Quiz 1 Linux

Malware and software vulnerabilities are related because:
- Both have the potential to cause problems by misusing a user's authority

Malware which poses as legitimate software is a :
- Trojan Horse

Signature-based antimalware often fails because of:
- False negatives: new malware (100% correct)

Malware which spreads directly to other computer is a :
- Worms

A GNU/Linux distribution typically does NOT:
- Cost money to download

Which of these statements about Richard Stallman is FALSE:
- He created the linux kernel

On Unix each process has its own address space, which means:
- The kernel cannot access the memory processes

Which of these statements about the GPL licence is FALSE:
- It grants the right to trademarks OR It grants the right to modify the program

On Unix, each process is associated with:
- A user account identity

Dennis Ritchie created which programming language for UNIX:
- C

Mac OS X is certified Unix:
- True

Many penetration test are conducted from Linux systems, this is primarily because:
- Many tools for testing security are available for Linu, and distrubutions are available that conveniently bundle testing tools

On Unix, filenames can include symbols such as a*
- True

UNIX was created at:
- AT&T Bell Labs

The term "free software" emphasises:
- The freedom granted

Unix was created in which programming languages

- Assembly and C

Unix security was originally designed to:
- Protect users from each others

Which of these systems are Unix certified?
- Darwin
- Solaris
- Mac OS X

Linux Torvalds is:
- Creator, chifed architect, and coordinator of the Linux kernel

The Unix ___ typically enforces security features.
The missing word is:
- Kernel

On Unix, filenames REQUIRE file extensions: for example, .JPG
- False

UNIX security was originally designed for:
- Multiple users sharing computers via dumb terminals

Linux is certified Unix:
- False

/bin/bash is an example of:
- An absolute filename

Large corporations hire programmers to contribute to Linux:
- True

Android runs the Linux kernel:
- True

On Unix each process has its own address space, which means:
- Processes cannot modify each others allocated memory

Unix security was originally designed to :
- Protect users from each other

On Unix, filenames are typically NOT case sensitive:
- False

An example of Unix-Like system (not officially Unix) is:
- Mac OS X

Copyleft means:

- That copyright does not apply

Which of these statements about Richard Stallman is FALSE:
He created the Linux kernel
-

On Unix, filenames can include symbols such as a *
- True

On Unix each process has its own address space, which means:
- Processes cannot communicate with each other

The term “open source software” emphasises:
- The freedom granted

UNIX is now a :
- Trademark, and standard

Unix security was originally designed to:
- Protect users from each other

Quiz 2 Malware

Malware which speaks directly to other computer is a:
- Worm (100% Correct)

Malware is software which:
- Is designed to do malicious things (100% Correct)

Black-lists provide more security than white-lists but are harder to maintain
- False (100% Correct)

If malware was run as a normal user on Unix, it could easily:
- Read and modify your personal documents (100% Correct)

Anomaly – based antimalware works by:
- Detecting suspicious activity (100% Correct)

If malware was run as the root user on Unix, it could easily:
- All of these listed options (100% Correct)

  (the listed options were: Read and modify your personal documents, Modify the way your computer boots up, Read and modify any files on the computer)

Signature-based antimalware often fails because of:
- False negatives: new malware (100% Correct)

Signature- based malware detection relies on:
- Detecting known malware code and techniques (100% Correct)

The “$PATH” environment variable specifies:
- Where to find programs (100% Correct) [double check in Raghav’]

Which command will show the options for configuring the windows/shell_bind_tcp payload?
- msfpayload windows/shell_bind_tcp O (100% Correct)

Malware which spreads directly to other computers is a:
- Worm

An infected computer that is under the control of an attacker is known as a :
- Zombie (100% Correct)

Software that hides the presence of malware is a:
- Rootkit (100% Correct)

When you run a program (on a typical OS without sandboxing) you are trusting that program with access to all of your files and documents
- True (100% Correct)

Standard Windows and Unix access controls as normally configured can..:

- Restrict the amount of damage that malware can do (100% Correct)

Which of the following is NOT a form of “selective execution”:

- Software patching (100% Correct)

Digitally signed programs (executables with digital signatures) typically proves:

- Who the author was (100% Correct)

A malicious program that copies itself into other local programs is a :

- Virus (100% Correct)

Which of the following is TRUE of msfencode:

- It takes as input a payload and reencodes it to something else that has the same effect (100% Correct)

Malware that is running as a normal Unix account can:

- Read all of the user’s personal files and Web history (100% correct)

Malware which poses as legitimate software is a :

- Trojan horse

Why shouldn’t the $PATH environment variable inclue “.” (the current directory)?

- An attacker could place a script in a directory, which you may accidentally execute (100% correct)

Which of the following statements is TRUE?

- An EXE wrapper can join a Trojan horse and a normal prog into one so that it apps less malicious to a user

A program that has been digitally signed:

- Proves who authored the software, assuming you check and trust the certificate authority (CA) and no one else has the author’s private key (100% correct)

Which of the following commands will generate an executable that adds a user to a Windows system:

- Msfpayload windows/adduser USER = tux PASS = lives X > t.exe

Quiz 3 Vulnerabilities

A payload that gives the attacker a command prompt is known as a (n):

- Shell Code (100% correct)

Which of these interfaces for MSF can be used to exploit a vulnerability in a remote service?

- All of the abv

A mistake by a software developer can result in enabling attackers to take control of the program

- True (100% correct)

If an attacker starts as a normal user, and ends up as a superuser (root or Admin), they have managed:

- Vertical privilege escalation (100% correct)

What is wrong with the following use of msfconsole?
use exploit/multi/samba/usermap_script
set PAYLOAD cmd/unix/reverse
exploit

- The attacker forgot to set options such as IP addresses and ports (100% correct)

In Metasploit, which of these types of modules are intended to evade detection?

- Encoding (100% correct)

Which of the foll is NOT a software vulnerability?

- Software designed to be malicious (100% correct)

A method of mitigating the effects of software vulnerabilities is to (best answer):

- Keep software up-to-date (100% correct)

A payload that connects back to the attacker and grants them a command line access, is knows as a:

- Reverse shell

A programmer makes a mistake that introduces a security problem. This is known as a (n):

- Software vulnerability (100% correct)

A program that takes advantage of a programming mistake to take control of a computer is:

- An exploit (100% correct)

A reverse shell is more likely to evade firewalls than a bind shell?

- True (100% correct)

A payload that give the attacker a command prompt is known as (n):

- Shell code (100% correct)

While studying a program, you notice that it accidentally lets any user access all the system passwords. This is an example of a (n):

- Software vulnerability (100% correct)

Malicious code inserted during an attack that connects back to the attacker to grant access to the computer is an example of a (n):

- Payload

Posting details of a new software vulnerability to the Internet, without first contacting the software authors or vendors, is know s as:

- Full disclosure (100% correct)

If an attacker starts with access to a user “bob”, and ends up with access to user “fred”. They have managed:

- Horizontal privilege escalation (100% correct)

Which of the following is NOT a type of module available in Metasploit Framework (MSF)?

- Malware

What is wrong with the foll use of msfconsole?
Use exploit/multi/samba/usermap_script
Set PAYLOAD cmd/windows/reverse
Set RHOST 192.168.1.1
Set LHOST 192.168.1.2
Set LPORT 7777
Exploit

- This payload is not compatible with this exploit (100% correct)

Which of the foll would be most likely to help you identify any soft installed on a machine that was vulnerable to attack via a buffer overflow?

- Software updates (100% correct)

The window of vulnerability is the time betn:

- When a version of soft comes out containing a security problem until the time the end user updates to a version…….. (100% correct)

The code that takes affect after compromising a system is known as a (n):

- Payload

A payload that waits for the attacker to connect and grants them command line access, is known as a :

- Reverse Shell

Quiz 4 – Footprinting

The Whois protocol uses which port?

- TCP port 43

Passive info gathering is likely to be detected by:

- None of these (100% correct)

The Dnsmap tool is designed to:

- Guess subdomain names (100% correct)

The steps of an attack typically involve this sequence of events:

- Info gathering, exploitation, and post-exploitation (100% correct)

Whois can provide an attacker with:

- All of theses (100% correct)
  [contact details…… , Name servers, Mail servers]

Put the stages of attack into the correct order

- 1) Footprinting 2) Scanning 3) Enumeration 4) Exploitation 5) Post- Exploitation (100% correct)

A DNS zone transfer on an org's DNS server would be considered:

- Active info gathering (100% correct)

Given a domain name, an attacker could determine IP address using:

- The dig command (100% correct)

Dig google.co.uk ANY

- A listing of various types of DNS recs (100% correct)

Info gathering does not usually involve

- Exploitation (100% correct)

RIPE and ARIN are examps of:

- Regional Internet registries (100% correct)

Given a single IP address, the attacker can likely use Whois and DNS to discover:

- All of these (100% correct)

Starting with a domain such as google.com, what technique could be used to find domains such as mail.google.com?

- Subdomain brute-forcing (100% correct)

Dig +short leedsmet.ac.uk MX

- Mail servers (100% correct)

Passive info gathering is likely to be detected by:

- None of these (100% correct)

Dig @8.8.8.8 mydomain.co.uk AXFR

- Attemps a zone transfer on mydomain.co.uk using the 8.8.8.8 server (100% correct)

Dig +short –x 130.57.5.70
The above command will return what?

- IP address that the domain name resolve to (wrong)

Starting with a single IP address, how could an attacker determine the range of IP addresses used by the company?

- Whois (100% correct)

Dig +short google.co.uk AAAA

- Ipv6 address

Dig @8.8.8.8 mydomain.co.uk
The above cmd does what?

- Attempts to resolve the Ip address for mydomain.co.uk using the DNS server 8.8.8.8 (100% correct)

Given a domain name, an attacker could determine IP address(es) using:

- The dig command (100% correct)

A DNS zone transfer conducted by an attacker is an example of:

- A software vulnerability

Whois is:

- All of these (100% correct)
  [db, program, protocol]

Quiz 5 Scanning

What will the foll cmd do?
Sudo nmap –sU 10.72.35.207

- Perform a scan that uses a connection-less IP protocol (100% correct)

What will the foll cmd do?
Sudo nmap –p 22 10.72.35.207

- Scan for an SSH server (100% correct)

A ping sweep can tell you:

- Which hosts are live (100% correct)

How many possible TCP ports exist?

- 65535 (100% correct)

What will the foll cmd do?
Sudo nmap –sX 10.72.35.207

- Performs a scan that sets the FIN, PSH, and URG flags (100% correct)

Nmap –sn –PE 192.168.1.1
What does the abv cmd do?

- A ping sweep (a ping req) of a single system (100% correct)

After what stage of an attack would an attacker most likely identify which attacks would likely succeed against a system?

- Exploitation (wrong)

Which of the foll techniques (on its own) CANNOT be used to determine what version of a soft is running on a remote syst?

- SYN Scan (100% correct)

What will the foll cmd do?
Sudo nmap –p 25, 110 10.72.35.207

- Scan for an email server (100% correct)

Given the below invocation and output of Nmap, what can you conclude?

Nmap 10.72.35.110-112 –p22
Starting Nmap 5.61TEST2 (http://nmap.org) at 2013-10-15 16:16 BST
Nmap scan report for 26212pc.dyn.leedsmet.ac.uk (10.72.35.111)
Host is up (0.0016s latency)
PORT STATE SERVICE
22/tcp closed ssh

- Of the systems scanned, only one is live and IS NOT accepting connections to port 22

The term “attack surface” refers to:

- The various ways an attacker can interact with a sys or soft (100% correct)

What will the foll cmd do?
Sudo nmap –sT 10.72.35.207

- Perform a scan that connects using a full TCP three-way handshake (100% correct)

If you try to connect to a remote system on port 80 using Telnet or Netcat, and you cannot connect, then you can deduce that:

- There is no webserver on the host, or it is blocked by a firewall (100% correct)

Scanning can be used:

- All of these (100% correct)

Namp –sn 192.168.1.1
What does the abv cmd do?

- Attemps a series of actions to detect that the host is live (inc an ICMP echo req and ICMP timestamp req) (100% correct)

What will the following command do?
Sudo nmap -sS 10.72.35.207

- Perform a scan that does not complete the three-way handshake (100% correct)

A SYN scan works by:

- Competing the full three-way handshake (wrong)

What will the foll cmd do?
Sudo nmap –p21 10.72.35.207

- Scan for a ftp server (100% correct)

What will the foll cmd do?
Sudo nmap –p25 10.72.35.207

- Scan for an email server (100% correct)

For i in (1…254)
Do
Ping –c 1 –W 1 192.168.1.$i |grep ‘from’
Done
Which of the foll comments is true of the abv ping sweep Basch Script?

- Either It will disp the result of every req, regardless of resp OR It could take upto 255 secs (over 4 mins) to complete

If a server does not send any response packet when a client tried to connect, which of the foll is most probable?

- The port is waiting for a port knocking seq

Given the below invocation and output of Nmap, what can you conclude?

Nmap 10.72.35.110-112 –p22
Starting Nmap 5.61TEST2 (http://nmap.org) at 2013-10-15 16:16 BST
Nmap scan report for localhost(127.0.0.1)
Host is up (0.000028s latency)
PORT STATE SERVICE
22/tcp open ssh

- The local sys has an ssh server running (100% correct)

Namp –sL 192.168.1.1
What does the abv cmd do?

- Simply resolves the DNS name for the IP address (100% correct)

What will the foll cmd do?
Sudo nmap –p 23 10.72.35.207

- None of these services (100% correct)

In order for a TCP connection to be establishes, what order are the foll packets sent?

- SYN, SYN/ACK, ACK (100% correct)

Which of the foll statements is true of a SYN scan?

- It is faster for the scanner, since it does not need to estab a full TCP connec (100% correct)

Sudo nmap –p 23 10.72.35.207

- None of these services (100% correct)

Namp –sL 192.168.1.1
What does the abv cmd do?

- Simply resolves the DNS name for the IP address (100% correct)

What will the foll cmd do?
Sudo nmap –p25 10.72.35.207

- Scan for an email server (100% correct)

What will the foll cmd do?
Sudo nmap –p21 10.72.35.207

- Scan for a ftp server (100% correct)

What will the following command do?
Sudo nmap -sS 10.72.35.207

- Perform a scan that does not complete the three-way handshake (100% correct)

Namp –sn 192.168.1.1
What does the abv cmd do?

- Attemps a series of actions to detect that the host is live (inc an ICMP echo req and ICMP timestamp req) (100% correct)

Quiz 6 Exploits

Which of the following is not an exploit framework ?

- Nessus

Metasploit, Core Impact and CANVAS are exploit frameworks wheras Nessus is a vulnerability scanner.

Common Vulnerabilities and Exposures (CVE) is a database containing which of the following ?

- Brief details and link for public vulnerabilities

What is a disadvantage of using Armitage's "Find Attacks" feature ?

- Not as thorough as a vulnerability scan : false positives and false negetives.

Stand-alone exploits were traditionally written in which programming language ?

- C

Who founded the Metasploit Project ?

- HD Moore

Which of the follwing would complile the file "/usr/share/exploitdb/platforms/windows/remote/66.c" to an exeutable named "bam"?

- gcc /usr/share/exploitdb/platforms/windows/remote/66.c -o bam

Which of the following would be the most effective msfconsole command to search for exploits against Linux ?

- Search type:exploit platform: 'Linux'

What does the following command do ?
Searchsploit windows

- Searches a local copy of The Exploit DB

Which of the following will not provide you with the working exploit code ?

- CVE database

Which of the following would be a valid CVE-ID?

- CVE-2004-0012

Software Vulnerabilities in operating system, such as the Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability, are becoming rarer, and many more attacks are now found In webservices and applications ?

- True

Metasploit exploit modules are written in which programming language ?

- Ruby

In msfconsole, what command would you use to set the attack target to a host in the Metasploit database running a webserver ?

- Services -p 80 –R

A current organization should NOT use Windows Server 2000 as a webserver. Why not ?

- Windows 2000 contains many security vulnerabilities such as buffer overflows, which will never be fixed since it has reached end of lifecycle.

CVE is run by which of the following ?

- The MITRE Corporation

If an exploit gives an attacker arbitrary code execution as LocalSystem, then this means:

- The attacker can run commands on the system, and basically has full control over a Windows system

What port does CVE-2003-0352 affect?

- 135

Which of the foll is NOT an interface to MSF?

- Nessus

A CVE –ID is used to:

- Uniquely identify vulnerabilities across tools and services

Quiz 7 Post Exploitations

After successful exploitation, the attack surface usually changes

- True

Distcc is a network service to distribute compilation……Which of the foll statesments are true?

- This is a security issue, because this can give an attacker shell access to the sys, and depending on the sys could open they sys up to local privilege esc attack

If an attacker attacked a Windows sys and obt a bind shell using Metasploit, which of the foll would almost certainly be true?

- The attacker would be able to run commands on the windows sys

On a Windows sys, if an attacker has managed to compromise a sys, and find they have a security idenifier (SID) of "S-1-5-1180------- 500" which of the foll will the attacker likely be able to modify?

- All of these

Which of the foll is a disadvantage (for an attacker) of setting up a backdoor on a compromised system?

- It involves writing to disk, which leaves evidence

Linus:~> id –u
1000
Given the abv output, which of the foll will the attacker likely be able to modify?

- File belonging to the corresponding user

Meterpreter was originally developed by:

- Matt miller

Which of the foll would give an attacker the ability to do the most amt of damage?

- A root shell

Linus:~> id –u
0
Given the abv output, which of the foll will the attacker likely be able to modify?

- All of these

During post-exploitation on a compromised Linux system, an attacker may run "uname -a". Why?

- To determine the version of the linux kernel and distro, which could potentially lead to discovering further vulnerabilities.

Msf>use post/linux/gather/hashdump
Msf post (checkvm) > set SESSION 1
Msf post (checkvm) > exploit
Given the abv comds, what could an attacker do with the output?

- They could try to crack the hashes

Which of the foll would typically only happen during post-exploitation?(not earlier in an attack)

- Make modifications to protected files

If an attacked system is logging to a secure remote server, which of the foll methods could be used to effectively cover the tracks of an attacker?

- Disabling logging from the attacked system

An advantage (for an attacker) of installing a rootkit, is that:

- It persists on the victim system (possibly providing the attacker with a backdoor) and hides its presence to cover the attacker's tracks

Someone monitoring network traffic could easily read all the commands an attacker sends to Meterpreter

- False

Which of the foll statements about Meterpreter are true?

- Meterpreter makes life easier for the attacker, since it includes lots of features

Linux:~> cat/etc/shadow

Cat: /etc/shadow: Permission denied

Given the output abv, which of the foll is the most likely security context?

- UID = 2

An exploit that is run as a normal user and is used to obtain superuser access, is known as:

- A local privilege escalation exploit

An attacker could use pivoting to:

- All of these

If an attacker gets a shell with the security context of a normal user:

- It is sometimes possible to use a local privilege escalation attack to get superuser shell, if there is vulnerability present

Port Forwarding would be used by an attacker:

- For pivoting attacks thru a compromised sys

Meterpreter>getuid

What would the above command be used to do?

- Determine the security context

Which of the following would typically only happen during post exploitation? (Not earlier in an attack)

- Make modifications to protected files

Not other options like (Launching an exploit, attacks to obtain priviledges not normally afforded to the attacker, information gathering)

Msf > use post/linux/gather/checkvm

Msf post(checkvm) > show options

Msf post(checkvm) > set SESSION 1

Msf post (checkvm) > exploit

Given the sequence of commands, what has the attacker done ?

- Run a post-exploitation module to gather information from a compromised system

A sandbox can typically be used to:

- Restrict what an attacker can do after taking control of a process

Quiz 8 – Vulnerabilities Ethics

Confidentiality is:

- Privacy (wrong)

Alice breaks into a botnet while conducting research, and finds that the botnet is causing harm to others by collecting credit card numbers, mining Bitcoin, and intercepting and modifying bank transactions. She is faced with the decision: does she shutdown a large number of zombies on the botnet, thereby protecting thousands of people, or does she continue to study the botnet to try find a way to permanently stop it.
Deciding to shutdown the zombies would be an example of what kind of ethical reasongs?

- Consequentialism (wrong)

Bob discovers a new soft vulnerabiliy, and he decides to release the exploit code publicly without notifying the software authors. He believes that it is the best way to get the authors to fix the problem fastest.
This is an example of what type of ethical reasoning?

- Consequentialism

Which of these approaches to ethics emphasises the importance of improving the overall good to the society?

- Utilitarianism

Local Web Proxies such as Burp Suites or WebScarab are primarily used for:

- Testing a website for security problems, by intercepting requests betn an attacker and a server

Which of the foll is NOT a vulverability scanner?

- MSF

OpenVAS is a fork of which project?

- Nessus

Which of the foll tools includes scripts for performing vulnerability analysis scans?

- Nmap

If a vulnerability scanner reports that port 80 is open a web server what should you do:

- Nothing , this is normal

Which of the foll is NOT an advantage of vulnerability scanning vs penetrating testing

- Thorough and complete

A vulnerability scan will never scrash the sys being scanned:

- False

If a vulnerability scan reports that s sys is vulnerable to the RPC DCOM buffer overflow vulnerability, then this sys could be attacked/exploited using:

- Standalone exploit code

Which of the foll would NOT be conducted during a typical vulnerability scan?

- Exploit vulnerabilities

Carol discovers a new software vulneb and she decides to sell the info to a third party. She believes that it is the right thing do do, since she put the work into finding the flaw and deserves to be paid for her work, regardless of any consequences. This is can example of what type of ethical reasoning?

- Egoism

Alice discovers a new software vulnerability and she desides to notify the soft devs one month before releasing info abt the flaw publicly. She belives that is the right thing to do., since although releasing the info could result in harm, overall it provides incentive for a fix to be released and the end result is that systems are more secure.

This is an example of what type of ethical reasoning?

- Consequentialism

Eve discovers a new soft vulneb, and she decides to notify the soft devs without releasing any info publicly. She belives that is the right thing to do., since moral people do not help attackers, and she is a moral person. This is :

- Virtue Ethics

If Nessus detects that a server has port 443 open, this most likely means:

- That it is probably a web server

If a Nessus scan reports that a sys is vulneb to a remote exploit with arbitrary code exec, this means:

- An attacker MAY be able to run comds on this service

Which of the foll rights are related to right to privacy?

- All of these

Vulnerability analysis vs penetration testing

- Vulnerability analysis generates more false positives

Port scanning vs Vulnerability analysis which one is automated and reports more vulnerability of the system.

- Vulnerability analysis using Retina