



Laboratorio di sicurezza dei protocolli di rete - lab_000

19 Gennaio 2007

**Master in progettazione e gestione di
sistemi di rete - III edizione**



Dipartimento di
Informatica



Benvenuti!

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica





Alessio L.R. Pennasilico

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica





Alessio L.R. Pennasilico

Lab_000 Sicurezza dei Protocolli

Security Evangelist @ Alba S.T.



Dipartimento di
Informatica





Alessio L.R. Pennasilico

Lab_000 Sicurezza dei Protocolli

Security Evangelist @ Alba S.T.

Member / Board of Directors:



Dipartimento di
Informatica





Alessio L.R. Pennasilico

Lab_000 Sicurezza dei Protocolli



Dipartimento di Informatica

Security Evangelist @ Alba S.T.

Member / Board of Directors:

AIP, AIPSI, CaCert, CLUSIT, HPP, ILS, IT-ISAC, LUGVR, OPSI, Metro Olografix, No1984.org, OpenBeer/OpenGeeks, Recursiva.org, Sikurezza.org, Spippolatori, VoIPSA, Thawte.





Il programma del laboratorio di sicurezza dei protocolli



Agenda lab 000

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

□ Presentazione



- Presentazione
- DLGs 196/03



- Presentazione
- DLGs 196/03
- Penetration Test



- Presentazione
- DLGs 196/03
- Penetration Test
- Gestione di una CA





Agenda lab 001

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

Agenda lab 001

Lab_000 Sicurezza dei Protocolli

- La posta elettronica
 - servizi in plain-text
 - servizi con SSL



Dipartimento di
Informatica

Agenda lab 001

- ❑ La posta elettronica
 - ❑ servizi in plain-text
 - ❑ servizi con SSL

- ❑ Crittografia Personale
 - ❑ GPG
 - ❑ S/MIME





Agenda lab 010

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

- Gestione delle Patch
 - WSUS



- Gestione delle Patch
 - WSUS

- Gestione di un Antivirus
 - Trendmicro





Agenda lab 011

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

- Ruleset di un Firewall



- Ruleset di un Firewall
 - OpenBSD e PF.





Agenda lab 100

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

- Creazione e gestione di VPN



- ❑ Creazione e gestione di VPN
 - ❑ OpenBSD ed ISAKMPD





Agenda lab 101

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

- Hardening di una infrastruttura
VoIP basata su SIP





Lab_000 Sicurezza dei Protocolli

Laboratorio 000



Dipartimento di
Informatica

- Presentazione
- DLGs 196/03
- Penetration Test
- Gestione di una CA





Presentazione

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

Nome



Dipartimento di
Informatica

Nome

Conoscenze pregresse



Nome

Conoscenze pregresse

Esperienze precedenti



- Presentazione
- DLGs 196/03
- Penetration Test
- Gestione di una CA





La situazione in Italia

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

In Italia esiste il DLG.s 196/03 che impartisce sia delle linee guida sul come gestire il trattamento dei dati.





In Italia esiste il DLG.s 196/03 che impartisce sia delle linee guida sul come gestire il trattamento dei dati. L'allegato B inoltre definisce le misure tecniche "minime" di sicurezza da rispettare.



Dati personali

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica



b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;



Dati sensibili

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica



d) "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;



Dati Giudiziari

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica



e) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualita' di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;



Misure minime

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

✓ Redazione del DPS



Misure minime

Lab_000 Sicurezza dei Protocolli

- ✓ Redazione del DPS
- ✓ Antivirus aggiornato ogni 3/6 mesi



Dipartimento di
Informatica

Misure minime

Lab_000 Sicurezza dei Protocolli

- ✓ Redazione del DPS
- ✓ Antivirus aggiornato ogni 3/6 mesi
- ✓ Backup giornaliero/settimanale



Dipartimento di
Informatica

Misure minime

- ✓ Redazione del DPS
- ✓ Antivirus aggiornato ogni 3/6 mesi
- ✓ Backup giornaliero/settimanale
- ✓ Firewall aggiornato ogni 3/6 mesi



Misure minime

- ✓ Redazione del DPS
- ✓ Antivirus aggiornato ogni 3/6 mesi
- ✓ Backup giornaliero/settimanale
- ✓ Firewall aggiornato ogni 3/6 mesi
- ✓ Password di almeno 8 caratteri



Misure minime

- ✓ Redazione del DPS
- ✓ Antivirus aggiornato ogni 3/6 mesi
- ✓ Backup giornaliero/settimanale
- ✓ Firewall aggiornato ogni 3/6 mesi
- ✓ Password di almeno 8 caratteri
- ✓ Patch ogni 3/6 mesi



Misure minime vs. idonee

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

Le misure “minime” di sicurezza devono sempre essere rispettate.



Le misure “minime” di sicurezza devono sempre essere rispettate.

Tuttavia la legge stessa “suggerisce” di adottare misure “idonee” a proteggere i dati in nostro possesso.





La sicurezza

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

La sicurezza non è un prodotto.





La sicurezza

**La sicurezza non è un prodotto.
La sicurezza è un processo
continuo.**

- Presentazione
- DLGs 196/03
- Penetration Test
- Gestione di una CA





Vulnerability Assessment

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica



Si tratta di una procedura atta ad individuare “possibili” vulnerabilità presenti sulla rete attraverso l’utilizzo di tool automatici che confrontano quel che trovano con un database di vulnerabilità conosciute.



PenTest

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica



Durante un PT è ammessa ogni azione reale concordata con il cliente. La vulnerabilità viene realmente sfruttata per verificarla.



Durante un PT è ammessa ogni azione reale concordata con il cliente. La vulnerabilità viene realmente sfruttata per verificarla.

Non si escludono tentativi di social-engineering, accessi dalla rete wifi, ...



Metodologie

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

E' fondamentale utilizzare uno standard per eseguire le verifiche, per renderle valutabili e ripetibili.





E' fondamentale utilizzare uno standard per eseguire le verifiche, per renderle valutabili e ripetibili.

Lo standard più accreditato ad oggi è OSSTMM di ISECOM.



Nessus

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica



Nessus è un programma multiplatforma, opensource, che esegue un network scan e confronta i servizi rilevati con un database di vulnerabilità conosciute.



Report

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica



Nessus non è molto preciso, ma permette, in modo chiassoso, di ottenere molte informazioni con poca fatica.



Nessus non è molto preciso, ma permette, in modo chiassoso, di ottenere molte informazioni con poca fatica.

Il report prodotto non deve essere considerato “finale” ma deve essere rivisto e verificato da una persona competente.



Nessus non è molto preciso, ma permette, in modo chiassoso, di ottenere molte informazioni con poca fatica.

Il report prodotto non deve essere considerato “finale” ma deve essere rivisto e verificato da una persona competente.

Può essere considerato un buon inizio per un VA, o utilizzato nella prima fase di un PT.



LAB

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica



➔ Avviare VMware

- ➔ Avviare VMware
- ➔ Eseguire la macchina virtuale “Linux”



- ➔ Avviare VMware
- ➔ Eseguire la macchina virtuale “Linux”
- ➔ Installare ed eseguire il server Nessus



- ➔ Avviare VMware
- ➔ Eseguire la macchina virtuale “Linux”
- ➔ Installare ed eseguire il server Nessus
- ➔ Configurare il server Nessus



- ➔ Avviare VMware
- ➔ Eseguire la macchina virtuale “Linux”
- ➔ Installare ed eseguire il server Nessus
- ➔ Configurare il server Nessus
- ➔ Installare ed eseguire la console Nessus



- ➔ Avviare VMware
- ➔ Eseguire la macchina virtuale “Linux”
- ➔ Installare ed eseguire il server Nessus
- ➔ Configurare il server Nessus
- ➔ Installare ed eseguire la console Nessus
- ➔ dare il target





- ➔ Avviare VMware
- ➔ Eseguire la macchina virtuale “Linux”
- ➔ Installare ed eseguire il server Nessus
- ➔ Configurare il server Nessus
- ➔ Installare ed eseguire la console Nessus
- ➔ dare il target
- ➔ visualizzare il report



Analisi del report

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

Leggiamo assieme e commentiamo il report generato.





- Presentazione
- DLGs 196/03
- Penetration Test
- Gestione di una CA



Traffico in chiaro

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica



Tutto il traffico in transito su Internet può facilmente essere visualizzato e modificato da qualsiasi nodo attraversato dal traffico stesso.



Utilizzo della crittografia

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

I certificati provvederanno a garantire che il traffico non sia stato modificato in transito, fosse protetto da occhi indiscreti e provenisse da chi ci aspettavamo.





Il problema dei certificati

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

Il problema dei certificati

Chiunque può generare dei certificati
atti a proteggere la comunicazione.



Il problema dei certificati

Chiunque può generare dei certificati atti a proteggere la comunicazione.

E' necessario stabilire un metodo per verificare che il certificato del sito www.alba.st sia davvero il certificato di Alba e non un certificato generato da altri a nome di Alba.

Il problema dei certificati

Chiunque può generare dei certificati atti a proteggere la comunicazione.

E' necessario stabilire un metodo per verificare che il certificato del sito www.alba.st sia davvero il certificato di Alba e non un certificato generato da altri a nome di Alba.



Certification Authority

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

Un documento di identità è valido per convenzione: viene accettato poiché emesso da un ente di cui tutti abbiamo deciso di fidarci, in virtù dei controlli che esegue per emetterlo.





Un documento di identità è valido per convenzione: viene accettato poiché emesso da un ente di cui tutti abbiamo deciso di fidarci, in virtù dei controlli che esegue per emetterlo.

Le CA emettono certificati ritenuti validi per lo stesso motivo.



Crittografia

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica



Ogni infrastruttura o comunicazione sicura, che utilizzi la crittografia si basa su un elemento “segreto”, password o certificato che sia riconosciuto come valido da tutti i device coinvolti nella comunicazione.



Scambio chiavi

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica



Lo scambio di questa “password” è la fase più critica: chi dovesse intercettare lo scambio potrebbe poi “ascoltare” la comunicazione.



Chiave asimmetriche

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

Chiave asimmetriche

Avere una chiave “privata” ed una “pubblica” ci preserva dai rischi dello scambio della password/chiave.



Avere una chiave “privata” ed una “pubblica” ci preserva dai rischi dello scambio della password/chiave.

Solo noi possediamo la nostra chiave privata, la nostra chiave pubblica viene pubblicata su Internet a disposizione di chi vuole parlare con noi.



LAB

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica



- Avviare la macchina Windows di VMware

- ➔ Avviare la macchina Windows di VMware
- ➔ Verificare il contenuto del traffico HTTP



- Avviare la macchina Windows di VMware
- Verificare il contenuto del traffico HTTP
 - installare ed eseguire wireshark/ethereal



- Avviare la macchina Windows di VMware
- Verificare il contenuto del traffico HTTP
 - installare ed eseguire wireshark/ethereal
- Generare una richiesta di certificato da IIS



- ➔ Avviare la macchina Windows di VMware
- ➔ Verificare il contenuto del traffico HTTP
 - ➔ installare ed eseguire wireshark/ethereal
- ➔ Generare una richiesta di certificato da IIS
- ➔ Inoltrare la richiesta alla CA





- ➔ Avviare la macchina Windows di VMware
- ➔ Verificare il contenuto del traffico HTTP
 - ➔ installare ed eseguire wireshark/ethereal
- ➔ Generare una richiesta di certificato da IIS
- ➔ Inoltrare la richiesta alla CA
- ➔ Approvare la richiesta dalla MC della CA



- ➔ Avviare la macchina Windows di VMware
- ➔ Verificare il contenuto del traffico HTTP
 - ➔ installare ed eseguire wireshark/ethereal
- ➔ Generare una richiesta di certificato da IIS
- ➔ Inoltrare la richiesta alla CA
- ➔ Approvare la richiesta dalla MC della CA
- ➔ Installare il certificato ottenuto su IIS



- ➔ Avviare la macchina Windows di VMware
- ➔ Verificare il contenuto del traffico HTTP
 - ➔ installare ed eseguire wireshark/ethereal
- ➔ Generare una richiesta di certificato da IIS
- ➔ Inoltrare la richiesta alla CA
- ➔ Approvare la richiesta dalla MC della CA
- ➔ Installare il certificato ottenuto su IIS
- ➔ Verificare di nuovo il contenuto del traffico HTTP

Bibliografia

<http://www.alba.st/>

<http://www.mayhem.hk/>

<http://www.matteoflora.com/>

<http://www.camera.it/parlam/leggi/deleghe/Testi/03196dl.htm>

<http://www.isecom.org/osstmm/>

<http://www.mediaservice.net/>

<http://www.nessus.org/>

<http://www.thawte.com/repository/index.html>

Grazie ad Andrea Lisi <http://www.scint.it/> per l'idea di scrat :)





Conclusioni

Lab_000 Sicurezza dei Protocolli



Dipartimento di
Informatica

Conclusioni

- ✓ La sicurezza non è un prodotto ma un processo



Conclusioni

- ✓ La sicurezza non è un prodotto ma un processo
- ✓ Adeguarsi alla legge è necessario, ma non sufficiente



Conclusioni

- ✓ La sicurezza non è un prodotto ma un processo
- ✓ Adeguarsi alla legge è necessario, ma non sufficiente
- ✓ Le verifiche di sicurezza vanno fatte periodicamente e secondo procedure adeguate e standardizzate



Grazie!

Queste slide sono disponibili su

<http://www.scienze.univr.it/fol/main?ent=avvisoin&cs=105>

Per domande od approfondimenti:

alessio@alba.st



Dipartimento di
Informatica

These slides written by
Alessio L.R. Pennasilico
aka mayhem. They are
subjected to Creative
Commons Attribution-
ShareAlike 2.5 version;
you can copy, modify,
sell. "Please" cite your
source and use the same
licence :)