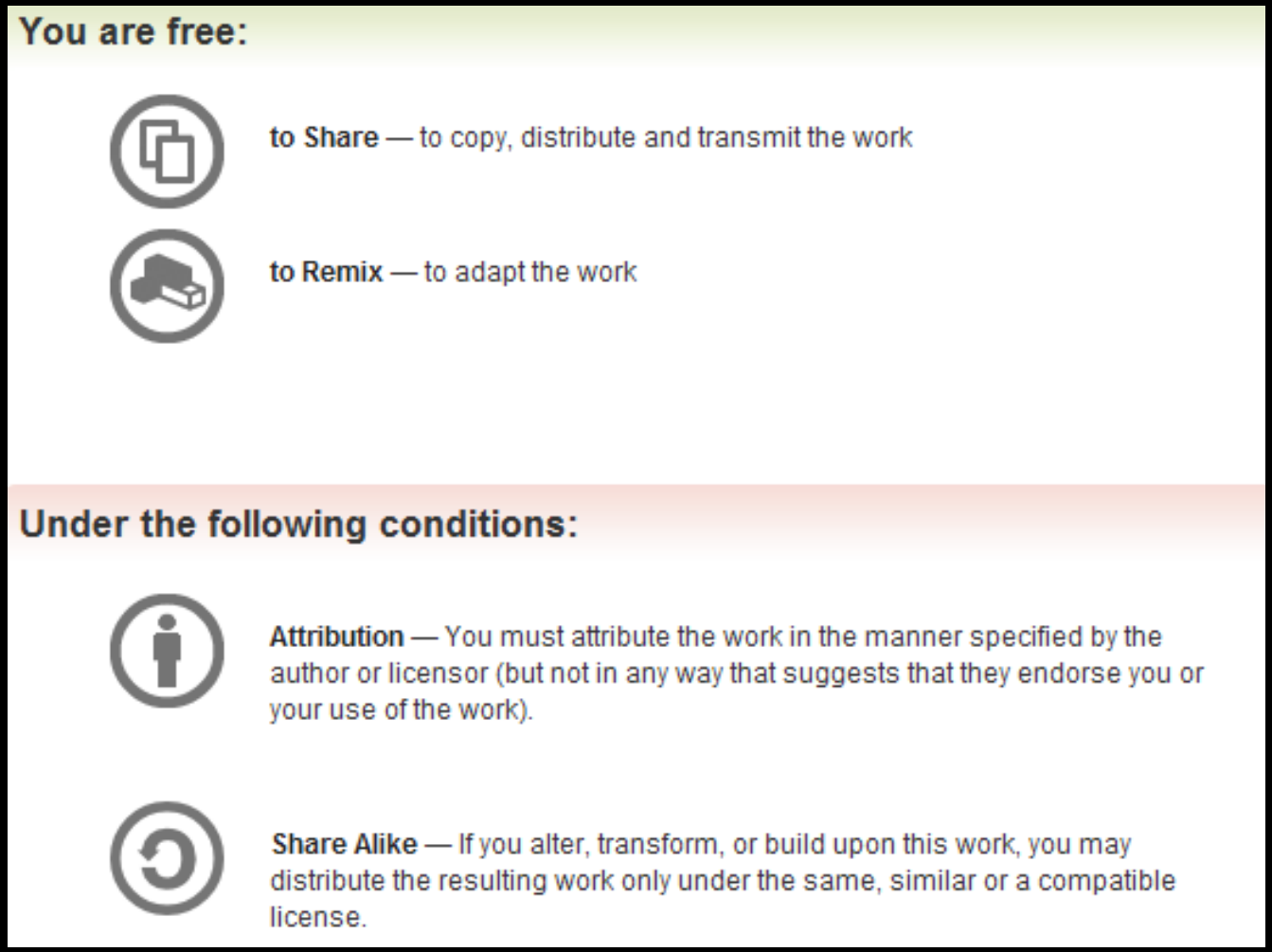
Hacking Techniques & Intrusion Detection

Ali Al-Shemery
arabnix [at] gmail

All materials is licensed under a Creative Commons "Share Alike" license.

- http://creativecommons.org/licenses/by-sa/3.0/



whoami

- Ali Al-Shemery
- Ph.D., MS.c., and BS.c., Jordan
- More than 14 years of Technical Background (mainly Linux/Unix and Infosec)
- Technical Instructor for more than 10 years (Infosec, and Linux Courses)
- Hold more than 15 well known Technical Certificates
- Infosec & Linux are my main Interests

Post-Exploitation

“Shell is Only the Beginning” Darkoperator

Outline

- Why Post-Exploitation
- Post-Exploitation RoE
- Infrastructure Analysis
- Pillaging
- Sensitive Data
- User Information
- System Configurations
- High Value/Profile Target
- Data Exfiltration
- Persistence
- Cleanup

Why?

- Determine the value of the machine compromised,
- Maintain control of the machine for later use,
- Value depends on sensitivity of data and usefulness in further compromising the network,
- Helps identify and document:
  - sensitive data,
  - identify configuration settings,
  - communication channels,
  - and relationships with other network devices.
- Go beyond Exploit verification
- Shows how vulnerabilities can be chained to gain higher level of access (real-life attacks!!!)

Post-Exploitation RoE

- Protect the client
- Protect yourself

Infrastructure Analysis

Network Config.

- Interfaces
- Routing
- DNS Servers
- Proxy Servers (Net/App Level)
- ARP Table

Network Services

- Listening Services (TCP, UDP, etc),
- VPN Connections,
- Directory Services,
- Neighbors

Pillaging

- Obtaining information from targeted hosts
  - files containing personal information,
  - credit card information,
  - passwords, etc.
- Satisfy the goals or as part of the pivoting process.
- Location of this data will vary depending on the type of data.
- Knowledge of commonly used applications, server software and middleware is very important.
- Special tools may be necessary to obtain, extract or read the targeted data from some systems.

Check?

- Installed Software,
- Installed Services:
  - Security Services
  - File/Printer Shares
  - Database Servers
  - Directory Servers
  - Name Servers
  - Deployment Services
  - Certificate Authority
  - Source Code Management Server
  - Dynamic Host Configuration Server
  - Virtualization
  - Messaging
  - Monitoring and Management
  - Backup Systems
  - Others please add…

Sensitive Data

- Key-logging,
- Screen Capture,
- Network Traffic Capture,
- Previous Audit Reports (lucky day)!

User Information

- On System,
- Web Browsers,
- IM Clients

System Configuration

- Password Policy,
- Security Policies,
- Configured WiFi Networks and Keys.

High Value/Profile Targets

- Can be identified and further expanded from the targets identified in the pre-engagement meetings thru the analysis of:
  - Data gathered,
  - Interactions of those systems,
  - Services they run.
- This view of the operation and interactions of these high value/profile targets helps in the identification and measurement of impact that can be gained to the business do to the data and processes and to the overall integrity of the client's infrastructure and services.

Data Exfiltration

- Mapping of all possible exfil paths,
- Testing exfiltration paths,
- Measuring control strengths

Persistence

- Autostart Malware
- Reverse Connections
- Rootkits
  - User Mode
  - Kernel Based
- C&C medium (http, dns, tcp, icmp)
- Backdoors
- VPN with credentials

Diving Further (Infra.)

- From Compromised System:
  - Upload tools, local system tools, ARP Scan, Sweeping, DNS Enum, Directory Services Enum, Brute force, Execute Further Exploits
- Thru Compromised System:
  - Port Forwarding, Proxy, VPN, Execute Further Exploits

Cleanup

- Process of cleaning the system after completing the penetration test.
  - User account: connect-back users
  - Binaries installed: executables, scripts, backdoors, rootkits, etc
  - Temp Files
- Restore original configuration setting if modified.
- Leave no trace
- Proper archiving and encryption of evidence to be handed back to customer

Note: Ensure documented steps of exploitation

Special Thanks

to the Penetration Testing Execution Standard (PTES) Team …

Summary

- Explained what is PE, and why its needed,
- The need to check the Post-Exploitation RoE,
- What do we mean by Infrastructure Analysis,
- What is Pillaging,
- What is Sensitive Data, and how to identify it,
- What User Information we need to gather,
- What are System Configurations, and where to check for them,
- Explained what is High Value/Profile Target, and what business impact they could lead if compromised,
- What do we mean by Data Exfiltration,
- What is Persistence, and methods to perform it,
- What is the Cleanup phase, and why is it necessary.

References

- Penetration Testing Execution Standard, http://www.pentest-standard.org/index.php/Main_Page,
- Linux/Unix/BSD Post-Exploitation Command List, https://docs.google.com/document/d/1ObQB6hmVvRPCgPTRZM5NMH034VDM-1N-EWPRz2770K4/edit?pli=1,
- Windows Post-Exploitation Command List, https://docs.google.com/document/d/1U10isynOpQtrIK6ChuReu-K1WHTJm4fgG3joiuz43rw/edit?pli=1,
- OSX Post-Exploitation, https://docs.google.com/document/d/10AUm_zUdAQGgoHNo_eS0SO1K-24VVYnulUD2x3rJD3k/edit?pli=1,
- Metasploit Post Exploitation Command List, https://docs.google.com/document/d/1ZrDJMQkrp_YbU_9Ni9wMNF2m3nIPEA_kekqqqA2Ywto/edit?pli=1,
- Post-Exploitation Command List, http://www.room362.com/blog/2012/8/25/post-exploitation-command-lists-request-to-edit.html,