Recognizing Application Attacks

Module Overview

Privilege escalation

Cross-site scripting

Injection attacks

Error handling

Replay attacks

API attacks

SSL stripping

Driver manipulation

Privilege Escalation

Obtaining elevated privileges (i.e. Administrator or Root) on the target

- Dump the SAM (local accounts file)
- Retrieve /etc/passwd file
- Look for insecure file shares
- DLL pre-loading
- Insecure or weak security on processes

Many vulnerabilities enable an attacker to gain system-level permissions

Cross Site Scripting (XSS)

Techniques used to hijack sessions

- Can be **non-persistent** (emails, blog posts, etc)
- **Persistent** (server based) where an attacker doesn’t need to actively target a user

Specially crafted URLs sent in an e-mail, instant message, blog posts, etc

Non-Persistent

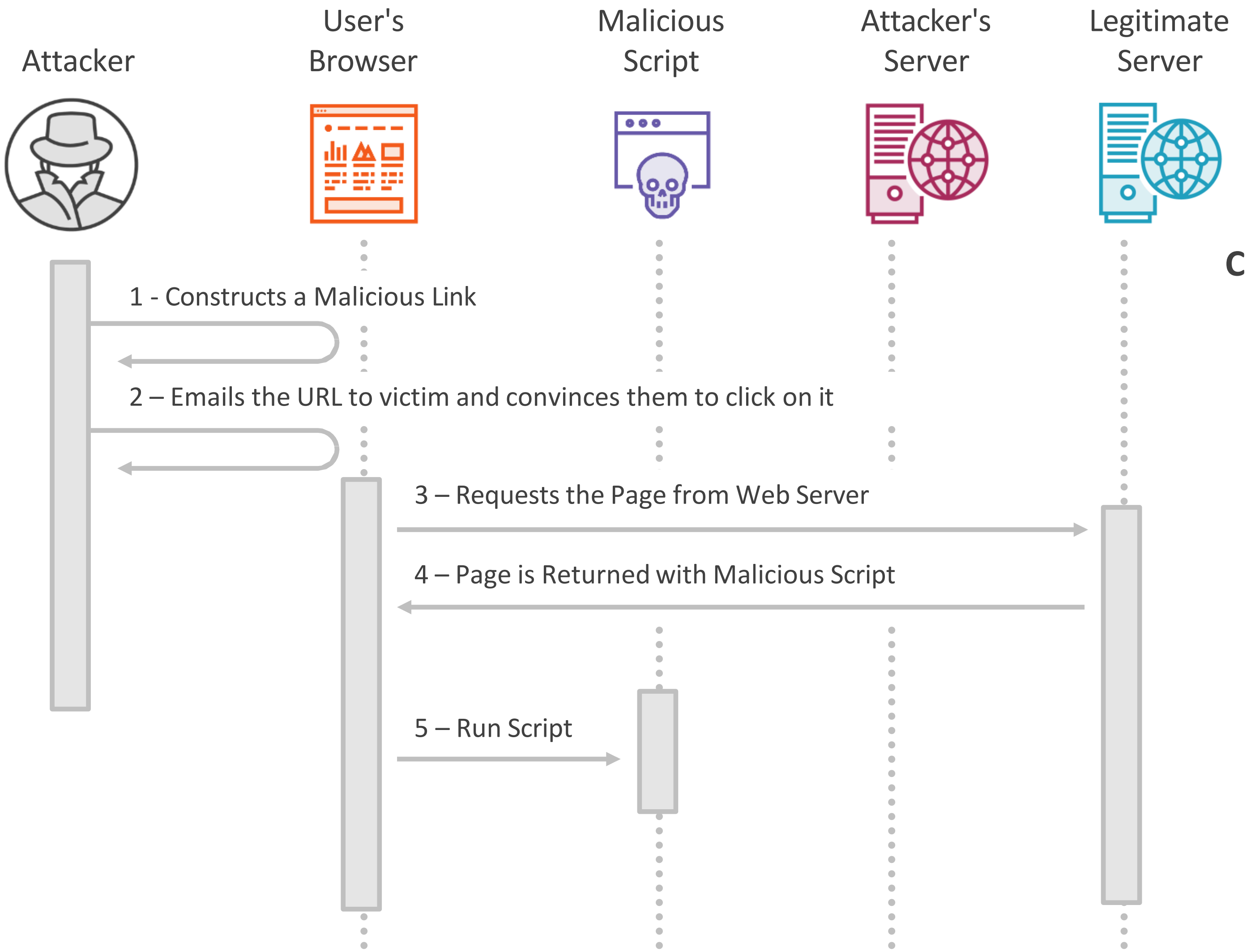
Can be non-persistent and be used to hijack sessions, etc

DOM Based

Server based and can execute on a victim’s PC by visiting an infected site

Persistent

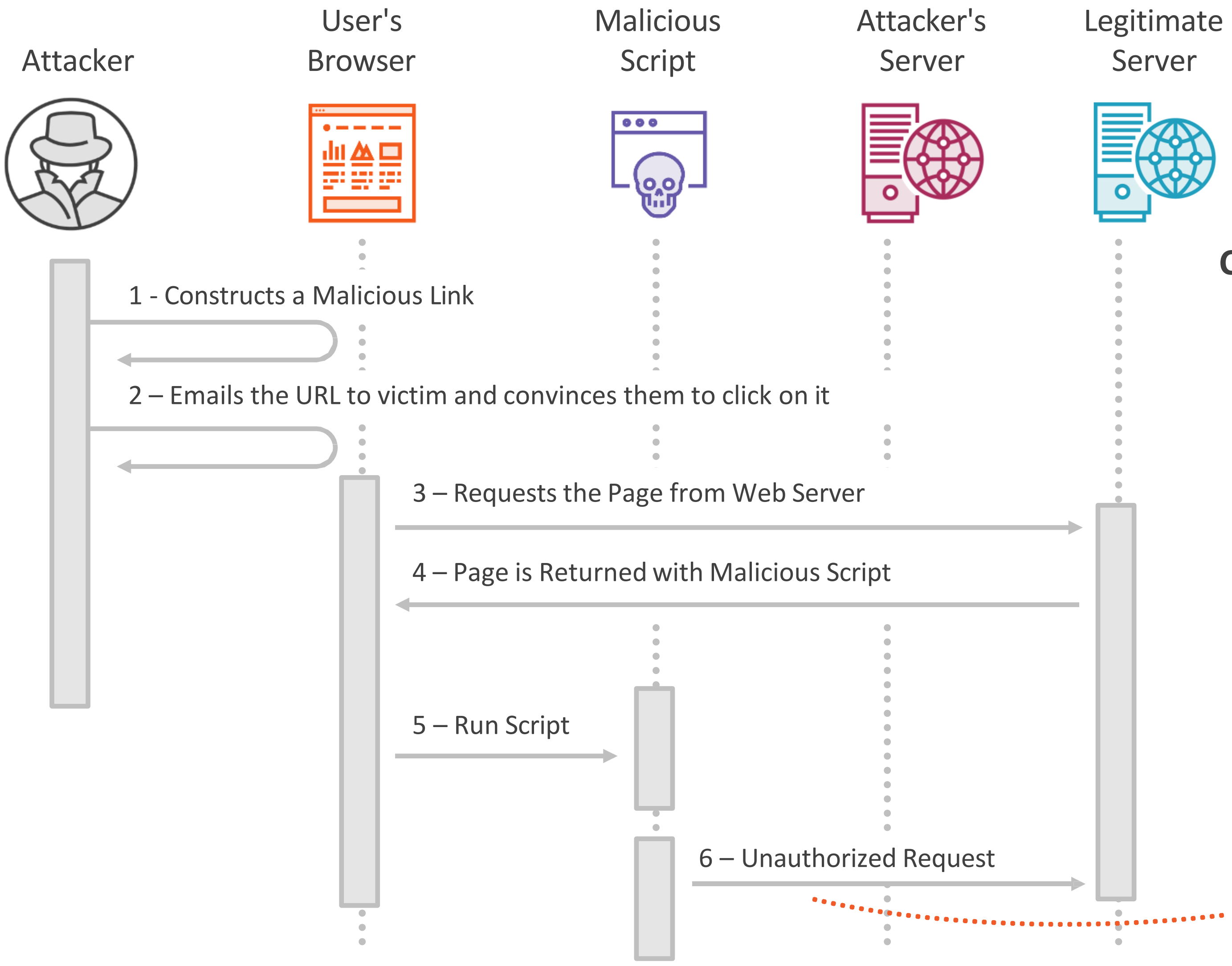
Cross Site Scripting (XSS)


Attacker
User's Browser
Malicious Script
Attacker's Server
Legitimate Server
1 - Constructs a Malicious Link
2 – Emails the URL to victim and convinces them to click on it
3 – Requests the Page from Web Server
4 – Page is Returned with Malicious Script
5 – Run Script

Cross-Site Scripting via Email

- User is sent an email containing a malicious link and is convinced to click on the link
- The URL is sent to the legitimate site, along with the malicious code which then executes in the victim's web browser
- The attacker could then issue additional requests to the legitimate server, post data to other parts of the site, etc

Cross Site Scripting (XSS)


Attacker
User's Browser
Malicious Script
Attacker's Server
Legitimate Server
1 - Constructs a Malicious Link
2 – Emails the URL to victim and convinces them to click on it
3 – Requests the Page from Web Server
4 – Page is Returned with Malicious Script
5 – Run Script
6 – Unauthorized Request

Cross-Site Scripting w/ Unauthorized Request

- User is sent an email containing a malicious link and is convinced to click on the link
- The URL is sent to the legitimate site, along with the malicious code which then executes in the victim's web browser
- The attacker could then issue additional requests to the legitimate server, post data to other parts of the site, etc

User is unaware of this request!

SQL Injection

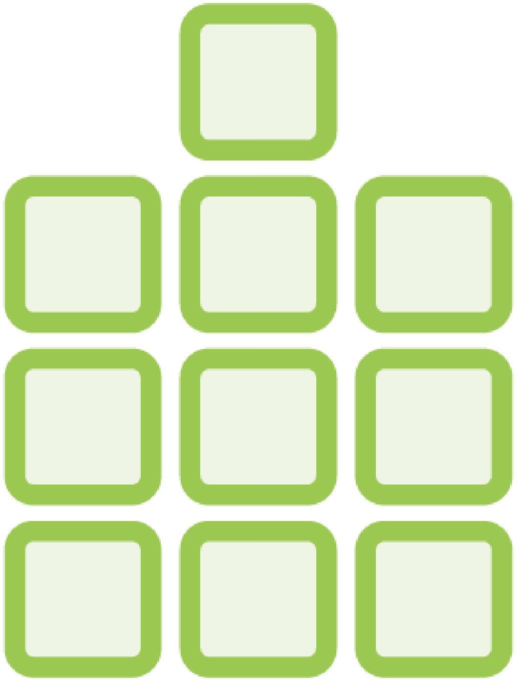
SQL (Structured Query Language)

- Modifying the SQL query that’s passed to web application,
- SQL server, etc

Adding code into a data stream

- Bypass login screens
- Vulnerable websites return usernames, passwords, etc., with the right SQL injection
- Cause the application to “throw” an error and crash (allowing an attacker remote access)

DLL Injection

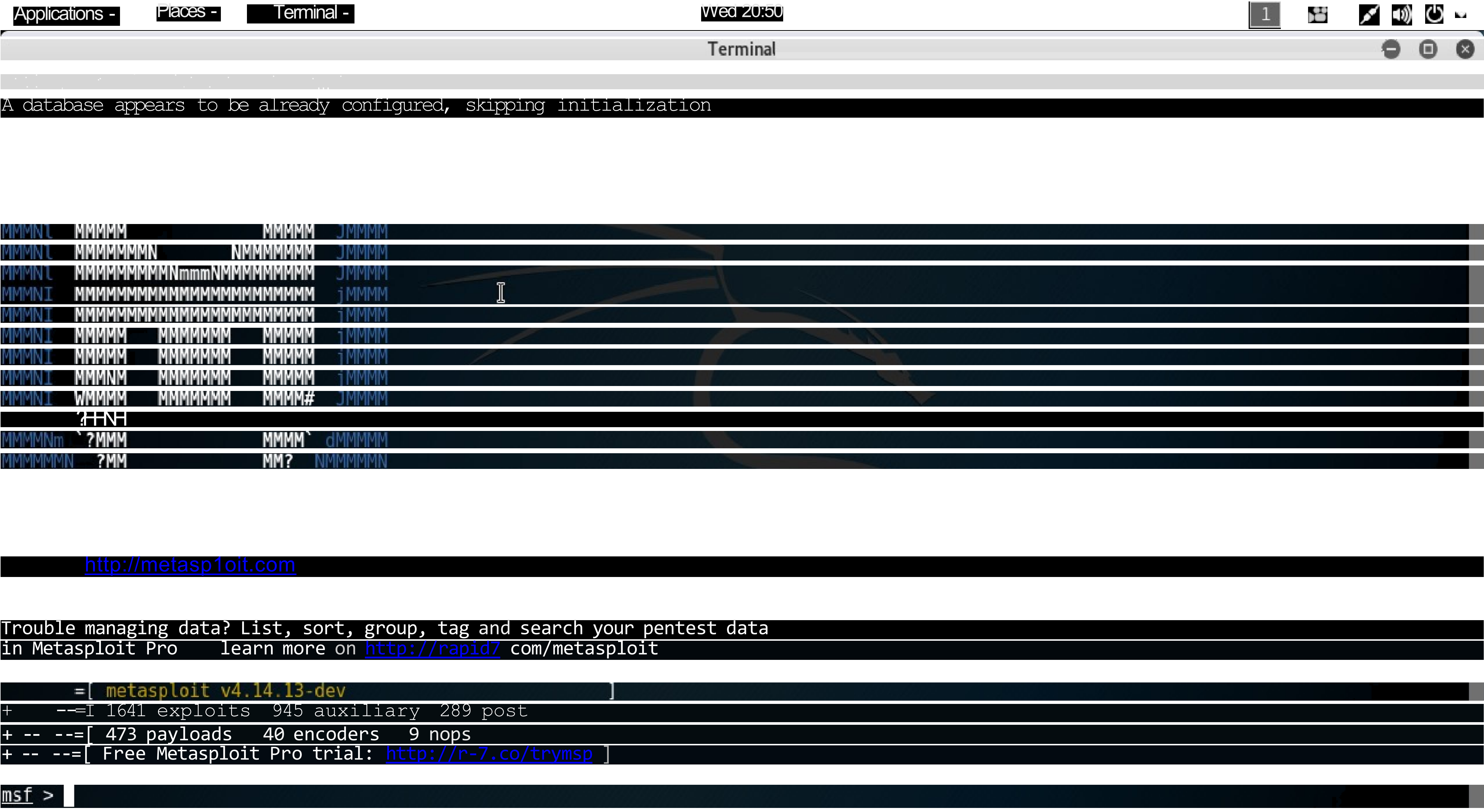


DLL Injection is a process of inserting code into a running process

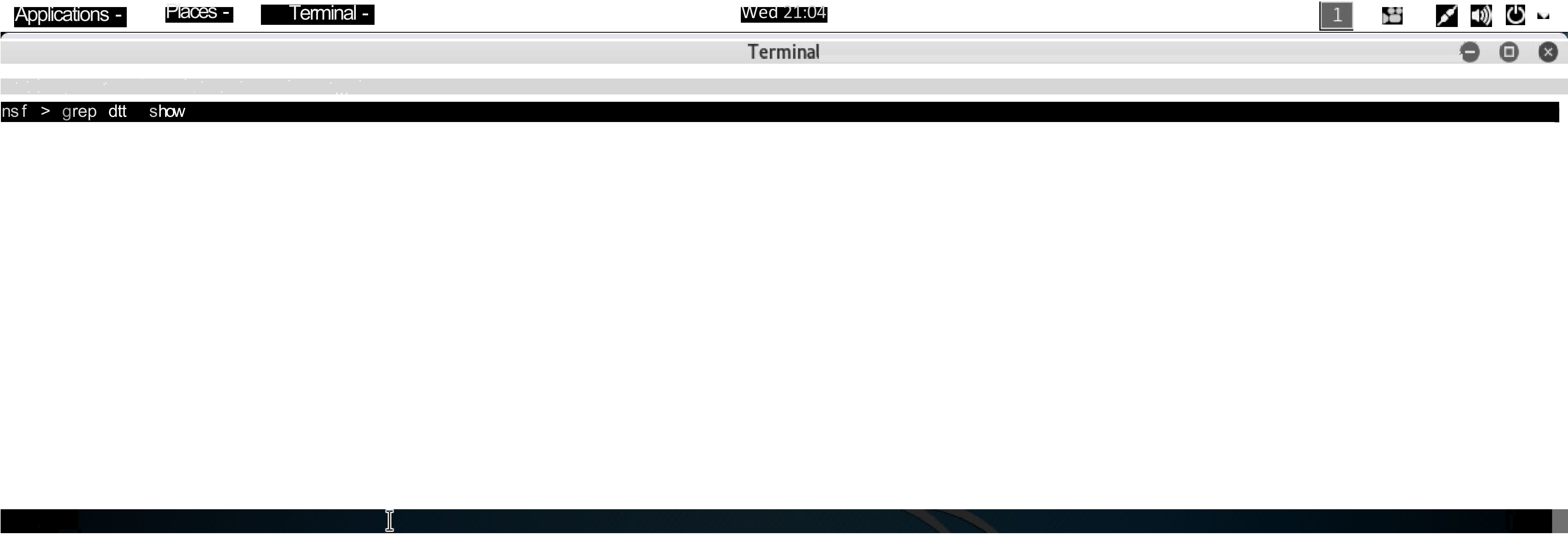
Four basic steps:

1. Attach to the process
2. Allocate Memory within the process
3. Copy the DLL or the DLL Path into the processes memory and determine appropriate memory addresses
4. Instruct the process to Execute your DLL

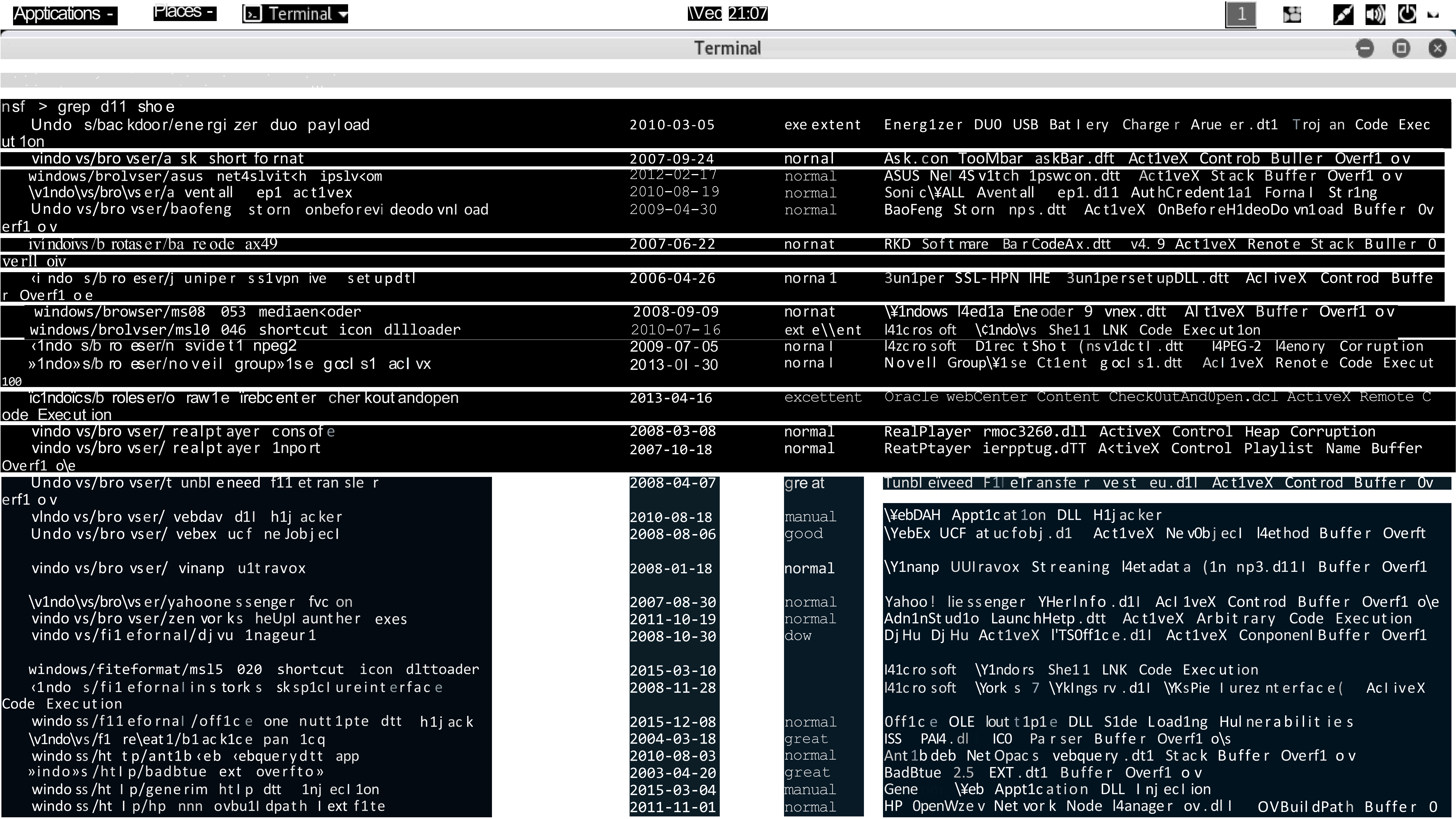
DLL injection attacks can be created manually or pen testing tools like Metasploit can automate the process



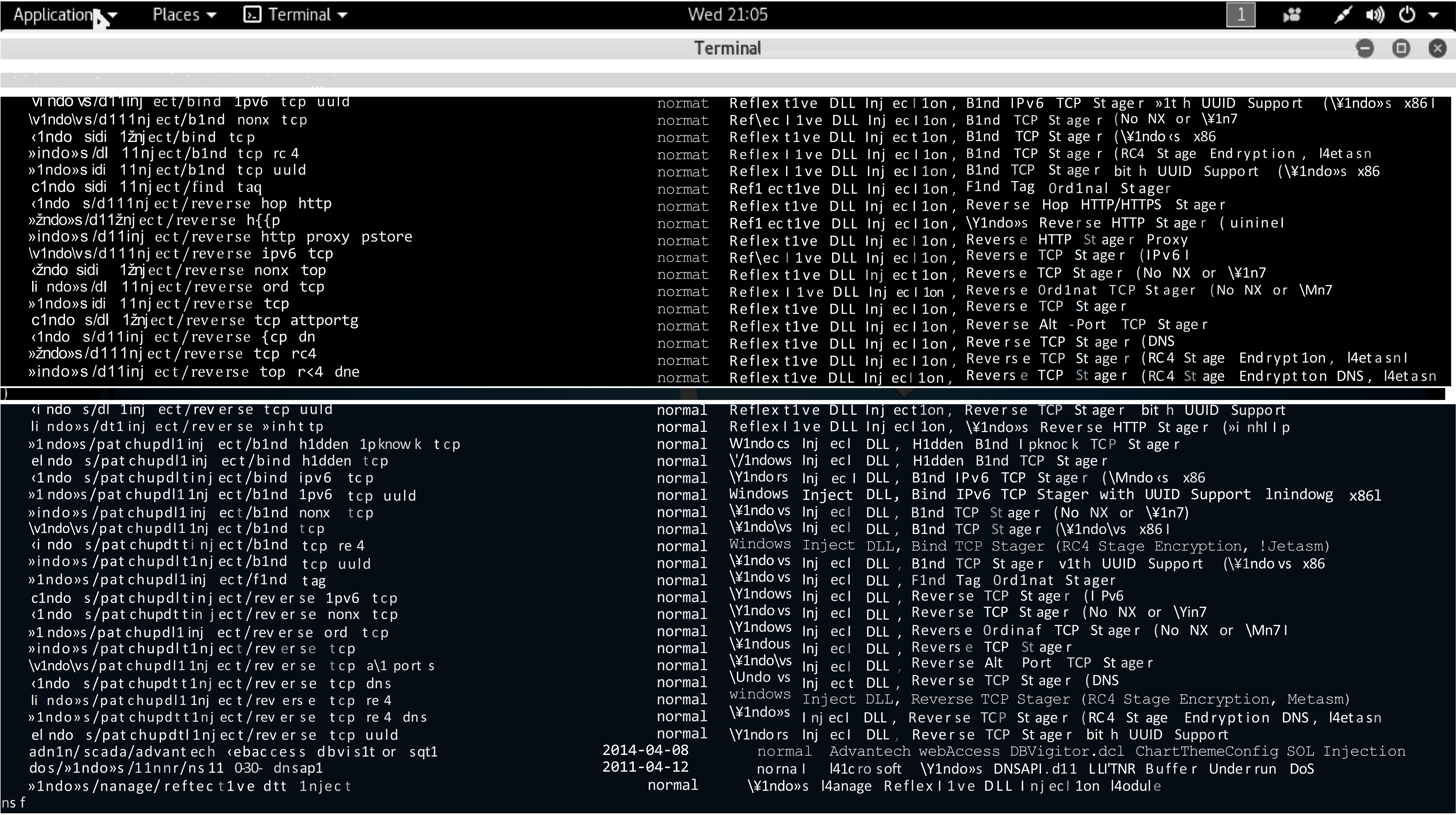
```
A database appears to be already configured, skipping initialization




MMMNL  MMMMM                MMMMM  JMMMM
MMMNL  MMMMMMMN          NMMMMMMM  JMMMM
MMMNL  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
       ?HHNH
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN



        http://metasp1oit.com


Trouble managing data? List, sort, group, tag and search your pentest data
in Metasploit Pro    learn more on http://rapid7 com/metasploit

       =[ metasploit v4.14.13-dev                              ]
+    --=I 1641 exploits  945 auxiliary  289 post
+ -- --=[ 473 payloads   40 encoders   9 nops
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```



```
nsf > grep dtt show
```



```
nsf  > grep d11  sho e
   Undo  s/bac kdoor/ene rgi zer  duo  payl oad                          2010-03-05       exe extent    Energ1zer  DUO  USB  Bat l ery  Charge r  Arue er .dt1  Troj an  Code  Exec
ut 1on
   vindo vs/bro vser/a sk  short fo rnat                                  2007-09-24       nornal        Ask.con  TooMbar  askBar.dft  Act1veX  Controb  Buller  Overf1 o v
   windows/brolvser/asus  net4slvit<h  ipslv<om                           2012-02-17       normal        ASUS  Nel 4S v1tch  1pswc on.dtt   Act1veX  St ack  Buffer  Overf1 o v
   \v1ndo\vs/bro\vs er/a  vent all    ep1  act1vex                        2010-08-19       normal        Soni c\¥ALL  Aventall   ep1.d11  AuthCredent1a1  Forna l  St r1ng
   Undo vs/bro vser/baofeng   st orn   onbefo revi deodo vnl oad          2009-04-30       normal        BaoFeng  St orn   nps.dtt   Act1veX  OnBefo reH1deoDo vn1oad  Buffer  Ov
erf1 o v
   ivíndoivs/b rotas er/ba  re ode  ax49                                  2007-06-22       nornat        RKD  Soft mare  Ba r CodeAx.dtt   v4. 9  Act1veX  Renote  St ack  Buller  O
ve rll  oiv
   ‹i ndo  s/b ro  eser/j  uniper  ss1vpn  ive   set updtl                2006-04-26       norna 1       3un1per  SSL-HPN  IHE   3un1perset upDLL.dtt   Acl iveX  Controd  Buffe
r  Overf1  o e
    windows/browser/ms08  053  mediaen<oder                               2008-09-09       nornat        \¥1ndows  l4ed1a  Ene oder  9  vnex.dtt   Al t1veX  Buffer  Overf1 o v
   windows/brolvser/msl0  046  shortcut  icon  dllloader                  2010-07-16       ext  e\\ent   l41c ros oft   \¢1ndo\vs  She11  LNK  Code  Execut 1on
   ‹1ndo  s/b  ro  eser/n  svidet1  npeg2                                 2009-07-05       norna l       l4zc ro soft   D1rec t Sho t  (ns v1dct l .dtt    l4PEG-2  l4enory  Corruption
   »1ndo»s/b ro  eser/no veil  group»1se  gocl s1  acl vx                 2013-0l -30      norna l       Novell  Group\¥1se  Ct1ent  g ocl s1.dtt   Acl 1veX  Renote  Code  Execut
100
   ic1ndoics/b  roles er/o  raw1e  irebc ent er  cher kout andopen        2013-04-16       excettent     Oracle webCenter Content CheckOutAndOpen.dcl ActiveX Remote C
ode  Execut ion
   vindo vs/bro vser/ realpt ayer  cons of e                              2008-03-08       normal        RealPlayer  rmoc3260.dll  ActiveX  Control  Heap  Corruption
   vindo vs/bro vser/ realpt ayer  1nport                                 2007-10-18       normal        ReatPtayer  ierpptug.dTT  A<tiveX  Control  Playlist  Name  Buffer
Overf1  o\e
   Undo vs/bro vser/t  unbl eneed  f11 et ran sle  r                      2008-04-07       gre at        Tunbl eïveed  F1l eTr ansfe r   ve st  eu.d1l  Act1veX  Controd  Buffer  Ov
erf1 o v
   vlndo vs/bro vser/  vebdav  d1l   h1j ac ker                           2010-08-18       manual        \¥ebDAH  Appt1c at 1on  DLL  H1j ac ker
   Undo vs/bro vser/  vebex  ucf  ne Jobj ecl                             2008-08-06       good          \YebEx  UCF  at ucfobj.d1   Act1veX  Ne vObj ecl  l4ethod  Buffer  Overft

   vindo vs/bro vser/  vinanp  u1t ravox                                  2008-01-18       normal        \Y1nanp  UUlravox  St reaning  l4etadat a  (1n  np3.d11l  Buffer  Overf1

  \v1ndo\vs/bro\vs er/yahoone ssenger  fvc on                             2007-08-30       normal        Yahoo!  lie ssenger  YHerlnfo.d1l  Acl 1veX  Controd  Buffer  Overf1  o\e
   vindo vs/bro vser/zen vor ks  heUpl aunther   exes                     2011-10-19       normal        Adn1nSt ud1o  LaunchHetp.dtt   Act1veX  Arbit rary  Code  Execution
   vindo vs/fi1 efornal/dj vu  1nageur1                                   2008-10-30       dow           DjHu  DjHu  Act1veX  l'TSOff1c e.d1l  Act1veX  Conponenl Buffer  Overf1

  windows/fiteformat/msl5  020  shortcut   icon   dlttoader               2015-03-10                     l41c ro soft   \Y1ndors  She11  LNK  Code  Execution
  ‹1ndo  s/fi1 efornal ins tork s   sksp1cl ureint erfac e                2008-11-28                     l41c ro soft   \York s  7  \YkIngs rv .d1l  \YKsPie  l urez nt erface(    Acl iveX
Code  Execution
   windo ss/f11 efornal /off1c e  one  nutt1pte  dtt    h1jack            2015-12-08       normal        Off1c e  OLE  lout t1p1e  DLL  S1de  Load1ng  Hulnerabilit ies
  \v1ndo\vs/f1  re\eat1/b1ac k1ce  pan  1cq                               2004-03-18       great         ISS   PAI4.dl    ICO   Pa rser  Buffer  Overf1  o\s
   windo ss/ht  t p/ant1b‹eb  ‹ebqueryd tt   app                          2010-08-03       normal        Ant1b deb  Net Opac s  vebquery.dt1  St ack  Buffer  Overf1 o v
   »indo»s /htl p/badbtue  ext   overfto»                                 2003-04-20       great         BadBtue  2.5   EXT.dt1  Buffer  Overf1 o v
   windo ss/ht l p/generim  htl p  dtt    1nj ecl 1on                     2015-03-04       manual        Gene      \¥eb  Appt1cation  DLL  l nj ecl ion
   windo ss/ht l p/hp  nnn  ovbu1l dpath  l ext f1te                      2011-11-01       normal        HP  OpenWze v  Net vor k  Node  l4anager  ov.dl l    OVBuildPath  Buffer  O
```



```
 vi ndo vs/d11inj ect/bind 1pv6 tcp uuld                          normat  Reflex t1ve DLL Inj ec l 1on, B1nd IPv6 TCP St age r »1t h UUID Support (\¥1ndo»s x86 l
\v1ndo\vs/d111nj ect/b1nd nonx tcp                                normat  Ref\ec l 1ve DLL Inj ec l 1on, B1nd TCP St age r (No NX or \¥1n7
 ‹1ndo sidi 1žnject/bind tcp                                      normat  Reflex t1ve DLL Inj ect 1on, B1nd TCP St age r (\¥1ndo ‹s x86
»indo»s /dl 11nject/b1nd tcp rc 4                                 normat  Reflex l 1ve DLL Inj ec l 1on, B1nd TCP St age r (RC4 St age Endryption, l4etasn
»1ndo»s idi 11nj ect/b1nd tcp uuld                                normat  Reflex l 1ve DLL Inj ec l 1on, B1nd TCP St age r bit h UUID Support (\¥1ndo»s x86
 c1ndo sidi 11nject/find taq                                      normat  Ref1 ect1ve DLL Inj ec l 1on, F1nd Tag Ord1nal St ager
 ‹1ndo s/d111nj ect/reverse hop http                              normat  Reflex t1ve DLL Inj ec l 1on, Reverse Hop HTTP/HTTPS St age r
»žndo»s/d11žnject/reverse h{{p                                    normat  Ref1 ect1ve DLL Inj ec l 1on, \Y1ndo»s Reverse HTTP St age r ( uininel
»indo»s /d11inj ect/reverse http proxy pstore                     normat  Reflex t1ve DLL Inj ec l 1on, Revers e HTTP St age r Proxy
\v1ndo\vs/d111nj ect/reverse ipv6 tcp                             normat  Ref\ec l 1ve DLL Inj ec l 1on, Revers e TCP St age r (IPv6 l
 ‹žndo sidi 1žnject/reverse nonx top                              normat  Reflex t1ve DLL Inj ect 1on, Revers e TCP St age r (No NX or \¥1n7
 li ndo»s /dl 11nject/reverse ord tcp                             normat  Reflex l 1ve DLL Inj ec l 1on, Revers e Ord1nat TCP St ager (No NX or \Mn7
»1ndo»s idi 11nj ect/reverse tcp                                  normat  Reflex t1ve DLL Inj ec l 1on, Revers e TCP St age r
 c1ndo s/dl 1žnject/reverse tcp attportg                          normat  Reflex t1ve DLL Inj ec l 1on, Reverse Alt -Port TCP St age r
 ‹1ndo s/d11inj ect/reverse {cp dn                                normat  Reflex t1ve DLL Inj ec l 1on, Reverse TCP St age r (DNS
»žndo»s/d111nj ect/reverse tcp rc4                                normat  Reflex t1ve DLL Inj ec l 1on, Reve rs e TCP St age r (RC4 St age Endrypt1on, l4etasnl
»indo»s /d11inj ect/reverse top r<4 dne                           normat  Reflex t1ve DLL Inj ec l 1on, Revers e TCP St age r (RC4 St age Endryptton DNS, l4etasn
)
 ‹i ndo s/dl 1inj ect/rev erse tcp uuld                           normal  Reflex t1ve DLL Inj ect1on, Reverse TCP St age r bit h UUID Support
 li ndo»s/dt1inj ect/rev erse »inhttp                             normal  Reflex l 1ve DLL Inj ec l 1on, \¥1ndo»s Reverse HTTP St age r (»i nhl l p
»1ndo»s/pat chupdl1inj ect/b1nd h1dden 1pknow k tcp               normal  W1ndo cs Inj ecl DLL, H1dden B1nd l pknoc k TCP St age r
 el ndo s/pat chupdl1inj ect/bind h1dden tcp                      normal  \'/1ndows Inj ecl DLL, H1dden B1nd TCP St age r
 ‹1ndo s/pat chupdltinj ect/bind ipv6 tcp                         normal  \Y1ndo rs Inj ec l DLL, B1nd IPv6 TCP St age r (\Mndo ‹s x86
»1 ndo»s/pat chupdl1 1nj ect/b1nd 1pv6 tcp uuld                   normal  Windows Inject DLL, Bind IPv6 TCP Stager with UUID Support lnindowg x86l
»indo»s /pat chupdl1inj ect/b1nd nonx tcp                         normal  \¥1ndo vs Inj ecl DLL, B1nd TCP St age r (No NX or \¥1n7)
\v1ndo\vs/pat chupdl1 1nj ect/b1nd tcp                            normal  \¥1ndo\vs Inj ecl DLL, B1nd TCP St age r (\¥1ndo\vs x86 l
 ‹i ndo s/pat chupdttinj ect/b1nd tcp re 4                        normal  Windows Inject DLL, Bind TCP Stager (RC4 Stage Encryption, !Jetasm)
»indo»s /pat chupdlt1nj ect/b1nd tcp uuld                         normal  \¥1ndo vs Inj ecl DLL, B1nd TCP St age r v1th UUID Support (\¥1ndo vs x86
»1ndo»s /pat chupdl1inj ect/f1nd tag                              normal  \¥1ndo vs Inj ecl DLL, F1nd Tag Ord1nat St ager
 c1ndo s/pat chupdltinj ect/rev er se 1pv6 tcp                    normal  \Y1ndows Inj ecl DLL, Reverse TCP St age r (l Pv6
 ‹1ndo s/pat chupdttin ject/rev er se nonx tcp                    normal  \Y1ndo vs Inj ecl DLL, Reverse TCP St age r (No NX or \Yin7
»1 ndo»s/pat chupdl1inj ect/rev er se ord tcp                     normal  \Y1ndows Inj ecl DLL, Revers e Ordinaf TCP St age r (No NX or \Mn7 l
»indo»s /pat chupdlt1nj ect/rev er se tcp                         normal  \¥1ndous Inj ecl DLL, Revers e TCP St age r
\v1ndo\vs/pat chupdl1 1nj ect/rev er se tcp a\1 port s            normal  \¥1ndo\vs Inj ecl DLL, Reverse Alt Port TCP St age r
 ‹1ndo s/pat chupdtt1nj ect/rev er se tcp dns                     normal  \Undo vs Inj ect DLL, Reverse TCP St age r (DNS
 li ndo»s/pat chupdl1 1nj ect/rev ers e tcp re 4                  normal  windows Inject DLL, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
»1ndo»s /pat chupdtt1nj ect/rev er se tcp re 4 dns                normal  \¥1ndo»s l nj ecl DLL, Reverse TCP St age r (RC4 St age Endryption DNS, l4etasn
 el ndo s/pat chupdtl1nj ect/rev er se tcp uuld                   normal  \Y1ndo rs Inj ecl DLL, Reverse TCP St age r bit h UUID Support
adn1n/scada/advant ech ‹ebaccess dbvis1t or sqt1         2014-04-08      normal  Advantech webAccess DBVigitor.dcl ChartThemeConfig SOL Injection
dos/»1ndo»s/11nnr/ns11 030- dnsap1                       2011-04-12      norna l  l41cro soft \Y1ndo»s DNSAPI.d11 LLI'TNR Buffe r Underrun DoS
»1ndo»s/nanage/reftect1ve dtt 1nject                                  normal  \¥1ndo»s l4anage Reflex l 1ve DLL l nj ecl 1on l4odule
ns f
```

LDAP Injection

LDAP = Lightweight Directory Access Protocol

- “Address Book” of user accounts used to authenticate users
- Identifies level of access, group memberships, etc

Similar to SQL injection attacks in that the query that is passed to the web server is modified to include malicious query statements or code

XML Injection

Form Input Example

```
<input type="text" size=20 name="userName">Insert the username</input>
```

Underlying Code

```
String ldapSearchQuery = "(cn=" + $userName + ")";
 System.out.println(ldapSearchQuery);
```

String Passed From the Web Browser

```
“crees) (| (password = * ) )”
```

```
<?xml version="1.0"?>

<!DOCTYPE results [<!ENTITY harmless SYSTEM
"file:///var/www/config.ini">]>

<results>

    <result>&harmless;</result>

</results>
```

XML Injection

Attack technique that manipulates the logic of an XML application or service

- Could be used to inject XML into a statement that alters a path to a file to disclose sensitive information

Pointer Dereference

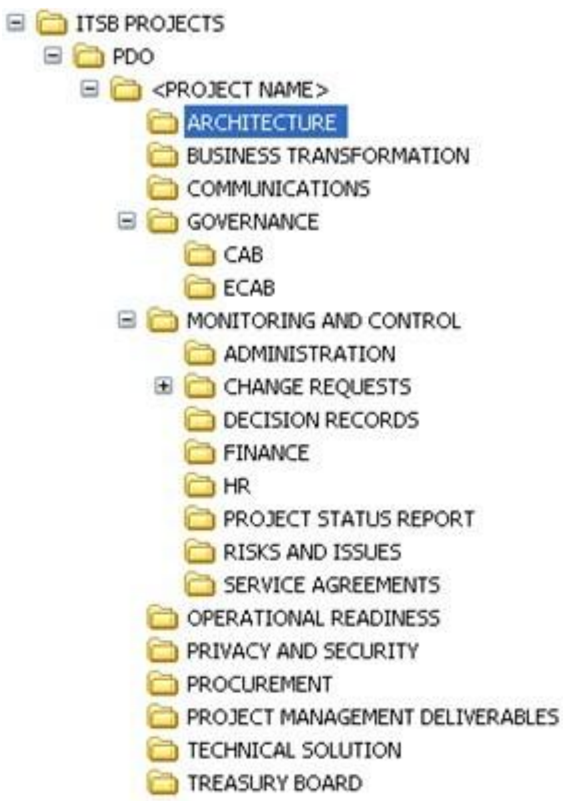
Vulnerability that can cause an application to throw an exception error, which typically results in the application crashing

- Can be leveraged for a DoS attack against the entire system
- Remote code execution

C/C++, Assembly or any other language that uses pointers is potentially vulnerable to this type of attack

Directory Traversal/Command Injection

- Attack that manipulates user input to cause the application to traverse a directory structure and access files not intended to be visible
  - Known as the ../ or “dot slash” attack
  - Directory climbing
  - Backtracking



- ITSB PROJECTS
  - PDO
    - <PROJECT NAME>
      - ARCHITECTURE
      - BUSINESS TRANSFORMATION
      - COMMUNICATIONS
      - GOVERNANCE
        - CAB
        - ECAB
      - MONITORING AND CONTROL
        - ADMINISTRATION
        - CHANGE REQUESTS
        - DECISION RECORDS
        - FINANCE
        - HR
        - PROJECT STATUS REPORT
        - RISKS AND ISSUES
        - SERVICE AGREEMENTS
      - OPERATIONAL READINESS
      - PRIVACY AND SECURITY
      - PROCUREMENT
      - PROJECT MANAGEMENT DELIVERABLES
      - TECHNICAL SOLUTION
      - TREASURY BOARD

Buffer Overflow

Attack that causes a system or app to crash or behave unexpectedly

- Writing more data than the buffer can handle
- Data is written to adjacent memory

Calls or pointers to jump to a different address than what was intended

- Can contain user executable code which could allow remote code execution

Race conditions

A race condition occurs when a pair of routine programming calls in an application do not perform in the sequential manner that was intended

- Potential security vulnerability if the calls are not performed in the correct order

Potential Vulnerabilities

- Authentication: Trust may be assigned to an entity who is not who it claims to be
- Integrity: Data from an untrusted (and possibly malicious) source may be integrated
- Confidentiality: Data may be disclosed to an entity impersonating a trusted entity, resulting in information disclosure

Time of Check

Type of race condition

- Attacker is able to gain access prior to an authentication check
- Inserts code or alters authentication to disrupt normal authentication processes
- Administrator see the intrusion, reset passwords, etc., but the attacker may still have access
  - Attacker could remain logged in with old credentials

Also referred to as Time of Check to Time of Use (TOCTTOU)

Secure Coding Concepts (m1-6)

Application development is often a balancing act between time to market and security

- Building for security adds to development time
  - Critical – If you don't have time to find the vulnerabilities, the bad guys will

"If you don't have time to do it right the first time…

...How are you going to have time to go back and do it twice?"

Secure Coding Concepts

Error and exception handling

- What does the application do when it encounters an error?
  - Does it continue running, restart a process or module, or completely crash?
- If it crashes, does it give an attacker elevated privileges
  - Keys to the castle?

Secure Coding Concepts

Input Validation

- Validate/sanitize what is entered at the client side and/or server side before it's processed
- Mitigate attacks such as Cross Site Scripting (XSS)
- SQL Injection attacks

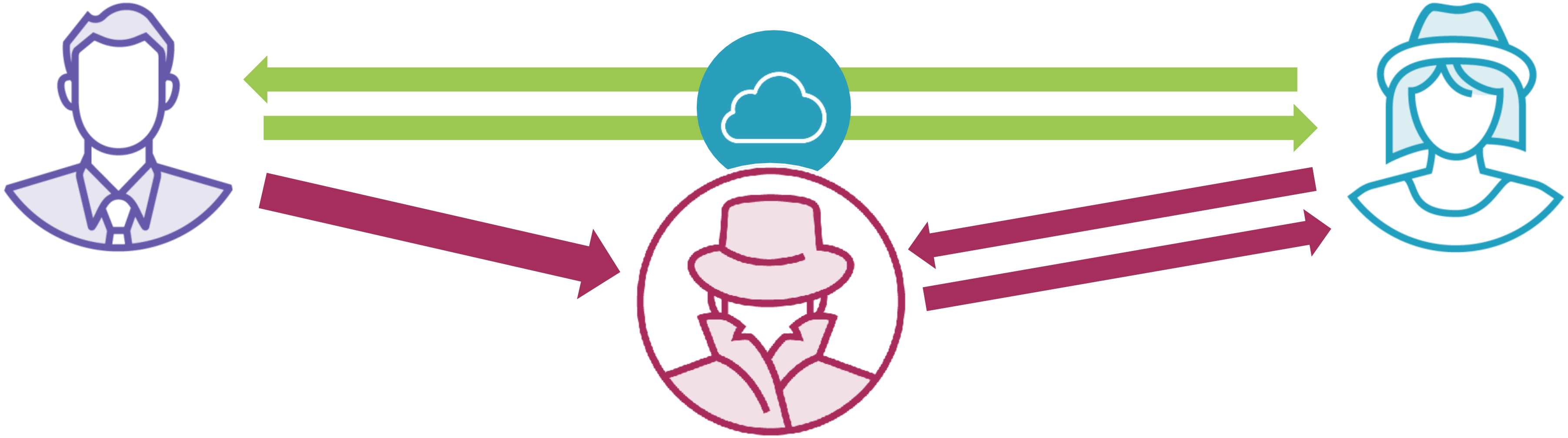
metasploit
Exploit-Me
A suite of Firefox web application security testing tools.
Add-ons for Firefox
netsparker
web application security scanner

Replay Attacks

Sniffing the wired or wireless network, a replay attack captures packets and puts them back on the wire

- Packets can potentially be modified and retransmitted to look like legitimate packets

Sequencing helps mitigate the effectiveness of this type of attack



Integer Overflow

Integer overflow condition occurs when the result of an arithmetic operation exceeds the maximum size of integer type used to store it.

When the overflow occurs, the interpreted value appears to “wrap around” the max value and start at the min value

- Could allow transactions to be reversed (i.e. money sent instead of received)

Cross Site Request Forgery (XSRF)

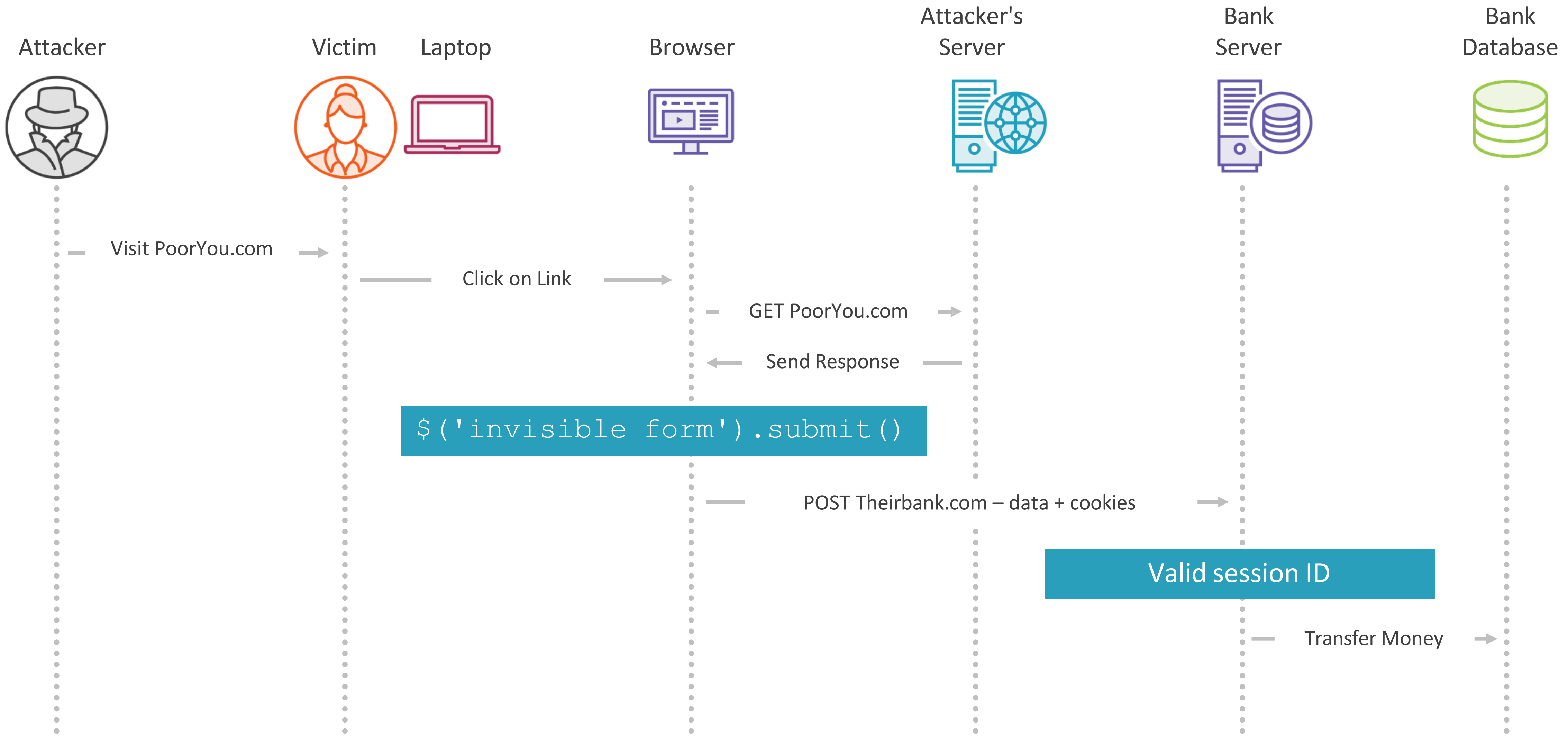
Exploiting a website’s trust in a user (application, IP address, etc)

Often referred to as one-click attack or session riding

- CSRF or “See-Surf”

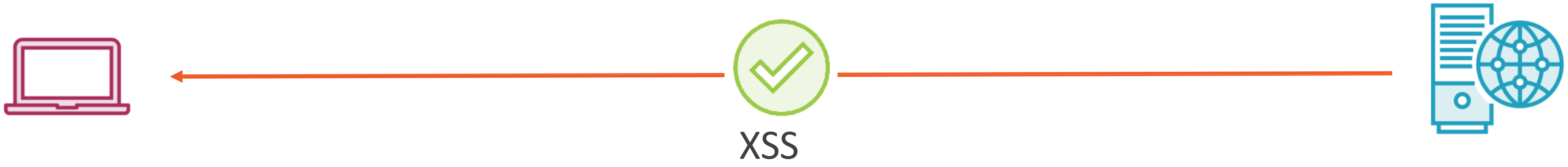
Requires victim to have recently visited the target website and have a valid cookie (not expired)

XSRF Example

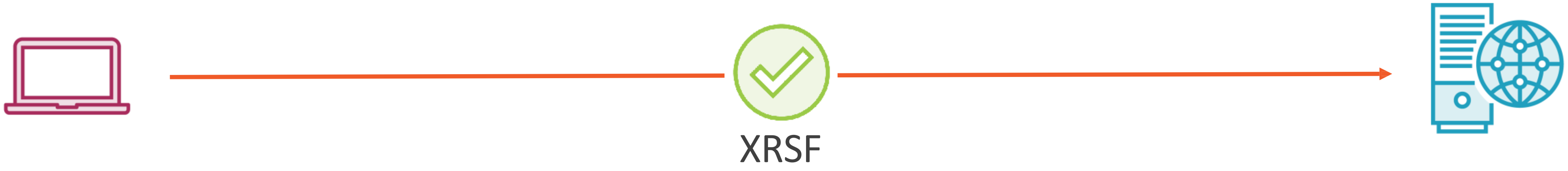


XSS and XSRF Distinction

In an XSS attack, the browser runs malicious code because it was served from a site it trusts



In an XSRF attack, the server performs an action because it was sent a request from a client it trusts



DDoS

Large scale attack against a target

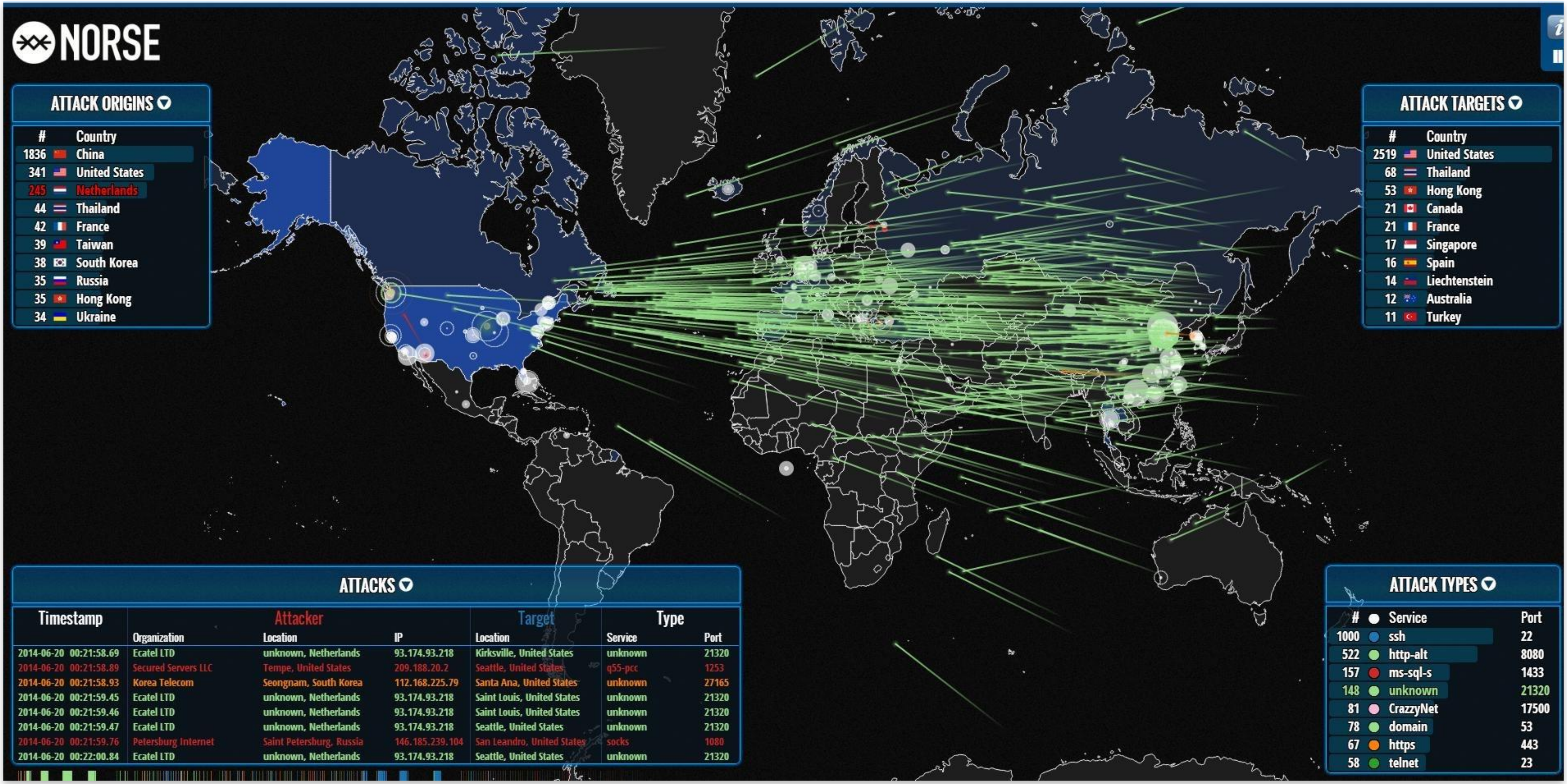
- Botnets
- Bot herders
- Command and Control (C&C) Center

C&C issues command(s) to botnet zombies to initiate attack against a target

- Could be hundreds, thousands or millions of zombies comprising a botnet army

DoS (Denial of Service)

- Similar type of attack but on much smaller scale



NORSE

ATTACK ORIGINS

#	Country
1836	China
341	United States
245	Netherlands
44	Thailand
42	France
39	Taiwan
38	South Korea
35	Russia
35	Hong Kong
34	Ukraine

ATTACK TARGETS

#	Country
2519	United States
68	Thailand
53	Hong Kong
21	Canada
21	France
17	Singapore
16	Spain
14	Liechtenstein
12	Australia
11	Turkey

ATTACKS

Timestamp	Attacker			Target	Type	
	Organization	Location	IP	Location	Service	Port
2014-06-20 00:21:58.69	Ecatel LTD	unknown, Netherlands	93.174.93.218	Kirksville, United States	unknown	21320
2014-06-20 00:21:58.89	Secured Servers LLC	Tempe, United States	209.188.20.2	Seattle, United States	q55-pcc	1253
2014-06-20 00:21:58.93	Korea Telecom	Seongnam, South Korea	112.168.225.79	Santa Ana, United States	unknown	27165
2014-06-20 00:21:59.45	Ecatel LTD	unknown, Netherlands	93.174.93.218	Saint Louis, United States	unknown	21320
2014-06-20 00:21:59.46	Ecatel LTD	unknown, Netherlands	93.174.93.218	Saint Louis, United States	unknown	21320
2014-06-20 00:21:59.47	Ecatel LTD	unknown, Netherlands	93.174.93.218	Seattle, United States	unknown	21320
2014-06-20 00:21:59.76	Petersburg Internet	Saint Petersburg, Russia	146.185.239.104	San Leandro, United States	socks	1080
2014-06-20 00:22:00.84	Ecatel LTD	unknown, Netherlands	93.174.93.218	Seattle, United States	unknown	21320

ATTACK TYPES

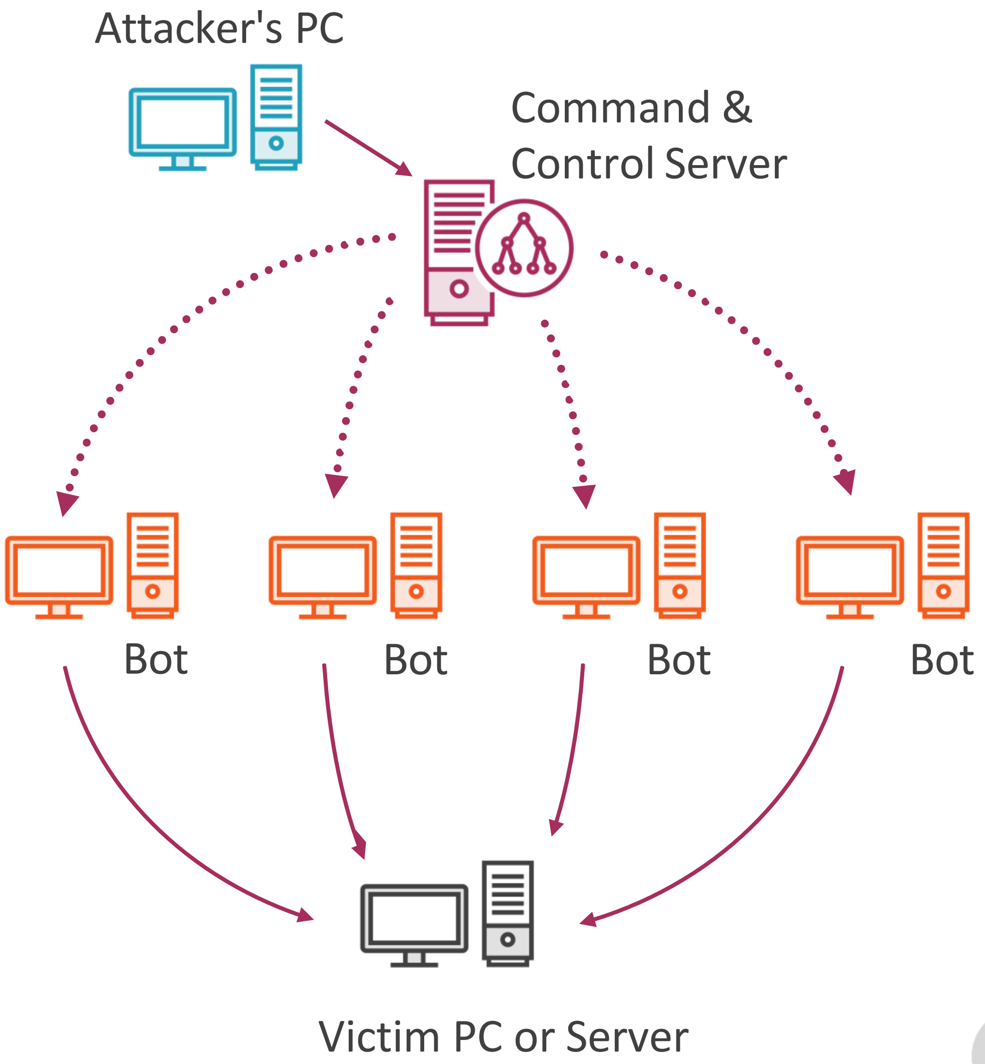
#	●	Service	Port
1000	●	ssh	22
522	●	http-alt	8080
157	●	ms-sql-s	1433
148	●	unknown	21320
81	●	CrazzyNet	17500
78	●	domain	53
67	●	https	443
58	●	telnet	23

Distributed Denial of Service (DDoS) Attack From Points in China against the United States

Resource Exhaustion

Attack whereby a malicious user executes code or processes on a machine over and over until all resources are exhausted

Denial of Service (DoS) or Distributed Denial of Service (DDoS) are examples of this type of attack



Application Programming Interface (API) Attacks

Gartner states that By 2022, API abuses will move from **an infrequent** to the **most-frequent attack vector,** resulting in data breaches for enterprise web applications

API Attack

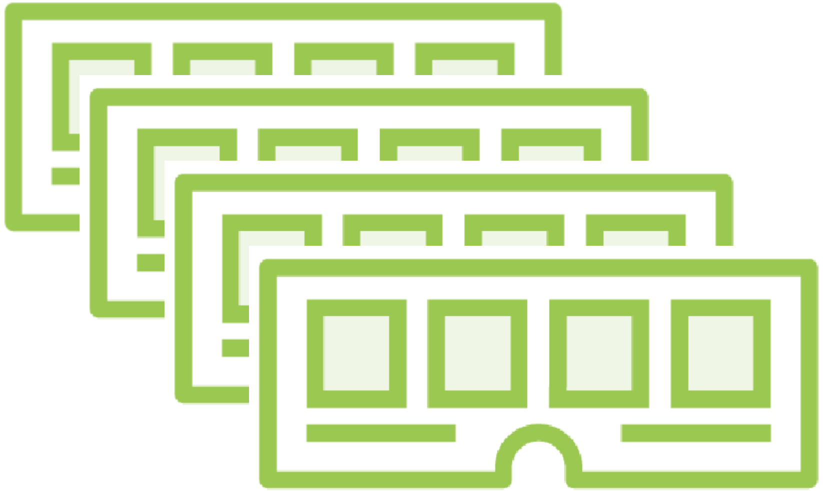
- Hostile usage of an API
  - Injection attacks
  - DoS/DDoS Attacks
  - Authentication hijacking
  - Data exposure
  - MitM attacks
- Traditional methods of protection don’t work
  - WAF and simple port blocking
  - Continuously evolving APIs

Memory Leak

A memory leak is typically an unintentional consumption of memory. The application fails to release the memory once it's no longer needed

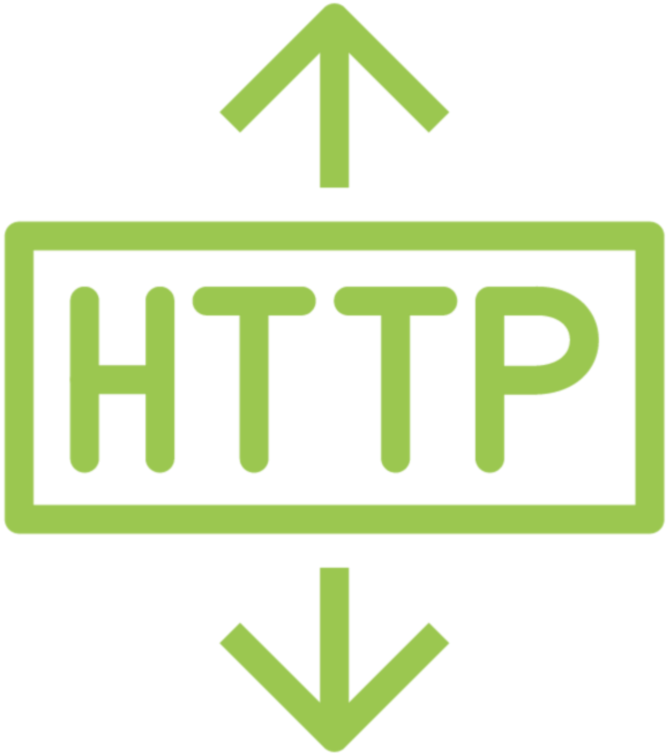
This consumption of resources can over time lead to a variety of issues:

- Degraded system performance
- Abnormal system behavior
- System crashes
- Denial of Service (DoS)



Threat actors can use those vulnerabilities to try and crash a system to gain elevated privileges or take a system offline via a Denial of Service (DoS) attack

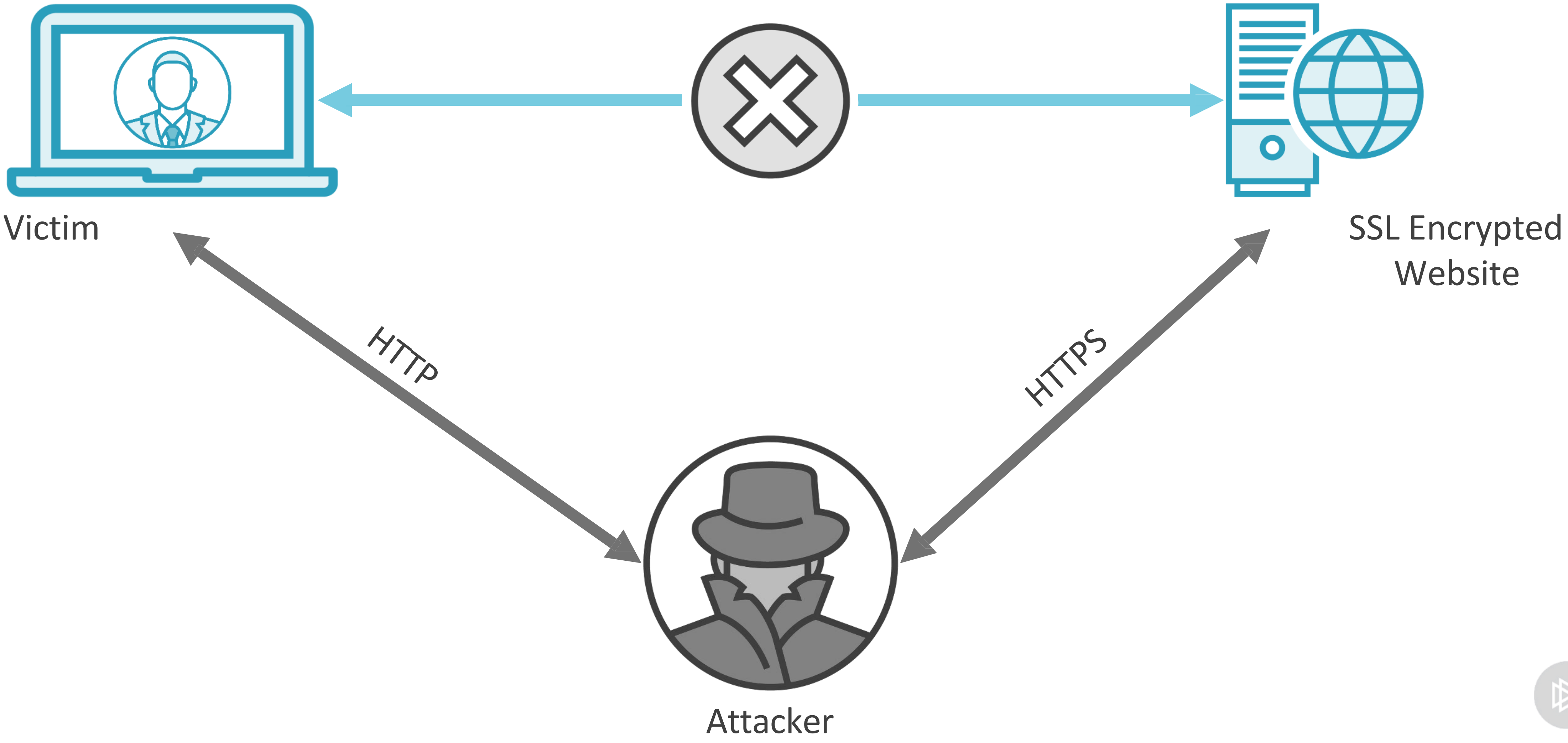
SSL Stripping



MitM type of attack that strips away SSL encryption

- Enables an attacker to intercept traffic between victim and target
- Enterprise users, wired or Wi-Fi hotspots, etc.

SSL Stripping Example



SSL Stripping Mitigations

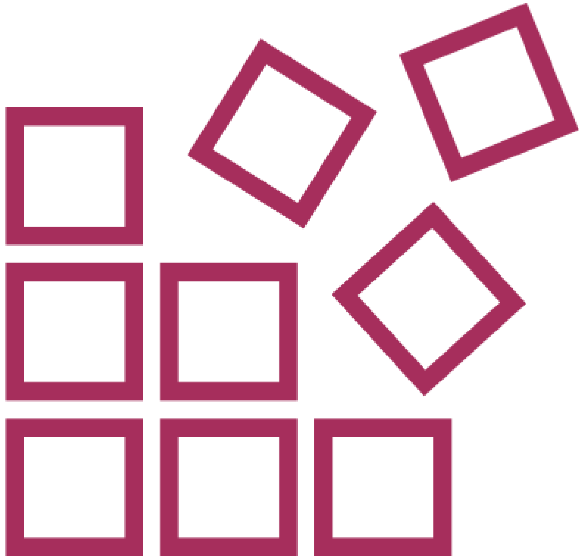
Use SSL everywhere

- Not just on pages that contain sensitive data

Use HSTS

- HTTP Strict Transport Security
- Forces clients/browsers to connect over HTTPS

Shimming



Shim databases are part of Microsoft Window’s Application Compatibility Infrastructure

- Used to maintain compatibility with legacy applications
- Can be used for malicious purposes by custom shim databases to install code, patches, etc.

Refactoring

Modifying an application’s source code without changing the underlying functionality

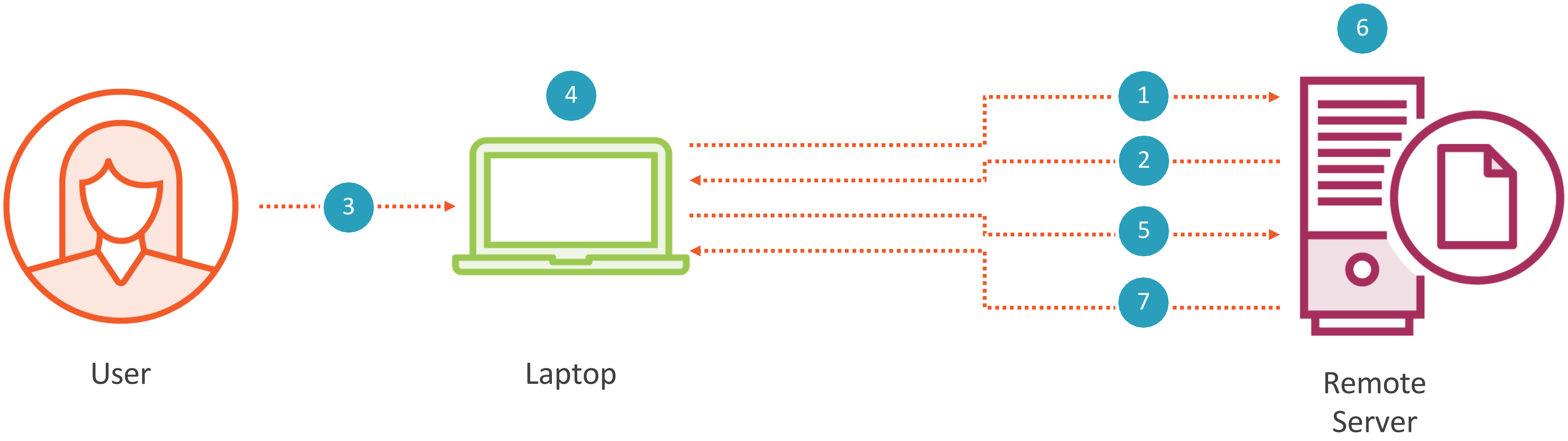
Refactoring (Purpose)

Fix bugs, patch code and tighten up security without changing or adversely affecting the underlying functionality

Pass the Hash

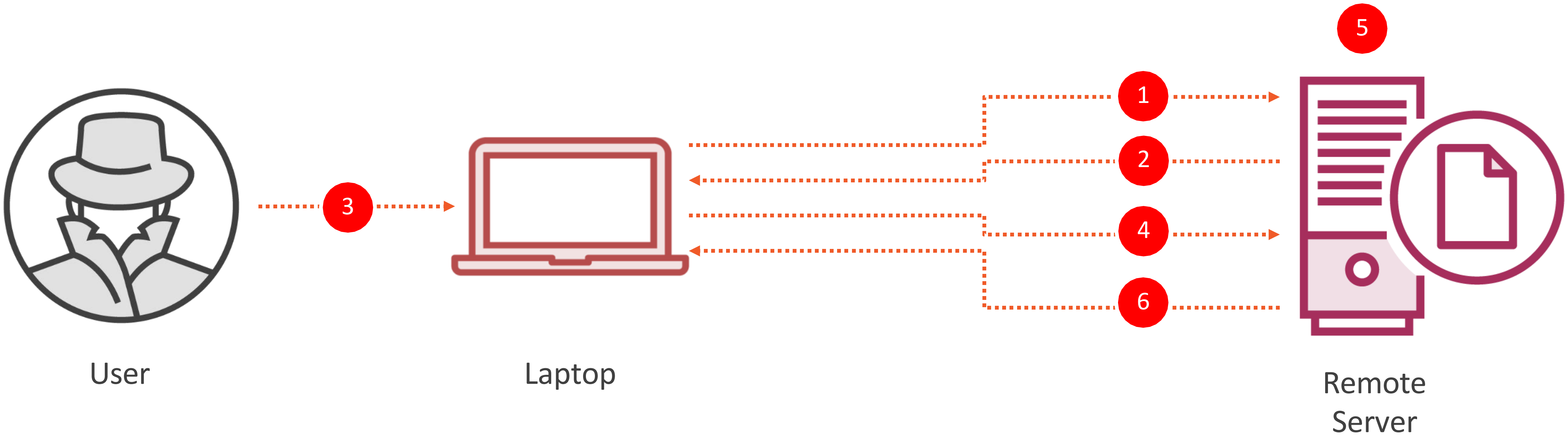
Harvesting a user’s password hash to authenticate to a remote server or service

Pass the Hash



1. User wants to access remote resource
2. Server sends authentication challenge
3. User enters their credentials (username/password)
4. Password in converted to a hash value
5. Hash value is sent to the server
6. Server checks the hash value against the expected value
7. Access is granted to resource (assuming hash values match)

Pass the Hash



1. **Hacker** wants to access remote resource
2. Server sends authentication challenge
3. **Hacker** enters username and **stolen hash value**
4. Hash value is sent to the server
5. Server checks the hash value against the expected value
6. Access is granted to resource (assuming hash values match)

Module Review

Privilege escalation

Cross-site scripting

Injection attacks

Error handling

Replay attacks

API attacks

SSL stripping

Driver manipulation