Section 9: Testing Your Infrastructure

110.Vulnerability Scanning Tools

Tools

1. Tracert(Windows)/Traceroute(MAC)
2. Advanced IP Scanner (Freeware/Network Discovery Tool)
3. nmap (Network Discovery Tool/Port Scanner)

4.MBSA (Microsoft Baseline Security Analyzer)
- Refers to microsoft knowledge database

Vulerability Assessment tools
1. Nessus
2. Nexpose
3. OpenVAS

```
        * National Vulnerability Database, etc is referenced by tools like
OpenVAS.
```

Quick Review

- Vulnerabiltiy scanning is a big job - there is no one perfect tool
- These tools use the Nations Vulnerability Database as a source
- Simple networks can likely use simple vulnerability scanners like Nessus, Nexpos or OpenVas

---

111.Vulnerability Scanning Assessment

Vulnerability Assesments are usually handled by management and require authorization before starting an assessment.

Credentialed vs. Non-credentialed Vulnerability assessments
- Credentialed (You have user names and passwords) - Internal view
- Non-Credentialed (You do not have user names and passwords) - External view

Intrusive vs. Non-intrusive
- Non-intrusive (Doing an assesment but not dropping any payloads into the system), only identifying the vulnerabilities

Misconfigurations can cause vulnerabilities

False Positive: When an assessment says there is a problem, but there aren't actually any issues

Compliance: *compliance package (Ruleset for vulnerability assessments)

Quick Review:

- Management determines when vulnerability scanning is done **GET AUTHORIZED

- Misconfigurations often are vulnerabilities
- Vulnerability scanners can be configured to scan against different databases or rule sets

---

112.Social Engineering Principles

Social Engineering Priciples

1. Authority: to impersonate or imply a position of authority
2. Intimidation: to frighten by threat
3. Consensus: to convice of a general group agreement
4. Scarcity: to describe a lack of something
5. Familiarity: to imply a closer relationship
6. Trust: to assure reliance on their honesty and integrity
7. Urgency: to call for immediate action

**Memorize these principles for the exam

Quick Review:

- Social engineering principles are focused more on peoples behavior as opposed to their physical actions
- Never give out any sensitive information

113.Social Engineering Attacks

1. Physical attacks
    1. Tailgating (Following someone through a locked door)
    2. Unauthorized Access (Lock your computer when you walk away)
    3. Shoulder Surfing (Looking over someones shoulder) - Screen filter
    4. Dumpster Diving (Digging through trash to find sensitive information)
2. Virtual Attacks
    1. Phishing - Emails used to steal personal information
    2. Spear Phishing - Phishing that is directed to a single person/organization
    3. Whaling - Spear phishing that targets senior management and executives
    4. Vishing - Uses the telephone system to get private information
    5. Hoax - Warns that something bad is happening but it isn't
    6. Watering hole attack - An attempt to infect websites that a group of end users would normally go to gain access to their information or network

Quick Review:

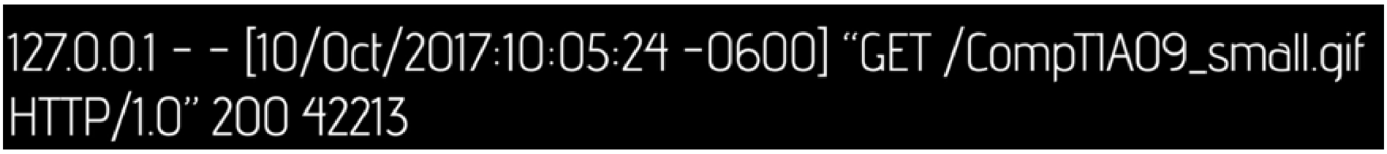
- Recognize different types of social engineering attacks

---

114. Attacking Web Sites

- Need to be able to read log files

1. CLF (Common Log Format)



```
127.0.0.1 - - [10/Oct/2017:10:05:24 -0600] "GET /CompTIA09_small.gif
HTTP/1.0" 200 42213
```

1. Need to be able to Identify (Left to Right in the above image)
    1. Host - the FQDN of the client, or its IP address

    2. Ident - if the IdentityCheck directive is enabled and the client machine runs ident, then this is the identity information reported by the client

    3. Authuser - if requested, URL requires a successful basic HTTP authentication then the username is the value of this token

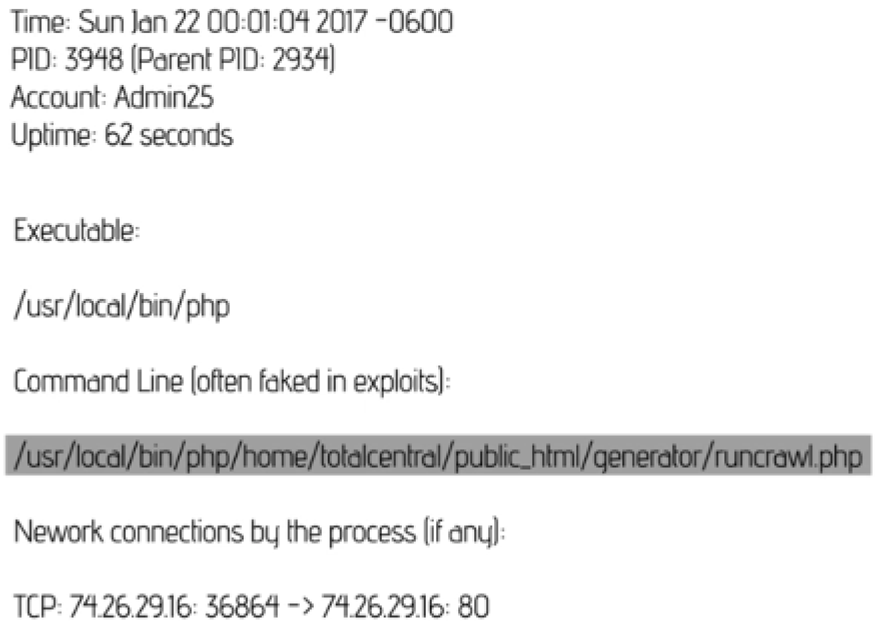
    4. Date - the data and time of the request

    5. Request - the request line from the client enclosed in double quotes ""

    6. Status - the three-digit HTTP status code returned to the client

    7. Bytes - the number of bytes in the object returned to the client, excluding all HTTP headers

2. cPanel



```
Time: Sun Jan 22 00:01:04 2017 -0600
PID: 3948 (Parent PID: 2934)
Account: Admin25
Uptime: 62 seconds

Executable:

/usr/local/bin/php

Command Line (often faked in exploits):

/usr/local/bin/php/home/totalcentral/public_html/generator/runcrawl.php

Nework connections by the process (if any):

TCP: 74.26.29.16: 36864 -> 74.26.29.16: 80
```

Types of attacks that are unique to Web Sites
1. Cross-site scripting (XSS) - Client-side script injected into trusted web sides

2. XML Injections - An attack technique used to manipulate or compromise the logic of an XML application or service
- Inserts XML information that should be there altering the logic of the program

*Be comfortable reading log files

Quick Review:
- Cross-site scripting (XSS) is a common type of injection attack that affects web sites and web applications
- XML injections are very small changes that have big consequences

115.Attacking Applications

How do we do these attacks?
1. Injection attacks - You add some extra input into an application
1. Code injection - You add extra code to the application to make it do other things

    2. Command Injectiong - Uses the application to get to the underlying OS
        1. SQL (Structured Query Language)
            1. inner Join
            2. insert into
            3. select from

    4. LDAP injections (Lightweight Directory Access Protocol)
        1. LDAP based on X.500

```
                ![Screen Shot 2020-08-04 at 6.19.33 PM.png](_resources/5f3c8b6db2ce47a994dfdcffec26700f.png)

                Entire thing is called:
                        DN = Distinguished Name

                Left to right in the DN
                        CN = Common Name
                        OU = Organizational Units
                        DC = Domain Components

2. Buffer Overflow
        1. A Buffer is temporary memory to store data before the info gets put into the app
        1. A Buffer Overflow is just inputting so much information the the buffer breaks

3. Integer Overflow
        1. e.g. typing a massive value into a calculator and it causses an error (Can't handle large values)
        2. *For the exam "There are xbytes, and ynumber of bits don't fit"
```

Quick Review:
- Injection attacks is insertion into an application (code injection, command injection , etc)
- LDAP is based on the X.500 protocol
- Buffer and integer overflow attacks are inputs into application forms that exceed the maximum allowed bits

---

116.Exploiting a Target

- Vulnerability test does not try to grab data
- Penetration Tests DO try to grab data

Pentest Steps:

```
1. Get Authorization
        1. Define the targets
        2. Attack model
                1. White box
                        1. Attackers have extensive knowledge about the target
                        2. Attackers are more like trusted insiders
                        3. Cheapest and fastest model for a pentest
                2. Black box
                        1. attackers know nothing about the target
                        2. attackers are more like strangers
                        3. external hacking
                        4. Potentially expensive and slow
                3. Gray box
                        1. Somewhere between white and black

2. Discovering vulnerablities
        1. Reconnaissance
        2. Try to get information

        Three different ways to do this
                1. Passive Discovery : not putting any of your packets on the target (Nothing from a computer is going to the target)
                2. semi Passive discovery : Putting packets onto the target but you aren't doing anything that will trigger alarms or IDS
                3. Active Discover : Putting packets downrange, running scanners and tools (nmap, etc). Could be blocked by IDS/Firewall

3. Exploit Vulnerabilites
        1. Grab user names and passwords
        2. Take data from a database
        3. Corrupt a webpage

        Tools:
                - Metasploit (Pentesting Framework)
                - Kali Linux

        What we have to do to exploit a target:
                1. Start with an inital exploitation
                2. Pivot - uses the compromised system to attack other systems (e.g. intial exploit gains Root access, now you can pivot to do a bunch of other things with that root access.)
                3. Persistence - To connect again easily with your target with open timelines (Penetration tests take lots of time)
                4. Privilege Escalation - Ability to gain elevted acces to data and network resources
```

Quick Review:

- No penetration without prior authorization
- Know your attack models
- Know your reconnaissance methods

117.Vulnerability Impact

Scenarios that should be considered for the exam

1. Embedded Systems
   1. Need patches, antimalware, firewalls, etc
   2. Danger is that we forget to take care of them the way that we would any other device
2. Lack of vendor support
   1. If a vendor no longer supports the biggest vulnerability is that there is not patch mangement or solutions to issues
      1. Throw away the item and get something that has proper vendor support
3. Weak Configuration
   1. Provide the best possible configuration we can
4. Misconfiguration
   1. We have incorrectly configured something
   2. Failed to turn on a firewall
   3. Faild to turn off unused services
5. Improperly configured accounts
   1. We have a user or system account that doesnt have the correct rights and permissions
      1. Not enough permissions/rights
      2. Too many permissions/rights
6. Vulnerable Business Processes
   1. Storing non-essential personal identifiable information
7. Memory/buffer vulnerabilities

   Running out of memory:
   1. Resource Exhaustion
   2. memory leak

   Overflows:

   3. Integer Overflow
   4. Buffer Overflow

   Sneaking in a back door, no big obvious performace symptoms:

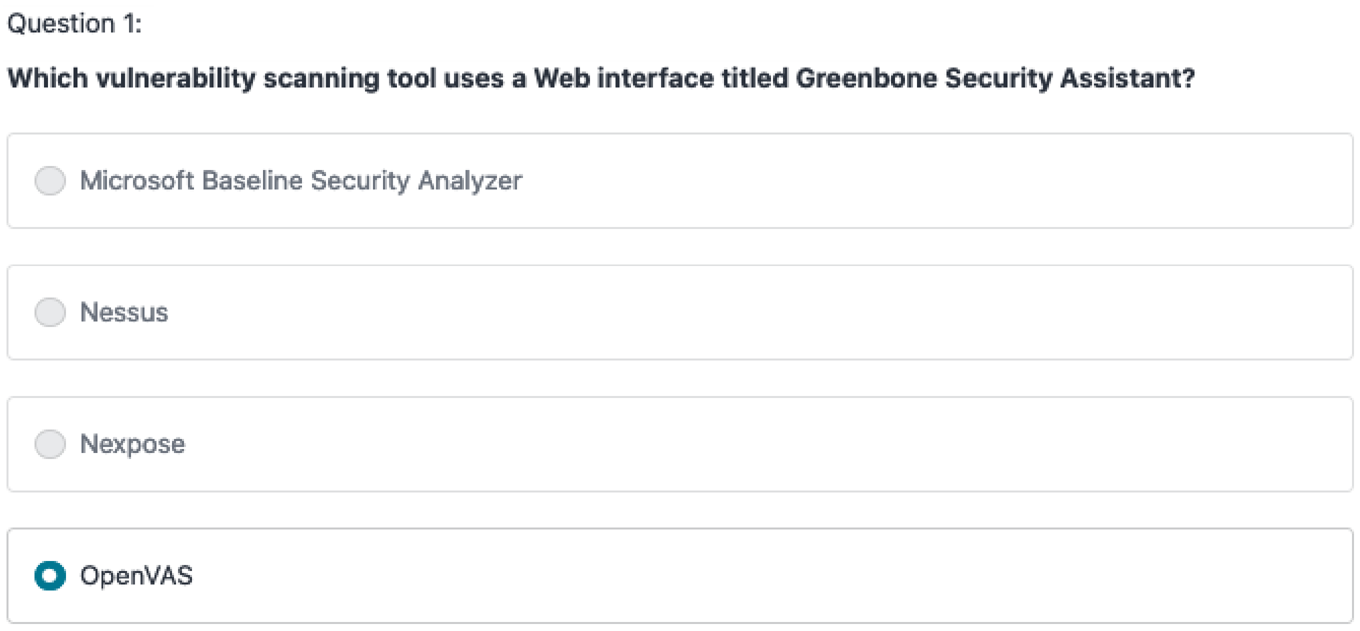
   5. Pointer difference
   6. DLL injection
8. System Sprawl/Un-documented assets - Stuff outside the umbrella of administration that leaves us open to vulnerablity

Quick Review:

- Lack of vendor support for software or hardware means no more security patches; find a new source or newer version!
- Misconfiguration, weak configuration, and outdated protocols leave exposure points in a system

- Memory/buffer vulnerabilities include things like resource exhaustion, memory leak, integer overflow, and buffer overflow

QUIZ



Question 1:

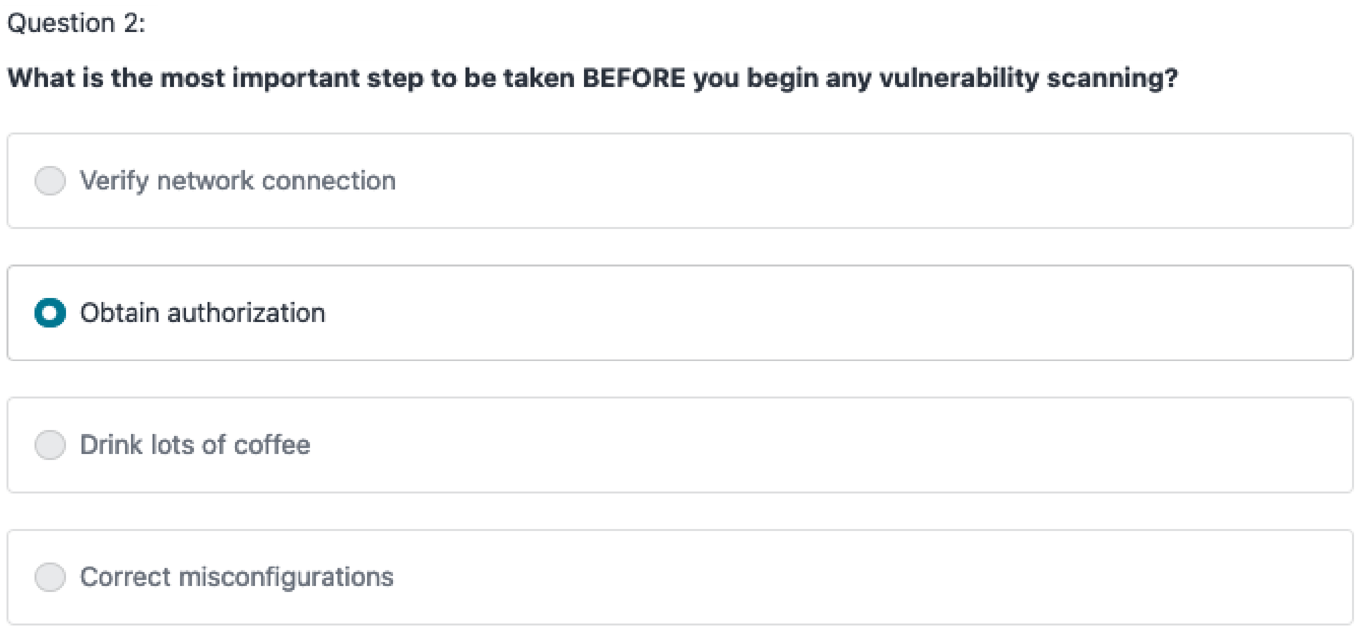
Which vulnerability scanning tool uses a Web interface titled Greenbone Security Assistant?

○ Microsoft Baseline Security Analyzer

○ Nessus

○ Nexpose

● OpenVAS



Question 2:

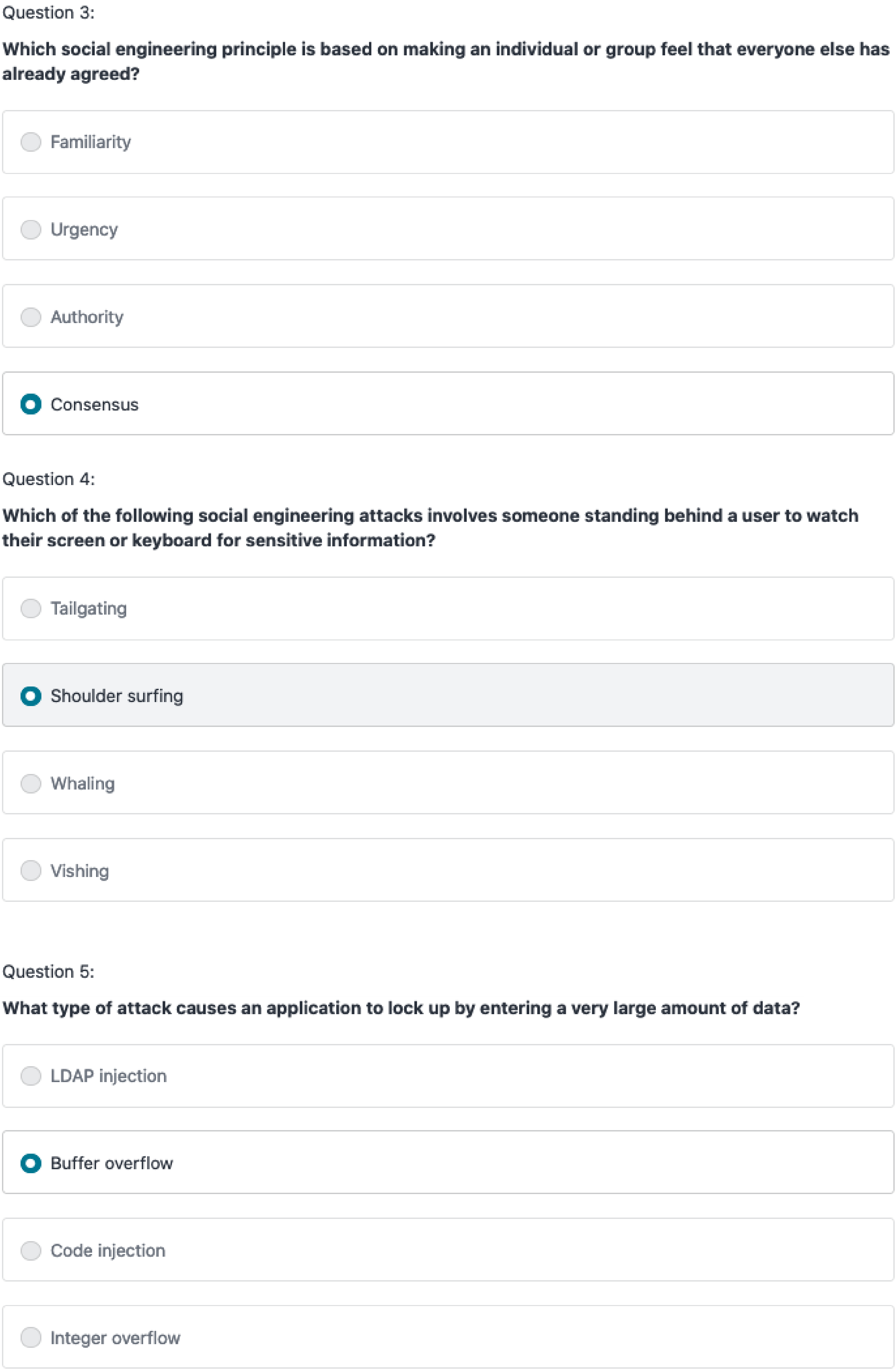
What is the most important step to be taken BEFORE you begin any vulnerability scanning?

○ Verify network connection

● Obtain authorization

○ Drink lots of coffee

○ Correct misconfigurations



Question 3:

Which social engineering principle is based on making an individual or group feel that everyone else has already agreed?

○ Familiarity

○ Urgency

○ Authority

● Consensus

Question 4:

Which of the following social engineering attacks involves someone standing behind a user to watch their screen or keyboard for sensitive information?

○ Tailgating

● Shoulder surfing

○ Whaling

○ Vishing

Question 5:

What type of attack causes an application to lock up by entering a very large amount of data?

○ LDAP injection

● Buffer overflow

○ Code injection

○ Integer overflow

Question 6:

Which type of pen testing is performed by someone who has extensive information about the system(s) to be attacked?

● White box

○ Black box

○ Gray box

○ Redbox

Question 7:

Which impact is likely to cause a system to stop functioning?

○ Race conditions

○ Lack of vendor support

○ Storage of non-essential information

● Integer overflow