Exam Report: 6.2.5 Practice Questions

Date: 5/2/2020 6:26:42 pm
Time Spent: 0:54

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 20%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Hugh, a security consultant, recommended the use of an internal and external DNS to provide an extra layer of security. Which of the following DNS countermeasures is being used?

- Digital signatures
- ~~DNS zone transfer~~
- Split DNS
- DNS zone restriction

Explanation

DNS splitting, splitting the DNS into internal and external groups, provides an added layer of security.

DNS zone restrictions ensure that a server only provides copies of zone files to specific servers.

Digital signatures help with DNS zone restriction.

DNS zone transfers are designed to provide updated network and access information to the DNS servers.

References

TestOut Ethical Hacker Pro - 6.2 Enumeration Countermeasures
[e_enum_counter_eh1.exam.xml Q_ENUMCOUNTER_ENUM_COUNTER_DNS_01_EH1]

Question 2: Correct

Diana, a penetration tester, executed the following command. Which answer describes what you learn from the information displayed?

```
> ls -d testoutdemo.com
[UnKnown]
 testoutdemo.com.               SOA    server2012 hostmaster. (6 900 600 86400 3600)
 testoutdemo.com.               NS     server2012
 testoutdemo.com.               MX     10   67.192.129.235
 server1                        A      67.192.129.239
 server2                        A      67.192.129.240
 server3                        A      67.192.129.241
 www                            A      67.192.129.238
 testoutdemo.com.               SOA    server2012 hostmaster. (6 900 600 86400 3600)
> _
```

- There are DNS restrictions in place.
- DNS translation is being used.
- Split DNS is being used.
- This is a DNS zone transfer.

Explanation

A DNS zone transfer is a mechanism available for administrators to replicate DNS databases across a set of DNS servers. Organizations should take measures not to allow zone transfers to just anyone.

DNS zone restrictions ensure that a server only provides copies of zone files to specific servers.

Split DNS is used to split DNS into internal and external groups.

DNS translates domain names to IP addresses so browsers can load web pages.

References

TestOut Ethical Hacker Pro - 6.2 Enumeration Countermeasures
[e_enum_counter_eh1.exam.xml Q_ENUMCOUNTER_ENUM_COUNTER_DNS_02_EH1]

Question 3: Incorrect

After the enumeration stage, you have are considering blocking port 389. Your colleague has advised you to use caution when blocking ports that could potentially impact your network. Which of the following necessary services could be blocked?

- ~~DNS~~
- SNMP
- SMTP
- LDAP

Explanation

Hardening against LDAP enumeration can be tricky. Although blocking LDAP port 389 is an option, you can't always block ports, or you'll risk impacting your network. Blocking LDAP ports could prevent your clients from querying necessary services. The best way to secure LDAP is to review and implement the security settings and services available with your server software.

The most basic way to counteract SMTP exploitation is to simply ignore messages to unknown recipients instead of sending back error messages.

The SNMP is used to manage devices such as routers, hubs, and switches. The easiest way to prevent SNMP exploitation is to block, or at least monitor, activity on ports 161 and 162 and any other port you've configured for SNMP traffic.

DNS zone restrictions ensure that a server provides copies of zone files to only specific servers.

References

TestOut Ethical Hacker Pro - 6.2 Enumeration Countermeasures
[e_enum_counter_eh1.exam.xml Q_ENUMCOUNTER_ENUM_COUNTER_LDAP_01_EH1]

Question 4: Incorrect

Which of the following is the most basic way to counteract SMTP exploitations?

- Monitor ports, remove agents, update systems, and change default passwords.
- Ignore messages to unknown recipients instead of sending back error messages.
- ~~Restrict zones to ensure where zones are copied, use digital signatures, and split zones.~~
- Review and implement the security settings and services available with your server software.

Explanation

The most basic way to counteract SMTP exploitation is to simply ignore messages to unknown recipients instead of sending back error messages.

Hardening against LDAP enumeration can be tricky. Although blocking LDAP port 389 is an option, you can't always block ports, or you'll risk impacting your network. Blocking LDAP ports could prevent your clients from querying necessary services. The best way to secure LDAP is to review and implement the security settings and services available with your server software.

SNMP is used to manage devices such as routers, hubs, and switches. The easiest way to prevent SNMP exploitation is to block, or at least monitor, activity on ports 161 and 162 and any other port you've configured for SNMP traffic.

DNS zone restrictions ensure that a server provides copies of zone files to only specific servers.

References

TestOut Ethical Hacker Pro - 6.2 Enumeration Countermeasures
[e_enum_counter_eh1.exam.xml Q_ENUMCOUNTER_ENUM_COUNTER_SMTP_01_EH1]

Question 5: Incorrect

Robby, a security specialist, is taking countermeasures for SNMP. Which of the following utilities would he most likely use to detect SNMP devices on the network that are vulnerable to attacks?

- Currport
- SNscan
- Scany
- ~~Colasoft~~

Explanation

SNscan is a utility that is used to detect SNMP devices that are vulnerable to attacks.

Scany is a scanner application for iOS devices. It scans networks, websites, and ports to find open network devices. It can obtain domain and network names and include basic networking utilities such as ping,traceroute, and whois.

Colasoft is a packet crafting software that can be used to modify flags and adjust other packet content.

Currports lists all open TCP and UDP ports on your computer. It also provides information about which process opened the port, which user created the process, and what time it was created.

References

TestOut Ethical Hacker Pro - 6.2 Enumeration Countermeasures
[e_enum_counter_eh1.exam.xml Q_ENUMCOUNTER_ENUM_COUNTER_SNMP_01_EH1]