NAS WIRELESS

Weekly Notice – NAS-Secure Example 1

From: notice@security-bulletins.com
Sent: Monday, January 11, 2020 9:00 AM
To: My Technicians
Subject: Network Detective Weekly Notice – Customer ABC

==========
Customer ABC (NDA1-99ZZ)
==========

ADDED 1 Computer to Domain: myco
    GRANDE-PC (192.168.6.14)

REMOVED 1 Computer from Domain: myco
    PITSTOP-PC (192.168.6.14)

ADDED 5 DNS A-Records to Domain: myco
    kalmans-mbp-2.corp.myco.com (192.168.6.62)
    grande-pc.corp.myco.com (192.168.6.14)
    michaels-spectre.corp.myco.com (192.168.6.158)
    mikes-iphone.corp.myco.com (192.168.6.156)
    rakealgreensair.corp.myco.com (192.168.6.122)

CHANGED 3 DNS A-Records from Domain: myco
    at-lt.corp.myco.com from 192.168.6.26 to 192.168.6.153
    desktop-hkljptn.corp.myco.com from 192.168.6.79 to 192.168.6.85
    proactive-gw.corp.myco.com from 192.168.6.122 to 192.168.6.17

ADDED 1 User to Domain: myco
    Carl Grande (CMGRANDE)

ADDED 2 Printers to Domain: myco
    Brother MFC-9320CW Printer (GRANDE-PC; IP: 192.168.6.14)
    Brother HL-6180DW series Printer (GRANDE-PC; IP: 192.168.6.14)

REMOVED 2 Printers from Domain: myco
    Brother MFC-9320CW Printer (PITSTOP-PC; IP: 192.168.6.14)
    Brother HL-6180DW series Printer (PITSTOP-PC; IP: 192.168.6.14)

DETECTED 5 New Broadcasted Wireless Networks
    PEMGuest (RSNA_PSK)
    CSI_Guest (RSNA_PSK)
    HP-Print-78-LaserJet 1102 (IEEE80211_Open)
    ngHub_319437N205B2F (RSNA_PSK)

Weekly Notice – NAS-Secure Example 2

From: notice@security-bulletins.com <notice@security-bulletins.com>
Sent: Monday, January 25, 2020 8:00 AM
To: My Technicians
Subject: Network Detective Weekly Notice – Customer ABC

==========
Customer ABC (NDA1-99ZZ)
==========

FOUND 9 New Internal Vulnerabilities
    Discard port open (Severity: High; CVSS: 10; OID: 1.3.6.1.4.1.25623.1.0.11367; Nodes Affected: REMOTE)
    Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468) (Severity: High; CVSS: 10; OID: 1.3.6.1.4.1.25623.1.0.902269; Nodes Affected: REMOTE)
    Microsoft Remote Desktop Protocol Remote Code Execution Vulnerabilities (2671387) (Severity: High; CVSS: 9.3; OID: 1.3.6.1.4.1.25623.1.0.902818; Nodes Affected: REMOTE, PROIT30DEV)
    Microsoft Windows SMTP Server DNS spoofing vulnerability (Severity: Medium; CVSS: 6.4; OID: 1.3.6.1.4.1.25623.1.0.100624; Nodes Affected: REMOTE)
    Microsoft RDP Server Private Key Information Disclosure Vulnerability (Severity: Medium; CVSS: 6.4; OID: 1.3.6.1.4.1.25623.1.0.902658; Nodes Affected: REMOTE, PROIT30DEV)
    Quote of the day (Severity: Medium; CVSS: 5; OID: 1.3.6.1.4.1.25623.1.0.10198; Nodes Affected: REMOTE)
    Chargen (Severity: Medium; CVSS: 5; OID: 1.3.6.1.4.1.25623.1.0.10043; Nodes Affected: REMOTE)
    Microsoft Windows SMTP Server MX Record Denial of Service Vulnerability (Severity: Medium; CVSS: 5; OID: 1.3.6.1.4.1.25623.1.0.100596; Nodes Affected: REMOTE)
    DCE Services Enumeration (Severity: Medium; CVSS: 5; OID: 1.3.6.1.4.1.25623.1.0.10736; Nodes Affected: REMOTE, PROIT30DEV, TOM-WIN8, MARY-PC, ACCOUNTING-HP)
    Deprecated SSLv2 and SSLv3 Protocol Detection (Severity: Medium; CVSS: 4.3; OID: 1.3.6.1.4.1.25623.1.0.111012; Nodes Affected: REMOTE)