The Broken Web:
Identifying Weaknesses and Strengthening Internet Security

Steve Antoniewicz
02/19/2009

© 2009 NET2S, Inc.
Hello...

I am:
- Steve Antoniewicz
- Security Researcher
- Technologist
- Certified in a bunch of stuff
- Employed by
  - NET2S / British Telecom

We are going to talk about:
- Crime
- Hackers
- The Internet
Quiz!
Motivators

Disclosed Incidents

* Source: http://www.xiom.com/whid
Evasion Techniques

- **Foreign-hosted servers**

![World map with countries highlighted]

- **Countries which the U.S. maintains diplomatic relations, but does not have extradition treaties with**

- **Countries which have neither diplomatic relations nor extradition treaties with the U.S.**
Evasion Techniques

- Compromised hosts

- Open WiFi
  - Public Networks
  - Home / Corporate Networks
Phishing

Goals
- Monetary Theft
- Identity Theft

2007 - $3.2 Billion Lost
- 3.6 Million adults in the US

* Source Gartner
Phishing

Design
- Vulnerability R+D
- Scam Page Design
- Email Design

Collection
- Vulnerability Scanning
- Email Address Harvesting

Delivery
- Mass Mailing

Profit
- Credential Collection / Cashing
Phishing

Germany, Italy, United Kingdom, France And Norway...

10:27:16 < maggi> C99 R57 mail List Uk/US/Ger/ty/Aol/De >>>
10:27:18 < securecode> :Selling: Root SHell Cpanel VPS+RDP For AMS Or for what u want Sock All Contery Mail List Uk/Us/Ger/Ar/Tyrkey And Leads Mail List C99 R57 Shell FTP Hacked SMTP All Contery IP Fresh OR web Orange VNC WEmail Cvv2/UK/US Rapidshare/Agg Heather/hacked Shopadmin US Fulls/US/Pecliers/With/IP...
10:28:58 < securecode> :Selling: Ebbey Login 15K nationwide 40K HSBC 50K And Scam Page All Contery For sell with Letters Dump+Pin Track 1 Track 2 Look All PeoPle Dont MSG for trade or For Share:) i want Just LR:) to Sell ALL OK?
10:28:58 < securecode> Scanner FOR SMTP-- Scanner For Root Scanner For Remote Desktop-RDP ITS all Windows to USE i have AND Scann Linux Root and Win Root Scanner Rapidshare Scanner C99 R57 Scanner Database Witch 1 Error you Connect here Look All PeoPle Dont MSG for trade or For Share:) i want Just LR:) to Sell ALL OK?
10:28:58 < maggi> Script Php Mailer SMTP Orange.Fr Wanndo.Fr Optuss BigPond >>>>
10:28:59 * DUMPS* Selling dumps ( US , Ca , FRance , SPAIN , Germany and some EU ) extracted from hotel database ( on Sale ) ... ( Verified +v user here! you will not lose your money ... LOW LOW LOW PRICES ON BULK msg me now ) Ricki_Monday@comp.com [mail]
10:29:00 < TradeCC> w00t3d is selling CC/CVV fullz dob/ssn/PIN US,UK, Lot of fresh unspammed email, , msg w00t3d for more info
10:29:00 < maggi> ShopAdmin USA Without cvv2 Uptime 3 Days 15 Orders day >>>>
10:29:02 < maggi> Fullz/USA Citi Bank Bank Of America >>>>
10:29:02 * Skimmer For Sale Europe and united states DUMPS Platinum/gold/classic are available each for a price I accept only Webmoney/WesternUnion ! Nigerian rippers FUCK OFF! 4x and admins can verify first
10:29:02 < TradeCC> MaStErBoY Is Selling AU Cvv2, Fulls , Paypal Accounts, SMTP, VNC ACCOUNTs RDP ...
10:29:04 * GODy Us\UK\IT\Au\Ca => Cvv2 each 3$ - DUMPS SKIMMED AND GENERATED - SHOPADMINS - PAYPALS VERIFIED ! I GIVE PREVIEWS PROOFS SCREENSHOTS !
10:29:04 < maggi> RapidShare Account 300 Days >>>>

© 2009 NET2S, Inc.
Botnets

**Software Robots**
- Autonomous
- Command and Control
- IRC

**Complex**
- “Conficker” currently has estimated 9,000,000 hosts
  - Capable of 10 billion spam messages / day
DDoS for Cyber Warfare

- RBN v Estonia
- RBN v Georgia
Insider Threats

“Insiders”
- Generally trusted
- Easy access to resources
- Know how the system works
- Understand data

Goals
- State / Military
- Economic
  - Trade Policy / Secrets
- Corporate
  - Acquire competitive advantage
  - Fraud
Rogue Trader - $7.2 Billion Loss

   - Risk Score: 125

   - Risk Score: Low

3. Creates a false portfolio and begins issuing trades circumventing credit and trade size controls (late 2006).
   - Risk Score: Low
   - Flags: Failure to detect inappropriate access or SOD violation.
   - Periodic access reviews and SOD policy enforcement were ineffective or not in place.

4. Enters fabricated 'offsetting' trades before nightly reconciliation, concealing his fictitious trade positions (throughout 2007).
   - Risk Score: Low
   - Flags: Inadequate user activity logging/monitoring.
   - Limited visibility into system activity by business management enables policy violations and suspicious activities to go undetected.

5. Misappropriates names and passwords of colleagues to mask his fraud.
   - Risk Score: Low
   - Flags: Ineffective user authentication and identity risk management.
   - Without strong authentication, Société Générale is unable to prevent the unauthorized use of passwords. Quantifying identity risk would have highlighted Jérôme Kerviel's unusual activity.

   - Risk Score: Low
   - Flags: Ineffective IT risk management.
   - An identity risk management framework would have provided an additional layer of IT risk controls that would have been difficult for Kerviel to subvert.

7. Forges trade acknowledgement from Deutsche Bank that goes unconfirmed, triggering an investigation (Jan. 2008).
   - Risk Score: Low
   - Flags: Weak access controls and activity monitoring.
   - Société Générale is left to rely upon external events to reveal the ongoing fraud rather than their own controls.


9. Court orders Kerviel to jail to await trial (Feb. 2008).

Risk Score: MEDIUM

Business Role: Trader
Société Générale

Access to Salesforce System & Data
Access Policy Violations
Compliance Management Review

Risk Score: HIGH

Business Role: Middle Office
Société Générale

Access to Salesforce System & Data
Access Policy Violations
Compliance Management Review
Custom Enterprise Web Application

Enterprise Security API


Existing Enterprise Security Services/Libraries

© 2009 NET2S, Inc.
OWASP WebGoat

Bypass a Path Based Access Control Scheme

The 'guest' user has access to all the files in the lesson_plans directory. Try to break the access control mechanism and access a resource that is not in the listed directory. After selecting a file to view, WebGoat will report if access to the file was granted. An interesting file to try and obtain might be a file like tomcat/conf/tomcat-users.xml

Current Directory is: C:\WebGoat-5.1\tomcat\webapps\WebGoat\lesson_plans

Choose the file to view:
- AccessControlMatrix.html
- BackDoor.html
- BasicAuthentication.html
- BlindSqlInjection.html
- BufferOverflow.html
- ChallengeScreen.html
- ClientSideFiltering.html
- ClientSideValidation.html
- CommandInjection.html
- ConcurrencyCart.html
- CrossSiteScripting.html
- CSRF.html
- DangerousEval.html
- DBCrossSiteScripting.html
- DBSQLInjection.html

View File
Learning

Hacking Challenges
- http://www.hackthissite.org
- http://www.dareyourmind.net

Education / Tools
- http://www.owasp.org
Q+A