DEFENSIVE SECURITY

Post Exploitation Adversary Simulations - Network Data Exfiltration Techniques Training

1. Training description.
2. Key learning objectives.
3. Who should attend.
4. Prerequisite knowledge.
5. HW / SW requirements.
6. Full agenda.
7. Time duration.
8. Training keywords.
9. Trainer Bio.
10. Customers.
11. Contact.

TRAINING DESCRIPTION:

The Post Exploitation Adversary Simulations - Network Data Exfiltration Techniques training class has been designed to present students the modern and emerging tools and techniques available for network data exfiltration, testing and bypassing DLP/IDS/IPS/FW systems, protocol tunneling, hiding, pivoting and generating malicious network events. Highly technical content and only a hands-on practical approach guarantees that the usage of this transferred knowledge & technologies in real production environments will be easy, smooth and repeatable.

As for the introduction we will cover the latest APT-style campaigns using malware samples, analyze the top C2 network communication techniques seeing in the wild and map the findings directly to ATT&CK Framework, kill chain methodology and defense in depth strategy. We will also go slightly (with live examples OFC!) through the importance of network baselining, memory forensics, automated malware analysis systems and finally the real threat simulation tactics which are the key important aspects of this training.

Next, we will deep dive into the individual network protocols, services and techniques commonly in use by adversaries in corporate networks and discuss the characteristic security detection features. Using available set of tools (more than 50 different tools and frameworks - check the Keywords section list below), the student will play one by one with well prepared exfiltration, pivoting and tunneling use-cases to generate the true network symptoms of modern attacker behavior.

KEY LEARNING OBJECTIVES → We will explore in details how to:

- run a different types of TCP/UDP reverse and bind shells across Windows and Linux systems, pivot to the next subnets, configure a port forwarding & proxying and find what are the network traffic artifacts of such actions
- manually generate a single malicious packets, ex. to saturate a DHCP server using Python, flood the network service from C code or start a BF by using hydra or medusa
- generate your own malicious payloads and raw TCP/UDP custom encrypted traffic channels undetectable by security products
- simulate DNS DGA traffic, run a DNS TXT tunnels and remote shells, exfiltrate data using DNS MX and how to gain the Internet connection on the plane or in the hotel for free!
- clone, armor and phish popular websites
- create domain fronting setup
- achieve a big file ICMP packet dripping covert channel and monitor ICMP traffic
- use a different HTTP headers and methods for stealing the data also with combination of web application injection techniques and walk through the world of webshells
- detect and understand a TLS/SSL-based anomalies and exfiltration methods
- run a Powershell scripts in post-exploitation stage for leaking the data and bypass AV/EDR
- cheat a security platforms by running internal WMI, Websockets, VOIP or P2P covert channels
- hide a stolen data in binary file, WAV file, Image file or exfiltrate data from air-gapped system using hops
- configure the station to connect to anonymizers like external VPN, TOR, Open proxy and 'ping' to the IP/domains tagged on the globally recognized security feeds, rules or phishy lists
- use a popular cloud-based services for C2 communication and data stealing, ex. Pastebin, Twitter, AWS and many more
- replay a malicious PCAP files and in terms of network behaviour and analyze the malware samples using Cuckoo
- the syntax of signature-based rules works, how Suricata or Bro IDS can help you detect adversary tactics and what are the differences between this two IDS engines
- and a combination of many, many more.

Through hands-on lab exfiltration, this training delivers you a bigger picture of what you really need to care about when thinking initially or improving lately your SOC environment or Red and Blue team skills, your SIEM deployments, your DLP/IDS/IPS installations or Machine-Learning and anomaly detection security solutions.

All the above training description is based on pure hands-on laboratory where student will run every single action or chained scenarios on his own in the dedicated virtual-lab network. This class will focus on x86/x64 architecture, IPv4/IPv6 networks and target Linux and Windows environments.

In terms of IDS/IPS/Data Leakage Protection and for better understanding the current status of your network security posture, the training experience will help you understand risks, identify network security blind spots and unexpected, uncovered spaces by simulating a real, offensive cyber adversary network behavior. Become confident that your SOC / network security really works!

WHO SHOULD ATTEND:

- Red and Blue team members
- Security / Data Analytics
- CIRT / Incident Response Specialists
- Network Security Engineers
- SOC members and SIEM Engineers
- AI / Machine Learning Developers
- Chief Security Officers and IT Security Directors

PREREQUISITE KNOWLEDGE:

- An intermediate level of command line syntax experience using Linux and Windows
- Fundament knowledge of TCP/IP network protocols
- Penetration testing experience performing enumeration, exploiting, and lateral movement is beneficial, but not required
- Basic programming skills is a plus, but not essential

HW / SW REQUIREMENTS:

- At least 20GB of free disk space
- At least 8GB of RAM
- Students should have the latest Virtualbox installed on their machine
- Full Admin access on your laptop

FULL AGENDA:

1. Introduction:
    a. ATT&CK Framework.
    b. TTP, Kill chain & Defense in depth.
    c. The importance of:
        i. network traffic baseline profiling
        ii. memory forensics
        iii. real threat simulations != penetration tests
        iv. log correlation

2. Modern RAT’s implementation and popular APT&C2 malware communication design - real use cases:
    a. The review of the latest APT campaigns
    b. Multi-Staging
    c. Network Link chaining
    d. Hiding
    e. Data Obfuscation
    f. Transfer/protocol limits
    g. Timing channels / scheduled jobs / packet dripping

3. TCP/UDP bind and reverse shells:
    a. Meterpreter + Veil Framework:
        i. bypassing payloads
        ii. common and exotic ports
        iii. routing, pivoting & port forwarding

    b. CLI tips & tricks:
        i. netcat / nc / cryptocat / telnet / socat / curl / wget / xxd / rsync
        ii. /dev/tcp
        iii. PTY
        iv. PHP / Perl / Python / Ruby / Java / ASP shellz

    c. TCP/UDP raw socket tunnels
    d. Generate your own network shellcode & analyze the Exploit-db Shellcode Archive

4. General bypassing, exfiltration, tunneling, pivoting, proxying and C2 techniques:
    a. ICMP
    b. DNS:
        i. Authoritative vs recursive
        ii. CDN theory & domain fronting
        iii. Fast-flux domains
        iv. Dictionary and random characters DGA

    - v. DNS proxy
    - vi. DNS anomalies

  - c. HTTP/S & web application exploitation techniques combo:
    - i. HTTP 404
    - ii. HTTP headers:
      1. Etag
      2. Cookies
      3. User-agent
      4. Accept
      5. If-None-match
    - iii. GET/POST
    - iv. Website cloning and armoring
    - v. WebDAV
    - vi. Websockets
    - vii. Certificate exfiltration & TLS/SSL anomalies
    - viii. *Injections + exfiltration
    - ix. HTTP redirects
    - x. Webshells
    - xi. HTTP anomalies

  - d. WMI / PS-remote
  - e. Proxy / Socks
  - f. SSH / SFTP / SCP
  - g. LDAP
  - h. FTP / TFTP
  - i. SMB / NFS
  - j. RDP
  - k. Anonymizers:
    - i. VPN
    - ii. TOR
    - iii. Open Proxy

  - l. POP3 / SMTP / IMAP
  - m. VOIP
  - n. P2P
  - o. IRC
  - p. IPv6
  - q. + chaining of aboves and many more.

5. Cloud-based exfiltration and C2 channels:
  - a. Twitter
  - b. Pastebin
  - c. Github

    d. Slack
    e. Youtube
    f. Office 365
    g. Gmail / Google Docs
    h. AWS / Google Cloud
    i. Skype
    j. Dropbox
    k. Soundcloud
    l. Tumblr

6. Windows & Powershell exfiltration tools:
    a. AD / LDAP properties
    b. Empire

7. Just a Browser Exfiltration:
    a. audio/video exfil
    b. keylogging

8. Hoping from air-gapped networks.
9. USB attacks and network exfiltration combo.
10. The art of data hiding → steganography examples:
    a. Binary
    b. WAV
    c. Image
    d. VOIP
    e. Routing Protocol
    f. Screen

11. Signature-based event analytics, rule bypassing & malicious network traffic generation:
    a. Suricata ET / VRT rules vs attacker → the syntax rules of the rules
    b. Bro IDS log “features” for deep low-level network baselining
    c. Threat Intelligence feeds, lists and 3rd party APIs:
        i. IP reputation lists
        ii. Malware feeds
        iii. Phishing feeds
        iv. C2 lists
        v. Open Proxy lists
        vi. Tor exit-nodes
        vii. Censys / VT / Passive Total
        viii. Shodan

    d. Replaying and analysing malicious PCAP files.

12. Adversary simulation moves, actions, tools & automated platforms:
    a. In&Out Simulated Network Exfiltration Platform
    b. APT simulator
    c. Dumpster Fire
    d. Firebolt
    e. Flightsim
    f. Armoring:
        i. Nmap NSE scripts
        ii. MiTM/Spoofing/TCP flooding
        iii. Port Knocking
        iv. Brute force
        v. DHCP starvation
        vi. Info disclosure on SMB/CIFS shares

13. Summary → recommended defensive/protection tactics, tools and platforms.

TIME DURATION:

- 3 days of very intensive training (9:00-17:00)

TRAINING KEYWORDS:

- impacket, pyexfil, scapy, metasploit/meterpreter, Veil Framework, proxychains, poshC2, dns2tcp, pupy, tcpreplay, suricata, bro IDS, sg1, nmap, det, xfltreat, pytbull, wireshark, tcpdump, sysdig, hping, fruityC2, tuna, RATTE, Powersploit, PowerShell Empire, nishang, corkscrew, Egress-assess, pivoter, hydra, SELKS, Security Onion, wondjina, trevor C2, sharpSocks, WSC2, sqlmap, BeeF Framework, twittor, torify, TheFatRat, cloakify, WMIsploit, certreq, SSH, ngrep, nping, iptables, Merlin, udp2raw, Volatility Framework, SILK, nfdump, NativePayload_IP6DNS, dnsmasq, thc-flood, knockd, dnstwist, yersinia, DNSexfiltrator, SMBmap, testssl, firebolt, dumpster fire, APT simulator, cuckoo, moloch, icmptunnel, transmission, openvswitch, ngrok

---

REVIEWS:

- “Excellent content, great stuff and awesome knowledge from the trainer.”
- “Excellent balance between breadth and depth of contents, great materials.”

- “Awesome OSDS @brucon training, learned a lot! Was a pleasure to meet you.”
- “Very good course, the instructor was very knowledgeable and answered all our questions. Course exceeded my expectations, great job!”

TRAINER BIO:

- Leszek Miś is the Founder of Defensive Security (www.defensive-security.com) and VP, Head of Cyber Security in Collective Sense (www.collective-sense.com) where he was responsible for strategy, business analysis, and technical product security research & feature recommendations. He has over 13 years of experience in IT security market supporting the world’s largest customers in terms of exfiltration simulations and penetration tests, infrastructure hardening and general IT Security consultancy services. Next, to that, he has 10 years of experience in teaching and transferring a deep technical knowledge and his experience. He has trained 500+ students with the average evaluation on a 1-5 scale: 4.9. He is an IT Security Architect with offensive love and recognized expert in enterprise Open Source Security solutions market. Leszek provides network data exfiltration simulation services, web application & infrastructure penetration tests and OSINT. He specializes in low-level Linux/OS hardening and defensive security of web application platforms (ex. think about integration of WAF+BeeF!). He is also known and respected trainer/examiner of Red Hat solutions and author of many IT Security workshops:

    - Open Source Defensive Security → The Trinity of Tactics for Defenders.
    - Post Exploitation Adversary Simulations → Network Data Exfiltration Techniques.
    - The Art of Modern Deception Techniques for Blue Teams.
    - SELinux → Development & Administration of Mandatory Access Control Policy.
    - Advanced RHEL/CentOS Defensive Security & Hardening.
    - ModSecurity → Development and Management of Web Application Firewall rules.
    - FreeIPA → Identity Management for Linux Domain Environments & Trusts.

- As a speaker, trainer or just a participant he attended many conferences like Brucon 2017/2018, OWASP Appsec USA, FloCon 2018("May the data stay with U!"), SuriCon 2017, HITBSecConf, AlligatorCon, Semafor, Exatel Security Days, Confidence 2016("Honey(pot) flavored hunt for cyber enemy), PLNOG 2016 ("Yoyo! It's us, packets! Catch us if you can"), NGSEC 2016 ("Many security layers for many defensive opportunities"), Open Source Day 2010/2011/2012/2013/2014, SysDay 2008 ("SELinux vs exploits"), Confitura 2014 ("Detection and elimination of threats in real time - OWASP Appsensor in action."), Red Hat Roadshow 2014, OWASP Chapter Poland 2015("Does your WAF can handle it?), ISSA, InfoTrams 2015, BIN Gigacon 2015("Mapping pen testers knowledge for the need to protect a critical IT infrastructure").

- The holder of many certificates:
    - Offensive Security Certified Professional (OSCP)
    - Red Hat Certified Architect (RHCA)
    - Red Hat Certified Security Specialist (RHCSS)
    - Splunk Certified Architect
    - Comptia Security+

CUSTOMERS:

- PGNiG
- Stack Overflow
- Daily Motion
- Alior Bank
- Ministry of Finance
- Millennium Bank
- Nazwa.pl
- Rekord Systemy Informatyczne
- IBS S.A.
- Cinkciarz.pl
- Rockwell Automation
- Esky.pl
- LPP S.A.
- ARiMR
- TUV
- Polkomtel

CONTACT:

- Email: info@defensive-security.com
- Mobile: 0048 791 611 309 (Poland) / 0048 791 83 10 18
- Website: https://www.defensive-security.com