Mini-Project 3 Checkpoint 1

ECE/CS 498DS

Spring 2020

br17, ashar29, anunays2

Task 0

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

http.pcap represents attacker activity and **http2.pcap** represents the legitimate activity
We recognize the attacker activity by the presence of #cmd in the content_type header

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

No. There are no 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

Ans: **1521394990.853758**

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

Ans: 172.17.0.2

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

Ans: **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	occurence	content_type_length
0	%{(#_='multipart/form-data').(#dm=@ognl.OgnlCo...	3	818
1	%{(#_='multipart/form-data').(#dm=@ognl.OgnlCo...	1	806
2	%{(#_='multipart/form-data').(#dm=@ognl.OgnlCo...	2	845
3	%{(#_='multipart/form-data').(#dm=@ognl.OgnlCo...	1	810
4	.multipart/form-data~${#context['com.opensymph...	3	144
6	application/x-www-form-urlencoded	4	33

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**	***command-line utility for downloading files from the web***
ls	**Yes**	***command-line utility for listing the contents of a directory or directories given to it via standard input***
cat	**Yes**	***command allows us to create single or multiple files, view contain of file, concatenate files and redirect output in terminal or files***
cd	**No**	**-**
insmod	**Yes**	***trivial program used to insert module to the linux kernel in any location***
ssh	**No**	**-**
lsmod	**No**	**-**

Task 1 – Host Logs Analysis

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

```
array(['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'],
      dtype=object)
```

Total records: 303
Unique modules: 90

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

rk is the attacker controlled kernel module

Task 1 – Host Logs Analysis

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

Check if the module name **rk** exists in os log query data and verify if it has been added at least once in the vulnerable server

	name	hostIdentifier	calendarTime	unixTime	epoch	counter	action	decorations.host_uuid	decorations.username	columns.name	...	colu
0	system_info	ubuntu	Tue Feb 6 00:33:05 2018 UTC	1517877185	0	38463	added	D5882FBF-1D65-4A30-B216-77F664B7D3B0	root	rk	...	
42	kernel_module	ubuntu	Tue Feb 6 00:34:09 2018 UTC	1517877249	0	0	added	D5882FBF-1D65-4A30-B216-77F664B7D3B0		rk	...	
2882	kernel_module	ubuntu	Mon Mar 19 15:58:54 2018 UTC	1521475134	0	100	added	D5882FBF-1D65-4A30-B216-77F664B7D3B0	root	rk	...	

3 rows × 27 columns

Task 1 – Host Logs Analysis

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

The file name is **known_hosts**

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.)

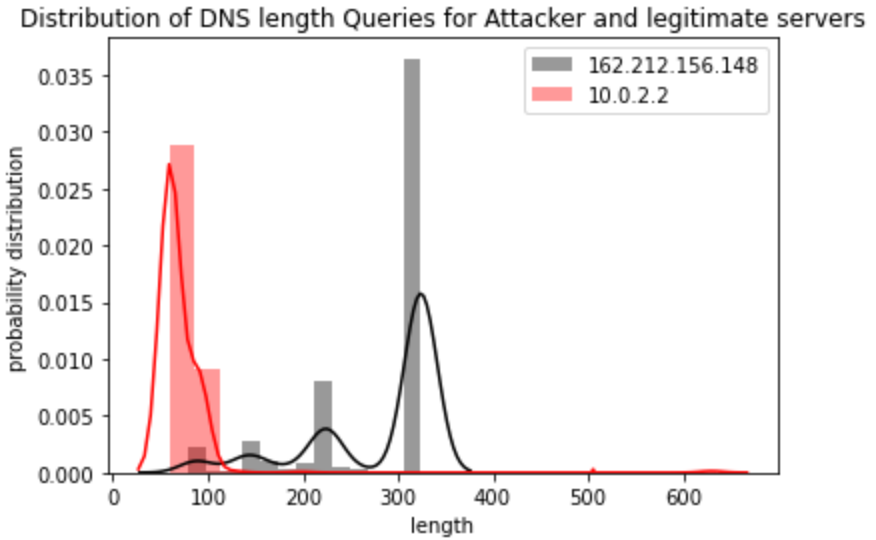
The naïve attacker didn’t extract any internal hostnames. It is verified by checking if **known_hosts** are present in the content_type of http and it wasn’t

Task 1 – DNS Traffic Analysis

1. (a) Provide the IP address of the attacker-controlled DNS server:
162.212.156.148 (This is present in the attacker file http)

1. (b) Provide the IP address of the legitimate-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)
S1 = 0	0.7727
S1 = 1	0.2273

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

S1 = 0 (No attack) maximizes the marginal probability P(S1)

Task 2

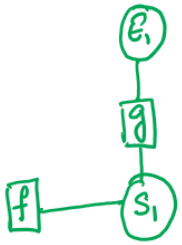
Task 2.4 Suppose you have already observed the event E1=1, provide the probability P(S1).

S1	P(S1/E1=1)
S1 = 0	0.6939
S1 = 1	0.3061

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

S1 = 0 (No attack) has the higher probability when E1 = 1 is observed.

Task 2.6 Verification of 2.5 through hand calculation.



$$\mu_{E_1 \to g(E_1)} = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \begin{matrix} B=0 \\ B=1 \end{matrix}$$

$$\mu_{g \to S_1(g)} = \sum_{E_1 \in \{0,1\}} g(S_1, E_1) \times \mu_{E_1 \to g}(E_1)$$

$$= \begin{bmatrix} 0.1 \\ 0 \end{bmatrix} \begin{matrix} S_1=0 \\ S_1=1 \end{matrix} \times 1 + \begin{bmatrix} 0.2 \\ 0.5 \end{bmatrix} \begin{matrix} S_1=0 \\ S_1=1 \end{matrix} \times 1$$

$E_1 = 0$ $\qquad$ $E_1 = 1$

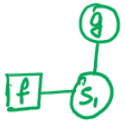
$$g \to \begin{bmatrix} 0.3 \\ 0.5 \end{bmatrix} \qquad f \to \begin{bmatrix} 0.85 \\ 0.15 \end{bmatrix}$$

$$S_1 \to \begin{bmatrix} 0.3 \times 0.85 \\ 0.5 \times 0.15 \end{bmatrix} = \begin{bmatrix} 0.255 \\ 0.075 \end{bmatrix}$$

$Z = 0.33$. After normalizing →

$$P(S_1) = \begin{matrix} S_1=0 \\ S_1=1 \end{matrix} \begin{bmatrix} 0.772 \\ 0.227 \end{bmatrix}$$

When $E_1 = 1$ is observed –



$S_1=0$ $\quad g \to \begin{bmatrix} 0.2 \\ 0.5 \end{bmatrix}$ $\quad f \to \begin{bmatrix} 0.85 \\ 0.15 \end{bmatrix}$

$S_1=1$

$$P(S) = g \times f = \begin{bmatrix} 0.17 \\ 0.075 \end{bmatrix}$$

After normalizing –

$$\therefore \begin{matrix} S_1=0 \\ S_1=1 \end{matrix} \begin{bmatrix} 0.6939 \\ 0.3061 \end{bmatrix}$$

Task 3

Task 3.0 : Tables for Severity factor function f1 to f9

	state_name	f1	f2	f3	f4	f5	f6	f7	f8	f9
0	benign	0.936	1.0	0.553333	0.553333	0.553333	0.875	0.02	0.02	0.02
1	discovery	0.064	0.0	0.000000	0.000000	0.000000	0.000	0.00	0.00	0.00
2	access	0.000	0.0	0.000000	0.000000	0.000000	0.000	0.00	0.00	0.00
3	lateral_movement	0.000	0.0	0.000000	0.000000	0.000000	0.000	0.00	0.00	0.00
4	privilege_escalation	0.000	0.0	0.446667	0.446667	0.446667	0.000	0.00	0.00	0.00
5	persistence	0.000	0.0	0.000000	0.000000	0.000000	0.125	0.00	0.00	0.00
6	defense_evasion	0.000	0.0	0.000000	0.000000	0.000000	0.000	0.00	0.00	0.00
7	collection	0.000	0.0	0.000000	0.000000	0.000000	0.000	0.00	0.00	0.00
8	exfiltration	0.000	0.0	0.000000	0.000000	0.000000	0.000	0.98	0.98	0.98
9	command_and_control	0.000	0.0	0.000000	0.000000	0.000000	0.000	0.00	0.00	0.00
10	vulnerable_code_execution	0.000	0.0	0.000000	0.000000	0.000000	0.000	0.00	0.00	0.00

Task 3

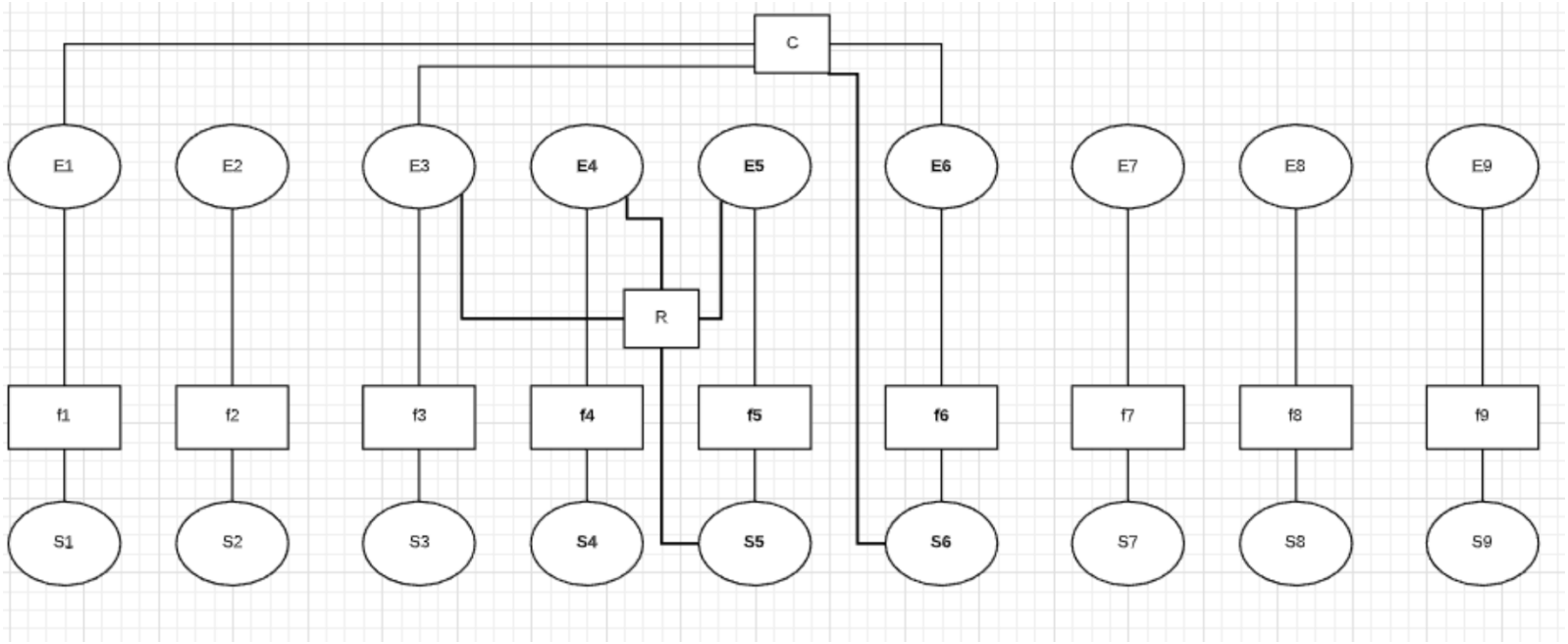
Task 3.1 : Tables for factor commonality and repetitiveness factor functions

Most Common Event Sequence	Factor Function	Attack States	Probability
Scan Sensitive_URI New_Kernel_Module	c	Persistence	0.0714

Most Frequent Repetitive Event Sequence	Factor Function	Attack States	Probability
Sensitive_URI Sensitive_URI Sensitive_URI	r	Privilege escalation	0.0664

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

State_name	Benign	Discovery	Access	Lateral_ mo vement	Privilege_ escalation	Persistence	Defense_ evasion	Collection	Exfiltration	Command_ and_control	Vulnerable _code_ execution
S1	0.936	0.064	0	0	0	0	0	0	0	0	0
S2	1	0	0	0	0	0	0	0	0	0	0
S3	0.553333	0	0	0	0.446667	0	0	0	0	0	0
S4	0.553333	0	0	0	0.446667	0	0	0	0	0	0
S5	0	0	0	0	1	0	0	0	0	0	0
S6	0	0	0	0	0	1	0	0	0	0	0
S7	0.02	0	0	0	0	0	0	0	0.98	0	0
S8	0.02	0	0	0	0	0	0	0	0.98	0	0
S9	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 Action	No-op Action	No-op Action	No-op Action	Monitor Action	Monitor Action	Stop Attack Action	Stop Attack Action	Stop Attack Action

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

At t=7, the model should recommend to stop the attack

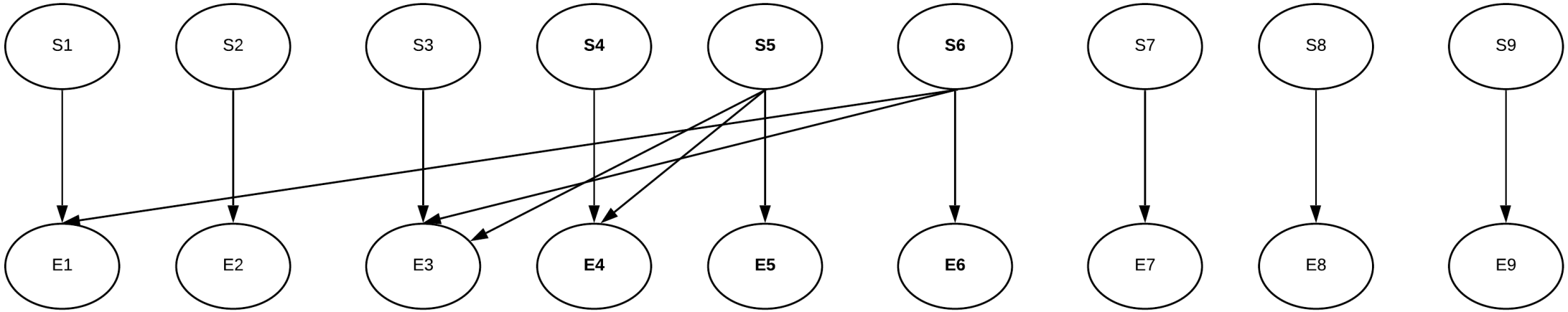
Task 3

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

The most probable states for S1-S6,S8,S9 remain the same because S7 and E7 are an independent entity disconnected from the other states and events. No message/beliefs are passed onto another nodes due to which their probabilities are independent of S7 and E7

Task 3

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



Task 3

Task 3.8.b. What parameters are needed for this HMM model to work?

1) Transition Probability Matrix (Chance of moving from one state to another)
2) Emission Probabilities (Probability of an event happening)
3) Initial distribution of hidden states (Pi)

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

1) Factor graphs can represent both casual and non-casual relationships with undirected network.

2) Factor graphs can take all the past states into consideration for finding the probability distribution of each states unlike HMM which assumes that current state depends only on its immediate past state. In essence, it is a superset to HMMs

Task 4

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

It is not possible to detect the attack using only one event. For example, when we consider event e1, there can be any official user who can login to the current equifax website to look up some information. It is **only by observing a sequence of past events**, we can say that the server is 100% on attack

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

1) **Login** - The system admin is logged into the server to check for some network issues and he is mistaken as an attacker

2) **Sensitive URI** - The company would have prompted for all the users to download .exe. for instance that would provide a set of instructions to the users in their OS. This could be mistaken as an URI from a suspicious source like an attacker. *Ref:* https://www.computerhope.com/jargon/e/execfile.htm

3) **New executable file** - For a new update, a new .exe file by the system admin can be uploaded which can be mistaken as an attacker's file.

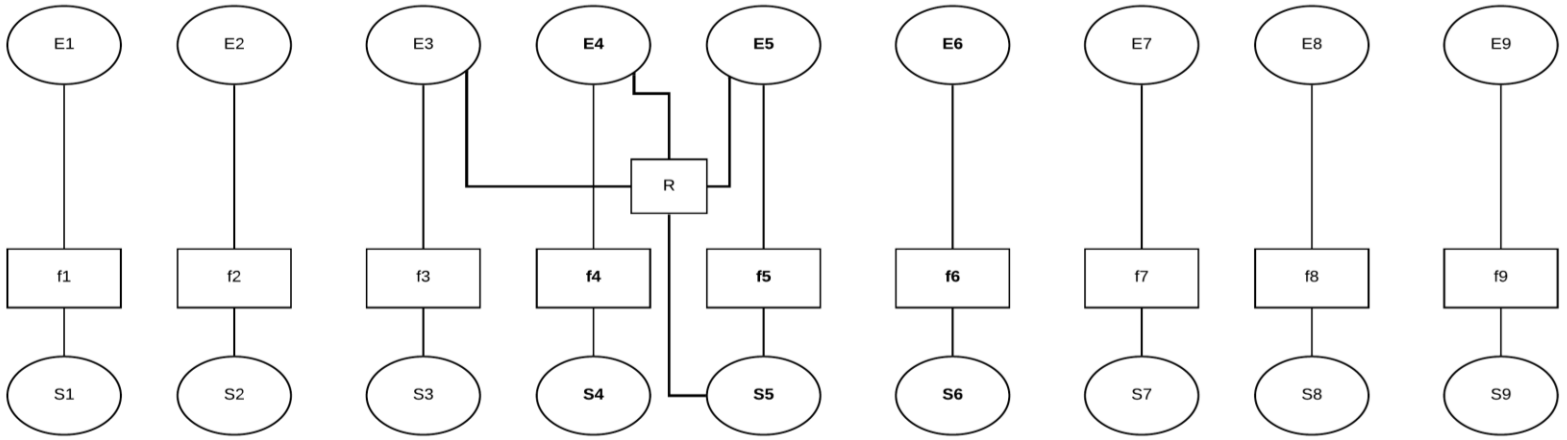
4) **Home page overwritten with a new link** - The server admin might want the users to access the domain quite easily and could have renamed it, but it might have been misunderstood as being done by an attacker

5) **Webserver restarted** - A system admin is restarting the webserver after performing some modifications in the configuration. This might be misleading as the system might think that there is an attack in progress

6) **Scan** - When an auto-scanner is run by the server like **website vulnerability scanner**, it might be misunderstood as an attacker invading privacy. Ref: https://pentest-tools.com/website-vulnerability-scanning/website-scanner

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.

Common Variable: Scan, Login, Sensitive URI
Common Factor Function: R(repetitive factor function)