CS Games 2017

Security - Theoretical (30%)

Participants	2
Booklet	1
Total Value	6%
Practical duration	2 hours 30 minutes
Theoretical duration	30 minutes

1. Complete the following sentences :

   Hack the *planet*

   PoC || *gtfo*

2. Popular *ezine*, famous for publishing the legendary *«Smashing The Stack For Fun And Profit» article: phrack*

3. Acronyms

APT	*advanced persistent threat*
C2/C&C	*command & control server*
MitM	*man in the middle*
LPE	*local privilege escalation*
WAF	*web application firewall*

4. Associate the breaches to the perpetrator

Perpetrator	↔	**Breach**
Phineas Fisher		Democratic National Committee (DNC)
Jeremy Hammond (Anarchaos)		HackingTeam
Impact Team		Ashley Madison
Guccifer 2.0		Stratfor email leaks

Phin Fisher→HT, Jeremy→Stratfor, Impact→AM, Guccif→DNC

5. What are the three types of XSS (Cross-site scripting)?

   1. *stored*
   2. *blind*

3. dom

6. This DNSSEC record can be used to enumerate domains from a zone:

   Answer: *nsec, nsec3, also accepted axfr even though it is not a dnssec record, it still leaks domains in poorly configured zones*

7. Describe the PHP null-byte injection vulnerability:

   include($_GET["page"].".php") → if we put a nullbyte in ?page=foo%00, we can reference files with their suffixes cut off, ie /etc/passwd\0.php → /etc/passwd

8. What port should be filtered (blocked) on a firewall if you want to block all *ping* (ICMP) traffic? *trick question, icmp is layer 3 vs ports are layer 4*

9. What type of devices does the Mirai malware target in order to spread further? *iot, webcams etc*

10. Technique used by malware operators in order to avoid sinkholes :

    domain Generation Algorithm

11. Name the bug/vulnerability

```
GET /cgi-bin/process.cgi HTTP/1.1
Host: foobar.com
User-Agent: () { :; }; /bin/id
```

    bashbleed, shellshock, etc

12. Why is it important to disable the TRACE HTTP method on your web servers? (ie **TRACE** / HTTP/1.1)

xss could use TRACE request verb and the web server would echo back the request in full, including the cookies. this way, a simple xss can leak cookies, even “httponly” cookies

13. Find the vulnerability/risk in this snippet:

```
server = request.get_var(“server”);
response.send("""HTTP/1.1 200 OK
              Date: Wed, 15 Mar 2017 22:27:43 GMT
              Server: %s
              Cookie: PHPSESSID=877c22163d8df9deb342c7333cfe38a7
              Content-Type: text/html\r\n\r\n""" % server);
```

response splitting https://en.wikipedia.org/wiki/HTTP_response_splitting

14. Briefly describe the following mitigation mechanism used in binary executables:

    1. PIE & ASLR:

Main module is loaded at random location in memory.

    2. RELRO:

Set init and finit arrays to read-only (And if full-relro, set the PLT/GOT table to read-only)

    3. SMEP:

Prevent execution of user space from kernel

    4. NX bit

Prevent execution of data

15. Find the vulnerabilities and risks this software introduces to a program. Briefly describe them:

```
char* get_name(int doPrint) {
  char* name = malloc(1000);
  gets(name);
  if (doPrint) {
    printf(name);
    free(name);
  }
  // Cleanup!
```

```
  free(name);
  return name;
}
```

gets lead to buffer overflow
format string vuln
Double free if doprint true
return freed buffer (use after free)