Registri Distributi & Proxy

Gregorio D'Agostino

31 Maggio 2021

Agenda

- Esercitazione
- Registri condivisi
- Attacchi e difesa
- Anche i manager sbagliano
- Proxy
- Sicurezza al livello trasporto TLS

Violazioni Etiche (Ethical Hacking)

- Abbiamo visto la volta scorsa alcuni comandi di linea che possono aiutare a violare i siti. In particolare il comando nstat.

Violazioni Etiche (Ethical Hacking)

- Abbiamo visto la volta scorsa alcuni comandi di linea che possono aiutare a violare i siti. In particolare il comando nstat.
- Esistono gli Hacking Tools, (potremmo tradurre "strumenti di violazione") che aiutano l'hacker non professionista a violare (o tentare di) i siti.
- Gli "hacker tools" forniscono un'interfaccia grafica con cui chiunque può porre in atto gli attacchi più comuni: line injection; command injection etc. Basta che vi sia un programma attivo on line (anche solo ping o smpt per la posta) che usa PHP o MySQL o qualunque altro server noto.

Violazioni Etiche (Ethical Hacking)

- Abbiamo visto la volta scorsa alcuni comandi di linea che possono aiutare a violare i siti. In particolare il comando nstat.
- Esistono gli Hacking Tools, (potremmo tradurre "strumenti di violazione") che aiutano l'hacker non professionista a violare (o tentare di) i siti.
- Gli "hacker tools" forniscono un'interfaccia grafica con cui chiunque può porre in atto gli attacchi più comuni: line injection; command injection etc. Basta che vi sia un programma attivo on line (anche solo ping o smpt per la posta) che usa PHP o MySQL o qualunque altro server noto.
- I tentativi di violazione possono anche essere perpetrati autonomamente dal gestore del sistema o da un professionista autorizzato. In questo caso si tratta di "Ethical Hacking"

Violazioni Etiche (Ethical Hacking)

- Abbiamo visto la volta scorsa alcuni comandi di linea che possono aiutare a violare i siti. In particolare il comando nstat.
- Esistono gli Hacking Tools, (potremmo tradurre "strumenti di violazione") che aiutano l'hacker non professionista a violare (o tentare di) i siti.
- Gli "hacker tools" forniscono un'interfaccia grafica con cui chiunque può porre in atto gli attacchi più comuni: line injection; command injection etc. Basta che vi sia un programma attivo on line (anche solo ping o smpt per la posta) che usa PHP o MySQL o qualunque altro server noto.
- I tentativi di violazione possono anche essere perpetrati autonomamente dal gestore del sistema o da un professionista autorizzato. In questo caso si tratta di "Ethical Hacking"
- Adesso vedremo uno strumento pubblico che chiunque può utilizzare per analizzare la propria rete:nmap

Violazioni Etiche (Ethical Hacking)

- Abbiamo visto la volta scorsa alcuni comandi di linea che possono aiutare a violare i siti. In particolare il comando nstat.
- Esistono gli Hacking Tools, (potremmo tradurre "strumenti di violazione") che aiutano l'hacker non professionista a violare (o tentare di) i siti.
- Gli "hacker tools" forniscono un'interfaccia grafica con cui chiunque può porre in atto gli attacchi più comuni: line injection; command injection etc. Basta che vi sia un programma attivo on line (anche solo ping o smpt per la posta) che usa PHP o MySQL o qualunque altro server noto.
- I tentativi di violazione possono anche essere perpetrati autonomamente dal gestore del sistema o da un professionista autorizzato. In questo caso si tratta di "Ethical Hacking"
- Adesso vedremo uno strumento pubblico che chiunque può utilizzare per analizzare la propria rete:nmap
- Si tratta di un software open source scaricabile al sito https://nmap.org/download.html. In particolare lo strumento dotato dell'interfaccia grafica per l'utente GUI (Graphic User

Violare (hackerare) un sito o un nodo (host)

- L'ispezione delle porte aperte è di solito il primo passo per un attacco; in genere poi si provano le principali vulnerabilità note o se ne cercano nuove.

Violare (hackerare) un sito o un nodo (host)

- L'ispezione delle porte aperte è di solito il primo passo per un attacco; in genere poi si provano le principali vulnerabilità note o se ne cercano nuove.
- Per trovare nuove vulnerabilità tipicamente si forniscono input al server al di fuori di quanto previsto dal programmatore e questo consente accesso ad aree di memoria che dovrebbero essere irraggiungibili.

Violare (hackerare) un sito o un nodo (host)

- L'ispezione delle porte aperte è di solito il primo passo per un attacco; in genere poi si provano le principali vulnerabilità note o se ne cercano nuove.
- Per trovare nuove vulnerabilità tipicamente si forniscono input al server al di fuori di quanto previsto dal programmatore e questo consente accesso ad aree di memoria che dovrebbero essere irraggiungibili.
- Ma si possono utilizzare le vulnerabilità note se il gestore del sistema non ha ancora installato le patch.

Violare (hackerare) un sito o un nodo (host)

- L'ispezione delle porte aperte è di solito il primo passo per un attacco; in genere poi si provano le principali vulnerabilità note o se ne cercano nuove.
- Per trovare nuove vulnerabilità tipicamente si forniscono input al server al di fuori di quanto previsto dal programmatore e questo consente accesso ad aree di memoria che dovrebbero essere irraggiungibili.
- Ma si possono utilizzare le vulnerabilità note se il gestore del sistema non ha ancora installato le patch.
- Per avere una lista di comuni "hacker tools" (strumenti grafici per violare i siti) basta cercare queste parole su un motore di ricerca.

Violare (hackerare) un sito o un nodo (host)

- L'ispezione delle porte aperte è di solito il primo passo per un attacco; in genere poi si provano le principali vulnerabilità note o se ne cercano nuove.
- Per trovare nuove vulnerabilità tipicamente si forniscono input al server al di fuori di quanto previsto dal programmatore e questo consente accesso ad aree di memoria che dovrebbero essere irraggiungibili.
- Ma si possono utilizzare le vulnerabilità note se il gestore del sistema non ha ancora installato le patch.
- Per avere una lista di comuni "hacker tools" (strumenti grafici per violare i siti) basta cercare queste parole su un motore di ricerca.
- L'esistenza degli "hacker tools", che sono in aumento, ha ampliato il numero di potenziali attaccanti.

Esercitazione con Zenmap

- Vediamo zenmap in azione sulle mie macchine.

Registri Distribuiti

- La Blockchain è una tecnologia informatica usata per sedimentare informazioni in ordine cronologico irreversibile. Ogni evento fa riferimento al precedente in modo inalterabile. Si tratta di un registro (pubblico) condiviso distribuito e rappresenta un esempio di tecnologia per i registri distribuiti DLT (Distributed Ledger Technology)

Registri Distribuiti

- La Blockchain è una tecnologia informatica usata per sedimentare informazioni in ordine cronologico irreversibile. Ogni evento fa riferimento al precedente in modo inalterabile. Si tratta di un registro (pubblico) condiviso distribuito e rappresenta un esempio di tecnologia per i registri distribuiti DLT (Distributed Ledger Technology)
- Facendo una foto con la copertina di un giornale ci si assicura che essa sia successiva alla data di pubblicazione. L'analogo informatico (più sofisticato) è la blockchain.

Registri Distribuiti

- La Blockchain è una tecnologia informatica usata per sedimentare informazioni in ordine cronologico irreversibile. Ogni evento fa riferimento al precedente in modo inalterabile. Si tratta di un registro (pubblico) condiviso distribuito e rappresenta un esempio di tecnologia per i registri distribuiti DLT (Distributed Ledger Technology)
- Facendo una foto con la copertina di un giornale ci si assicura che essa sia successiva alla data di pubblicazione. L'analogo informatico (più sofisticato) è la blockchain.
- Per realizzare una blockchain occorrono un gruppo di soggetti paritetici (peer) che condividono le stesse informazioni (anche tramite canali non protetti) e un algoritmo di hash per marcare indelebilmente i messaggi.

Registri Distribuiti -cont

- Ad ogni evento da condividere corrisponde un blocco che aggiunge in input il blocco precedente e la data e aggiunge in output il digest della sequenza totale. Ogni volta che uno dei pari verifica il blocco aggiunge la sua firma.

Registri Distribuiti -cont

- Ad ogni evento da condividere corrisponde un blocco che aggiunge in input il blocco precedente e la data e aggiunge in output il digest della sequenza totale. Ogni volta che uno dei pari verifica il blocco aggiunge la sua firma.
- Dopo aver creato un blocco e condiviso non è più possibile modificare i contenuti precedenti, ovvero lo si potrebbe fare se fossimo in grado di alterare il contenuto mantenendo lo stesso hash.

Registri Distribuiti -cont

- Ad ogni evento da condividere corrisponde un blocco che aggiunge in input il blocco precedente e la data e aggiunge in output il digest della sequenza totale. Ogni volta che uno dei pari verifica il blocco aggiunge la sua firma.
- Dopo aver creato un blocco e condiviso non è più possibile modificare i contenuti precedenti, ovvero lo si potrebbe fare se fossimo in grado di alterare il contenuto mantenendo lo stesso hash.
- La tecnologia DLT dei registri distribuiti (in particolare Blockchain) si sta diffondendo molto velocemente e viene adottata per garantire l'inalterabilità dei contenuti (a meno che tutti i pari siano daccordo per riscriverli).

Registri Distribuiti -cont

- Ad ogni evento da condividere corrisponde un blocco che aggiunge in input il blocco precedente e la data e aggiunge in output il digest della sequenza totale. Ogni volta che uno dei pari verifica il blocco aggiunge la sua firma.
- Dopo aver creato un blocco e condiviso non è più possibile modificare i contenuti precedenti, ovvero lo si potrebbe fare se fossimo in grado di alterare il contenuto mantenendo lo stesso hash.
- La tecnologia DLT dei registri distribuiti (in particolare Blockchain) si sta diffondendo molto velocemente e viene adottata per garantire l'inalterabilità dei contenuti (a meno che tutti i pari siano daccordo per riscriverli).
- La tecnologia non garantisce che il contenuto dei blocchi sia veritiero, ma ne impedisce le future manipolazioni: garantisce la cosiddetta Non ripudiation.

Applicazioni della Blockchain

- Registro aziendale verificato da fornitori e clienti. Si crea una lista di operazioni ordinate per gestire un'azienda. Ad esempio le provenienze delle merci o i trattamenti da esse subiti. Una volta condivisa l'n-esimo blocco, non si può più modificarlo a meno di trovare un blocco con lo stesso digest. Se una azienda farmaceutica dichiara di aver ricevuto una partita di un prodotto chimico in una certa data, poi non può più dichiarare il contrario.

Applicazioni della Blockchain

- Registro aziendale verificato da fornitori e clienti. Si crea una lista di operazioni ordinate per gestire un'azienda. Ad esempio le provenienze delle merci o i trattamenti da esse subiti. Una volta condivisa l'n-esimo blocco, non si può più modificarlo a meno di trovare un blocco con lo stesso digest. Se una azienda farmaceutica dichiara di aver ricevuto una partita di un prodotto chimico in una certa data, poi non può più dichiarare il contrario.
- Un'altra applicazione possibile è una emeroteca: basta che ci sia un altro soggetto che condivide le copie dei giornali e non è più possibile modificarle.

Applicazioni della Blockchain

- Registro aziendale verificato da fornitori e clienti. Si crea una lista di operazioni ordinate per gestire un'azienda. Ad esempio le provenienze delle merci o i trattamenti da esse subiti. Una volta condivisa l'n-esimo blocco, non si può più modificarlo a meno di trovare un blocco con lo stesso digest. Se una azienda farmaceutica dichiara di aver ricevuto una partita di un prodotto chimico in una certa data, poi non può più dichiarare il contrario.
- Un'altra applicazione possibile è una emeroteca: basta che ci sia un altro soggetto che condivide le copie dei giornali e non è più possibile modificarle.
- Praticamente qualunque registro può essere garantito.

Applicazioni della Blockchain

- Registro aziendale verificato da fornitori e clienti. Si crea una lista di operazioni ordinate per gestire un'azienda. Ad esempio le provenienze delle merci o i trattamenti da esse subiti. Una volta condivisa l'n-esimo blocco, non si può più modificarlo a meno di trovare un blocco con lo stesso digest. Se una azienda farmaceutica dichiara di aver ricevuto una partita di un prodotto chimico in una certa data, poi non può più dichiarare il contrario.
- Un'altra applicazione possibile è una emeroteca: basta che ci sia un altro soggetto che condivide le copie dei giornali e non è più possibile modificarle.
- Praticamente qualunque registro può essere garantito.
- L'applicazione più famosa è Bitcoin una criptovaluta definita dal suo autore Satoshi Nakamoto "A Peer-to-Peer Electronic Cash System"

Bitcoin

- Dato il blocco n-esimo se un componente della catena trova un blocco fittizio aggiuntivo in modo tale che il digest risultante inizi con i primi k bit nulli (ad esempio 128). Questo elemento è un bit-coin.

Bitcoin

- Dato il blocco n-esimo se un componente della catena trova un blocco fittizio aggiuntivo in modo tale che il digest risultante inizi con i primi k bit nulli (ad esempio 128). Questo elemento è un bit-coin.
- Essendo difficili da ottenere, come per le opere d'arte, si attribuisce ai bit-coin un valore.

Bitcoin

- Dato il blocco n-esimo se un componente della catena trova un blocco fittizio aggiuntivo in modo tale che il digest risultante inizi con i primi k bit nulli (ad esempio 128). Questo elemento è un bit-coin.
- Essendo difficili da ottenere, come per le opere d'arte, si attribuisce ai bit-coin un valore.
- Le transazioni con cui si condividono i bit-coin o le operazioni di compra-vendita vengono realizzate con una blockchain. La hash function utilizzata è sha-512.

Bitcoin

- Dato il blocco n-esimo se un componente della catena trova un blocco fittizio aggiuntivo in modo tale che il digest risultante inizi con i primi k bit nulli (ad esempio 128). Questo elemento è un bit-coin.
- Essendo difficili da ottenere, come per le opere d'arte, si attribuisce ai bit-coin un valore.
- Le transazioni con cui si condividono i bit-coin o le operazioni di compra-vendita vengono realizzate con una blockchain. La hash function utilizzata è sha-512.
- Adesso i bitcoin vengono anche quotati in borsa e il loro prezzo è molto volatile.

Valore economico dei Bitcoin

- I bitcoin non sono una vera valuta, sono come i punti delle compagnie aeree o dei supermercati: si possono convertire in beni o servizi, ma non si potrebbero utilizzare per pagare prestazioni di lavoro o altro. In realtà vengono spesso utilizzati anche come valuta, violando di fatto le leggi.

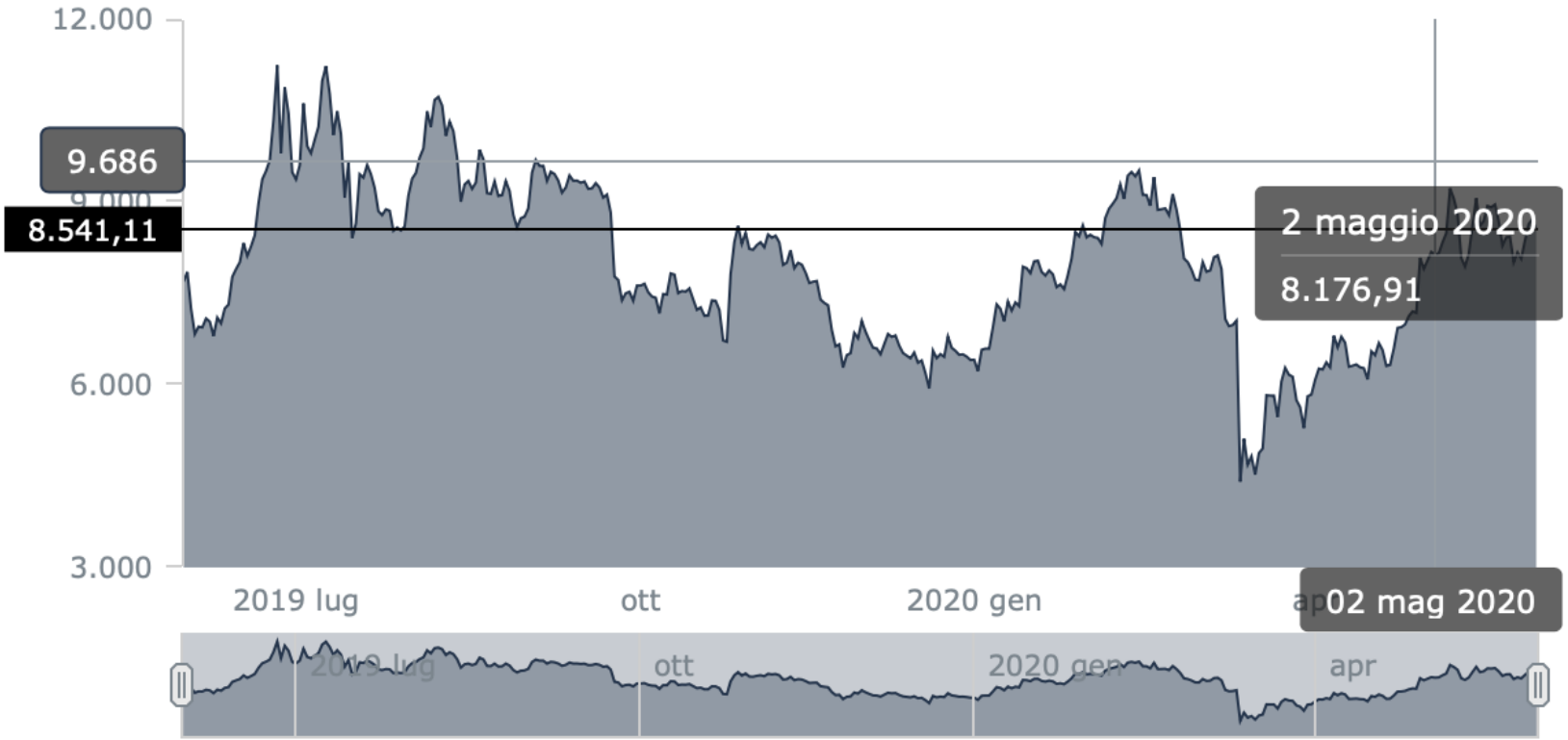
Valore economico dei Bitcoin

- I bitcoin non sono una vera valuta, sono come i punti delle compagnie aeree o dei supermercati: si possono convertire in beni o servizi, ma non si potrebbero utilizzare per pagare prestazioni di lavoro o altro. In realtà vengono spesso utilizzati anche come valuta, violando di fatto le leggi.
- La lunghezza della sequenza degli zeri da ottenere è modificata da coloro che gestiscono il sistema a cui si registrano tutti i pari. Durante il tempo questa lunghezza si è sempre allungata e quindi ottenere un bitcoin per ispezione diretta (si dice mining) è diventato sempre più oneroso computazionalmente.

Valore economico dei Bitcoin

- I bitcoin non sono una vera valuta, sono come i punti delle compagnie aeree o dei supermercati: si possono convertire in beni o servizi, ma non si potrebbero utilizzare per pagare prestazioni di lavoro o altro. In realtà vengono spesso utilizzati anche come valuta, violando di fatto le leggi.
- La lunghezza della sequenza degli zeri da ottenere è modificata da coloro che gestiscono il sistema a cui si registrano tutti i pari. Durante il tempo questa lunghezza si è sempre allungata e quindi ottenere un bitcoin per ispezione diretta (si dice mining) è diventato sempre più oneroso computazionalmente.
- Oggi, il tempo di calcolo per produrre un bitcoin richiede un grande dispendio di energia elettrica e l'allocazione di risorse di calcolo, quindi sono nati dei malware (criptominer) che fanno eseguire i calcoli per trovare il blocco il cui digest ha la proprietà voluta da una rete di bot infetta. Si tratta di un esempio illegale di parasitic computing, in questo caso, un grid computing (calcolo distribuito in rete) non autorizzato.

Quotazioni in borsa dei Biticoin



*I dati intraday e in tempo reale sono tratti dalle quotazioni di prodotti OTC.

Dati completi Bitcoin/Euro (BTC/EUR)

Contratti elettronici

- Basandosi su una criptovaluta (o comuqnue sullo scambio di tokens a cui i pari attribuiscono un valore), è possibile rendere automatico il pagamento al conseguimento di un risultato verificabile informaticamente. Si fa eseguire un codice concordato dalle parti e verificato in modalità registro distribuito il cui punto di uscita al conseguimento di un risultato è la transazione della criptovaluta (o i token). Questi programmi vengono denominati Contratti elettronici.

Contratti elettronici

- Basandosi su una criptovaluta (o comuqnue sullo scambio di tokens a cui i pari attribuiscono un valore), è possibile rendere automatico il pagamento al conseguimento di un risultato verificabile informaticamente. Si fa eseguire un codice concordato dalle parti e verificato in modalità registro distribuito il cui punto di uscita al conseguimento di un risultato è la transazione della criptovaluta (o i token). Questi programmi vengono denominati Contratti elettronici.
- In realtà non sono veri contratti perché non si registrano dal notaio e non sono soggetti a modifiche future in itinere.

Contratti elettronici

- Basandosi su una criptovaluta (o comuqnue sullo scambio di tokens a cui i pari attribuiscono un valore), è possibile rendere automatico il pagamento al conseguimento di un risultato verificabile informaticamente. Si fa eseguire un codice concordato dalle parti e verificato in modalità registro distribuito il cui punto di uscita al conseguimento di un risultato è la transazione della criptovaluta (o i token). Questi programmi vengono denominati Contratti elettronici.
- In realtà non sono veri contratti perché non si registrano dal notaio e non sono soggetti a modifiche future in itinere.
- Il termine contratto elettronico tende ad essere utilizzato in senso lato indicando un codice che regola gli scambi tra soggetti in maniera inalterabile dalle parti. Il grande difetto è che se si è commesso un errore di programmazione le criptovalute che vengono immobilizzate a garanzia del pagamento non sono più stornabili (nelle versioni attuali).

Sniffing

- Il termine sniffing indica un particolare tipo di origliamento (eavedropping) fatto a tappeto su una rete (o una parte di essa) o un server.

Sniffing

- Il termine sniffing indica un particolare tipo di origliamento (eavedropping) fatto a tappeto su una rete (o una parte di essa) o un server.
- Di solito lo sniffing consiste nel creare una banca dati (log) delle comunicazioni origliate in rete.

Sniffing di reti ad Hub

- Una rete ad hub, è una rete senza switch ma solo con ripetitori a stella (o ad albero) che al più amplificano il segnale.

Sniffing di reti ad Hub

- Una rete ad hub, è una rete senza switch ma solo con ripetitori a stella (o ad albero) che al più amplificano il segnale.
- Per sniffare una rete ad hub, basta porre la propria scheda di rete in modalità "promiscua". Normalmente per risparmiare risorse di calcolo la scheda di rete ignora tutti i frame che sono indirizzati a MAC diversi. in modalità "promiscua" invece si continua a rispondere solo ai propri frame, ma gli altri si leggono e memorizzano.

Sniffing di reti ad Hub

- Una rete ad hub, è una rete senza switch ma solo con ripetitori a stella (o ad albero) che al più amplificano il segnale.
- Per sniffare una rete ad hub, basta porre la propria scheda di rete in modalità "promiscua". Normalmente per risparmiare risorse di calcolo la scheda di rete ignora tutti i frame che sono indirizzati a MAC diversi. in modalità "promiscua" invece si continua a rispondere solo ai propri frame, ma gli altri si leggono e memorizzano.
- Il contenuto dei frame viene poi analizzato, catalogato e memorizzato.

Sniffing di reti con switch

- Le reti normalmente hanno dei meccanismi di "switching" (istradamento al livello data-link cioè scelta della porta dove inoltrare i frame) realizzati dagli switch che inoltrano il traffico solo in alcune porte. Quindi riceviamo solo una parte limitata del traffico al livello data-link.

Sniffing di reti con switch

- Le reti normalmente hanno dei meccanismi di "switching" (istradamento al livello data-link cioè scelta della porta dove inoltrare i frame) realizzati dagli switch che inoltrano il traffico solo in alcune porte. Quindi riceviamo solo una parte limitata del traffico al livello data-link.
- Per realizzare lo sniffing occorre ingannare gli switch fingendo di avere degli ip diversi. Questo si realizza tramite il protocollo ARP (Address Resolution Protocol) ed in particolare la tecnica è detta ARP Poisoning (avvelenamento dell'ARP). Il protocollo ARP associa agli IP l'indirizzo fisico MAC.

Sniffing di reti con switch

- Le reti normalmente hanno dei meccanismi di "switching" (istradamento al livello data-link cioè scelta della porta dove inoltrare i frame) realizzati dagli switch che inoltrano il traffico solo in alcune porte. Quindi riceviamo solo una parte limitata del traffico al livello data-link.
- Per realizzare lo sniffing occorre ingannare gli switch fingendo di avere degli ip diversi. Questo si realizza tramite il protocollo ARP (Address Resolution Protocol) ed in particolare la tecnica è detta ARP Poisoning (avvelenamento dell'ARP). Il protocollo ARP associa agli IP l'indirizzo fisico MAC.
- In pratica si realizza uno spooffing al livello IP. Questo è possibile perché ogni switch ha le sue tabelle di conversione ARP (ARP Tables) che possono essere continuamente aggiornate senza una verifica da parte di una authorità certificante.

Sniffing di reti con switch

- Le reti normalmente hanno dei meccanismi di "switching" (istradamento al livello data-link cioè scelta della porta dove inoltrare i frame) realizzati dagli switch che inoltrano il traffico solo in alcune porte. Quindi riceviamo solo una parte limitata del traffico al livello data-link.
- Per realizzare lo sniffing occorre ingannare gli switch fingendo di avere degli ip diversi. Questo si realizza tramite il protocollo ARP (Address Resolution Protocol) ed in particolare la tecnica è detta ARP Poisoning (avvelenamento dell'ARP). Il protocollo ARP associa agli IP l'indirizzo fisico MAC.
- In pratica si realizza uno spooffing al livello IP. Questo è possibile perché ogni switch ha le sue tabelle di conversione ARP (ARP Tables) che possono essere continuamente aggiornate senza una verifica da parte di una authorità certificante.
- Basta dire allo switch con cui si comunica normalmente che il nostro IP è associato al MAC address di un gataway e riceveremo il traffico ad esso destinato.

Sniffing di reti con switch

- Ovviamente bisogna essere in grado di gestire il traffico come se si fosse veramente il gataway. Si devono ricopiare i pacchetti e instradarli come se si fosse il vero routing.

Sniffing di reti con switch

- Ovviamente bisogna essere in grado di gestire il traffico come se si fosse veramente il gataway. Si devono ricopiare i pacchetti e instradarli come se si fosse il vero routing.
- Un metodo più diretto per realizzare lo sniffing consiste nel mettere un malware nel router che esegue il monitoraggio, filtra i messaggi interessanti ed invia il contenuto ad un nodo di raccolta.

Contromisure allo spooffing

- Lo spooffing può servire anche solo a realizzare un MIM (Man in the Middle) su uno specifico nodo non necessariamente un gataway o un server di rete. In ogni caso esistono delle contromisure.

Contromisure allo spooffing

- Lo spooffing può servire anche solo a realizzare un MIM (Man in the Middle) su uno specifico nodo non necessariamente un gataway o un server di rete. In ogni caso esistono delle contromisure.
- La più semplice contromisura consiste nell'eseguire dei controlli sulle tabelle temporanee dell'ARP fissando che alcuni indirizzi sono riservati o anche assegnare dei valori fissi di MAC ad ogni canale fisico di comunicazione. Realizzare un log dei cambiamenti di IP consente l'analisi ex post ma non risolve il problema.

Contromisure allo spooffing

- Lo spooffing può servire anche solo a realizzare un MIM (Man in the Middle) su uno specifico nodo non necessariamente un gataway o un server di rete. In ogni caso esistono delle contromisure.
- La più semplice contromisura consiste nell'eseguire dei controlli sulle tabelle temporanee dell'ARP fissando che alcuni indirizzi sono riservati o anche assegnare dei valori fissi di MAC ad ogni canale fisico di comunicazione. Realizzare un log dei cambiamenti di IP consente l'analisi ex post ma non risolve il problema.
- Esiste un protocollo ethernet specifico di identificazione (al livello data-link) detto 802.1x che chiede delle credenziali per l'attribuzione di un mac address e la conseguente attivazione delle comunicazioni. Utilizzando tale protocollo ad ogni variazione di IP si evita lo sniffing di rete.

Spoofing a vari livelli

- Lo spooffing può essere realizzato a diversi livelli DATA-LINK, IP, name.

Spoofing a vari livelli

- Lo spooffing può essere realizzato a diversi livelli DATA-LINK, IP, name.
- Al livello data-link si inganna lo switch prendendo un falso MAC address.

Spoofing a vari livelli

- Lo spooffing può essere realizzato a diversi livelli DATA-LINK, IP, name.
- Al livello data-link si inganna lo switch prendendo un falso MAC address.
- Al livello IP bisogna impadronirsi di un falso IP, ma poi fare in modo da far pervenire ugualmente il traffico al destinatario.

Spoofing a vari livelli

- Lo spooffing può essere realizzato a diversi livelli DATA-LINK, IP, name.
- Al livello data-link si inganna lo switch prendendo un falso MAC address.
- Al livello IP bisogna impadronirsi di un falso IP, ma poi fare in modo da far pervenire ugualmente il traffico al destinatario.
- Al livello name bisogna ingannare i DNS server associando il proprio IP al name che si intende origliare.

Spoofing a vari livelli

- Lo spooffing può essere realizzato a diversi livelli DATA-LINK, IP, name.
- Al livello data-link si inganna lo switch prendendo un falso MAC address.
- Al livello IP bisogna impadronirsi di un falso IP, ma poi fare in modo da far pervenire ugualmente il traffico al destinatario.
- Al livello name bisogna ingannare i DNS server associando il proprio IP al name che si intende origliare.
- Ricorrendo alle autorità di certificazione si evitano gli ultimi due.

Errori comuni di gente famosa

- Anche Mark Zukerberg (co-fondatore di Facebook) ha usato una password facile dadada. Notizia del corriere della Sera dell'otto giugno 2016:
  Hacker violano la password di Zuckerberg: era ¡¡ dadada ¿¿
  Quali sono le 25 password più usate
  di Massimo Sideri
  Attacco mirato perché reiterato sulla stessa username di una stessa piattaforma.

Gli intermediari: Proxy

- Nelle applicazioni in rete spesso si utilizzano degli "intermediari" (proxy) cioè delle piattaforme intermedie per realizzare le proprie attività. In particolare le comunicazioni in rete possono essere sempre realizzate tramite queste piattaforme che fanno le veci di altri.

Gli intermediari: Proxy

- Nelle applicazioni in rete spesso si utilizzano degli "intermediari" (proxy) cioè delle piattaforme intermedie per realizzare le proprie attività. In particolare le comunicazioni in rete possono essere sempre realizzate tramite queste piattaforme che fanno le veci di altri.
- Nella comunicazioni con l'esterno il gestore di una LAN può richiedere l'obbligo di passare attraverso un proxy dove vengono filtrate le attività consentite e tracciate le richieste accettate e non. Il passaggio attraverso u proxy può consentire di aggirare un firewall o evitare il passaggio attraverso un nodo indesiderato (perché infetto o di dubbia reputazione). I proxy possono essere utilizzati anche per forzare l'istradamento dei messaggi secondo certe rotte.

Altri proxy

- Un altro tipo di proxy sono i reverse proxy (proxy inversi) che consentono (in modo trasparente) di potenziare le attività di un server (ad esempio http) condividendo una parte del carico delle attività. Ad esempio google, facebook ed altri motori di ricerca o social network possono basarsi su proxy.

Altri proxy

- Un altro tipo di proxy sono i reverse proxy (proxy inversi) che consentono (in modo trasparente) di potenziare le attività di un server (ad esempio http) condividendo una parte del carico delle attività. Ad esempio google, facebook ed altri motori di ricerca o social network possono basarsi su proxy.
- Gli open proxy sono delle piattaforme che consento a tutti, tramite un cambiamento di socket (coppia IP, porta) di nascondere l'origine dei pacchetti. Vi sono dei fornitori di servizio che (a pagamento) consentono l'anonimato della navigazione. In alcuni casi sono distribuiti sulla rete in modo che il traffico richiesto dall'utente venga distribuito anche geograficamente. Vengono spesso utilizzati per ingannare i motori di ricerca oppure per anonimizzare il richiedente di un servizio di rete.

Altri proxy

- Un altro tipo di proxy sono i reverse proxy (proxy inversi) che consentono (in modo trasparente) di potenziare le attività di un server (ad esempio http) condividendo una parte del carico delle attività. Ad esempio google, facebook ed altri motori di ricerca o social network possono basarsi su proxy.
- Gli open proxy sono delle piattaforme che consento a tutti, tramite un cambiamento di socket (coppia IP, porta) di nascondere l'origine dei pacchetti. Vi sono dei fornitori di servizio che (a pagamento) consentono l'anonimato della navigazione. In alcuni casi sono distribuiti sulla rete in modo che il traffico richiesto dall'utente venga distribuito anche geograficamente. Vengono spesso utilizzati per ingannare i motori di ricerca oppure per anonimizzare il richiedente di un servizio di rete.
- Per migliorare la tracciabilità dei pacchetti alcuni siti non consentono accesso a pacchetti provenienti da open proxy.

Altri proxy -cont

- Allo stesso modo un router in uscita può impedire tramite un firewall di collegarsi ad un proxy esterno.

Altri proxy -cont

- Allo stesso modo un router in uscita può impedire tramite un firewall di collegarsi ad un proxy esterno.
- Affinché una piattaforma agisca da proxy (ed in particolare da open proxy) è necessario che sia installato un applicativo che gestisce il traffico.

Altri proxy -cont

- Allo stesso modo un router in uscita può impedire tramite un firewall di collegarsi ad un proxy esterno.
- Affinché una piattaforma agisca da proxy (ed in particolare da open proxy) è necessario che sia installato un applicativo che gestisce il traffico.
- Esistono molti proxy di uso comune anche basati su software open source ad esempio HTTP Proxy (webcaches) e HTTP Server Web Apache, SQUID (web proxy gnu).

Altri proxy -cont

- Allo stesso modo un router in uscita può impedire tramite un firewall di collegarsi ad un proxy esterno.
- Affinché una piattaforma agisca da proxy (ed in particolare da open proxy) è necessario che sia installato un applicativo che gestisce il traffico.
- Esistono molti proxy di uso comune anche basati su software open source ad esempio HTTP Proxy (webcaches) e HTTP Server Web Apache, SQUID (web proxy gnu).
- Quando l'installazione avviene tramite malware e contro la volontà del gestore, della piattaforma questa viene denominata zombie.

Altri proxy SOCKS

- SOCKS è un abbreviazione di SOCKetS (unione IP e porta).

Altri proxy SOCKS

- SOCKS è un abbreviazione di SOCKetS (unione IP e porta).
- I proxy SOCKS sono studiati specificamente per superare eventuali firewall che impediscono il routing diretto tra due IP.

Altri proxy SOCKS

- SOCKS è un abbreviazione di SOCKetS (unione IP e porta).
- I proxy SOCKS sono studiati specificamente per superare eventuali firewall che impediscono il routing diretto tra due IP.
- Il server sul proxy SOCKS richiede una autenticazione, quindi non si violano le restrizioni poste in atto dai gestori delle reti coinvolte.

Transport Layer Security (TLS)

- Il TLS è un insieme di dispositivi di sicurezza che si colloca sopra il livello trasporto (quindi si basa su TCP) e consente autenticazione, integrità dei dati e confidenzialità (cifratura). Il protocollo standard venne definito da IETF (Internet Engineering Task Force ieft.org) nel documento RFC5246 (https://tools.ietf.org/html/rfc5246).

Transport Layer Security (TLS)

- Il TLS è un insieme di dispositivi di sicurezza che si colloca sopra il livello trasporto (quindi si basa su TCP) e consente autenticazione, integrità dei dati e confidenzialità (cifratura). Il protocollo standard venne definito da IETF (Internet Engineering Task Force ieft.org) nel documento RFC5246 (https://tools.ietf.org/html/rfc5246).
- Il protocollo realizza una sessione tra un client ed un server e segue la logica venditore-cliente, quindi il meccanismo base di autenticazione è unilaterale cioè solo il server si autentica verso il client. Il venditore (server) dimostra l'autenticità dei propri prodottti, non il cliente. Esistono comunque meccanismi che consentono anche al server di richiedere l'autenticazione del client.

Transport Layer Security (TLS)

- Il TLS è un insieme di dispositivi di sicurezza che si colloca sopra il livello trasporto (quindi si basa su TCP) e consente autenticazione, integrità dei dati e confidenzialità (cifratura). Il protocollo standard venne definito da IETF (Internet Engineering Task Force ieft.org) nel documento RFC5246 (https://tools.ietf.org/html/rfc5246).
- Il protocollo realizza una sessione tra un client ed un server e segue la logica venditore-cliente, quindi il meccanismo base di autenticazione è unilaterale cioè solo il server si autentica verso il client. Il venditore (server) dimostra l'autenticità dei propri prodottti, non il cliente. Esistono comunque meccanismi che consentono anche al server di richiedere l'autenticazione del client.
- Il server invia un certificato digitale al client che lo verifica utilizzando la chiave pubblica del server disponbile presso una autorità certificante. Il certificato fornito dall'autorità certificante associa IP, url (Uniform Resource Locator descrittore univoco risorsa di rete) e la chiave pubblica.

Certificati

- I certificati rilasciati dalla autorità di certificazione sono di due tipi: SSL Domain Validated (DV) e SSL Organization Validated (OV)

Certificati

- I certificati rilasciati dalla autorità di certificazione sono di due tipi: SSL Domain Validated (DV) e SSL Organization Validated (OV)
- SSL DV certifica solo che il dominio è stato venduto ad un soggetto ed è depositato, ma non si fanno controlli sull'organizzazione.

Certificati

- I certificati rilasciati dalla autorità di certificazione sono di due tipi: SSL Domain Validated (DV) e SSL Organization Validated (OV)
- SSL DV certifica solo che il dominio è stato venduto ad un soggetto ed è depositato, ma non si fanno controlli sull'organizzazione.
- SSL OV certifica che esiste l'azienda e che è regolarmente registrata alla camera di commercio o all'agenzia delle entrate, certifica la Personalità giuridica (Legal entity)

Certificati

- I certificati rilasciati dalla autorità di certificazione sono di due tipi: SSL Domain Validated (DV) e SSL Organization Validated (OV)
- SSL DV certifica solo che il dominio è stato venduto ad un soggetto ed è depositato, ma non si fanno controlli sull'organizzazione.
- SSL OV certifica che esiste l'azienda e che è regolarmente registrata alla camera di commercio o all'agenzia delle entrate, certifica la Personalità giuridica (Legal entity)
- Chiunque scaricando la suite openssl (open source) può creare e gestire un sito di certificazione e distribuire certificati digitali.

Garanzia delle società di certificazione

- In Italia l'AGID (Agenzia per l'Italia digitale) ha il compito di accreditare le società di certificazione. L'ente vigila sulla serietà delle società e sui metodi utilizzati per la certificazione.

Garanzia delle società di certificazione

- In Italia l'AGID (Agenzia per l'Italia digitale) ha il compito di accreditare le società di certificazione. L'ente vigila sulla serietà delle società e sui metodi utilizzati per la certificazione.
- Le società più famose in Italia sono: Poste Italiane, Infocert, Aruba, etc

Garanzia delle società di certificazione

- In Italia l'AGID (Agenzia per l'Italia digitale) ha il compito di accreditare le società di certificazione. L'ente vigila sulla serietà delle società e sui metodi utilizzati per la certificazione.
- Le società più famose in Italia sono: Poste Italiane, Infocert, Aruba, etc
- Global Sign è una società di certificazione internazionale che https://www.globalsign.com/en/; un altra economica è GeoTrust Global CA etc. Le più famose sono: Comodo, Let?s Encrypt, Symantec, digicert etc.

URL Uniform Resource Locator

- Come abbiamo visto, un URL (Uniform Resource Locator) è una sequenza di caratteri che consente di raggiungere in modo univoco qualsiasi documento in rete.

URL Uniform Resource Locator

- Come abbiamo visto, un URL (Uniform Resource Locator) è una sequenza di caratteri che consente di raggiungere in modo univoco qualsiasi documento in rete.
- Il formato generico di un url è il seguente (alcuni campi possono mancare):
  protocollo://<username:password@>nomehost
  <:porta></percorso><?querystring><#fragment
  identifier>
  http://gordion.casaccia.enea.it/SicurezzaInformatica/
  Lectures/Lesson0x-congruences.pdf

URL Uniform Resource Locator

- Come abbiamo visto, un URL (Uniform Resource Locator) è una sequenza di caratteri che consente di raggiungere in modo univoco qualsiasi documento in rete.
- Il formato generico di un url è il seguente (alcuni campi possono mancare):
  protocollo://<username:password@>nomehost
  <:porta></percorso><?querystring><#fragment identifier>
  http://gordion.casaccia.enea.it/SicurezzaInformatica/Lectures/Lesson0x-congruences.pdf
- Il protocollo può essere http, ftp, https, mms (protocollo microsoft unicast sulla porta 1755). In alcuni vecchi protocolli come ftp si possono mettere le credenziali in chiaro ma è sconsigliato ed in disuso. Il nome del dominio è necessario, mentre gli altri campi sono opzionali.

Applicazioni del TLS

- Il TLS è utilizzato come supporto per il protocollo https, per la posta elettronica (identificazione dei mail servers) e messaggeria varia. Si basa su "connessioni" una modalità di trasporto per scopi specifici. Una sessione può avere diverse connessioni: praticamente non occorre iniziare il processo per la sicurezza se il client accede a diversi servizi.

TLS specifiche

- Essenzialmente per mantenere la sessione il protocollo TSL (o SSL) consente le seguenti operazioni: negoziato, allerta e cambio di cifratura.

TLS specifiche

- Essenzialmente per mantenere la sessione il protocollo TSL (o SSL) consente le seguenti operazioni: negoziato, allerta e cambio di cifratura.
- Durante il normale scambio di pacchetti TCP/IP il protocollo di allerta (allert) può fornire degli avvisi (warning) o interrompere la connesione (fatal error). Nel primo caso si avvisa di una vulnerabilità (rispetto ad esempio alla certificazione se scade un certificato); nel secondo caso le inconsistenze nelle comunicazioni rendono la sessione insicura e viene chiusa (ad esempio cambio di IP o fallimento di una verifica).

TLS specifiche

- Essenzialmente per mantenere la sessione il protocollo TSL (o SSL) consente le seguenti operazioni: negoziato, allerta e cambio di cifratura.
- Durante il normale scambio di pacchetti TCP/IP il protocollo di allerta (allert) può fornire degli avvisi (warning) o interrompere la connesione (fatal error). Nel primo caso si avvisa di una vulnerabilità (rispetto ad esempio alla certificazione se scade un certificato); nel secondo caso le inconsistenze nelle comunicazioni rendono la sessione insicura e viene chiusa (ad esempio cambio di IP o fallimento di una verifica).
- Il protocollo consente il cambio di cifratura, sincronizzando il momento (pacchetto) da cui si inizia ad utilizzare il nuovo metodo.

TLS specifiche

- Essenzialmente per mantenere la sessione il protocollo TSL (o SSL) consente le seguenti operazioni: negoziato, allerta e cambio di cifratura.
- Durante il normale scambio di pacchetti TCP/IP il protocollo di allerta (allert) può fornire degli avvisi (warning) o interrompere la connesione (fatal error). Nel primo caso si avvisa di una vulnerabilità (rispetto ad esempio alla certificazione se scade un certificato); nel secondo caso le inconsistenze nelle comunicazioni rendono la sessione insicura e viene chiusa (ad esempio cambio di IP o fallimento di una verifica).
- Il protocollo consente il cambio di cifratura, sincronizzando il momento (pacchetto) da cui si inizia ad utilizzare il nuovo metodo.
- La parte più delicata è il negoziato handshake (stretta di mano) in cui si definiscono il pacchetto di sicurezza in comune, si autentica il server (o anche il client) e si scambiano le chiavi per la comunicazione in chiave simmetrica.

Negoziato TLS

- La fase di negoziato è la più delicata perché da essa dipendono le fasi successive ed eventuali vulnerabilità. Si articola in quattro fasi

Negoziato TLS

- La fase di negoziato è la più delicata perché da essa dipendono le fasi successive ed eventuali vulnerabilità. Si articola in quattro fasi
- Fase 1: Scambio di "hello". Si definiscono le capacità di sicurezza. protocolli e relativa versione, codice identificativo della sessione (session ID), insieme delle capacità crittografiche condivise (cipher suite), eventuali metodi di compressione

Negoziato TLS

- La fase di negoziato è la più delicata perché da essa dipendono le fasi successive ed eventuali vulnerabilità. Si articola in quattro fasi
- Fase 1: Scambio di "hello". Si definiscono le capacità di sicurezza. protocolli e relativa versione, codice identificativo della sessione (session ID), insieme delle capacità crittografiche condivise (cipher suite), eventuali metodi di compressione
- Fase 2: Il Server invia il suo certificato e relativo message authentication code (MAC che non c'entra niente col MAC address); inizia lo scambio delle chiavi e (eventualmente) richiede il certificato al client.

Negoziato TLS

- La fase di negoziato è la più delicata perché da essa dipendono le fasi successive ed eventuali vulnerabilità. Si articola in quattro fasi
- Fase 1: Scambio di "hello". Si definiscono le capacità di sicurezza. protocolli e relativa versione, codice identificativo della sessione (session ID), insieme delle capacità crittografiche condivise (cipher suite), eventuali metodi di compressione
- Fase 2: Il Server invia il suo certificato e relativo message authentication code (MAC che non c'entra niente col MAC address); inizia lo scambio delle chiavi e (eventualmente) richiede il certificato al client.
- Fase 3 se richiesto il Client invia il suo certificato ed eventualmente la verifica del certificato. Prosegue lo scambio delle chiavi.

Negoziato TLS

- La fase di negoziato è la più delicata perché da essa dipendono le fasi successive ed eventuali vulnerabilità. Si articola in quattro fasi
- Fase 1: Scambio di "hello". Si definiscono le capacità di sicurezza. protocolli e relativa versione, codice identificativo della sessione (session ID), insieme delle capacità crittografiche condivise (cipher suite), eventuali metodi di compressione
- Fase 2: Il Server invia il suo certificato e relativo message authentication code (MAC che non c'entra niente col MAC address); inizia lo scambio delle chiavi e (eventualmente) richiede il certificato al client.
- Fase 3 se richiesto il Client invia il suo certificato ed eventualmente la verifica del certificato. Prosegue lo scambio delle chiavi.
- Fase 4 Si termina la fase di negoziato e si passa alla cifratura e algoritmo per il MAC scelti per la sessione.

Https

- Https significa Hypertext Transfer Protocol over TLS e rappresenta la versione sicura di http basata su TSL per la sicurezza della connessione.

Https

- Https significa Hypertext Transfer Protocol over TLS e rappresenta la versione sicura di http basata su TSL per la sicurezza della connessione.
- Quando il browser del client si collega al server inzia la fase di negoziato in cui solo il server si autentica e si instaura la sessione con la cifratura scelta (di solito a chiave simmetrica tipicamente AES).

Https

- Https significa Hypertext Transfer Protocol over TLS e rappresenta la versione sicura di http basata su TSL per la sicurezza della connessione.
- Quando il browser del client si collega al server inzia la fase di negoziato in cui solo il server si autentica e si instaura la sessione con la cifratura scelta (di solito a chiave simmetrica tipicamente AES).
- Utilizzando https il client è certo del sito a cui accede il quale può successivamente richiedere delle credenziali al client (ad esempio username e password) utilizzando un canale sicuro.

Esercitazione con Firefox

- Vedremo dove sono i certificati e le autorita certificanti.

Messaggio

- I gestori dei sistemi devono tenere aggiornati i propri sistemi operativi, i propri server ed i propri client. Devono ispezionare l'accesso alla propria rete.

Messaggio

- I gestori dei sistemi devono tenere aggiornati i propri sistemi operativi, i propri server ed i propri client. Devono ispezionare l'accesso alla propria rete.
- Si possono utilizzare professionisti che verificano i sistemi (a pagamento) identificando le vulnerabilità e suggerendo emendamenti.

Messaggio

- I gestori dei sistemi devono tenere aggiornati i propri sistemi operativi, i propri server ed i propri client. Devono ispezionare l'accesso alla propria rete.
- Si possono utilizzare professionisti che verificano i sistemi (a pagamento) identificando le vulnerabilità e suggerendo emendamenti.
- Chiunque può creare un servizio https (TLS+http) e costruire i propri certificati (ad esempio con openssl), ma solo i certificati provenienti da autorità di certificazioni note al client sono affidabili.

Messaggio

- I gestori dei sistemi devono tenere aggiornati i propri sistemi operativi, i propri server ed i propri client. Devono ispezionare l'accesso alla propria rete.
- Si possono utilizzare professionisti che verificano i sistemi (a pagamento) identificando le vulnerabilità e suggerendo emendamenti.
- Chiunque può creare un servizio https (TLS+http) e costruire i propri certificati (ad esempio con openssl), ma solo i certificati provenienti da autorità di certificazioni note al client sono affidabili.
- Le autorità di certificazione sono a loro volta accreditate da organismi nazionali o sovranazionali.

Messaggio

- I gestori dei sistemi devono tenere aggiornati i propri sistemi operativi, i propri server ed i propri client. Devono ispezionare l'accesso alla propria rete.
- Si possono utilizzare professionisti che verificano i sistemi (a pagamento) identificando le vulnerabilità e suggerendo emendamenti.
- Chiunque può creare un servizio https (TLS+http) e costruire i propri certificati (ad esempio con openssl), ma solo i certificati provenienti da autorità di certificazioni note al client sono affidabili.
- Le autorità di certificazione sono a loro volta accreditate da organismi nazionali o sovranazionali.
- I registri distribuiti (DLT) costituiscono uno strumento molto versatile ed in continua espansione per garantire la storicizzazione inalterabile dei dati (non ripudiation).
  Si possono utilizzare anche per creare valute elettroniche e contratti elettronici.