Perl is for pwn!

Sergey Romanov

YAPC::Russia 2012

Hello

- Sergey Romanov (sromanov on irc.perl.org)
- Do Perl for fun (also, for living)
- PeterPEN CTF team (SPbSU)
- Like alpacas

What is CTF anyway?

- Capture the Flag (CTF) is a computer security wargame

What is CTF anyway?

- Capture the Flag (CTF) is a computer security wargame
- CTF was popularized by DEFCON conference

How many of you heard of DEFCON?

What is CTF anyway?

- Capture the Flag (CTF) is a computer security wargame
- CTF was popularized by DEFCON conference

How many of you heard of DEFCON?

- Two basic types of competition

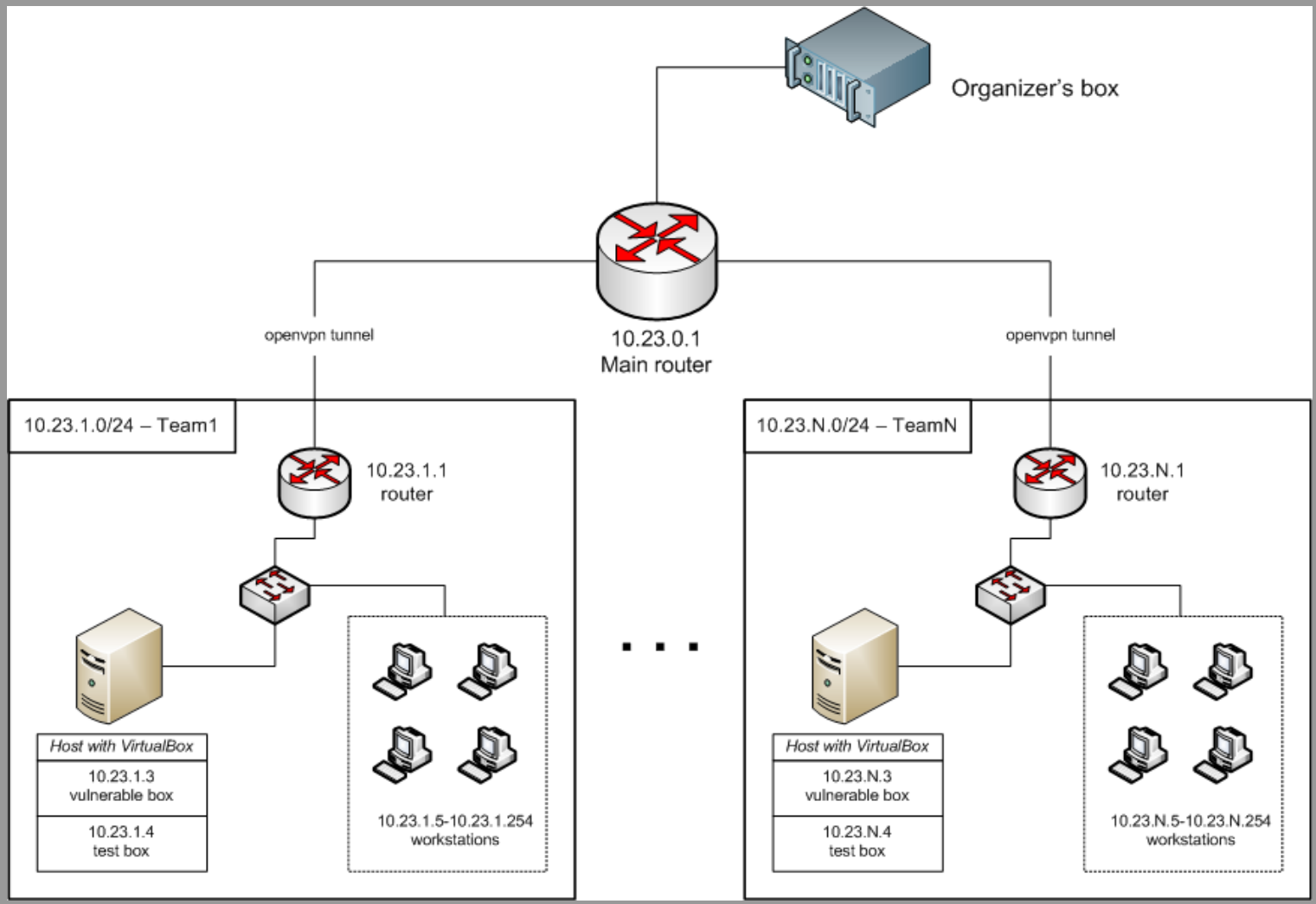
Type 1: Find the key

- Teams should solve tasks get points
- Different categories: web, reverse, packets, admin, ctb (crack-the-box), crypto, stegano etc
- It is common to do a qualification round as task-based CTF

Type 2: Steal the flag

- Vulnerable box – vurtual machine with pre-installed services
- Service – (vulnerable) application, accessible via network
- Flag – unique string (eg, "[a-z0-9]{32}=")

Network


Organizer's box
openvpn tunnel
10.23.0.1
Main router
openvpn tunnel
10.23.1.0/24 – Team1
10.23.1.1
router
Host with VirtualBox
10.23.1.3
vulnerable box
10.23.1.4
test box
10.23.1.5-10.23.1.254
workstations
10.23.N.0/24 – TeamN
10.23.N.1
router
Host with VirtualBox
10.23.N.3
vulnerable box
10.23.N.4
test box
10.23.N.5-10.23.N.254
workstations

How about Perl?

- Perl can be used during CTF game _heavily_

How about Perl?

- Perl can be used during CTF game _heavily_
- Just like any other modern, popular and convenient tool :)

How about Perl?

- Perl can be used during CTF game _heavily_
- Just like any other modern, popular and convenient tool :)
- But we'll concentrate on Perl for now

Where is Perl actually?

- Case 1: you're a participant
- Case 2: you're an organizer

CPAN & beyond

- helper scripts: text parsing, glue language etc

CPAN & beyond

- helper scripts: text parsing, glue language etc
- /usr/bin/lwp-*
- /usr/bin/md5pass

CPAN & beyond

- helper scripts: text parsing, glue language etc
- /usr/bin/lwp-*
- /usr/bin/md5pass
- find out yours, eg: **grep '/usr/bin/perl' /usr/bin/***

Gort, Klaatu barada nikto

Nikto2

Nikto2

- Web server scanner
- Tests over 6400 potentially dangerous files/CGIs, checks for outdated versions of over 1200 servers and version specific problems on over 270 servers
- Based on libwhisker2 by rain forest puppy (rfp)

Exploitfarm

- Written at Hackerdom (USU, Ekaterinburg)
- Accepts an exploit (eg, Perl script) and IP range of enemy teams
- Automates process of collecting flags and submitting them to jury check system

Organizing game

Let's make our own CTF

Task from RuCTF 2012 Quals

```
sub f(@d){
 return 0 unless @d;
 my $n = @d.elems;

 my @p;
 push @p, [0x100500 xx $n] for 0..^1+<$n;
 @p[0][0]=0;

 return [min]gather for 1,*+2...1+<$n-1 ->$x{
  for (1..^$n).grep({$x+&1+<$x})X(0..^$n).grep({$x+&1+<$x}) ->$z,$c{
   @p[$x][$z]=[min]@p[$x][$z],@p[$x+^1+<$z][$c],@d[$c][$z]
  }
  take @p[1+<$n-1][$_]+@d[$_][0] for ^$n
 }
}
```

(not so) Simple web-services examples

- POP3 server (UralCTF 4)
- Dating site (RuCTFE 2010)
- Picture search engine (RuCTFE 2011)

(not so) Simple web-services examples

- POP3 server (UralCTF 4)
- Dating site (RuCTFE 2010)
- Picture search engine (RuCTFE 2011)

All of the above were organized by Hackerdom

Complex system for CTF-style contests

- Written by Lexi Pimenidis, RWTH Aachen
- Gameserver, the Submitserver, and the Scoreserver
- Was used at CIPHER, op3n, UralCTF etc

Complex system for CTF-style contests

- Written by Lexi Pimenidis, RWTH Aachen
- Gameserver, the Submitserver, and the Scoreserver
- Was used at CIPHER, op3n, UralCTF etc
- There were no Ubic 6 years ago :)

Links

DEFCON CTF: http://www.ddtek.biz

RuCTF: http://ructf.org

PeterPEN: http://peterpen-ctf.net

BlackBox: http://blackbox.sibears.ru

Nikto2: http://cirt.net/nikto2

Exploitfarm: http://code.google.com/p/exploitfarm

CIPHER Gameserver: http://www.cipher-ctf.org/Gameserver.php

Twitter: @SR0MAN0V (yes, zeros instead of "O"s)

Thank you!

PS: DEFCON XX Quals start 2 Jun 2012! Join!