Perl Basics for Pentesters Part 2

Sanjeev Jaiswal (Jassi)

Perl Programmer and Security Enthusiast

#nullhyd (2016)

What we will cover

Part 1

Perl Introduction

Control structures and loops

Functions to memorize

Perl data Types

Special Variable

File handling

Part 2

Regular Expression

Perl Helpers

Perl codes basic examples

Modules to know

Scripts for Pentesting

Future Scope

Demo of tools like dnsenum, fierce, nikto, sqlninja

http://www.aliencoders.org/

Regular Expression

http://www.aliencoders.org/

Real Power of Perl

- **Regex operators:** m, s, tr
- **Metacharacters:** ^, $, ., \, |, (,), [,], *, +, ?, {, }
- **Quantifiers (iterators):** *, +, ?, {m}, {m,n}, {m,}
- **Characters classes:** [], ^(negation), - (ranges)
- **Character class abbr:** \d, \D, \s, \S, \w, \W,
- **Anchors:** ^, $, \b ,\B, \A,\Z, \z
- **Modifiers:** m,s,i,g,e,x etc.

http://www.aliencoders.org/

Real Power of Perl

- `next if $file =~ m/\.{1,2}/; #skip if its . or ..`
- `if($ARGV[0] =~/^(\d+\.){3}\d+$/) { .. } # IPv4`
- `$word =~ s/^\s+|\s+$//; #trim a word`
- `return int( (split /\./, $string)[0] ); #string to int conversion`
- `my $email =~ /^([a-zA-Z][\w\_\.]{6,15})\@([a-zA-Z0-9-]+)\.([a-zA-Z]{2,4})$/; #email validation`
- `my ($matched) = $content =~ /$phone_code(.*?)\d+/sg ? $1 : 'No Result.';`
- `my ($alexa_rank) = $content =~ m#globe-sm\.jpg(?:.*?)">(.*?)</strong>?#gis`
- `($version) = $content =~ /version\s+(\d+\.\d+(?:\.\d+)?)/mig; } # wp-version`
- `m#wp-(?:admin|content|includes)/(?!plugins|js).*?ver=(\d+\.\d+(?:\.\d+)?(?:[-\w\.]+)?)#mig; }`
- `$dob =~ #^((?:19|20)\d\d)[-/.](0[1-9]|1[012])[-/.](0[1-9]|[12][0-9]|3[01])$#; #yyyy-mm-dd format`

http://www.aliencoders.org/

Perl Modules to learn

http://www.aliencoders.org/

Modules useful for Pentesters

- **CGI –** Handles CGI request and responses
- **DBI** – for any database related stuffs
- **Net::IP –** manipulate IPv4/IPv6 address
- **Net::RawIP -** manipulate raw IP packets with interface to **libpcap**
- **Net::DNS –** DNS resolver implemented in Perl
- **Net::SNMP -** Object oriented interface to SNMP
- **IO::Socket -** Object interface to socket communications
- **WWW::Mechanize -** Automating web browsing
- **LWP::UserAgent –** web user agent class
- http://search.cpan.org/~jabra/ for all scan parsers

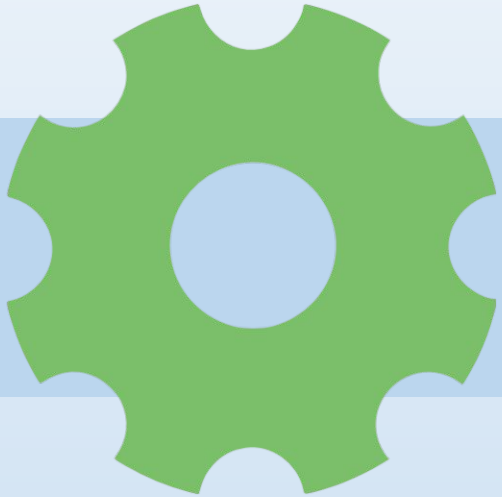
Perl Helpers

http://www.aliencoders.org/

- **perldoc perlmodlib** – modules with Perl distribution
- **perldoc perllocal** – Locally installed modules
- **perldoc perlfunc** – list of perl functions
- **perldoc perlop** – list of perl operators
- **perldoc perl** – overview of perl
- **perldoc -m Net::Ping** – see the code behind it ;)
- **perldoc -f map** – help for a specific function
- **perldoc IO::Socket** – documentation for the given module
- **man IO::Socket** – same as above
- **perl -MData::Dumper -e 'print 1 '** -module installed or not
- **perl -MCGI -e 'print "$CGI::VERSION \n" '** -module version

http://www.aliencoders.org/

Scripts for Pentesting



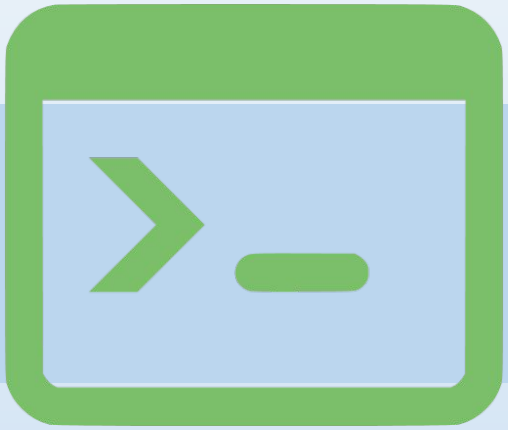
http://www.aliencoders.org/

Perl scripts in Kali/Others

- **dnsenum, dnswalk, fierce**
- **nikto -** web server scanner
- **sqlninja -** SQL Server injection and takeover tool
- **snmpenum, snmpwalk, snmpcheck**
- **arp-fingerprint –** Fingerpring a system using ARP
- **cisco-torch.pl, CAT**
- **WeBaCoo -** Web Backdoor Cookie Script kit
- **uniscan -** RFI, LFI and RCE, XSS, SQLi vulnerability scanner
- **Slowlowris -** HTTP DoS Tool

http://www.aliencoders.org/

Demo



http://www.aliencoders.org/

Kickstart with simple scripts

- DNS Info
- Header Response Info
- Website Details
- Get WordPress Version
- Simple Port scan
- IP from ifconfig
- Get GHDB list in a file
- Windows OS Version details

http://www.aliencoders.org/

Simple Port Scan


```
#!/usr/bin/perl

use strict;
 use warnings;
 use IO::Socket::INET;

my $socket;
 my $host = $ARGV[0] || die "Usage: perl $0 <hostname>\n";
 my @ports = qw(21 22 23 25 53 69 80 110 137 139 143 150 162 443 445);

for(@ports){
   my $success = eval {
   $socket = IO::Socket::INET->new(
      PeerAddr  => $host,
      PeerPort  => $_,
      Proto     => 'tcp' )
   };


  #If the port was opened, say it was and close it.
  if ($success) {
   print "Port $_ : Open\n";
   shutdown($socket, 2);
  }
 };
```

http://www.aliencoders.org/

Find WordPress Version


```
use WWW::Mechanize;
use LWP::UserAgent;
my $url = $ARGV[0] || die "Should pass site name $0 <sitename>\n";
$url = "http://".$url unless($url =~ m/^http/);

print "# Checking Response Header for generator tag\n";
my $meta_version = check_response_header( $url );
print_version( $url, $meta_version) if $meta_version;

print "# Checking readme.html source for the version\n";
my $readme_version = get_site_content( "$url/readme.html" );
print_version( $url, $readme_version ) if $readme_version;

print "# Checking wp-login.php source page for ?ver= instances \n";
my $login_ver = get_site_content( "$url/wp-login.php" );
print_version( $url, $login_ver ) if ( $login_ver );
```

http://www.aliencoders.org/

Get Header Response


```
use LWP::UserAgent;      # for web requests
use WWW::Mechanize;      # My favourite web scrapper module
$url = "http://".$url unless($url =~ m/^http/);

# Using LWP::UserAgent method 1
my $ua = LWP::UserAgent->new();
$ua->agent('Mozilla/5.0');

# connect and get
my $response = $ua->get($url);
print $response->headers()->as_string;

# Using WWW::Mechanize method 2
my $mech = WWW::Mechanize->new();
my $resp = $mech->get($url);
print $resp->headers->as_string;
```

http://www.aliencoders.org/

Save GHDB in text file


```
use WWW::Mechanize;
my $mech = WWW::Mechanize->new();
my $url = "http://www.exploit-db.com/google-dorks/";
$mech->get( $url );
my $link = $mech->find_link( url_regex => qr/ghdb/ );
my ($ghdb_count) = $link->[0] =~ m|ghdb/(\d+)/|;
my $exploit_url = "http://www.exploit-db.com/ghdb/";

open FH, "+<", "ghdb.txt" or die "Can\'t open ghdb.txt: $!\n";
chomp( my @ghdb_content = <FH> );
my $present_count = 0;
($present_count) = split(/\./, $ghdb_content[$#ghdb_content]) if(scalar @ghdb_content > 1);
binmode(FH, ":utf8");

for( ($present_count + 1) .. $ghdb_count ){
  my $final_url = $exploit_url."$_";
  my $mc = WWW::Mechanize->new();
  $mc->get( $final_url );
  my $dork = $mc->content();
  my $link = $mc->find_link( url_regex => qr/search|image.*?q=/);
  $link->[1] =~  s/[^[:ascii:]]+//g if($link->[1]);
  print FH "$_. $link->[1]\n" if($link->[1]);
}
close(FH);
```

http://www.aliencoders.org/

Get DNS Info of a site


```
use Net::DNS;
use Net::IP;
die "Usage: perl $0 [site_name|IP Address]\n" unless(scalar $ARGV[0]);
if($ARGV[0] =~/^(\d+\.){3}\d+$/){
  $ip_address = new Net::IP($ARGV[0],4);
} else {
  $site = $ARGV[0];
  $site =~ s#http[s]?://##;
  $site =~ s/www\.//;
}
my $res = Net::DNS::Resolver->new;
if($site){ show_ip();  show_ns();   show_mx();   show_soa(); }
show_ip_lookup() if($ip_address);
```

http://www.aliencoders.org/

Get IP from ifconfig


```
open my $in, "/sbin/ifconfig |";

my (@addrs);

while (my $line = <$in>)
{
    if ($line =~ /inet addr:((\d+\.){3}\d+)/)
    {
        push @addrs, $1;
    }
}
close($in);

print "You have the following addresses: \n", join("\n",@addrs), "\n";
```

http://www.aliencoders.org/

ALIEN CODERS

Future Scope

http://www.aliencoders.org/

We can do almost everything

- Can write DoS exploits
- Buffer overflow test
- MITM exploits
- Fuzzying
- Nmap scripts
- RFI,RCE exploits
- Network Pentesting
- Web Attacks automations
- Integrate with RE Tools
- Data Scrapping and many more

http://www.aliencoders.org/

Resources

http://www.aliencoders.org/

Links you can follow

- http://www.cpan.org/
- http://perldoc.perl.org/
- https://twitter.com/jabra
- http://www.sans.org/
- https://www.kali.org/
- https://www.blackhat.com/
- https://www.owasp.org/index.php/Perl
- http://www.aliencoders.org/forum/Forum-perl
- http://www.iconsdb.com for icons used

Books you can read

- **Learning Perl** by Brian D foy
- **Programming Perl** by Larry Wall
- **Penetration Testing with Perl** Douglas Berdeaux
- **Network Programming with Perl** Lincon D. Stein
- **Perl for System Administration** David Edelman

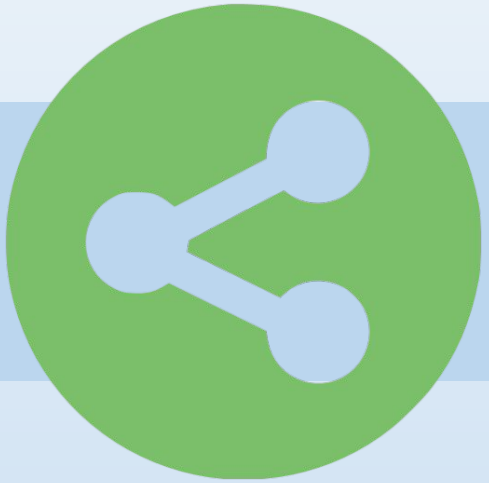
http://www.aliencoders.org/

People you can follow

- https://twitter.com/jabra Joshua Abraham
- https://twitter.com/weaknetlabs Douglas Berdeaux
- https://twitter.com/briandfoy_perl Brian D Foy
- https://twitter.com/davorg Dave Cross
- https://twitter.com/timtoady Larry Wall
- https://twitter.com/RandalSchwartz Randal L. Schwartz
- https://twitter.com/szabgab Gabor Szabo

http://www.aliencoders.org/

Support and share



http://www.aliencoders.org/

Learning through sharing

Website: http://www.aliencoders.org/

Facebook: https://www.facebook.com/aliencoders

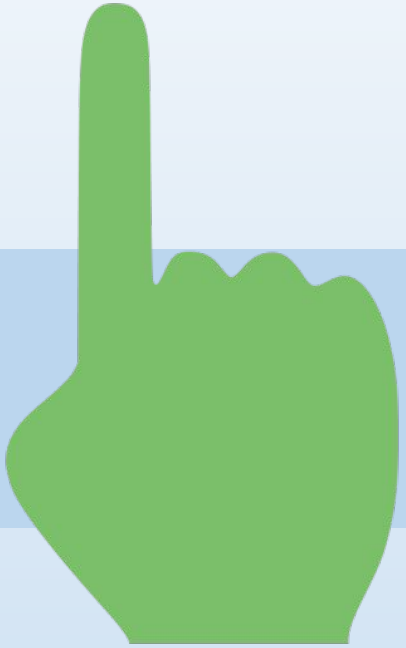
Slideshare: http://slideshare.net/jassics

Twitter: https://twitter.com/aliencoders

LinkedIn: https://www.linkedin.com/in/jassics

YouTube: http://www.youtube.com/c/flexmind

Questions



http://www.aliencoders.org/