Assignment 6

Abbas Khan , Mariia Rybalka , Linara Adilova

July 5, 2016

Task 6.1 (theoretical): Fast-Flux, Double-Flux

Fast-Flux networks are the bunch of IP addresses associated with single domain name and changing very fast (every 3 minutes for example). So, every time the client will try to connect to the server, he actually will be redirected to different final destinations. The mothership node of such network will be requested every time when there is a request and will decide on the end node to direct it. Double-Flux networks introduce one more random layer to the Fast-Flux - the authoritative name server. So when the user will send a request, he will be first trying to resolve the domain name and he will be redirected every time to different name servers for resolving it. These types of networks are used by attackers to redirect users to their illegal websites with malicious content. It is very hard to follow these redirections as it always changes, so it is a good protected phishing attack. [1]

Task 6.2 (theoretical): Buzzword Bingo

- **Advanced Persistent Threat (APT)** - kind of attack to get unauthorised access to network data. Its goal not to bring any damage, but, being undetected for the long time, get access to some highly valuable (government, corporation, etc) data and/or to be able to monitor it. APT searches the way to enter the network, and then slowly tries to reach target data. [2]
  Example: The Stuxnet computer worm.

- "**Spear phishing** is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information." [3]
  Example: In June of 2015, Ubiquiti Networks Inc., an American network technology company, lost $46.7 Million because of a spear phishing e-mail. The finance department of the company were made to believe that they are receiving real requests (by emails) for transferring money to some accounts and they just did it. [4]

- **Exploit kits** are toolkits used to exploit security holes primarily to spread malware. These toolkits come packaged with exploit codes. These exploit kits target software such as Adobe Flash, Java, Microsoft Silverlight, Internet Explorer - software that are commonly installed and used in most PCs. There are a number of ways how exploit kits arrive in a computer. Blackhole exploit kit, one of the many known exploit kits in existence, is known to spread via spam. When an exploit kit successfully exploits an insecure software in a computer, the typical payload is the installation of another malware. [5]

- **Ransomware** is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key. [6]
  Example: First cases of ransomware infection were detected in Russia in 2005-2006. One of the varians known as TROJ_CRYZIP.A that zips the files, removes the files themselves and that zip is password protected. Also it leaves a text file for the user with a note, that he should pay in order to get the files back. [6]

Task 6.3 (theoretical): Firewalls

1. Computers from the subnet 192.168.10.* can access any addresses from every port on port 80 with TCP connection and they can initialise the connection. The same subnet computers can be accessed by any address from the 80th port on any port with TCP connection, but only for already established connection. So the first two rules allows TCP exchange for subnet with other addresses. Computers from the subnet 192.168.20.* can access computers from the subnet 10.10.10.* from port 443 to any port by TCP connection and they can establish this connection. And computers from 10.10.10.* can answer from any port to port 443 for 192.168.20.* for established connections. All the other connections are prohibited.

2. Table of rules:

Rule	Src. IP	Dest. IP	Protocol	Src. port	Dest. port	ACK bit	Action
1	172.16.16.*	104.230.14.102	TCP	*	17	*	permit
2	104.230.14.102	172.16.16.*	TCP	17	*	yes	permit
3	*	172.16.16.16	TCP	*	80	*	permit
4	172.16.16.16	*	TCP	80	*	yes	permit
5	*	*	*	*	*	*	deny

Task 6.4 (theoretical) TOR

TOR network is a secure network for saving the connections from traffic analysis or any type of tracking. The concept is rather simple - there are some nodes that can be used as steps while reaching the requested server. Every time when TOR client requests the server the random path through these nodes will be generated (some TOR clients will save the path for around ten minutes to work faster). On every connection nodes negotiate on set of encryption keys. And, moreover, none of the nodes does not know the source and destination of the whole request - it knows only the node that it received packet from and the node that it sends the packet to. [7]
If try to access 3g2upl4pq6kufc4m.onion with simple browser it will give "Server not found" error. The reason that it is not usual domain name, that can be resolved as usual - it is a TOR node. In order to be able to access these kind of addresses browser should be able to send requests through TOR net. For these purposes special extensions for TOR browsing should be installed.

Task 6.5 (practical): Simple Buffer Overflow

Nothing here =(

Task 6.6 (bonus) Multiple Choice

Q1: What ISO/OSI layers does a packet filter usually inspect? - 2) Layer 3 and 4
Q2: What method can NOT be used during a TLS connection establishment (to an HTTPS webserver)? - 3) RADIUS
Q3: Which key(s) belong into an X.509 certificate? - 2) The public key
Q4: Consider you want to connect to a LAN that has 802.1X-controlled ports. What traffic is allowed to pass before a successful authentication? - 1) EAPoL

Task 6.7 (bonus) Citing Correctly

"Centralized botnets are easy targets for takedown efforts by computer security researchers and law enforcement." [8] However, there are also peer-to-peer botnets.
...
The authors propose a graph model to capture the vulnerabilities of P2P botnets and apply it several malware families in order to asses their resilience against different attacks [8]. ...

References

[1] The Honeynet Project Blog *https://www.honeynet.org/node/131*

[2] What is Advanced Persistent Threat? *https://containment.comodo.com/why-comodo/advanced-persistent-threat.php*

[3] Spear phishing definition *http://searchsecurity.techtarget.com/definition/spear-phishing*

[4] Spear phishing real life examples *http://resources.infosecinstitute.com/spear-phishing-real-life-examples/*

[5] Exploit Kit definition *http://www.trendmicro.com/vinfo/us/security/definition/Exploit-Kit*

[6] Ransomware definition *http://www.trendmicro.com/vinfo/us/security/definition/Ransomware*

[7] Tor project, overview *https://www.torproject.org/about/overview.html.en*

[8] SoK: P2PWNED - Modeling and Evaluating the Resilience of Peer-to-Peer Botnets *Plohmann et al.* Fraunhofer FKIE, Bonn, Germany, daniel.plohmann@fkie.fraunhofer.de