Expert Knowledge Elicitation for Skill Level Categorization of Attack Paths

Terézia Mézešová
Pavol Jozef Šafárik University
Slovakia

Hayretdin Bahsi
Tallinn University of Technology
Estonia
attack path
SEQUENCE OF VULNERABILITIES
AN ATTACKER NEEDS TO EXPLOIT
TO REACH A TARGET IN A NETWORK

systematic comparison of intrusion scenarios
Attacker (internet)

Perimeter firewall

Internal firewall

Communication server

Data storage

Operating station

AttackerLocated (internet)

accessMalicious Input

CVE-2010-0483

executeCode (Communication server)

Multihop access

CVE-2010-0494

netAccess (Data storage)

Remote exploit

executeCode (Data storage)
Expert Knowledge Elicitation

0
8 experts
CSIRT
pentesting

1
Understand key skills for attackers

2a
Identify concrete skills sets for attacker categories

2b
Map CVSS metrics values to attackers skills
<table>
<thead>
<tr>
<th>Skill Level</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Script Kiddies</strong></td>
<td>run downloaded scripts, configure exploits, obtain leaked credentials, use malware, use brute force methods</td>
</tr>
<tr>
<td><strong>Moderately Skilled Attackers</strong></td>
<td>knowledge of attacking tools, reproduce proof of concepts, engage user’s action, pass multiple authn gates, hide traces afterwards</td>
</tr>
<tr>
<td><strong>High Skilled Attackers</strong></td>
<td>in-depth technical know-how, write functional exploits, demonstrate PoCs, hide on the network</td>
</tr>
</tbody>
</table>
## Skill Level Categorization | CVSS Basic score

<table>
<thead>
<tr>
<th>Attack Vector</th>
<th>User Interaction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network</strong> :</td>
<td><strong>None</strong> : Script Kiddies</td>
</tr>
<tr>
<td>Script Kiddies</td>
<td><strong>Required</strong> : Moderately Skilled</td>
</tr>
<tr>
<td>**Adjacent</td>
<td>Local** :</td>
</tr>
<tr>
<td>Moderately Skilled</td>
<td><strong>Authentication</strong></td>
</tr>
<tr>
<td><strong>Physical</strong> :</td>
<td><strong>None</strong> : Script Kiddies</td>
</tr>
<tr>
<td>–</td>
<td><strong>Single</strong> : Script Kiddies</td>
</tr>
<tr>
<td><strong>Privilege Required</strong></td>
<td><strong>Multiple</strong> : Moderately Skilled</td>
</tr>
<tr>
<td>None</td>
<td><strong>High</strong> :</td>
</tr>
<tr>
<td>Low : Script Kiddies</td>
<td><strong>High</strong> :</td>
</tr>
</tbody>
</table>
Skill Level Categorization | CVSS Temporal score

**Exploit Code Maturity**

High: Script Kiddies
Functional | Proof of Concept: Moderately Skilled
Unproven: Highly Skilled

**Report Confidence**

Confirmed: Script Kiddies
Reasonable: Moderately Skilled
Unknown: Highly Skilled
Skill Level | Difficulty of vulnerability \( d(v) \)

\[
d(v) = \max(m^{AV}, m^{PR}, m^{UI}, m^{Au}, m^{EC}, m^{RC})
\]

**CVE-2010-0483**


\( m^{AV} = \text{Script Kiddies}, m^{PR} = \text{Script Kiddies}, m^{UI} = \underline{\text{Moderately Skilled}}, m^{Au} = \text{Script Kiddies}, m^{EC} = \text{Script Kiddies}, m^{RC} = \text{Script Kiddies} \)

assigned level: *Moderately Skilled Attacker*
Skill Level | Difficulty of vulnerability $d(v)$

$$
    d(v) = \max(m^{AV}, m^{PR}, m^{UI}, m^{Au}, m^{EC}, m^{RC})
$$

CVE-2010-0483

*Attack Vector: Network*  
Privilege Required: None  
User Interaction: Required  
Authentication: None  
Exploit Code Maturity: High  
Report Confidence: Confirmed  

$m^{AV} = $ Script Kiddies  
$m^{PR} = $ Script Kiddies  
$m^{UI} = $ Moderately Skilled  
$m^{Au} = $ Script Kiddies  
$m^{EC} = $ Script Kiddies  
$m^{RC} = $ Script Kiddies

assigned level: *Moderately Skilled Attacker*
Skill Level | Difficulty of Attack Path $D(P)$

$$D(P) = \max(d(v_i) \text{ where } i \in \{1...n\})$$

1. CVE-2010-0483 (Moderately Skilled)
2. CVE-2010-0494 (Moderately Skilled)

assigned level: Moderately Skilled Attacker
Conclusion

Express required skill level for exploitation of an attack path

Prepare balanced hands-on offensive cyber exercises
Thank you for your attention.

terezia.mezesova@outlook.com  hayretdin.bahsi@ttu.ee