Cyber Security Workshop 2015

"System Hacking"

By

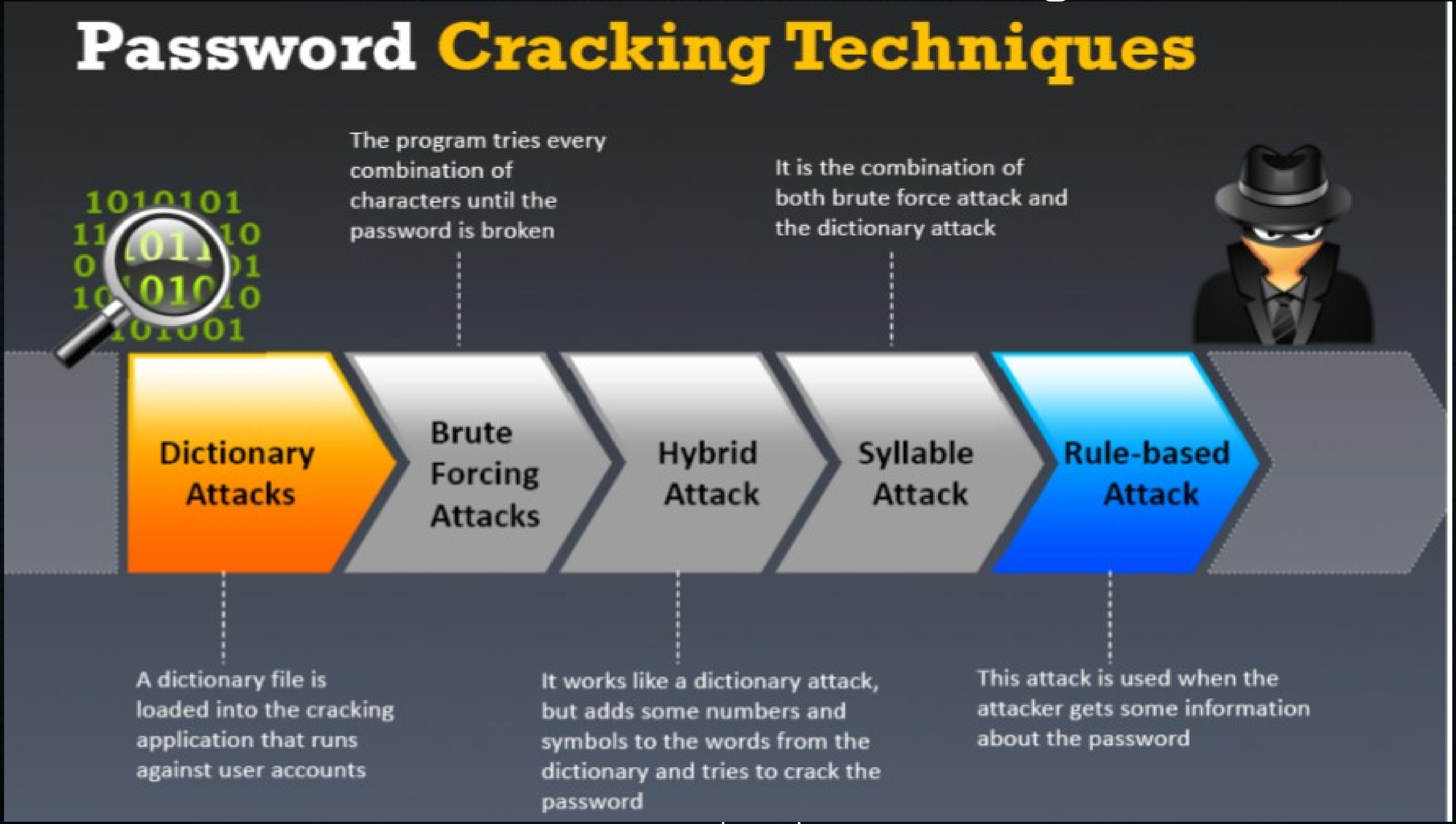
Ashish Belwase

KU Security Researchers

Password Cracking

- Most commonly used Attacks
- Depends on password complexity

Password Cracking



Password Cracking Techniques

Dictionary Attacks

A dictionary file is loaded into the cracking application that runs against user accounts

Brute Forcing Attacks

The program tries every combination of characters until the password is broken

Hybrid Attack

It works like a dictionary attack, but adds some numbers and symbols to the words from the dictionary and tries to crack the password

Syllable Attack

It is the combination of both brute force attack and the dictionary attack

Rule-based Attack

This attack is used when the attacker gets some information about the password

Password Cracking

- Cracking Windows Hash
  - Cd to system32/config
  - Bkhive SYSTEM /home/hash.txt
  - Samdump2 SAM /home/hash.txt > /home/hasfile.txt
  - More /home/hashfile.txt # display users
  - John /home/hashfile.txt –format=nt2 -users=test
- Cain & Abel
- Rainbow Table = ophcrack
  - https://www.objectif-securite.ch/en/ophcrack.php

Password Cracking

- Cracking Linux Passwords
  - /etc/shadow
  - John shadow
- Hashcat
  - Cp /etc/shadow hash.lst
  - Cat /etc/login.DEFS | grep ENCRYPT >> check hashing algo
  - Get password.lst
  - Hashcat -m 1800 -a 0 -o cracked.txt hash.lst password.txt

Generating wordlist

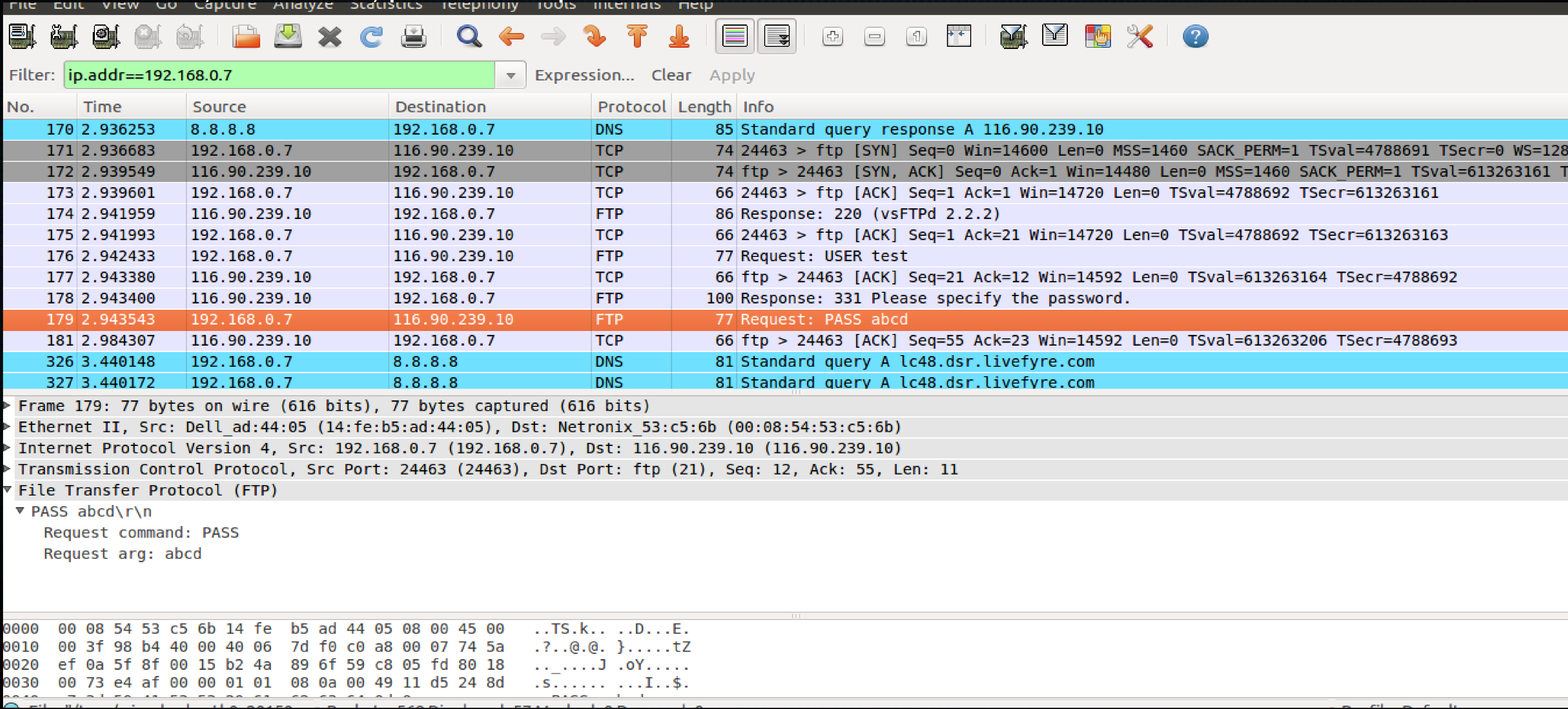
- Some information about passwords
- Crunch <min length> <max length> <list of strings> <dest>
- Crunch 4 4 012345 pw.txt

Bruteforcing

- FTP
  - Medusa -h 192.168.5.1 -U username.lst -P pass.lst -M ftp
- Router
  - Medusa -h 192.168.0.1 -U admin -P pass.lst -M http

Password Sniffing

- FileZilla,Wireshark,ip.addr==<ip>



Filter: ip.addr==192.168.0.7

```
No.   Time      Source         Destination    Protocol Length Info
  170 2.936253  8.8.8.8        192.168.0.7    DNS          85 Standard query response A 116.90.239.10
  171 2.936683  192.168.0.7    116.90.239.10  TCP          74 24463 > ftp [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=4788691 TSecr=0 WS=128
  172 2.939549  116.90.239.10  192.168.0.7    TCP          74 ftp > 24463 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=613263161 T
  173 2.939601  192.168.0.7    116.90.239.10  TCP          66 24463 > ftp [ACK] Seq=1 Ack=1 Win=14720 Len=0 TSval=4788692 TSecr=613263161
  174 2.941959  116.90.239.10  192.168.0.7    FTP          86 Response: 220 (vsFTPd 2.2.2)
  175 2.941993  192.168.0.7    116.90.239.10  TCP          66 24463 > ftp [ACK] Seq=1 Ack=21 Win=14720 Len=0 TSval=4788692 TSecr=613263163
  176 2.942433  192.168.0.7    116.90.239.10  FTP          77 Request: USER test
  177 2.943380  116.90.239.10  192.168.0.7    TCP          66 ftp > 24463 [ACK] Seq=21 Ack=12 Win=14592 Len=0 TSval=613263164 TSecr=4788692
  178 2.943400  116.90.239.10  192.168.0.7    FTP         100 Response: 331 Please specify the password.
  179 2.943543  192.168.0.7    116.90.239.10  FTP          77 Request: PASS abcd
  181 2.984307  116.90.239.10  192.168.0.7    TCP          66 ftp > 24463 [ACK] Seq=55 Ack=23 Win=14592 Len=0 TSval=613263206 TSecr=4788693
  326 3.440148  192.168.0.7    8.8.8.8        DNS          81 Standard query A lc48.dsr.livefyre.com
  327 3.440172  192.168.0.7    8.8.8.8        DNS          81 Standard query A lc48.dsr.livefyre.com
```

```
▶ Frame 179: 77 bytes on wire (616 bits), 77 bytes captured (616 bits)
▶ Ethernet II, Src: Dell_ad:44:05 (14:fe:b5:ad:44:05), Dst: Netronix_53:c5:6b (00:08:54:53:c5:6b)
▶ Internet Protocol Version 4, Src: 192.168.0.7 (192.168.0.7), Dst: 116.90.239.10 (116.90.239.10)
▶ Transmission Control Protocol, Src Port: 24463 (24463), Dst Port: ftp (21), Seq: 12, Ack: 55, Len: 11
▼ File Transfer Protocol (FTP)
  ▼ PASS abcd\r\n
      Request command: PASS
      Request arg: abcd
```

```
0000  00 08 54 53 c5 6b 14 fe  b5 ad 44 05 08 00 45 00   ..TS.k.. ..D...E.
0010  00 3f 98 b4 40 00 40 06  7d f0 c0 a8 00 07 74 5a   .?..@.@. }.....tZ
0020  ef 0a 5f 8f 00 15 b2 4a  89 6f 59 c8 05 fd 80 18   .._....J .oY.....
0030  00 73 e4 af 00 00 01 01  08 0a 00 49 11 d5 24 8d   .s...... ...I..$.
```