PENETRATION TEST & SECURITY STANDARDS

SCOTT TSE (MPHIL, CISSP, CISM, CEH)
WISHLOG@GMAIL.COM
NTT COM SECURITY (FORMELY INTEGRALIS)

INTRODUCTION
ABOUT SCOTT TSE

- Identify 0-day attack on web mail used by HKU, CUHK when studying Mphil
- Found multiple vulnerabilities on websites “secured” by

- Found >20k credit cards through SQL injection, unprotected admin page or even in share drive
- Conducted pentest in CN, TW, JP, Washington DC, Miami, Bermuda, Philippine, …
- Assisted one of the big4 to secure their websites and mobile MDM solution

BREAKDOWN

The “Security” Market

The not-so-dramatic hacking – Penetration Test

Web Application Scanning and Attacks

Security certificate on People

Security certificate on Enterprize

WHAT CAN YOU BUY IN “SECURITY” MARKET?

Extended reading: https://www.trustwave.com/downloads/Trustwave_WP_Global_Security_Report_2012.pdf

SERVICES

A long list of services category:

- **IT audit**
- **PCI compliance**
- **Vulnerability Scan**
- **Penetration Test**
- **Web app assessment**
- **Mobile phone / Mobile app assessment**
- **…**
- *** (The Integralis catalog)**

PRODUCTS

A wide range of Firewalls

Antivirus products

“Next generation” firewalls

- **FireEye**
- **PaloAlto**
- **Impreva**

ALTERNATIVES

Virus / Zero day exploits

Acquired by HP →

Stolen macbooks, phones from the “Deep web”

Hacking / DDOS services from IRC / forum

PENETRATION TEST

What is penetration test?

- To simulate real hacking activity in a control environment to analysis the potential risk exist in the enterprise

Why is it needed?

- Achieve ‘just enough’ security in economical way
- See what can a bad guy do
- Compliance requirement (Forced by 3rd parties)

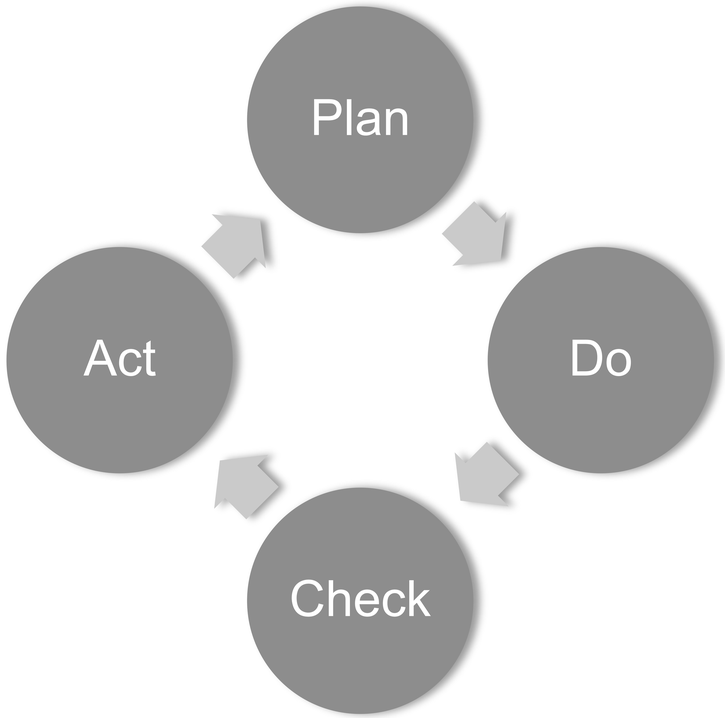
Who will need it?

- Government sectors
- Enterprise
- Hospitality
- Food and beverage
- Retails
- Bank

Extended reading: https://www.trustwave.com/downloads/Trustwave_WP_Global_Security_Report_2012.pdf

VULNERABILITY / RISK ASSESSMENT

- **Ways to deal with risk**
  - Ignore
  - Mitigate
  - Transfer
  - Reduce
- **Terminology:**
  - Information Security (IS) V.S. IT Security
  - IS Governance, Policy, Baseline, Guideline
  - Business Continuity, Disaster Recovery



VULNERABILITY / RISK ASSESSMENT

- **To “NAME” a vulnerability**
  - CVE V.S. CWE
  - Others: BID ####, MS##-####, OSVDB ###
- **To “Report” a vulnerability**
  - Standard: Security Content Automation Protocol SCAP
  - Entity: CERT, CVE, WooYun (Chinese),
- **References**
  - http://cwe.mitre.org
  - http://cvedetails.com

PENETRATION TEST HOW TO?

- **Internal Penetration test**
  - Plugin into internal network see what you “shouldn’t” see
- **External Penetration test**
  - “Browse” from cooperate web, see what you “shouldn’t” see
- **Standards, methodology:**
  - Open source pentest framework
    - http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html
  - NIST Special Pub
    - http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
  - OSSTMM
    - http://www.isecom.org/home.html
  - Orange Book (One of the Rainbow series)
  - UK, Canada’s standard

Extended reading: http://en.wikipedia.org/wiki/Penetration_test

PENETRATION TEST PHASES (GENERAL)

1. Define a scope with client (Good guy only)
2. Identify core value
3. Reconnaissance
4. Enumeration
5. Vulnerability Assessment / Exploitation
6. Further investigation / Pivoting
7. Get the core information, e.g. password, client data, company reports, financial data, e.g.
8. Plant rootkit and erase track (Bad guy only)

PENETRATION TEST PHASES (DETAILS)

1. **Plug into office network, guest network**
2. **Sniff for open protocols**
3. **Try default credentials**
4. **Identify open service and try exploits**
5. **Gain confidential information**
   - Company financial reports
   - Client data
   - Credentials
   - Credit card number
   - ID card number
   - …
6. **Reporting!**

DEMO

“owning a laptop”

- **Tools:**
  - Nmap, Metasploit, Nexpose

- **Warning: do not try it at home…**
  - Do it only under Adon’s supervision. ROFL

EXTERNAL ASSESSMENT

- **Assessment scope:**
  - Similar to internal assessment
- **Tricks**
  - Bypass firewall / IPS
  - UDP may not be blocked
    - SNMP
    - DNS
  - Test/Debug pages in production servers
  - Security Misconfiguration in IPv6
  - Unpatched Apache, IIS
  - Sql injection (To be discuss later)

WEB ASSESSMENT

- **Client-side attacks**
  - XSS, CSRF, etc
- **Server-side attacks**
  - SQL injection, Local / Remote file inclusion, etc
- **Standards**
  - OWASP, WASC, SANS

WEB ASSESSMENT

- **Dynamic web scanners**
  - Acuentix
  - HP WebInspect
  - IBM AppScan
  - Google skipfish
  - Nikto2
  - Arachni *
  - ZAP, Paros proxy
- **Static source code scanners**
  - CheckMarx *
- **Attack tools**
  - Dirbuster
  - SQLmap *
  - PadOracleAttack
- **Security Seals**
  - McAfee
  - Trustwave
  - CUHK … ☺
  - Given after purchasing scanning services
  - False sense of security

http://sectooladdict.blogspot.com/2011/08/commercial-web-application-scanner.html

DEMO

- **Automated tools**
  - Skipfish, Nikto2, Arachni
  - sqlmap
- **Semi-automated tools**
  - Zap Proxy

SECURITY STANDARDS

Extended reading: https://www.trustwave.com/downloads/Trustwave_WP_Global_Security_Report_2012.pdf

COMPLIANCE

- **What is a compliance?**
  - Make sure the business operations satisfy with regulatory standards
- **In Information [Technology] Security**
  - Highly recognized:
    - ISO27001
    - PCI-DSS
  - Other IS frameworks:
    - ITIL, COSO, COBIT, FISMA, OCTAVE, CMMI

Book: IT Audit, Control and Security
By Robert Moeller

PCI-DSS

- **Payment Card Industry – Data security standard**
- **Why exist**
  - A standard established by major payment brands
    - Visa, American Express, MasterCard, JCB, Discover
- **Who need it**
  - Merchants that accept online payments
  - If PCI compliance is done, financial loss goes to PCI when data security is breached
  - Otherwise, merchants will bear the risk and compensation for data security breach

PCI-DSS MERCHANTS TO BE AUDITED BY

- **Qualified Security Assessor (QSA)**
  - QSAs are approved by the Council to assess and prove the compliance with the PCI DSS
- **Approved Security Vendor (ASV)**
  - Responsible for SCANNING of customer facing payment card network
- **DIY: Self Assessment Questionnaire (SAQ)**
  - Self-assessment: Security CHECKLIST approach
  - Eligible only for Level 3-4 merchants
- **Depending on the nature of transactions,**
  - internal transactions go for QSA
  - customer-facing transactions go for ASV
  - small companies go for SAQ

PCI-DSS
MERCHANT TRANSACTION VOLUMES

Level 4

- < 20k Transaction per year

Level 3

- 20k – 1M Transaction per year

Level 2

- 1M – 6 M Transaction per year

Level 1

- > 6M Transaction per year
- Previous incidents of security breach or data compromise
- “They spot you”

PCI-DSS
PROCEDURES TO COMPLY

- Contact ASV or DIY
- Identify the scope and determine the target network range
- Conduct a scan by ASV or DIY
- Fix vulnerabilities / loopholes
- Rescan
- Confirm all KNOWN vulnerabilitiesare fixed
- Report to and Certify by QSA! Rescan every quarter……

PCI-DSS DOMAINS

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf
https://www.pcisecuritystandards.org/security_standards/documents.php?assocation=P

PCI-DSS, ISO27001 MAPPING

A 10.3.2 System acceptance		
A.10.4 Protection against malicious and mobile code		
A 10.4.1 Controls against malicious code	5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
	5.1.1	Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.
	5.2	Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.
A 10.4.2 Controls against mobile code		
A.10.5 BackUp		
A 10.5.1 Information Backup	9.5	Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.
A 10.6 Network security management		
A 10.6.1 Network controls	1.1	Establish firewall and router configuration standards that include the following
	1.1.2	Current network diagram with all connections to cardholder data, including any wireless networks.
	1.1.5	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP.
	1.1.6	Requirement to review firewall and router rule sets at least every six months
	1.2.2	Secure and synchronize router configuration files.
	2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.
	4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.
	11.4	Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.
	11.4	Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.
	2.2.2	Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.

‘LATEST’ TECHNOLOGY, TRENDS

- **Mobile App assessment**
- **Cloud security**
- **Security Information and Event Management (SIEM)**
- **Next Generation Firewall (NGFW)**
- **Web Application Firewall (WAF)**
  - Some WAF introduce new exploits ☺
  - http://www.andlabs.org/whitepapers/Split_and_Join.pdf
- **Exploits for sale come to a upper-ground business**
- **APT prevention: FireEye, PaloAlto**

SECURITY CERTIFICATES

Cisco Systems	CCNA Security • CCSP • CCIE Security
EC-Council	ENSA • CEH • CHFI • ECSA • LPT • CNDA • ECIH • ECSS • ECVP • EDRP • ECSP • ECSO
GIAC	GSIF • GSEC • GCFW • GCIA • GCIH • GCUX • GCWN • GCED • GPEN • GWAPT • GAWN • GISP • GLSC • GCPM • GLEG • G7799 • GSSP-NET • GSSP-JAVA • GCFE • GCFA • GREM • GSE
ISACA	CISA • CISM • CGEIT • CRISC
(ISC)²	SSCP • CAP • CSSLP • CISSP • ISSAP • ISSEP • ISSMP
ISECOM	OPST • OPSA • OPSE • OWSE • CTA
Offensive Security	OSCP • OSCE • OSWP
CREST	CREST Consultant
IACRB	CPT • CEPT
eLearnSecurity	eCPPT
SCP	SCNS • SCNP • SCNA
CERT	CSIH

Q & A

Extended reading: https://www.trustwave.com/downloads/Trustwave_WP_Global_Security_Report_2012.pdf