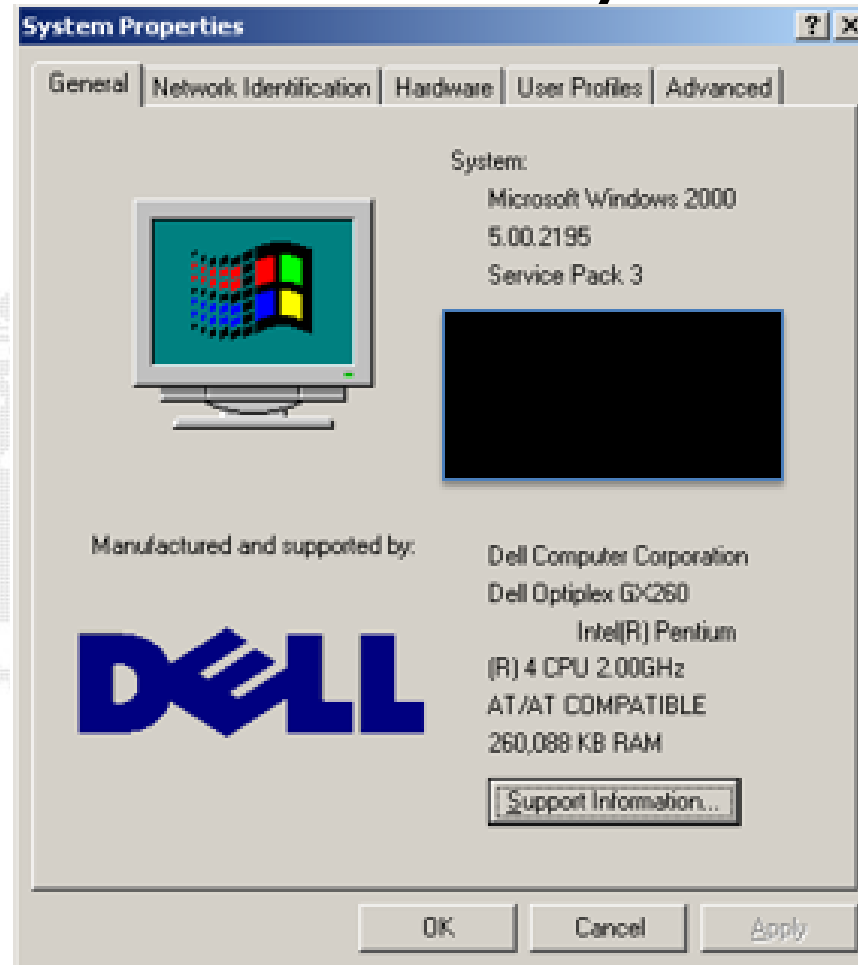
No Hardening

Vulnerable to Malware, DOS,
Hacking, & etc

Hacking, & etc



Obsolete System



Thank you

Corporate Office

CyberSecurity Malaysia,
Level 8, Block A,
Mines Waterfront Business Park,
No 3 Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan, Malaysia.

T : +603 8946 0999
F : +603 8946 0888
H : +61 300 88 2999

www.cybersecurity.my
info@cybersecurity.my



www.facebook.com/CyberSecurityMalaysia



twitter.com/cybersecuritymy



www.youtube.com/cybersecuritymy

