Gruppo auditing

- Scansioni **nessus** di primavera in partenza
- Nuovi tool allo studio: principalmente web app
  - zmap;
  - wig;
  - skipfish (**molto** pesante);
  - ecc. ecc.
- vm con tool fai-da-te (oltre nessus)

Pre-scansione di primavera

- **3871** nodi
- dns:
  - 72 (+2)
  - **24** non ufficiali
- smtp:
  - 59 (+2)
  - **37** non ufficiali
- web:
  - 1135
- ssh:
  - **1471**

Pre-scansione di primavera (WEB)

- 1317 ip candidati:
  - 718 porta 80, 599 porta 443
- **877** attivi:
  - 592 porta 80, 285 porta 443
- OS: 594 (**40% non più supportati**)
- CMS: 51 (**84% vulnerabili**)
- 29 stampanti

Sistemi operativi

Sistema Operativo	Non supportato	Supportato	Totali
CentOS	10	83	93
Debian	22	51	73
Fedora	53	6	59
FreeBSD	12	9	21
Windows	14	13	27
OpenBSD	39	7	46
RH Enterprise	8	23	31
Scientific Linux	11	106	127
Ubuntu	30	46	76
OpenSUSE	38	3	41

CMS

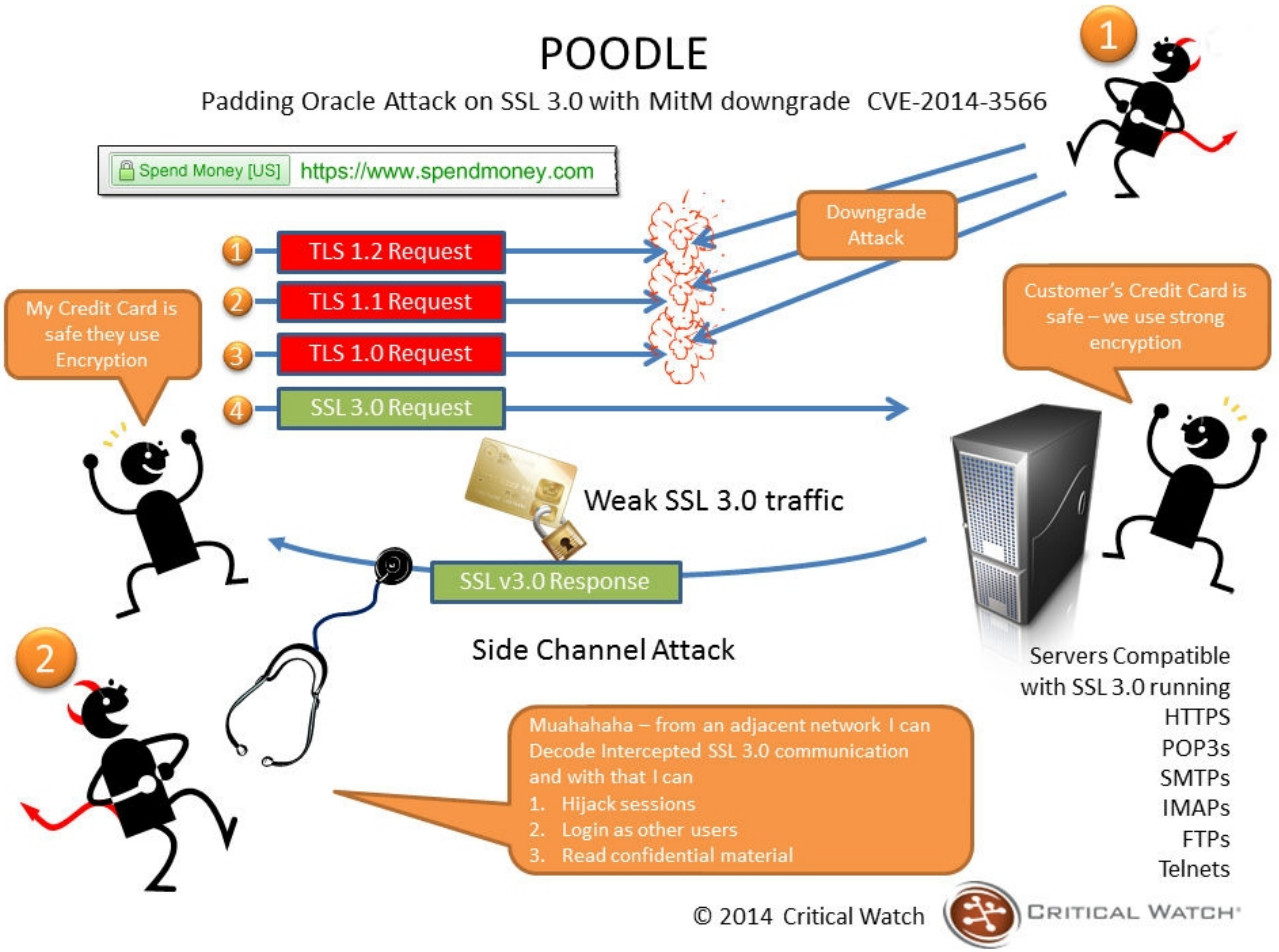
Prodotto	Vuln.	Non vuln.	Totale
Drupal	9	1	10
Joomla!	24	0	24
WordPress	9	1	10
phpMyAdmin	35	5	40
Django	?	?	3
DokuWiki	1	1	2
Plone	?	?	2
PHP	38	10	48

Piattaforme

Sistema	Totali
Apache 1	**5**
Apache 2.2	353
Apache 2.4	31
Microsoft IIS	20
Stampanti	**29**

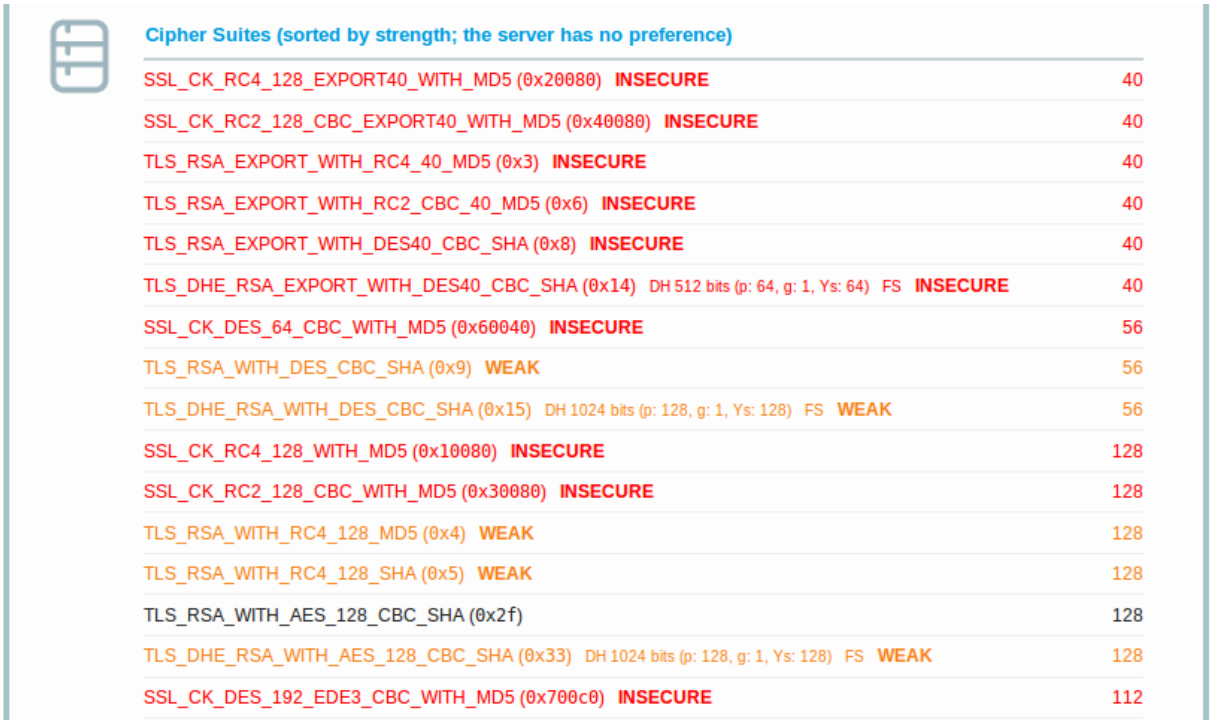
Poodle

- MITM che sfrutta SSLV3
- **260** server vulnerabili
- Istruzioni: **v.gd/ewudip**
- Verifica: **v.gd/dCQf6O**



Freak

- MITM che sfrutta protocolli a bassa sicurezza
- **75** server vulnerabili
- Istruzioni: **v.gd/avapij**
- Verifica: **v.gd/dCQf6O**



Cipher Suites (sorted by strength; the server has no preference)

SSL_CK_RC4_128_EXPORT40_WITH_MD5 (0x20080) **INSECURE**	40
SSL_CK_RC2_128_CBC_EXPORT40_WITH_MD5 (0x40080) **INSECURE**	40
TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x3) **INSECURE**	40
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x6) **INSECURE**	40
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x8) **INSECURE**	40
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0x14) DH 512 bits (p: 64, g: 1, Ys: 64) FS **INSECURE**	40
SSL_CK_DES_64_CBC_WITH_MD5 (0x60040) **INSECURE**	56
TLS_RSA_WITH_DES_CBC_SHA (0x9) **WEAK**	56
TLS_DHE_RSA_WITH_DES_CBC_SHA (0x15) DH 1024 bits (p: 128, g: 1, Ys: 128) FS **WEAK**	56
SSL_CK_RC4_128_WITH_MD5 (0x10080) **INSECURE**	128
SSL_CK_RC2_128_CBC_WITH_MD5 (0x30080) **INSECURE**	128
TLS_RSA_WITH_RC4_128_MD5 (0x4) **WEAK**	128
TLS_RSA_WITH_RC4_128_SHA (0x5) **WEAK**	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits (p: 128, g: 1, Ys: 128) FS **WEAK**	128
SSL_CK_DES_192_EDE3_CBC_WITH_MD5 (0x700c0) **INSECURE**	112

Gruppo Security

- Passive DNS
- DNSSec
- netflow

Tutorial CCR

- Firenze (GGI, Arcetri)
- 4-5 o 11-12 Novembre
- Programma
  - 1° giorno (9-18): 2 tutorial di 4h mane & sera
  - 2° giorno (9-13?): presentazioni
- Contribuite!
  - domande legal / poliziesche
  - idee per tutorial
  - offerte di presentazioni

Servizio TCS

- Nuovo fornitore (**Digicert**) da luglio
- Funzionalità non ancora del tutto chiare
- Attenzione ai certificati che scadranno nei primi mesi della nuova gestione!