Becoming a Hacker

Active Information Gathering

Sammy Tieng
stieng@cisco.com
ASIG

Everett Stiles
evstiles@cisco.com
ASIG

Chris McCoy
cmm@cisco.com
ASIG

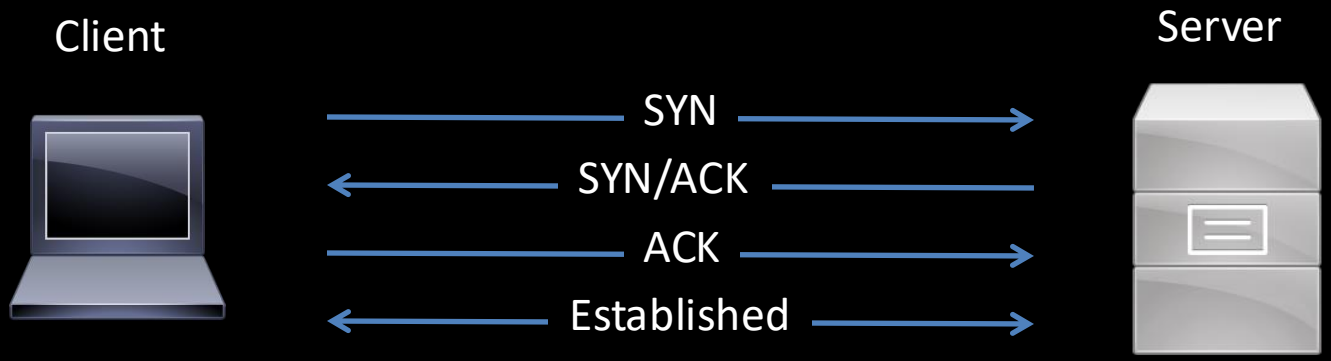
Nicholas Weigand
nweigand@cisco.com
ASIG

Nmap TCP SYN Scanning

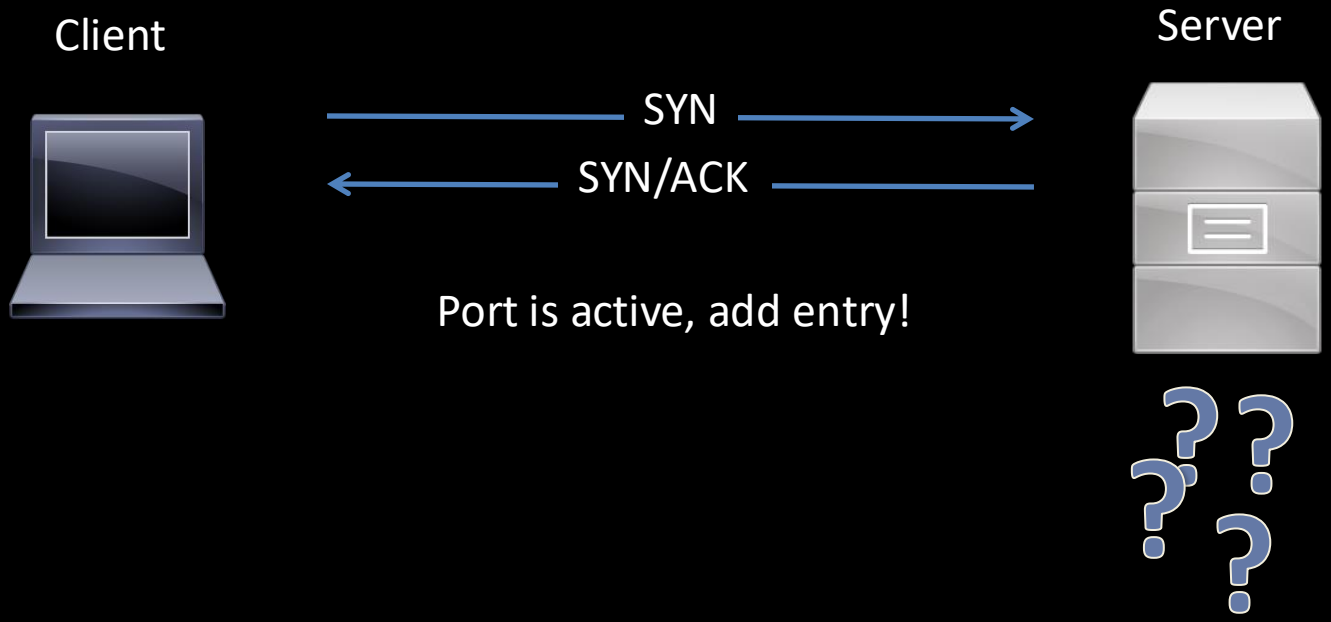
```
nmap -sS -p 21,22,80,443,445,3389 -v <IP Address>
```

- Validates host active via ICMP and SYN to pre-defined ports
- Sends SYN packet requests to TCP ports
- Waits for SYN/ACK, does not send ACK response
- Produce results!

TCP 3-way Handshake



TCP SYN Scan

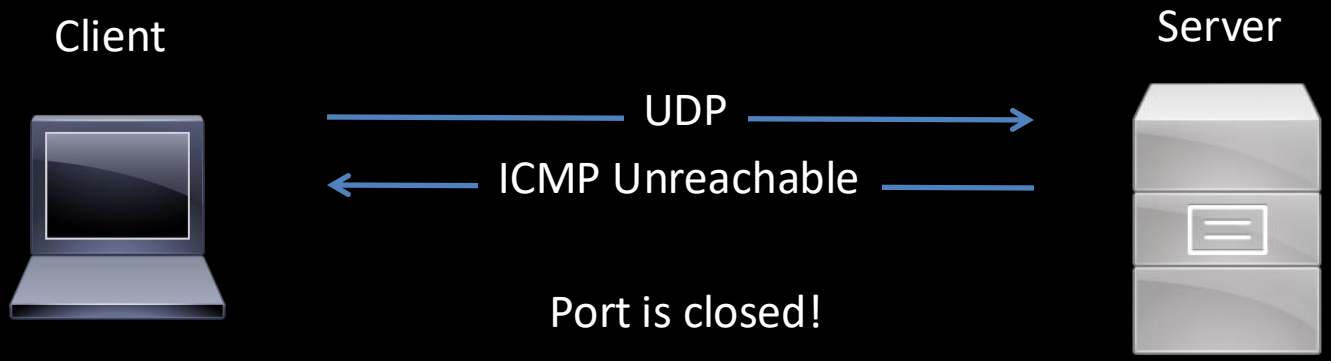


Nmap UDP Port Scanning

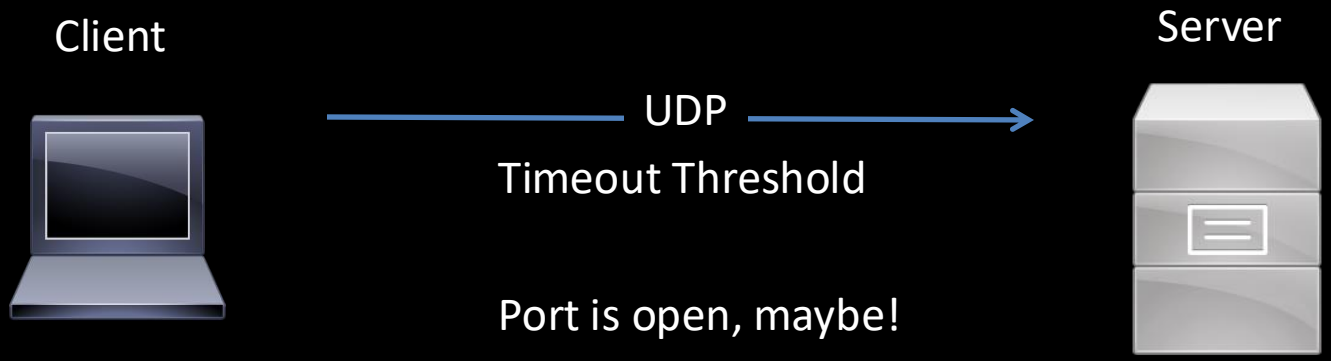
```
nmap -sU -p 161,7,199 -v <IP Address>
```

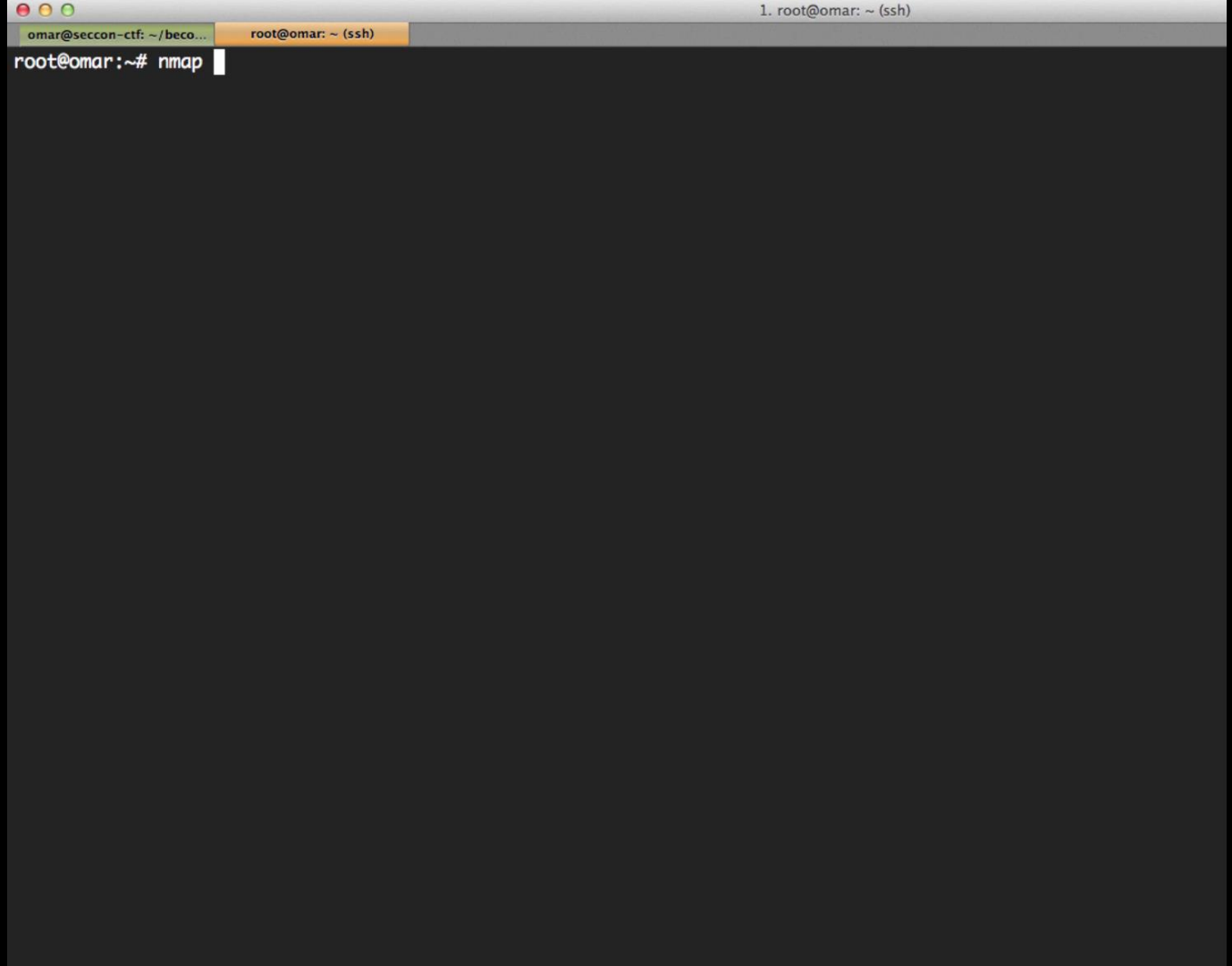
- Validates host active via ICMP
- Waits for ICMP or Timeout
- Produces result!

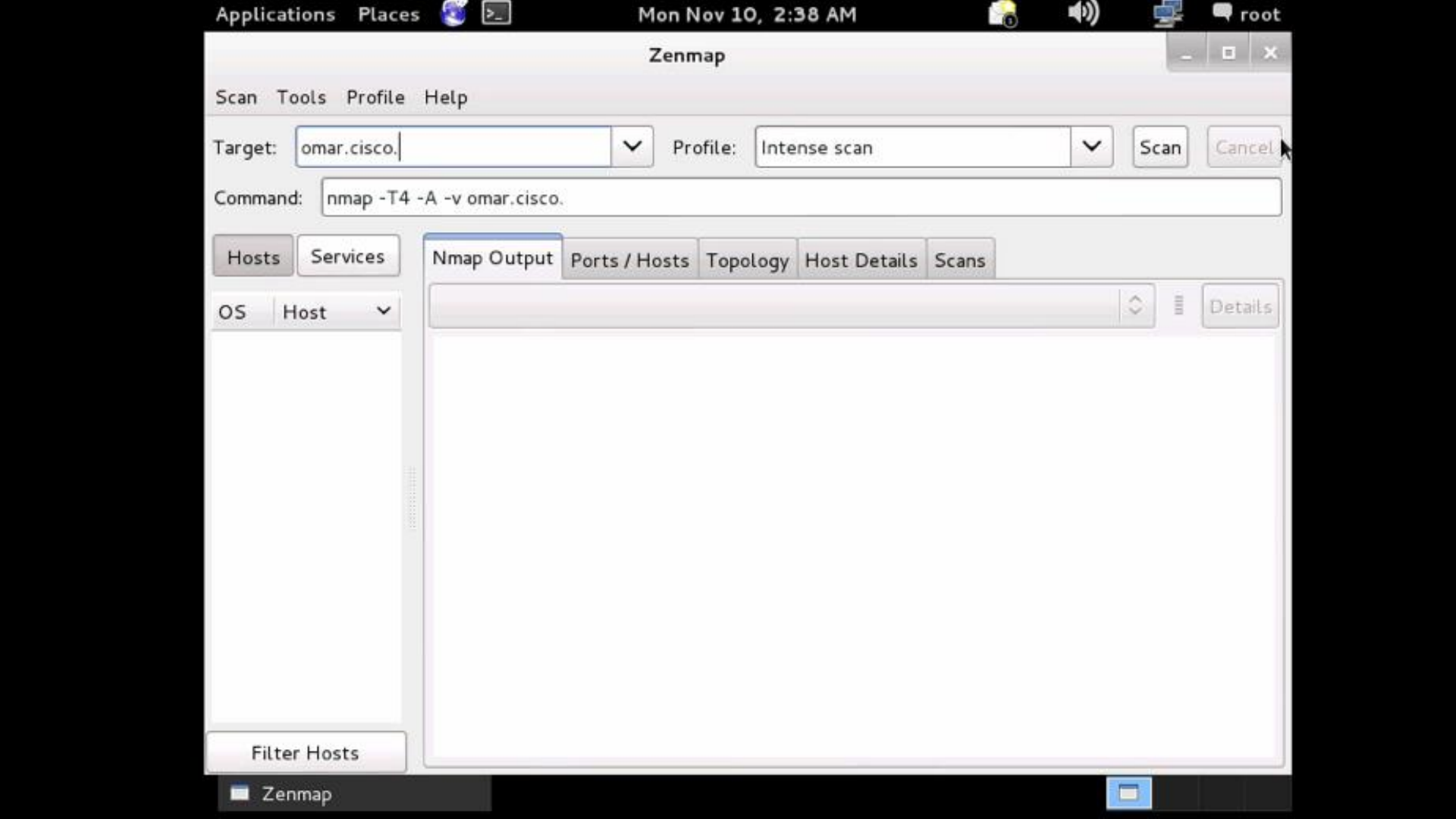
UDP Port Scanning



UDP Port Scanning




1. root@omar: ~ (ssh)
omar@seccon-ctf: ~/beco...
root@omar: ~ (ssh)
root@omar:~# nmap


Applications
Places
Mon Nov 10, 2:38 AM
root
Zenmap
Scan
Tools
Profile
Help
Target:
omar.cisco.
Profile:
Intense scan
Scan
Cancel
Command:
nmap -T4 -A -v omar.cisco.
Hosts
Services
OS
Host
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
Zenmap

NetCat, the Swiss-army Knife for TCP/IP

- Originally written by Hobbit in 1996
- Now “standard” in most LINUX releases
- In its simplest mode will send/receive data over TCP or UDP

```
nc mail.cisco.com 25
```

- Port scanning:

```
nc -vzu ip.address 80-89
```

- Listen on a port:

```
nc -vl 6666
```

- “Ncat” is nmap’s replacement for NetCat. Supports many more features and is regularly updated

Other Ways To Find Hosts

- SNMP scanning
  - Multiple interfaces / networks
  - SNMP scans are cheap at the packet level but noisy
- Routing Advertisements
  - Join the IGP and learn the networks
- Listen to the Wire
  - tcpdump, wireshark, ettercap, etc
- IPv6 Multicast Discovery
  - `Ping6 ff02::1`

Metasploit snmp_enum module

```
msf > use auxiliary/scanner/snmp/snmp_enum
msf auxiliary(snmp_enum) > show actions
      ...actions...
msf auxiliary(snmp_enum) > set ACTION <action-name>
msf auxiliary(snmp_enum) > show options
      ...show and set options...
msf auxiliary(snmp_enum) > run
```

Examples of Vulnerability Scanners

- Nessus
- OpenVAS
- Core Impact Scanner
- Nexpose
- GFI LanGuard
- Qualys
- Microsoft Baseline Security Analyzer (MBSA)
- Retina

More at: http://sectools.org/tag/vuln-scanners

Finding Web App Vulnerabilities

- Many Web Application scanners:
  - W3af – OpenSource
  - HP WebInspect
  - IBM AppScan
  - SQLmap
  - BurpSuite Proxy / BurpSuitePro Proxy
  - Etc...

Another Good List of Web App Commercial and Open Source Scanners

https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tool

Finding Exploits and Published Vulns

- Many web sites available:
  - http://www.exploit-db.com/
  - http://nvd.nist.gov/
  - http://cve.mitre.org/
  - http://www.osvdb.org/
  - http://www.rapid7.com/vulndb/index.jsp
  - http://www.kb.cert.org/vulns/
  - http://www.securityfocus.com/vulnerabilities
- Mailing Lists
  - Full Disclosure
  - Bugtraq
  - oss-sec

Fuzzing to Find New Vulnerabilities

- Fuzzing is the act of sending various parameters to test applications and services for their error handling
  - Buffer overflows
  - Format string variables
  - Directory traversal
  - SQL Injection
- Advanced fuzzing frameworks incorporate debuggers to catch and analyze faults
- The typical “dumb” fuzzer will find many faults but not all of them will be exploitable
  - No control over the stack
  - Input character limitations (must be digits, only alpha, etc)
- However even the most difficult bugs that some have thought not to be exploitable were found to be just that
- A fault discovered by a fuzzer should at least have some review by developers

Types of Fuzzers

- Commercial and Open Source products abound!
- Application Fuzzers
  - Focuses on application usability:
    - UI testing
    - Command-line options
    - SQL Injection, XSS, Session ID Tokens, etc
- Protocol Fuzzers
  - Understands a protocol such a FTP, Telnet, HTTP or can sit in-line and modify packets as they are transferred
- File Format Fuzzers
  - Modifies file data for faults in application processing

Metasploit Fuzzers

```
ame                                              Disclosure Date  Rank    Description
---                                              ---------------  ----    -----------
uxiliary/fuzzers/dns/dns_fuzzer                                   normal  DNS and DNSSEC Fuzzer
uxiliary/fuzzers/ftp/client_ftp                                   normal  Simple FTP Client Fuzzer
uxiliary/fuzzers/ftp/ftp_pre_post                                 normal  Simple FTP Fuzzer
uxiliary/fuzzers/http/http_form_field                             normal  HTTP Form Field Fuzzer
uxiliary/fuzzers/http/http_get_uri_long                           normal  HTTP GET Request URI Fuzzer (Incrementing Lengths)
uxiliary/fuzzers/http/http_get_uri_strings                        normal  HTTP GET Request URI Fuzzer (Fuzzer Strings)
uxiliary/fuzzers/smb/smb2_negotiate_corrupt                       normal  SMB Negotiate SMB2 Dialect Corruption
uxiliary/fuzzers/smb/smb_create_pipe                              normal  SMB Create Pipe Request Fuzzer
uxiliary/fuzzers/smb/smb_create_pipe_corrupt                      normal  SMB Create Pipe Request Corruption
uxiliary/fuzzers/smb/smb_negotiate_corrupt                        normal  SMB Negotiate Dialect Corruption
uxiliary/fuzzers/smb/smb_ntlm1_login_corrupt                      normal  SMB NTLMv1 Login Request Corruption
uxiliary/fuzzers/smb/smb_tree_connect                             normal  SMB Tree Connect Request Fuzzer
uxiliary/fuzzers/smb/smb_tree_connect_corrupt                     normal  SMB Tree Connect Request Corruption
uxiliary/fuzzers/smtp/smtp_fuzzer                                 normal  SMTP Simple Fuzzer
uxiliary/fuzzers/ssh/ssh_kexinit_corrupt                          normal  SSH Key Exchange Init Corruption
uxiliary/fuzzers/ssh/ssh_version_15                               normal  SSH 1.5 Version Fuzzer
uxiliary/fuzzers/ssh/ssh_version_2                                normal  SSH 2.0 Version Fuzzer
uxiliary/fuzzers/ssh/ssh_version_corrupt                          normal  SSH Version Corruption
uxiliary/fuzzers/tds/tds_login_corrupt                            normal  TDS Protocol Login Request Corruption Fuzzer
uxiliary/fuzzers/tds/tds_login_username                           normal  TDS Protocol Login Request Username Fuzzer
uxiliary/fuzzers/wifi/fuzz_beacon                                 normal  Wireless Beacon Frame Fuzzer
uxiliary/fuzzers/wifi/fuzz_proberesp                              normal  Wireless Probe Response Frame Fuzzer
```

Lab Exercise

becomingahacker.com