IT security agency essentials

Storia di un penetration test immaginario.

Francesco Ongaro <ascii@ush.it>
Antonio Parata <s4tan@ush.it>

Special thanks to jekil, naif, vecna, wisec,
Matteo Meucci, Icesurfer, evilaliv3.

(c) 2008 ush.it – a beautiful place
All right reserved.

Primo contatto

Viene a crearsi un'opportunita' commerciale.

- L'agenzia contatta il cliente. (few degrees of separation, ricerca, mass contact, ..)
- Il cliente contatta l'agenzia. (FDoS, leadership, ..)

Compiti del commerciale:

- Essere chiaro e consapevole.
- Analisi necessita' del cliente.
- Espone i servizi erogabili.
- Accordo su servizio e modalita' di esecuzione.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Hint: Materiali

Puo' accadere (ed in parte e' auspicabile) che il cliente non sia completamente a digiuno di IT security, per evitare brutte figure:

- Commerciale skilled. (terminologia esatta, conoscenza dei prodotti e dei servizi, conoscenza delle strategie di gestione del rischio, ..)
- Disporre di materiali *distribuibili* anonimizzati.
- Disporre di un esempio di contratto e manleva.
- Conoscenza del mercato. (offerte dei concorrenti, pricing, livello qualitativo, ..)

(c) 2008 ush.it - a beautiful place. All rights reserved.

Contratto

Definisce oneri ed onori delle parti. “Accordo formale di due o più parti per costituire, modificare o estinguere un rapporto giuridico. [..]”

- Cosa/come verra' testato. (IP ranges, domini, esclusioni, altre specifiche [es: “verticale”/massimo dettaglio o “orizzontale”/massima copertura])
- Tipo prodotto e metodologia. (VA, PT, NPT, WAPT, CR, ..)
- Output richiesto. (report, altri document distribuibili, ..)
- Data consegna lavori ed orari di testing.
- Indirizzi IP sorgente.
- Parte legale e manleve.
- Notifiche in corso d'opera.
- Contatti per le emergenze (DoS, ..)

(c) 2008 ush.it - a beautiful place. All rights reserved.

L’acquisto di servizi IT: case study

Aspetti legali negli SLA

- Definizione dello SLA.
- Funzione dello SLA.
- Qualificare l’inadempimento delle parti.
- Garantire/definire la qualità del servizio.
- Definire le aspettative delle parti.
- Consentire al fornitore del servizio di allocale le risorse.
- Key Performance Indicators (RAVs dell’OSSTMM?).
- Penali per violazione degli SLA.
- Penali per ritardo.
- Limitazioni/grace period.
- Performance credits.
- Benchmarking.
- Recesso.

* Questi punti sono tratti e adattati al contesto di questo seminario dalla presentazione “L’acquisto di servizi IT: case study” degli Avv. Domenico Colella e Laura Liguori.

(c) 2008 ush.it - a beautiful place. All rights reserved.

L’acquisto di servizi IT: case study

Altre valutazioni da fare

- Riservatezza delle informazioni, degli output. (reports, raw data, ..)
- Trattamento dei dati personali.
- Sub-appalto.
- Clausole di prevalenza.
- Distrazione del personale.
- Controversie.
- Cessione del contratto.

* Questi punti sono tratti e adattati al contesto di questo seminario dalla presentazione “L’acquisto di servizi IT: case study” degli Avv. Domenico Colella e Laura Liguori.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Definizione risorse

Risorse allocate dalla security agency:

- Forza lavoro. (referente/prj manager, pt monkeys, ..)
- Eventuali configurazioni aggiuntive. (software: es. Agenti, ..; hardware: es. Sonde, I[DP]S, ..)

Risorse allocate dal cliente:

- Referente attivita'. (contatti con i sistemisti/sviluppatori e col management)
- Eventuali configurazioni aggiuntive.
- Eventuale remediation in corso d'opera.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Definizione agenda

- Data ed ora inizio lavori.
- Data ed ora fine lavori.
- Data consegna documenti distribuibili (report, ..).

Attivita' su target sensibile:

- Orari attivita'.
- Esclusioni, varie ed eventuali.

Attivita' su target estremamente sensibile:

- Date e consegne checkpoint.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Pacchetto consegne

Una volta definiti tutti gli aspetti contrattuali ed operativi dell'attivita' le consegne vanno sintetizzate in un documento interno.

Questo documento e' ad uso degli esecutori materiali e rendendo chiare le consegne permette di minimizzare gli errori.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Servizi di sicurezza

I prodotti e servizi tipici dell'IT Security sono spesso sottoinsiemi uno dell'altro e/o si intersecano. Ad esempio le attivita' svolte nell'ambito di un VA praticamente rappresentano l'inizio di un PT e un PT ben fatto contiene parti tipiche del CR.

```
VA NPT WAPT 0DAY CR  RA REPORT
========= PT ========--==========
PHYSICAL SECURITY & SOCIAL ENG.
======== Ethical hacking ======
        (Tiger team like)
```

(c) 2008 ush.it - a beautiful place. All rights reserved.

Risk Managenemt

I prodotti di IT Security possono essere parte di una strategia di gestione della sicurezza, codificata in vari standard.

ISO 27001:2005 (ex: ISO 17799, BS7799), SoGP (Standard of Good Practice), CoBit, NERC 1300, HIPAA, PCI-DSS, NIST (pubblications, guidelines), BSI IT Baseline Protection Manual, ISO 15408, Sarban & Oxley, ..

Lo Standard ISO 27001:2005 è una norma internazionale che fornisce i requisiti di un Sistema di Gestione della Sicurezza nelle tecnologie dell'informazione (Information Security Management System - ISMS).

(c) 2008 ush.it - a beautiful place. All rights reserved.

Metodologie

ISECOM: OSSTMM (Open Source Security Testing Methodology Manual), Rules of Engagement

OWASP: Testing Guide, Code Review Project

WASC, ..

Certificazioni: OPST, OPSA, CISSP, CISA, CISM, ISO 27001 Lead Auditor, ..

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Definizione 1/4

VA = Vulnerability assessment

“A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. [..]”

http://en.wikipedia.org/wiki/Vulnerability_assessment

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Definizione 2/4

"[..] identifying, quantifying, and ranking [..]"

Identifying → Information Gathering

Viene chiamata anche fase di "Enumeration".

A → Discovery dei network. (AS, wired ethernet, wifi, ..)
B → Discovery degli host. (es: un host con piu' if o ip, ..)
C → Discovery delle porte e dei servizi.
D → Identificazione delle risorse implementate.

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Definizione 3/4

“[..] identifying, quantifying, and ranking [..]”

Quantifying → Qualificare e quantificare le vulnerabilita' identificate.

“designare, caratterizzare, contraddistinguere costituendo un criterio decisivo di valutazione o di classificazione [..]”

“esprimere in termini quantitativamente e numericamente valutabili la consistenza di un fenomeno [..]”

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Definizione 4/4

"[..] identifying, quantifying, and ranking [..]"

Ranking → PKI e sistemi metrici.

CVSS, CVSSv2
OWASP Testing Guide
DREAD (Michael Howard in "Writing secure code")
MS Advisories

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Enumeration 1/7

Il VA inizia con il discovery degli host, delle risorse (MPLS, routers, ..), dei servizi (demoni, ..) e delle applicazioni implementate.

Fornisce l'idea di massima della topologia della rete target, dei servizi erogati e potenzialmente anche delle dinamiche dei sistemi e del sistema di sistemi.

- Viene svolto nei primi giorni di attivita'. (volendo generalizzare si potrebbe dire che il primo terzo dell'attivita' viene dedicato all'information gathering)
- Permette di tunare l'attack lab. (routing, firewalling su target ed orari, traffic dump, ..)
- Fornisce al tester gli elementi base per capire dove direzionare gli sforzi.

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Enumeration 2/7

Host discovery (L2 vs L3):

- L2: ARP (Passivo: arpwatch, arpsnmp. Attivo: arpfetch, arp-sk, arping, arping2), UPNP (upnpscan, miniupnpc), Multicast (bonjour, ..), LLTD

- L3: ICMP (ping, fping, hping), TCP/UDP/ICMP syn, connect() (nmap, scanrand, etc), Embedded/Custom/Vendor (MNDP: MikroTik RouterOS Neighbor Discovery Protocol, CDP: Cisco Discovery Protocol), Passive (NetBIOS announces, IPX, broadcasts, p0f, tcpdump), Stack (ND/NDP: TCP/IP IPv6 Neighbor Discovery Protocol, SEND: TCP/IP IPv6 SEcure Neighbor Discovery), Routing (ICMP redirects, OSFP, HSRP, IGRP/Zebra, VRRP, OLSR, STAR, DART, ATR, DSR, AODV, ..), ..

(c) 2008 ush.it - a beautiful place. All rights reserved.

Hint: Tecniche di scanning

-sS	TCP SYN	>SYN <RST/SYN+ACK
-sT	TCP Connect()	>SYN <RST/SYN+ACK
-sW	TCP Window	>ACK <RST+WIN=0/4096
-sM	TCP Maimon	>ACK+FIN <RST/NULL
-sA	TCP ACK scan	>ACK <NULL/RST
-sU	UDP scan	>UDP <ICMP/NULL/DATA
-sN	TCP Null	>00000000 <RST/NULL
-sF	TCP FIN	>FIN <RST/NULL
-sX	TCP Xmas	>FIN+URG+PUSH <RST/NULL

…

Secrets of Network Cartography: A Comprehensive Guide to nmap
http://www.networkuptime.com/nmap/index.shtml

(c) 2008 ush.it - a beautiful place. All rights reserved.

Hint: Nmap

```
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sP: Ping Scan - go no further than determining if host is online
  -PN: Treat all hosts as online -- skip host discovery
  -PS/PA/PU [portlist]: TCP SYN/ACK or UDP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO [protocol list]: IP Protocol Ping
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  --top-ports <number>: Scan <number> most common ports
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
OS DETECTION:
  -O: Enable OS detection
```

(c) 2008 ush.it - a beautiful place. All rights reserved.

Hint: IDLE scan

http://seclists.org/bugtraq/1998/Dec/0079.html by Antirez
http://nmap.org/book/idlescan.html

Stealthy scan type that allows for a truly blind TCP port scan of the target and a mappin gout IP-based trust relationships between machines of the target network.

```
Nmap --help
  -sI <zombie host[:probeport]>: Idle scan
```

http://zzimma.antirez.com/post/Viva-Facebook-ovvero-storia-di-una-serata-milanese-di-10-anni-fa.html

(c) 2008 ush.it - a beautiful place. All rights reserved.

Hint: FTP bounce scan

Nmap script → ftp-bounce.nse
http://nmap.org/nsedoc/scripts/ftp-bounce.html

Checks to see if an FTP server allows port scanning using the FTP bounce method.

```
Nmap --help
  -b <FTP relay host>: FTP bounce scan
```

(c) 2008 ush.it - a beautiful place. All rights reserved.

Hint: ARP ping vs VPN interfaces

```
# ifconfig | grep "lo\|eth\|tun\|inet"
eth0      Link encap:Ethernet  HWaddr AA:BB:CC:DD:EE:FF
          inet addr:192.10.1.1  Bcast:192.10.1.255  eth0:7
 Link encap:Ethernet  HWaddr AA:BB:CC:DD:EE:FF
          inet addr:1.2.3.4  Bcast:1.255.255.255
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00
          inet addr:192.10.2.2  P-t-P:192.10.2.1
tun1      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00
          inet addr:10.1.0.1  P-t-P:10.1.0.2

# arping 10.1.0.1 -f
Unicast reply from 10.1.0.1 [AA:BB:CC:DD:EE:FF]  0.763ms
# arping 1.2.3.4 -f
Unicast reply from 1.2.3.4 [AA:BB:CC:DD:EE:FF]  0.798ms
# arping 192.10.1.1 -f
Unicast reply from 192.10.1.1 [AA:BB:CC:DD:EE:FF]  0.773ms
# arping 192.10.2.2 -f
Unicast reply from 192.10.2.2 [AA:BB:CC:DD:EE:FF]  0.773ms
```

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Enumeration 3/7

Always remember:

- Combinare tecniche diverse di scan.
- Scan progressivamente piu' dettagliati.
- Dumpare il (proprio) traffico, sempre.
- Banda satura → risultati meno affidabili.

Host Discovery with nmap by Mark Wolfgang, November 2002
http://moonpie.org/writings/discovery.pdf

FakeNetbiosDGM (NetBIOS Datagram)
FakeNetbiosNS (NetBIOS Name Service)
http://honeynet.rstack.org/tools.php

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Enumeration 4/7

Host fingerprinting, versioning, hostname e domain name:

L'hostname in particolare e' un'informazione fondamentale per comprendere il ruolo del sistema nella rete e puo' essere chiesto al target, chiesto ad un'altra macchina o puo' essere il target stesso a notificarlo (annunci, broadcast, ..).

L'hostname aiuta a comprendere anche come sono raggruppati tra di loro i sistemi (eg: DC01, DC02, ORA12, ..). Un host puo' avere piu' “alias” (vhost, domini, record dns, hostname e nomi impostati sui servizi e sulle applicazioni).

- Fingerprinting: p0f, nmap.
- Name e/o Versioning: DNS (dhcp), SNMP, RPC, Netbios (X-sharez, nbstat), IPX, WINS, HTTPS, ..

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Enumeration 5/7

Network topology discovery:

- Traceroute, TcpTraceroute.
- ICMP. (un ICMP type 13 con size superiore all'MTU di un certo hop puo' far si che uno dei router ritorni un pacchetto di errore “Frag needed and DF set”, ICMP Redirects, ..)
- Etherbat.

Quali sono i gateway? Quali gli IDS/IPS?

- Interfaccie promisque.
- Macchine che fanno IP Forwarding.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Hint: promisc detect

Nmap script → sniffer-detect.nse
http://nmap.org/nsedoc/scripts/sniffer-detect.html

Checks if a target on a local Ethernet has its network card in promiscuous mode.
http://www.securityfriday.com/promiscuous_detection_01.pdf.

```
Host script results:
|_ sniffer-detect: Likely in promiscuous mode (tests:
"11111111")
```

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Enumeration 6/7

Una volta identificati gli host.

Identificare un servizio:

- Porta. (nmap, /etc/services e simili)
- Banner.
- Risposta. (text vs binary; nmap, amap, amapcrap)

Connettersi ad un servizio:

- netcat (nc), sslclient
- Client nativo + wireshark/tcpdump

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Enumeration 7/7

Una volta effettuata una mappa quanto piu' precisa possibile di cio' da attaccare si passa ad una parte piu' attiva di enumeration che prende di mira i servizi che possono fornire informazioni aggiuntive e piu' specifiche.

Alcune tecniche di enumeration attive verranno esposte in seguito.

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Vulnerability scanning

Al termine della prima fase di discovery/enumeration/scanning e' opportuno lanciare in parallelo gli scanner automatici vista la durata del processo. E' opportuno non testare lo stesso servizio o host contemporaneamente con piu' tools e non saturare la banda altrimenti i risultati saranno meno attendibili.

Scanner automatici:

- Nessus. (una volta open, ora $ ma esiste un fork opensource: OpenVAS)
- GFI LANguard, ISS Internet Scanner, eEye Retina ($), Core Impact ($$), Qualys($$).
- X-Scan.
- MBSA (MS Windows).
- SAINT ($).
- Obsoleti: SARA, SATAN, ..

(c) 2008 ush.it - a beautiful place. All rights reserved.

diario.txt, come organizzarsi

Foglio di calcolo/TXT/DB Relazionale.

Host → OS, Host Name, Domain name, ..
Porta → Servizio, Demone, Versione, ..

Vulnerabilita' → Titolo, Descrizione, Note, Referenze, Exploit pubblici, Tools, ..

Exploitation → Console snapshots, Screenshots, Note, Riferimenti a file, .. (solo per PT)

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Checkpoint Enum.

Alla fine dell'enumeration al referente viene segnalato il risultato dell'operazione.

Contenuti del primo rapporto:

- Rapporto “Host discovery”.
- Segnalazione eventuali difficolta' tecniche.

Risposta al primo rapporto:

- Eventuali commenti del cliente.
- Eventuali incidenti.

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Qualificazione e quantificazione

Processo di verifica dell'esistenza di vulnerabilita' conosciute e relativi exploit o tools in grado di sfruttarle.

- google.com
- milw0rm.com
- packetstormsecurity.org
- archivi di FD (Full Disclosure), BT (BugTraq), Vulnwatch, ..
- secunia.com
- securityfocus.com
- osvdb.org (The Open Source Vulnerability Database)

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Ranking

Per ogni vulnerabilità identificata è necessario darne una valutazione in termini di criticità.

Esistono vari modelli:

DREAD Inventato da Michael Howard e David Le Blank

OWASP Ranking Sviluppato appositamente per la versione 2.0 della owasp testing guide

CVSS (Common Vulnerability Scoring System) è stato fino a poco tempo fa lo standard de facto

CVSSv2 il più utilizzato, è lo standard de facto

(c) 2008 ush.it - a beautiful place. All rights reserved.

Hint: Ranking CVSSv2 1/2

Diviso in:

Base Metrics. (Necessario, definisce le metriche di base)

Temporal Metrics. (Opzionale, definisce le metriche temporali)

Envirormental Metrics. (Opzionale, solo se definite le Temporal Metrics, definisce le metriche relative al contesto)

(c) 2008 ush.it - a beautiful place. All rights reserved.

Hint: Ranking CVSSv2 2/2

Base Score Metrics:

Exploitability Metrics

AccessVector – AccessComplexity – Authentication

Impact Metrics

ConfImpact – IntegImpact – AvailImpact

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Report e distribuibili

Componenti principali di un report distribuibile:

- Copertina con classificazione.
- Nota di riservatezza.
- Indice.
- Legenda dei simboli e delle convenzioni, glossario.
- Excecutive summary. (sunto di alto livello, destinato al management, con analisi storica quando possibile)
- Dettaglio dell'attivita'. (npt: per host, wapt: vhost, con cronologia)
- Remediation. (non sempre separato e sotto forma di remediation plan per I VA)

Anche nel caso di un PT puo' essere richiesto l'invio di un report in questa fase, il rischio e' che avvenga remediation o hardening prematuro.

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Deliverabile (dettaglio)

- IP
- Intervallo scansione (inizio, fine)
- Sistema operativo
- Vulnerabilita'
- Porta
- Descrizione
- Gravita' (ranking alto/medio/basso + CVSS)
- Referenze (CVE, BID)
- Rimedio
- Altri riferimenti

(c) 2008 ush.it - a beautiful place. All rights reserved.

VA: Remediation

Un remediation plan e' un'appendice che evidenzia gli step necessari ad eliminare le esposizioni evidenziate in un VA o PT.

Un buon tester e' spesso un buon sistemista e un buon sviluppatore, un'ottimo tester e' spesso un'ottimo sistemista e un'ottimo sviluppatore.

Fornire un remediation plan consistente e' uno degli indici di qualita' (se negli accordi).

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: Introduzione

Una volta effettuate le operazioni di discovery l'auditor tenta di ottenere informazioni con varie tecniche di enumerazione specifiche rispetto al singolo servizio.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: Public IP/Domains

$ whois example.com → registrant, admin, tech, registrar, ns
$ dig foo.example.com → 1.2.3.4
$ whois 1.2.3.4 → internet provider
$ resolveip 1.2.3.4 → reverse lookup (-;

Nmap script → Whois

http://nmap.org/nsedoc/scripts/whois.html
Queries the WHOIS services of Regional Internet Registries (RIR) and attempts to retrieve information about the IP Address Assignment which contains the Target IP Address.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: Finger (tcp/79)

“A program that displays information about a particular user or all users logged on the system, or a remote system. Typically shows full name, last login time, idle time, terminal line, and terminal location (where applicable).”

Nmap script → finger.nse

http://nmap.org/nsedoc/scripts/finger.html
Attempts to retrieve a list of usernames using the finger service.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: Ident (tcp/113)

The Identification Protocol provides a means to determine the identity of a user of a particular TCP connection. Given a TCP port number pair, it returns a character string which identifies the owner of that connection on the server's system.

Nmap script → auth-owners.nse

http://nmap.org/nsedoc/scripts/auth-owners.html
Attempts to find the owner of an open TCP port by querying an auth (identd - port 113) daemon which must also be open on the target system.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: RPC (tcp/111)

rpcclient, rpcinfo, Perl DCE::RPC

Nmap -sR (RPCGrind Scan)

Nmap script → rpcinfo.nse

http://nmap.org/nsedoc/scripts/rpcinfo.html
Connects to portmapper and fetches a list of all registered programs.

http://www.nessus.org/plugins/index.php?view=single&id=11111
http://www.nessus.org/plugins/index.php?view=single&id=10763
http://www.nessus.org/plugins/index.php?view=single&id=10223
http://www.nessus.org/plugins/index.php?view=single&id=20759
http://www.nessus.org/plugins/index.php?view=single&id=22319
http://www.nessus.org/plugins/index.php?view=single&id=25248

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: SNMP (tcp/161-162)

Comandi: snmpbulkget, snmpbulkwalk, snmpget, snmpgetnext, snmpinform, snmpset, snmpnetstat, snmpstatus, snmptable, snmptest, snmptranslate, snmptrap, **snmpwalk**, ..

Nmap script → snmp-sysdescr.nse

http://nmap.org/nsedoc/scripts/snmp-sysdescr.html
Attempts to extract system information from an SNMP version 1 service.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: DNS (tcp-udp/53)

AXFR

“AXFR is a mechanism for replicating DNS data across DNS servers. If, for example, the yale.edu administrator has two DNS servers, a.ns.yale.edu and b.ns.yale.edu, he can edit the yale.edu data on a.ns.yale.edu, and rely on AXFR to pull the same data to b.ns.yale.edu. [..]”

http://cr.yp.to/djbdns/axfr-notes.html
$ dig AXFR example.com @ns.example.com

Nmap script → dns-zone-transfer.nse

http://nmap.org/nsedoc/scripts/dns-zone-transfer.html
Requests a zone transfer (AXFR) from a DNS server.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: SMTP (tcp/25) 1/2

VRFY, EXPN, AUTH (secondo l'implementazione)

```
VRFY jones
250 jones@heaven.af.mil
VRFY smith
250 Locksmith <pick@heaven.af.mil>
VRFY foo
550 foo... User unknown


EXPN all
250-George Washington <george@wash.dc.gov>
250-Thomas Jefferson <tj@wash.dc.gov>
```

Medusa Parallel Network Login Auditor
http://www.foofus.net/jmk/medusa/medusa.html

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: SMTP (tcp/25) 2/2

Nmap script → smtp-commands.nse

http://nmap.org/nsedoc/scripts/smtp-commands.html
Attempts to use EHLO and HELP to gather the Extended commands supported by an SMTP server.

Demoni con implementazioni vulnerabili a leak di informazioni (es: messaggio di errore specifico per l'utente inesistente rispetto un errore generico di fallita autenticazione).

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: POP (tcp/110)

Nmap script → pop3-capabilities.nse

http://nmap.org/nsedoc/scripts/pop3-capabilities.html
Retrieves POP3 email server capabilities.

Demoni con implementazioni vulnerabili a leak di informazioni (es: messaggio di errore specifico per l'utente inesistente rispetto un errore generico di fallita autenticazione).

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: Netbios (tcp/137-139) 1/4

Nmap script → nbstat.nse

http://nmap.org/nsedoc/scripts/nbstat.html
Attempt's to retrieve the target's NetBIOS names and MAC address.

Nmap script → smb-enum-domains.nse

http://nmap.org/nsedoc/scripts/smb-enum-domains.html
Attempts to enumerate domains on a system, along with their policies.

Nmap script → smb-enum-sessions.nse

http://nmap.org/nsedoc/scripts/smb-enum-sessions.html
Enumerates the users logged into a system either locally, through a remote desktop client (terminal services), or through a SMB share.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: Netbios (tcp/137-139) 2/4

Nmap script → smb-enum-shares.nse

http://nmap.org/nsedoc/scripts/smb-enum-shares.html
Attempts to list shares using the srvsvc.NetShareEnumAll MSRPC function, then retrieve more information about each share using srvsvc.NetShareGetInfo.

Nmap script → smb-enum-users.nse

http://nmap.org/nsedoc/scripts/smb-enum-users.html
Attempts to enumerate the users on a remote Windows system, with as much information as possible.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: Netbios (tcp/137-139) 3/4

Nmap script → smb-os-discovery.nse

http://nmap.org/nsedoc/scripts/smb-os-discovery.html
Attempts to determine the operating system over the SMB protocol (ports 445 and 139).

Nmap script → smb-security-mode.nse

http://nmap.org/nsedoc/scripts/smb-security-mode.html
Returns information about the SMB security level determined by SMB.

Nmap script → smb-server-stats.nse

http://nmap.org/nsedoc/scripts/smb-server-stats.html
Attempts to grab the server's statistics over SMB and MSRPC.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: Netbios (tcp/137-139) 4/4

Nmap script → smb-system-info.nse

http://nmap.org/nsedoc/scripts/smb-system-info.html
Pulls back information about the remote system from the registry. Getting all of the information requires an administrative account, although a user account will still get a lot of it. Guest probably won't get any, nor will anonymous. This goes for all operating systems, including Windows 2000.

Windows Vista doesn't appear to have the WINREG binding (or it's different and I don't know it), so this doesn't support Vista at all.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: Apple Talk

The Apple Talk Protocol suite includes the following protocols:

AARP	AppleTalk Address Resolution Protocol
DDP	Datagram Delivery Protocol
RTMP	Routing Table Maintenance Protocol
AEP	AppleTalk Echo Protocol
ATP	AppleTalk Transaction Protocol
NBP	Name-Binding Protocol
ZIP	Zone Information Protocol
ASP	AppleTalk Session Protocol
PAP	Printer Access Protocol
ADSP	AppleTalk Data Stream Protocol
AFP	AppleTalk Filing Protocol

http://www.protocols.com/pbook/appletalk.htm

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: ICMP, Network stack

Internet Control Message Protocol

Nmap -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes

Nmap -sO: IP protocol scan

“ICMP Clock Synchronization”

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: Oracle

NGSSQuirrel for Oracle, Oscanner,
Oracle Auditing Tools (OAT), ..

Oracle TNS Listener Security

http://www.integrigy.com/security-resources/whitepapers/Integrigy_Oracle_Listener_TNS_Security.pdf

Lsnrctl (native)

http://www.oracleutilities.com/OSUtil/listener.html

Tnscmd (perl hack)

http://www.jammed.com/~jwa/hacks/security/tnscmd/tnscmd-doc.html

Oracle Ports for Network Services

http://www.chebucto.ns.ca/~rakerman/oracle-port-table.html

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: MS SQL (tcp/1433-1434)

NGSSQuirrel for MS SQL
NGSSQLCrack

Nmap script → ms-sql-info.nse

http://nmap.org/nsedoc/scripts/ms-sql-info.html
Attempts to extract information from Microsoft SQL Server instances.

Microsoft SQL Audit
(MS SQL Server Pinger, MS SQL Server Auditor) ($)

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: MySQL (tcp/3306)

DB Audit
http://www.softtreetech.com/idbaudit.htm

Nmap script → mysql-info.nse

http://nmap.org/nsedoc/scripts/mysql-info.html
Connects to a MySQL server and prints information such as the protocol and version numbers, thread ID, status, capabilities, and the password salt.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: HTTP (Vhost discovery)

Redirect sia nei response header http, Location:,
o a livello applicativo, meta redirect nell'<head>,
come JavaScript o semplice link.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: SSL (Vhost discovery)

Connettendosi ad un IP verso un servizio con SSL viene spesso presentato un certificato con come CN (Common Name) l'hostname o il dominio dell'applicazione.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: UPNP

Nmap script → upnp-info.nse

http://nmap.org/nsedoc/scripts/upnp-info.html

Attempts to extract system information from the UPnP service.

```
|  upnp-info:  System/1.0 UPnP/1.0 IGD/1.0
|_ Location: http://192.168.1.1:80/UPnP/IGD.xml
```

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: DHCP

Dynamic Host Configuration Protocol

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: NFS

List exported shares

showmount -e <server>

http://www.nessus.org/plugins/index.php?view=single&id=10437
http://www.nessus.org/plugins/index.php?view=single&id=11356
http://www.nessus.org/plugins/index.php?view=single&id=15984

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: TIME/DAYTIME

Time (tcp/37) → RFC-868

nc nist1.symmetricom.com 37 | hexdump

Daytime (tcp/13) → RFC-867

Nmap script → daytime.nse

http://nmap.org/nsedoc/scripts/daytime.html
Retrieves the day and time from the UDP Daytime service.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: NTP

“NTP è un protocollo per sincronizzare gli orologi dei computer all'interno di una rete [..]”

ntptrace - trace a chain of NTP servers back to the primary source

Net::NNTP - NNTP Client class

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: PPTP

Point-to-Point Tunneling Protocol
(tcp/1723) → RFC-2637

“A protocol which allows the Point to Point Protocol (PPP) to be tunneled through an IP network.”

Nmap script → pptp-version.nse

http://nmap.org/nsedoc/scripts/pptp-version.html
Attempts to extract system information from the point-to-point tunneling protocol (PPTP) service.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: HTTP

Siete invitati al terzo seminario della giornata per l'approfondimento di questo argomento.

Nmap scripts:

http://nmap.org/nsedoc/scripts/html-title.html
http://nmap.org/nsedoc/scripts/http-auth.html
http://nmap.org/nsedoc/scripts/robots.txt.html

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: so much to know

“too much technology, in too little time. And little by little ... we went insane.”

.aware - awarenetwork.org

ipp, mdns, rip, http, web app leaks, applications leak, proxy and reverse proxy, ..

(c) 2008 ush.it - a beautiful place. All rights reserved.

Enum: Considerazioni

Molte delle informazioni la cui estrazione e' stata esposta all'interno di questo capitolo rappresentano autonomamente vulnerabilita' di impatto in genere LOW appartenenti alla categoria Information leak.

All'interno del report devono essere segnalate e nella parte relativa alla Remediation e' opportuno indicare quali step sono necessari alla soluzione della vulnerabilita'.

(c) 2008 ush.it - a beautiful place. All rights reserved.

PT: Definizione 1/2

“è la metodologia di valutazione della sicurezza di un sistema o di una rete che simula l'attacco di un utente malintenzionato [..]”

Penetration tester, Auditor, Ethical Hacker, Tiger Team, .. (esecutore/i)

Black Box, White Box, Gray Box, .. (tipologie)

(c) 2008 ush.it - a beautiful place. All rights reserved.

PT: Definizione 2/2

Il PT e' quindi una “simulazione”:

Lo sforzo va dimensionato secondo il rischio e le risorse dell'attaccante che si vuole simulare. (eg: banca vs chiosco dei gelati)

Un PT ha un tempo minimo per risultare efficace.

Vi e' comunque una distorsione tra un reale attacco e un prodotto di IT Security. (no report, no coverage, etc)

(c) 2008 ush.it - a beautiful place. All rights reserved.

PT: Componenti principali

Target acquisition
Vulnerability Assessment
Vulnerability exploitation
Report-writing
Post-test consultation

http://www.penetration-testing-group.co.uk/ip.htm

(c) 2008 ush.it - a beautiful place. All rights reserved.

Hint: White Papers introduttivi

An Introduction to Network Vulnerability Testing

http://www.verisign.com.sg/guide/mss/vulnerabilitytest.pdf

Your First Penetration Test (Watchfire)

http://www.corecom.com/external/livesecurity/pentest.html

“There are many competent security auditing companies willing and able to perform penetration tests for you. You can find some of the most competent testers in some of the smaller companies. Investigate carefully. [..]”

Guide to IT Security Services

http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf

(c) 2008 ush.it - a beautiful place. All rights reserved.

PT: Scouting

Come visto nella slide “VA: Qualificazione e quantificazione” anche in un PT e' importante identificare le vulnerabilita' conosciute.

Dato pero' che un PT comprende anche la ricerca e lo sfruttamento di vulnerabilita' non conosciute e' bene che l'auditor faccia ricerche storiche sulle vulnerabilita' e sulle problematiche di servizi e demoni simili per meglio comprendere le aree di criticita' e direzionare i propri sforzi.

(c) 2008 ush.it - a beautiful place. All rights reserved.

NPT: Definizione

Network Penetration Test

Information Systems Security Assessment Framework (ISSAF)
http://www.oissg.org/content/view/71/71/

OSSTMM - Open Source Security Testing Methodology Manual
http://www.isecom.org/osstmm/

(c) 2008 ush.it - a beautiful place. All rights reserved.

NPT: Azioni 1/3

Bruteforcing: e' un attacco contro l'autenticazione di un sistema (normalmente una coppia utente:password). Normalmente time consuming e potenzialmente controproducente.

Il bruteforcing va effettuato in quattro livelli di intensita' crescente: default password, password deboli, dizionario, calcolo combinatorio/rcerca esaustiva.

(c) 2008 ush.it - a beautiful place. All rights reserved.

NPT: Azioni 2/3

Misconfiguration: Tende ad identificare e sfruttare l'errata configurazione di un servizio tale che sia possibile compiere delle azioni utili ai fini dell'attivita'.

La mancanza di autenticazione e' l'esempio classico di misconfiguration.

(c) 2008 ush.it - a beautiful place. All rights reserved.

NPT: Azioni 3/3

Exploitation: E' l'atto di sfruttare manualmente o attraverso l'uso di tool ed exploit una data vulnerabilita'.

Il penetration tester deve essere in grado di capire, modificare e verificare gli strumenti di terze parti oltre che crearne di nuovi secondo necessita'.

(c) 2008 ush.it - a beautiful place. All rights reserved.

NPT: Priorita'

Una delle abilita' fondamentali di un penetration tester e' quella di comprendere nel periodo limitato di tempo dell'attivita come priorizzare il proprio lavoro.

(c) 2008 ush.it - a beautiful place. All rights reserved.

NPT: Una bella verita'

I penetration test non vengono fatti dai tools e non sono automatizzabili. Gli attaccanti non sono tool e non sono automatici!

Un PT e' un prodotto artigianale il cui livello qualitativo e' determinato dall'esperienza e creativita' del tester.

(c) 2008 ush.it - a beautiful place. All rights reserved.

NPT: Alla ricerca dell'entry point

Applicazioni, utenze e sistemi informatici sono spesso in “trust” tra di loro.

- Trust relations
- Password reuse
- Password discovery
- “Domini” (Active directory, LDAP, NIS, Kerberos)

Distributed Metastasis: A Computer Network Penetration Methodology
(Andrew J. Stewart, August 12, 1999)
http://www.cs.umbc.edu/cadip/docs/NetworkIntrusion/distributed_metastasis.pdf
http://www.phrack.com/issues.html?issue=55&id=16

(c) 2008 ush.it - a beautiful place. All rights reserved.

NPT: Multilayered security issues

(Macchina A) Applicazione web Apache/Tomcat → Arbitrary file read “news.jsp?id=123&theme=../file.ext%00” → Password dell'utenza DB backend → (Macchina B) Exploitation post-auth del DBMS “Oracle 10g R1 xDb.XDB_PITRIG_PKG.PITRIG_DROP” → Accesso locale come utente Oracle (Java + .rhost) → Local privilege escalation “Solaris 10 libnspr” → Zone evasion telnet -l"-fuser" master → 0wn di tutti gli altri containers “zoneadm list -cv” + “zlogin -C -e\@ zone1” → NFS EMC^2 → Distributed Metastasis

(c) 2008 ush.it - a beautiful place. All rights reserved.

NPT: Frameworks

Esistono vari “exploitation framework”:

- Metasploit
- Immunity Canvas ($) *1
- Core Impact ($)

Exploit packs:

- D2 Exploitation Pack (http://www.d2sec.com/products.htm) *1
- Gleg Ltd's VulnDisco (http://gleg.net/vulndisco_pack_professional.shtml) *1
+ Argeniss Ultimate 0day Exploits Pack (http://www.argeniss.com/products.html)
- Underground, Ricerca, Gruppi, Honeypots, Web exploit packs, ..

(c) 2008 ush.it - a beautiful place. All rights reserved.

NPT: Toolbox

La toolbox del penetration tester:

- Centinaia di tools. (solo i tools a noi utili e di cui conosciamo l'utilizzo e l'effetto, quando possibile scegliere prodotti di cui sia disponibile il sorgente)

- Linux e MS Windows su due workstation fisiche.

- Decine di OS installati nelle loro varie versioni e service packs in comode VMs.

- Decine di applicazioni installate nelle VM.

(c) 2008 ush.it - a beautiful place. All rights reserved.

NPT: Documenti prodotti (Report, ..)

Il report di un NPT e' simile a quello del VA con l'eccezione che per ogni vulnerabilita' va specificato se si e' tentato o meno l'exploiting e se questo ha avuto esito positivo.

In tal caso vanno presentati i vari console snapshot e screenshot oltre che la descrizione del risultato conseguito e dell'impatto che ne deriva.

Si tende ad includere solamente le vulnerabilita' che sono state effettivamente sfruttare.

(c) 2008 ush.it - a beautiful place. All rights reserved.

NPT: Remediation

E' il capitolo del report in cui viene spiegata la soluzione consigliata alle vulnerabilita' (tutte o alcune).

Scritto per essere letto dai tecnici ed implementato.

Top 5 Things You Should Do With Your Penetration Test Results

(Punto 3: Work with your administrators and developers to build a remediation plan, then execute that plan.)
http://www.hurricanelabs.com/november2008_story_1

(c) 2008 ush.it - a beautiful place. All rights reserved.

WAPT: Definizione

Web Application Penetration Test

OWASP Testing Project

http://www.owasp.org/index.php/Category:OWASP_Testing_Project

Web Application Security Consortium (WASC)

http://www.webappsec.org/

(c) 2008 ush.it - a beautiful place. All rights reserved.

WAPT: Vettori di attacco 1.0

- Cross Site Scripting (XSS)
- Injection Flaws
- Malicious File Execution
- Insecure Direct Object Reference
- Cross Site Request Forgery (CSRF)
- Information Leakage and Improper Error Handling
- Broken Authentication and Session Management
- Insecure Cryptographic Storage
- Insecure Communications
- Failure to Restrict URL Access

Owasp Top 10 2007
http://www.owasp.org/index.php/Top_10_2007

(c) 2008 ush.it - a beautiful place. All rights reserved.

WAPT: Vettori di attacco 2.0

- Cross-site scripting in AJAX
- XML poisoning
- Malicious AJAX code execution
- RSS / Atom injection
- WSDL scanning and enumeration
- Client side validation in AJAX routines
- Web services routing issues
- Parameter manipulation with SOAP
- XPATH injection in SOAP message
- RIA thick client binary manipulation

Top 10 Web 2.0 Attack Vectors
http://www.net-security.org/article.php?id=949&p=1

(c) 2008 ush.it - a beautiful place. All rights reserved.

WAPT: Toolbox

Curl, wget, nc, ..

Firefox + Firebug + Venkman + TamperData + Live HTTP Headers + Hacker bar + ..

Web scarab, Burp Proxy, ..

Owasp CAL9000, OWASP DirBuster, XSS Cheat sheets (Rsnake), ..

sqlmap, sqlninja, ..

(c) 2008 ush.it - a beautiful place. All rights reserved.

CR: Definizione

“Code review is systematic examination (often as peer review) of computer source code intended to find and fix mistakes overlooked in the initial development phase, improving both the overall quality of software and the developers' skills.”

OWASP Code Review Project
http://www.owasp.org/index.php/Category:OWASP_Code_Review_Project

(c) 2008 ush.it - a beautiful place. All rights reserved.

CR: In sintesi

Siete invitati al terzo seminario della giornata per l'approfondimento di questo argomento.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Bug hunting

Siete invitati al terzo seminario della giornata per l'approfondimento di questo argomento.

(c) 2008 ush.it - a beautiful place. All rights reserved.

Grazie

HTTP → ush.it

Mail → {ascii@ush.it, s4tan@ush.it}

(c) 2008 ush.it - a beautiful place. All rights reserved.