

Su un Plug-in per le prove di verifica online

Nazzaro Antonio Autore, Pezzano Claudio Pezzano¹
docente Informatica presso I.T.C. L. Amabile Avellino
docente formatore su IWT Università di Salerno
via Giovanni Di Guglielmo 6, 83100 Avellino(AV)
E-mail info@antonionazzaro.it

¹*consulente-programmatore presso Eustema S.p.A Roma(RM)*
via Accademia degli apostoli,27 00147 Roma RM
E-mail claudio_pezzano@libero.it

Si esaminano ed analizzano alcuni aspetti relativi ai carichi dei web server per le piattaforme MOODLE e IWT. Le indagini si riferiscono alle attività online: di un Corso di recupero/sostegno su Excel erogato con piattaforma MOODLE, agli alunni della IV[^] I dell'ITC L. Amabile(Avellino) e di un percorso formativo online sui Learning Object erogato ai docenti dell'ITC L. Amabile con piattaforma IWT.

Con lo strumento NETSTAT, individuiamo e analizziamo i protocolli e servizi in uso durante una sessione di utilizzo di MOODLE, ma l'approccio vale anche per altre piattaforme.

Ipotizziamo uno scenario che, operi in background a favore del docente-esaminatore, per garantire che durante una seduta di verifica, il candidato non si avvalga di aiuti non consentiti dal patto formativo.

A tale scopo, proponiamo l'implementazione in pseudocodifica di un algoritmo che realizzi un plug-in, col quale l'esaminatore riceva utili informazioni su come si comporta l'esaminato durante una verifica online.

1.Introduzione

Negli ultimi tempi, la letteratura spesso e volentieri, sta offrendo contributi significativi sulla messa in sicurezza dei Centri di-elearning [6, Fleck R., Mc Queen T., 1999] e [11, Nazzaro, 2009], sull'applicazione della legge privacy nelle scuole e nei Centri [10, Nazzaro, 2006], [13, Piattaforma IWT(a), 2009], [9, MPI, 2003] su teorie e modelli di valutazione delle attività online [2, Calvani et al, 2007],[3, Calvani et al., 2008] e sulle interfacce utente per l'e-learning [1, Bevilacqua et al, 2009].

In questo lavoro, intendiamo, offrire un contributo mediante il quale, dopo aver analizzato ed esaminato il carico dei web server con lo strumento HTTPERF [8, Krishnamurthy, Rexford, 2002] e [12, Percorsi relativi alle guide ed al download del tool, 2010], ci avvaliamo del comando NETSTAT [5, Crovella, Krishnamurthy, 2006] e [13, Percorso relativo alla documentazione per l'utilizzo dello strumento,2010], per verificare se durante una prova di verifica online, l'esaminato si avvale di aiuti non consentiti.

Presentiamo, inoltre, sotto forma di pseudocodice un plug-in [4, Bruce S. D., Larry L. P., 2002] con il quale otterremo l'output di tutte le connessioni attive durante la prova.

Infine, presentiamo e compariamo due tipi di plug-in possibili, uno più elementare, l'altro più sofisticato, entrambi, rispondenti al nostro caso.

2. Analisi dei carichi dei web server

Anche se nelle successive tabelle, rappresentiamo le analisi dei carichi dei web server sia di IWT che di Moodle, per la nostra investigazione, non è restrittivo supporre che la piattaforma di e-learning dove è caricata la prova di verifica sia Moodle. In ogni caso, la prima cosa da fare è quella di andare a testare il carico del web server della piattaforma in modo tale da capire il limite superiore che il server riesce a gestire senza che vada in crash/down. Pertanto, simuliamo il traffico web sul sito antonionazzaro.it/moodle [Piattaforma Moodle, 2009] attraverso il tool `httpperf`, in questo modo, possiamo conoscere il massimo numero di richieste per secondo che può sostenere un web server. Ad esempio, il seguente comando: `httpperf --hog --server=www.antonionazzaro.it/moodle --num-conns=500 --rate=100 --timeout=5`, ci dice che, il timeout del server è di 5 sec e che `httpperf`, crea 500 connessioni ad un rate fissato di 100 per secondo all' host `www.antonionazzaro.it/moodle`, sfruttando qualsiasi porta TCP di cui ha bisogno, contestualmente, alla richiesta del documento di root: <http://antonionazzaro.it/moodle>. Tenendo conto del precedente esempio, per saperne di più sui vari parametri di cui si serve `httpperf` quando esamina il carico di un web server, risultano utili i seguenti elementi di conoscenza.

Output	Descrizione
Output Descrizione Reply size [B]: header 341.0 content 5332.0 footer 2.0 (total 5675.0) 127	lunghezza media di reply headers, content e footers
Reply Status	codici di stato (nel caso in esame le 500 richieste fatte sono andate a buon fine). Reply status: 1xx=0 2xx=500 3xx=0 4xx=0 5xx=0. Mostra un istogramma dei codici di stato ricevuti
CPU system :	tempo di utilizzo della CPU da parte dell'utente e da parte del sistema
CPU time [s]: user 0.35 system 6.93 (user 4.7% system 93.1% total 97.8%)	statistiche a livello della CPU lungo il corso dell'esperimento
NET I/O:	velocità dell' I/O sulla connessione
Errors: total 0 client-timo 0..	numero di possibili errori che possono verificarsi
Tempo speso per il test	tempo che intercorre tra la nostra richiesta al web server e la risposta ottenuta dal server stesso

Su un Pulg-in per le prove di verifica online

Nome sito	INPUT			OUTPUT		
	#Num. connessioni	Rate	Timeout	# Num richieste	# Num risposte	Tempo speso per il test
antonionazzaro.it/moodle	1	0	0	1	1	0.207s
antonionazzaro.it/moodle	100	10	5	100	100	10.111s
antonionazzaro.it/moodle	100	100	5	100	100	1.780s
antonionazzaro.it/moodle	1000	100	5	1000	997	14.988s
antonionazzaro.it/moodle	100	100	0	100	100	2.024s
antonionazzaro.it/moodle	500	100	5	500	500	7.449s
antonionazzaro.it/moodle	500	100	0	500	500	7.496s
antonionazzaro.it/moodle	200	10	0	200	200	20.106s
antonionazzaro.it/moodle	300	10	0	300	300	33.661s
antonionazzaro.it/moodle	400	10	0	400	400	40.112s
antonionazzaro.it/moodle	500	10	0	500	500	50.091s
antonionazzaro.it/moodle	1000	10	0	1000	1000	100.105s
antonionazzaro.it/moodle	1000	1	0	1000	1000	999.222s

Tabella 1 – Analisi carichi web server piattaforma Moodle.

Nome sito	INPUT			OUTPUT		
	#Num. connessioni	Rate	Timeout	#Num richieste	#Num risposte	Tempo speso per il test
itcamabile.momanet.it	1	0	0	1	1	0.441s
itcamabile.momanet.it	100	10	5	100	100	11.098s
itcamabile.momanet.it	100	100	5	100	100	1.454s
itcamabile.momanet.it	1000	100	5	1000	999	15.751s
itcamabile.momanet.it	100	100	0	100	100	2.091s
itcamabile.momanet.it	500	100	5	500	500	7.761s
itcamabile.momanet.it	500	100	0	500	487	8.003s
itcamabile.momanet.it	200	10	0	200	200	20.754s
itcamabile.momanet.it	300	10	0	300	300	35.106s
itcamabile.momanet.it	400	10	0	400	400	41.997s
itcamabile.momanet.it	500	10	0	500	495	50.112s
itcamabile.momanet.it	1000	10	0	1000	1000	104.492s
itcamabile.momanet.it	1000	1	0	1000	996	999.884s

Tabella 2 – Analisi carichi web server piattaforma IWT.

3. Alcune precisazioni e considerazioni sulle analisi svolte

Tutti i dati che ci vengono restituiti dal tool sono dati che dipendono dal tipo di connessione, dal traffico Internet, dall' hardware della macchina e dalle condizioni software della macchina e quindi non possono essere considerati dati assoluti. Questi risultati sono stati ottenuti durante misurazioni fatte di mattina e possiamo notare che il numero di richieste coincide in quasi tutti i casi con il numero di risposte e ciò implica che entrambi i web server reggono questo carico a discapito del tempo di risposta che si spera sia il più piccolo possibile. Una volta constatato che il web server di una determinata piattaforma regge il quantitativo di traffico da noi ipotizzato può essere necessario trovare delle euristiche per impedire "meccanismi di copia" al fine di evitare imprevisti dovuti al traffico, durante la seduta d'esame. Le misurazioni tra i web server di Moodle e di IWT sono pressoché simili sia per quanto riguarda il numero di richieste e di risposte ricevute che per il tempo speso per il test. I tempi di risposta del web server di IWT possono diminuire ed addirittura essere inferiori al web server di Moodle se in itcamabile.momanet.it, viene rimossa almeno una delle immagini *.jpg, in tal modo, infatti diminuisce la grandezza del pacchetto e ciò implica una riduzione del tempo di esecuzione del test.

4. Individuare gli aiuti online

Durante lo svolgimento in sede d'esame di una prova di verifica online mediante piattaforme di e-learning è anche utile sapere se il candidato non si stà avvalendo di nessun tipo di aiuto, come quello che ad esempio, potrebbe provenire dall'utilizzo di: manuali online, enciclopedie cartacee ma anche di altre persone fisiche. Con l'espressione aiuti online intendiamo tutti quei tipi di aiuti provenienti da Internet e da qualsiasi tipo di protocollo, potrebbe essere necessario evitare che l'utente apra altre pagine web, che invii e successivamente riceva e-mail di aiuto, si avvalga di invio di informazioni attraverso il protocollo FTP e così via.

Desideriamo quindi, che durante la prova online l'utente sul suo monitor apra l'unica pagina web (i.e. antonionazzaro.it/moodle/questionario.htm) contenente il test-questionario e nient'altro. Un modo oneroso, per evitare gli aiuti provenienti da Internet è quello di ricorrere ad un controllore fisico ma è possibile sopperire all'utilizzo di tale risorsa andando a monitorare le connessioni stabilite sulla macchina durante lo svolgimento della prova, come avviene quando ci si avvale dello strumento NETSTAT.

Nelle Figure 1 e 2, vediamo in esecuzione lo strumento NETSTAT, che mostra le connessioni TCP attive sul terminale ove è in esecuzione il comando stesso. In particolare, la successiva figura 1 mostra l'elenco delle porte TCP e UDP aperte sul computer. In particolare: **a** (all tutte le connessioni TCP/UDP), **n** (risparmia tempo sulle queries di richiesta DNS) ; **o** (visualizza il processo ID, ovvero ci dice quale processo del kernel locale si sta utilizzando).

```

C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\claudio>netstat -ano

Connessioni attive

Proto  Indirizzo locale          Indirizzo esterno          Stato                      PID
TCP    0.0.0.0:135                0.0.0.0:0                 LISTENING                  792
TCP    0.0.0.0:445                0.0.0.0:0                 LISTENING                  4
TCP    39.231.123.53:139         0.0.0.0:0                 LISTENING                  4
TCP    127.0.0.1:1026            127.0.0.1:27015          ESTABLISHED                248
TCP    127.0.0.1:1030            0.0.0.0:0                 LISTENING                  2708
TCP    127.0.0.1:5354            0.0.0.0:0                 LISTENING                  1900
TCP    127.0.0.1:10110          0.0.0.0:0                 LISTENING                  852
TCP    127.0.0.1:27015          0.0.0.0:0                 LISTENING                  1836
TCP    127.0.0.1:27015          127.0.0.1:1026           ESTABLISHED                1836
UDP    0.0.0.0:445                *:*:                       *:*:                       4
UDP    0.0.0.0:500                *:*:                       *:*:                       584
UDP    0.0.0.0:1025              *:*:                       *:*:                       1900
UDP    0.0.0.0:1035              *:*:                       *:*:                       924
UDP    0.0.0.0:1041              *:*:                       *:*:                       924
UDP    0.0.0.0:1042              *:*:                       *:*:                       924
UDP    0.0.0.0:1235              *:*:                       *:*:                       924
UDP    0.0.0.0:1236              *:*:                       *:*:                       924
UDP    0.0.0.0:1237              *:*:                       *:*:                       924
UDP    0.0.0.0:1238              *:*:                       *:*:                       924
UDP    0.0.0.0:1239              *:*:                       *:*:                       924
UDP    0.0.0.0:1240              *:*:                       *:*:                       924
UDP    0.0.0.0:1241              *:*:                       *:*:                       924
UDP    0.0.0.0:4500              *:*:                       *:*:                       584
UDP    0.0.0.0:61258             *:*:                       *:*:                       1900
UDP    39.231.123.53:123         *:*:                       *:*:                       860
UDP    39.231.123.53:137         *:*:                       *:*:                       4
UDP    39.231.123.53:138         *:*:                       *:*:                       4
UDP    39.231.123.53:1900        *:*:                       *:*:                       1000
UDP    39.231.123.53:5353        *:*:                       *:*:                       1900
UDP    127.0.0.1:123             *:*:                       *:*:                       860
UDP    127.0.0.1:1900            *:*:                       *:*:                       1000

```

Figura 1. Il comando NETSTAT -ano

Pertanto, con l'opzione `-ano`, viene visualizzato l'ID del processo di origine associato a ciascuna connessione, vengono mostrate tutte le connessioni (LISTENING e non) [`-a = --all`], non vengono risolti gli indirizzi IP e non si dispone del numero delle porte, allo scopo di risparmiare sui tempi, altrimenti richiesti per l'esecuzione delle queries DNS.

Utilizzando il comando NETSTAT con argomento `-no`, visualizziamo le sole connessioni stabilite (ESTABLISHED) come appare nella Figura 2, in modo da "filtrare" i dati, ottenendo solo quei dati i interesse.

```

C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\claudio>netstat -no

Connessioni attive

Proto  Indirizzo locale          Indirizzo esterno          Stato                      PID
TCP    39.231.123.53:3101         74.125.39.99:80           ESTABLISHED                1092
TCP    39.231.123.53:3104         74.125.39.106:80          ESTABLISHED                1092
TCP    39.231.123.53:3105         74.125.39.106:80          ESTABLISHED                1092
TCP    39.231.123.53:3108         92.122.213.8:80           ESTABLISHED                1092
TCP    39.231.123.53:3109         92.122.213.8:80           ESTABLISHED                1092
TCP    39.231.123.53:3110         92.122.213.8:80           ESTABLISHED                1092
TCP    39.231.123.53:3111         212.243.223.160:80        ESTABLISHED                1092
TCP    127.0.0.1:1026            127.0.0.1:27015          ESTABLISHED                248

```

Figura 2. Il comando NETSTAT -no

5. Costruire strumenti di controllo agenti dalla piattaforma.

Al fine di controllare l'utente in modo tale che non abbia ricevuto nessuna agevolazione al test/questionario attraverso la consultazione di materiale online, si può implementare uno script che lancia in background ripetutamente il comando NETSTAT, e poi invia al web server all'interno del body dei pacchetti IP le informazioni ottenute attraverso l'output di NETSTAT.

Con questo procedimento, saremo certi che sul computer dell'utente sia aperta, durante lo svolgimento del test/questionario, la sola pagina web necessaria alla prova di verifica. Sviluppiamo, al solito, la nostra investigazione ispirandoci a Moodle, ma il discorso vale anche per IWT, ove è possibile andare a crearsi dei package *ad hoc*, che consentono di avere un livello di sicurezza maggiore utile allo svolgimento di esami online.

La nostra idea è quella di lasciare inalterata l'interfaccia di Moodle aumentandone il livello di sicurezza, in questo modo, saremo sicuri che l'utente non si distoglierà per adattarsi ad una diversa interfaccia.

6. Pseudocodice dell'algoritmo

Passo 1) L'utente invia la richiesta a Moodle e si dichiara pronto ad iniziare il test/questionario.

Passo 2) Moodle invia nella risposta la necessità di installare un plug-in per consentire la corretta visualizzazione del test.

Passo 3) L'utente accetta l'installazione del plug-in ed al termine dell'installazione invia un feedback a Moodle indicandogli la corretta installazione in locale del plug-in.

Passo 4) Moodle invia nella risposta il test/questionario che l'utente dovrà compilare.

Passo 5) Periodicamente il plug-in installato andrà in esecuzione per controllare le porte utilizzate sulla postazione di lavoro e memorizzerà l'output, all'interno di un file di log.

Passo i) L'utente termina il test/questionario.

Passo i+1) Il plug-in che va in esecuzione localmente, subito dopo invierà a Moodle il file di log contenente tutte le connessioni stabilite dall'utente.

Passo n) Un addetto controllerà il file di log restituito dal plug-in e stilerà dei report da sottoporre all'esaminatore.

7. Struttura del Plug-in

Il plug-in autoinstallante sulla macchina client, ovvero, il computer dove si deve svolgere la prova di verifica, può essere di due tipi:

- soluzione 1, si tratta di un semplice file batch che invoca periodicamente da shell(prompt di comandi) lo strumento NETSTAT e l'output prodotto sarà ridirezionato all'interno del file outputnetstat.txt;
- soluzione 2, è quella del caso in cui, si vuole essere a conoscenza, oltre che delle connessioni in ascolto e stabilite sul computer del computer client, anche di tutte le sequenze di caratteri che l'utente digita e di tutte le operazioni che egli esegue.

In tal caso, occorrerà far installare all'utente un programma che lavora come tutti i classici programmi di keylogger [Bevilacqua et al, 2009], questo programma, infine, agirà in maniera nascosta ed in background per l'utente.

8. Comparazione tra i due possibili approcci risolutivi

Il primo tipo di plug-in è più semplice da implementare ed è molto più leggero rispetto ad un programma di keylogger.

Gli svantaggi di questo primo tipo di plug-in, sono i seguenti:

- si ottengono minori informazioni;
- è necessario ricorrere ad un esperto tecnico che consenta di tradurre il file di output in report riconoscibile all'esaminatore.

Il secondo tipo di plug-in consente di ottenere tutte le informazioni necessarie ed anche non necessarie, infatti, grazie ad esso viene monitorata la macchina client istante per istante e non risulta essere necessario l'ausilio di un esperto tecnico che traduca il file di output in report riconoscibili all'esaminatore perchè le informazioni di output ottenute sono già ben suddivise sottoforma di strutture tabellari. Questo secondo tipo di plug-in, presenta i seguenti svantaggi:

- risulta essere difficile e dispendioso effettuare un'implementazione *ad hoc*;
- i tempi di installazione del plug-in sono più lunghi

9. Conclusioni

Questa tecnica di analisi sulle prestazioni dei web server, ci fornisce dei dati temporanei, perché dipende da fattori, quali: l'evoluzione dell'hardware e/o la scoperta di nuovi algoritmi di instradamento dei dati sulla rete Internet. Mentre, per quanto riguarda la possibilità di individuare e neutralizzare, gli aiuti online durante una prova di verifica, abbiamo mostrato come sia possibile definire una procedura effettiva che riduca al minimo la probabilità che questi si verifichino.

In futuro ci auspichiamo che questo contributo potrà essere da sprone, per ottenere risultati, magari a "più mani", con i quali si riusciranno a costruire prove di verifica online al tempo stesso efficaci, efficienti e rispondenti alla dimensione etica della cultura digitale. Anche in questo caso, abbiamo avvertito la grande importanza che rivestono: la disponibilità, la riservatezza e l'integrità delle informazioni di tipo elettronico nella gestione e amministrazione di un Centro di e-learning.

Bibliografia

[1] Luca Bevilacqua, Nicola Capuano, Annunziata Cascone, Federico Ceccarini, Fabio Corvino, Ciro D'Apice, Ivano De Furio, Giovanna Scafuro, Gianluca Supino, Interfacce Utente Avanzate per l'e-learning, Journal of e-Learning and Knowledge Society, 5, 3, 2009, 95 – 104.

[2] Antonio Calvani, Antonio Fini, Marcello Molino, Maria Ranieri, Gruppi collaborativi online: come valutare interazioni efficaci, Journal of e-Learning and Knowledge Society, 3, 3, 2007, 93 – 102.

DIDAMATICA 2010

[3] Antonio Calvani, Antonio Cartelli, Antonio Fini, Maria Ranieri, Modelli e strumenti per la valutazione della competenza digitale nella scuola, Journal of e-Learning and Knowledge Society , 4, 3, 2008, 119-128 .

[4] Bruce S. Davie, Larry L. Peterson, Reti di calcolatori. Apogeo, 2002

[5] Crovella M., Krishnamurthy B., Internet Measurement: Infrastructure, Traffic and Applications, Wiley, July 2006

[6] Fleck R., McQueen T., Internet access, usage and policies in colleges and universities, URL:

<http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/701/611> (verificato il 1/2/2010), First Monday, Vol. 4, n.11, November 1999.

[7] HTTPERF, Percorsi relativi alle guide ed al download del tool, 2010, URL :

<http://httpperf.com/lore.com/> (verificato il 4/2/2010)

<http://www.hpl.hp.com/research/linux/httpperf/> (verificato il 4/2/2010)

[8] Krishnamurthy B., Rexford J., Web Protocols and Practice, Addison-Wesley, 2002

[9] MPI Servizio di Osservatorio Tecnologico per la scuola. Sicurezza informatica How-To URL: <http://www.osservatoriotecnologico.net/reti/howto.htm> (verificato il 1/2/2010), 2003.

[10] Nazzaro A., Scuola e Privacy. Indicazioni sull'applicazione del "Codice in materia di protezione dei dati personali" ai sistemi informativi scolastici. ANICIA, Roma, 2006.

[11] Nazzaro A., Tipicas estrucstras tecnologicas en los Centros di e-learning, Conferenza tenuta il 20/3/2009 all' Expoealearning di Barcellona, URL: <http://aeofl.tv> (verificato il 2/2/2010), 2009.

[12] NETSTAT, Percorso relativo alla documentazione per l'utilizzo dello strumento,2010 , URL:

<http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/netstat.mspx?mfr=true> (verificato il 4/2/2010)

[13] Piattaforma IWT, Progetto Corso Alta Formazione "ELMAPWIS", presso DIIMA/CRMPA Università di Salerno, URL: <http://193.205.191.145/IWTPortal/> (verificato il 1/2/2010), 2009a.

[14] Piattaforma IWT, Percorso formativo online per docenti di scuola secondaria finalizzato all'erogazione di corsi di recupero, Università di Salerno/MOMA, URL: <http://itcamabile.momanet.it> (verificato il 3/2/2010), 2009b.

[15] Piattaforma MOODLE , Corso di recupero su Excel online per alunni di scuola secondaria, ITC L. Amabile Avellino, <http://antonionazzaro.it/moodle> (verificato il 3/2/2010), 2009.