The Honeynet

PROJECT

How Attackers Go Undetected

Covering Your Tracks As You Move Along

Ayaz Ahmed Khan
Pakistan Honeynet Project
www.honeynet.org.pk

Prologue

- Breaking into systems is easy.
- Well, usually, it is.
- Covering up the mess you make out of a break-in, is hard to clean up.
- They say a criminal always leaves behind at least a single clue.

Prologue

- Hackers aren't criminals.
- They break into systems because they are curious.
- As long as it's a test system, you can be curious all you want.
- Otherwise, you are still a criminal.

Golden Rules

(to remember when breaking in :-P)

- When breaking into systems, always keep in mind:
  - It takes a lot of carefulness to **assume** no-one broke into the system.
  - It only takes a single mistake to **believe** something's fishy going on.
  - If you don't know the system you're breaking into well enough, back off.
  - You can and will get caught, if it is not your lucky day. (and if it is your lucky day, you'll get caught some other day)

- Don’t push your luck.
- If you get lucky once or twice, don’t get confident.
- A heavy does of paranoia is always healthy.
- At least, in this business, it is.
- They say expert drivers are involved in much more accidents – the new ones are too busy following the rules.

Why Break-in at all?

- What do you do when you have got an itch?
- You scratch it. :-)
- I am not defending anyone here – merely speaking my mind.

What am I going to talk about today?

- Definitely not how you break into systems.
- But, how you cover your tracks after you have broken in.
- And how you stay undetected.
- If not that, then how you throw those trying to trace you on a wild goose chase.

Wild Goose Chase

- Protecting attackers' privacy online sounds ironic.
- It means when the attacker breaks in, he never gets to show his true origin anywhere (almost).
- Tools that work to protect individual's privacy online can be (ab)used by attackers as well.

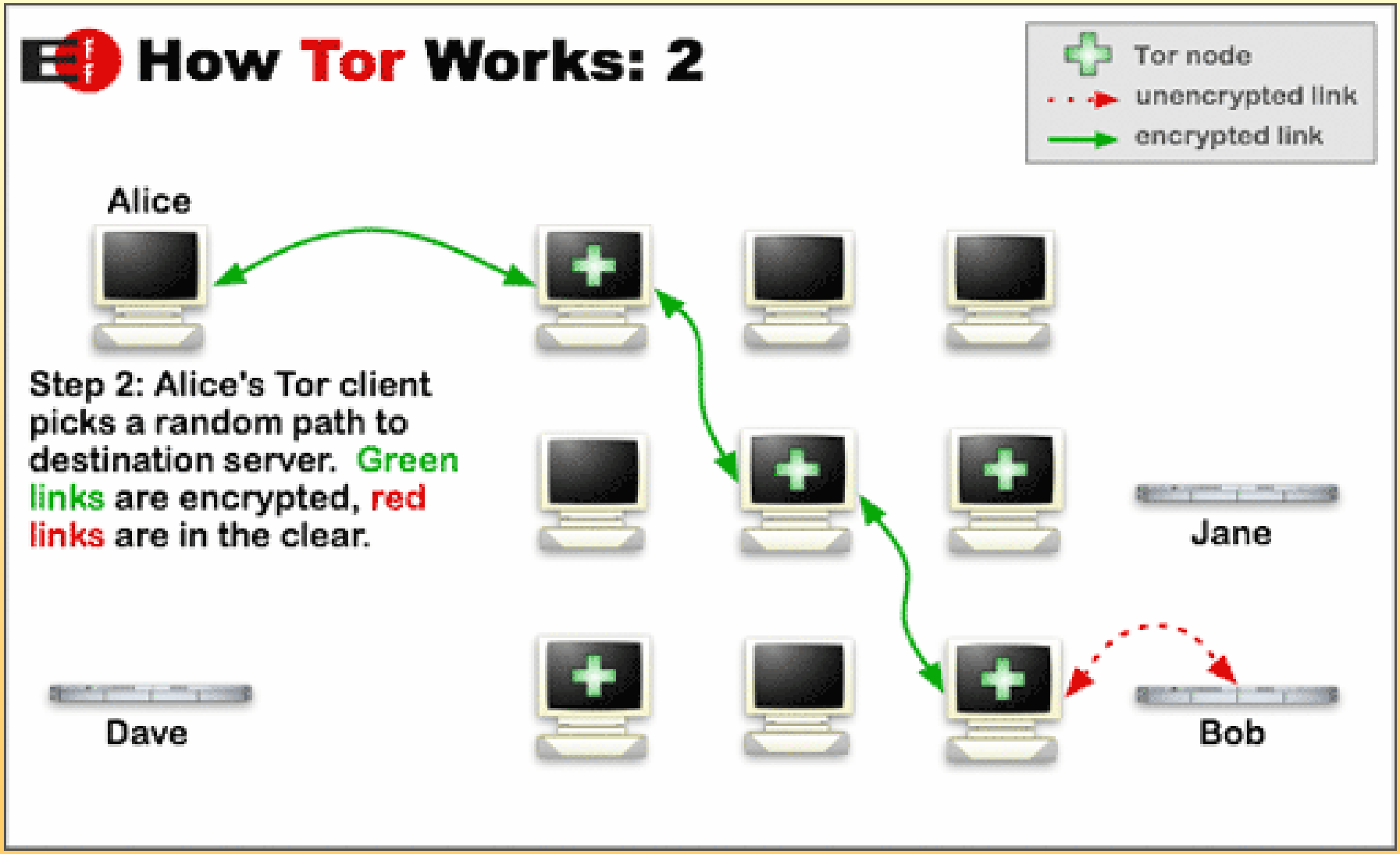
TOR: The Onion Router

- Let's talk about TOR
- Developed and managed by The Free Haven Project and promoted heavily by the Electronic Frontier Foundation (EFF).
- TOR makes possible many things.
  - Protect users' privacy
  - Protect against traffic analysis

TOR Circuits

- TOR nodes are everywhere.
- TOR client picks a virtual circuit, and sends encrypted packet over the circuit.
- Each hop in the circuit determines who the next node will be.
- Nodes only know about their immediate source and destination nodes. That's it.
- At every node, source/destination is different. Nodes don't know about other nodes.
- Beats traffic analysis to a great extent.
- For every connection, a new circuit is chosen randomly.

Courtesy tor.eff.org



How can TOR be (ab)used?

- It is as simple as pie.
- People have been using anonymizing proxies for a long time.
- TOR is ten steps ahead of that.
- It will do all the work for you.
- Just route your packets through TOR, and wait and watch.

Let's Run TOR First.

- TOR is running on 9050 on my Linux laptop.

```
ayaz$ netstat -ltn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:5802            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3690            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:587             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5902            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6002            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:9050          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN
[~/downloads/tor-0.2.0.2-alpha/src/or] [laptop]
ayaz$ Jul 25 13:26:41.842 [notice] Tor has successfully opened a circuit. Looks like client functionality is working.
```

Making a tunnel

- Everyone knows about the infamous nc (netcat).
- But we won't use that.
- We will use something more powerful and flexible than netcat
- SOCAT
- You can find it on freshmeat.net
- It supports too many things to list down here.
- Let's just say, it is right tool for the job.

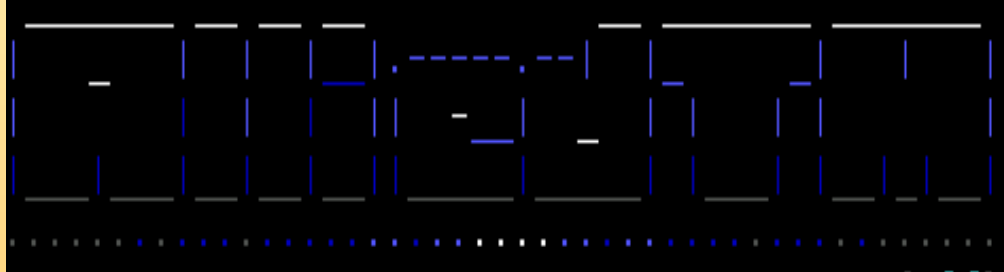
Who's the target?

- Obviously, I am not going to show you how I broke into some box.
- That in no way should be taken to mean that I **do** break into systems.
- I am going to get into www.ayaz.pk :-)
- SSH is open on www.ayaz.pk on 2229. Let's log through that and see how TOR protects us.

Setting Up a SOCAT tunnel through TOR

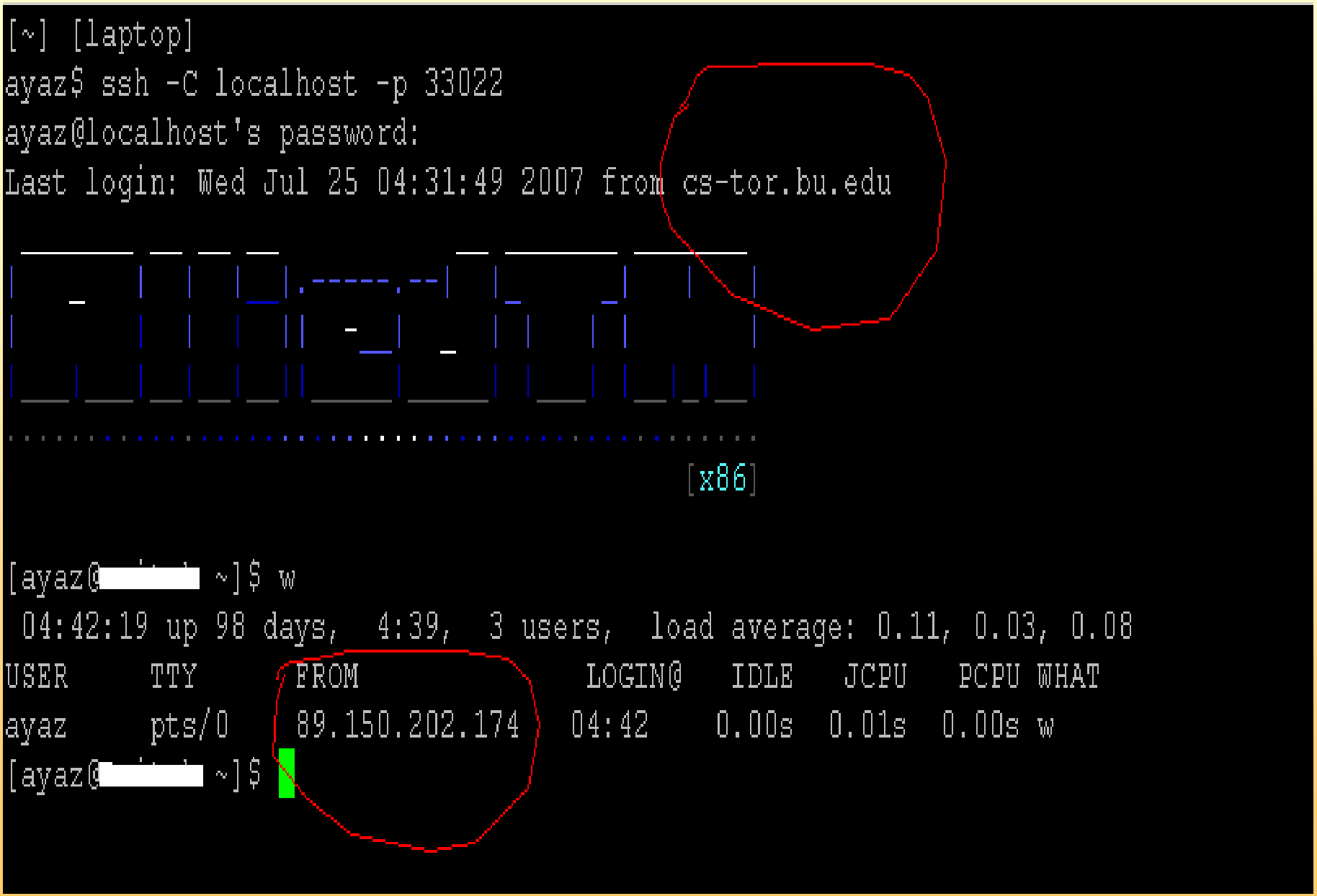
```
$ socat TCP4-LISTEN:33022,fork
  SOCKS4A:127.0.0.1:www.ayaz.pk:222
  9,socksport=9050
```

```
[~] [laptop]
ayaz$ ssh -C localhost -p 33022
The authenticity of host '[localhost]:33022 ([127.0.0.1]:33022)' can't be established.
RSA key fingerprint is [redacted].
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:33022' (RSA) to the list of known hosts.
ayaz@localhost's password:
Permission denied, please try again.
ayaz@localhost's password:
Last login: Wed Jul 25 04:26:15 2007 from [redacted]
```



```
                                                    [x86]

[ayaz@[redacted] ~]$ w
 04:31:55 up 98 days,  4:28,  3 users,  load average: 0.00, 0.03, 0.17
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
ayaz     pts/0    cs-tor.bu.edu     04:31    0.00s  0.01s  0.00s w
[ayaz@[redacted] ~]$
```


[~] [laptop]
ayaz$ ssh -C localhost -p 33022
ayaz@localhost's password:
Last login: Wed Jul 25 04:31:49 2007 from cs-tor.bu.edu
[x86]
[ayaz@ ~]$ w
04:42:19 up 98 days, 4:39, 3 users, load average: 0.11, 0.03, 0.08
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
ayaz pts/0 89.150.202.174 04:42 0.00s 0.01s 0.00s w
[ayaz@ ~]$

Every new connection uses a different, randomly selected, TOR circuit.

How else can attackers use this?

- TOR and socat, you mean?
- Oh, many many ways.
- They can launch exploits via TOR.
- They can scan systems via TOR.
- They can try web-based break-in tricks via TOR.
- Et cetera, et cetera.
- You know, Metasploit Framework, TOR, and socat make up for a very heinous exploitation tool set. ;-)
- Wait till someone integrates TOR with Nmap. Gives me the goose bumps.

But …

All this doesn't cover up your tracks. It only makes tracing you back to your little computer in your little room very very difficult, if not impossible.

Remember: TOR nodes run on systems all over the world. The more users who set up TOR nodes, the more powerful TOR gets, and the more difficult it becomes to do successful traffic analysis

Makes up for a happy attacker. :-D

Ghost In The Machine

- Wouldn't it be great if you could just be invisible after you break into a system?
- OK, OK, you need not point it out to me.
- Granted, that is old stuff.
- We have rootkits and what not that make it possible.
- I just want to show you something I wrote an year ago. Nothing fancy, but it works.

Logs

- Logs are an attacker's worst nightmare.
- And also his worst enemy.
- If you don't know enough about the system you have broken into, you don't know which thing is logging what where.
- Is Firewall logging? IDS, perhaps? SSH or telnet, maybe? Some other security monitoring system you don't know of?

LogFlusher

- I wrote a small C application that does something very simple but hideous on a Unix/Linux system.
- It cleans a few log files. Pretty naïve.
- But, take a look at the following screenshot.

:-P

```
[/home/ayaz] [khi]
root# w
 14:36:36 up 17 days, 23:01,  1 user,  load average: 0.07, 0.04, 0.01
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
ayaz     pts/0    124.29.203.107   12:20    0.00s  0.05s  0.09s sshd: ayaz [pri
[/home/ayaz] [khi]
root# ./logflusher ayaz 'pts/0' 1
[/home/ayaz] [khi]
root# w
 14:36:48 up 17 days, 23:02,  0 users,  load average: 0.06, 0.03, 0.01
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
[/home/ayaz] [khi]
root#
```

And, I am invisible.

Not completely, but to a great extent.

It is a nice little tool to clean up your login tracks. Mix it up with TOR and socat, and you can get pretty dangerous.

So, there you go ...

- That was only a quick insight.
- There are specialised rootkits that hook into the system call table and make you invisible.
- What is more important is knowing the system you are breaking into and knowing its defences.

Again ...

- You can and will get caught.
- A single mistake is all it takes.
- Know the system before you even attempt to break into it.
- Paranoia is not only healthy, it is a must have.
- You really don’t need to scratch the itch. ;-)

Questions, please?